Classification: Public

ICT infrastructure, privacy & security

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

Annex 2: Register of processors

CERTIFIED ISO/IEC 27001

Version 1.8

Table of contents

Introduction

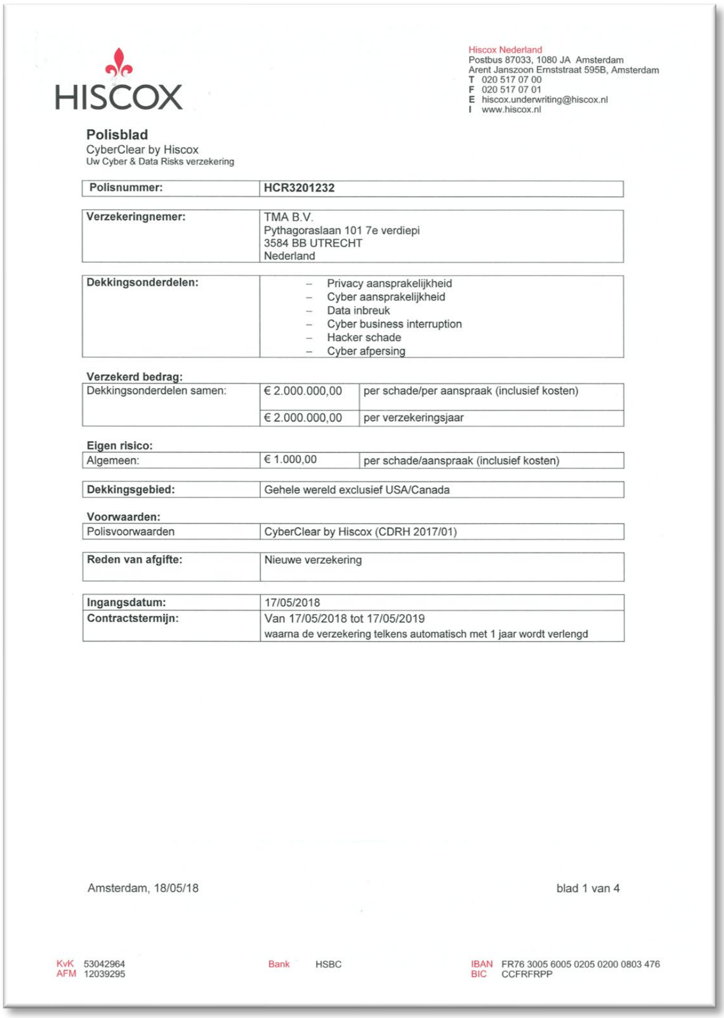
This document describes the system requirements, IT infrastructure and the security measures for the Talent Management System (TMS) of TMA B.V.

The Talent Management System (TMS) is the modular platform with TMA Tools and Content that TMA B.V. publishes online as a SaaS (Software as a Service) and where an organization gets one or more implementations in use if it has a license agreement with TMA B.V.

This document also describes how TMA B.V. takes into account the privacy of users. TMA is in possession of an ISO 27001 certification, which means that TMA is periodically checked whether it applies the guidelines within these standards in the right way. During these audits, the TMA B.V. established organizational and technical security measures checked and tested for their implementation. We refer to the articles within this document for the organizational and technical measures taken by TMA to secure the personal data and data.

CERTIFIED
LR
ISO/IEC 27001

In the unlikely event that an incident occurs in the field of data security and privacy that causes damage for which TMA B.V. is liable, TMA B.V. is insured up to an amount of 2 million Euros per year with 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

ICT infrastructure

System requirements

Users need the following technical matters at least to be able to use the TMS:

- A standalone Windows or Mac computer with an internet connection.
- A unique personal email address.
- At least the second to last version of one of the following browsers: Google Chrome, Apple Safari, Mozilla Firefox, Microsoft Edge.
- Browsers must support JavaScript, accept session variables, and the screen resolution must be at least 1024 x 768 pixels.
- To view the PDF reports one must have Adobe Acrobat reader from Adobe. You can download these free of charge from the Adobe website or a similar solution that can open PDF documents.
- Licensee's mail server(s) must accept the emails from the TMS.

Organizational requirements

The organization that uses the TMS is responsible for the use of the personal data from the TMS and draws up its own conditions for the use of the personal data. This means, for example, that this organization formalizes the following matters prior to the use of the TMS:

- Indicate the purposes and conditions for the use of personal data from the TMS. This can be built into the TMS if the organization using the TMS indicates this.
- Indicate who has access to the personal data. The organization that uses the TMS is responsible for assigning authorizations that allow specific users to access personal data from the TMS used. The manner of use of the personal data and the purpose of use are also the responsibility of the organization that uses the TMS.
- Whether or not to explicitly ask users for permission to use the personal data (a so-called opt-in function). This can be built into the TMS if the organization using the TMS indicates this.
- Whether or not to set up a so-called 'opt-out procedure' with which users can indicate afterwards that the personal data from the TMS may no longer be used.

ICT platform

The TMS uses the FIPS 140-2 certified Cloud of Microsoft Azure which is SOC 1, 2 and 3compliant. The TMS is built on the Microsoft .NET framework. We only use components that are also in the .NET Framework and or are provided by Microsoft as an add-on, unless there is a valid reason to deviate. All deviations will be documented including the reason for the deviation.
Below is an overview of the technical components we use:

- .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

External networks

There are two different links with external networks to describe.

1. The external network of the user of the TMS. These are the users who use the functionality of the TMS.
2. The external network of the party that maintains and develops the software. In the event of releases and bug fixes, this party has access to the production network in the form of rolling out a release or installing a fix or investigating (potential) software, functional error.

Hosting location(s)

The TMS is hosted on the Microsoft Cloud environment For the hosting location on Microsoft Azure, we have as our main location the location for Western Europe where the data center in Amsterdam is located. As a fallback location, the location in Northern Europe where the data center in Dublin is located was chosen. By the fallback location, we mean the location we switch to if there is a major outage in our main location. Furthermore, all backups that are made are stored at the location in Dublin.

Infrastructure

Because the TMS is hosted on the Microsoft Cloud environment, the maintenance of the infrastructure is carried out by the Cloud supplier. The supplier of the Cloud environment will carry out all maintenance on the infrastructure. If maintenance results in downtime, we will inform the users of our platform. As an application supplier, we also do not have access to the data centers and or the infrastructure.

Operating system

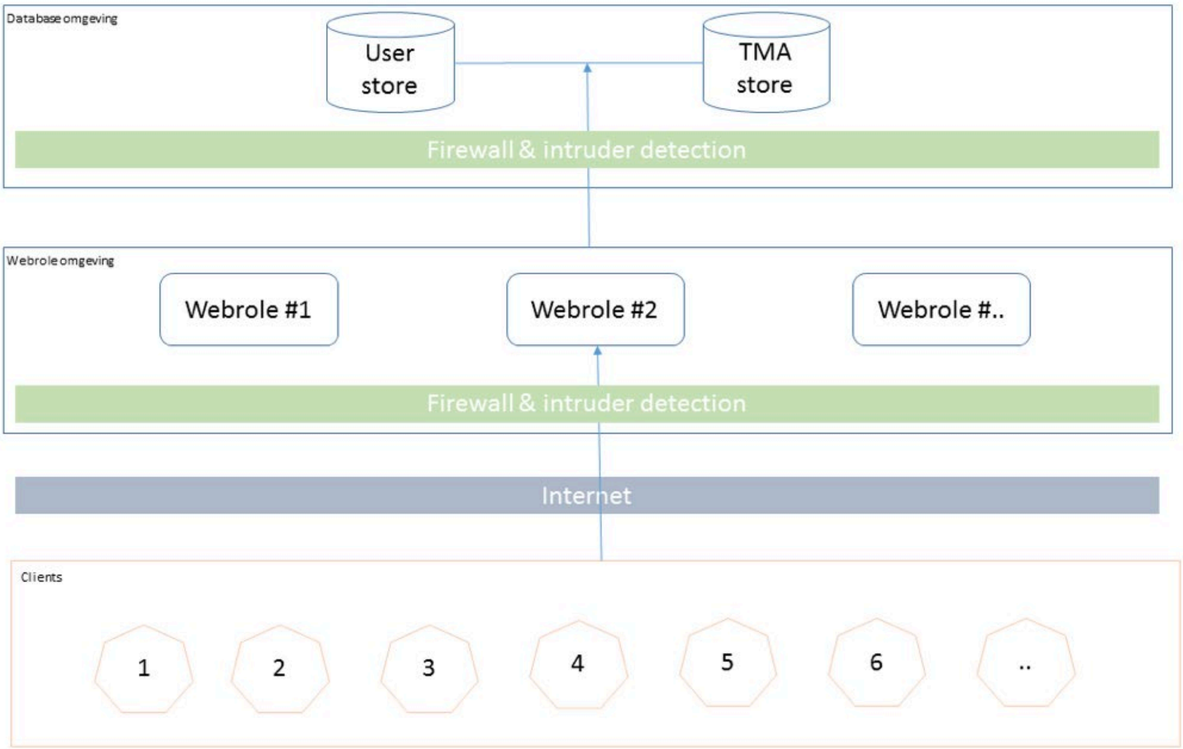
The TMS on the Microsoft Cloud environment is hosted within the so-called 'Web roles' and the maintenance of the operating system is done by the Cloud supplier. Due to the use of the so-called

'Web roles', we do not have access to the operating system, so the maintenance of the operating system is done by the Cloud supplier. The Microsoft Azure Cloud is known for the fact that the operating system is well maintained with the latest updates. On the Azure platform for the "App service" the antimalware for Azure is activated.

Web

Since we use the aforementioned 'Web roles', the maintenance is the same as that of the operating system as described in the chapter above. The 'Web roles' are set up in such a way that when the load of a web roll exceeds 80%, a second one is automatically added by the Cloud platform. And when the load of the main web role drops below 80%, the second one is automatically cleaned up again. As a result, we always have enough resources available at very busy times.

Visual display hosting environment



Database servers

The TMS databases are also hosted on Microsoft Azure as Azure SQL Databases. For each database there is a firewall where you can control access to the database. By default, everything is closed. By default, only the Web servers (Web Roles) will be able to access the database. However, there is an exception and that is when the databases are linked to the internet. When access to the database is required to execute a release or bug fix, the firewall of the database is adjusted for this limited time so that the IP number from where the release or bug fix is implemented has access to the database. When the release or bug fix installation is completed, the IP number is retrieved from the firewall of the databases.

TMS webrole back-up

The TMS (installed on the Azure Cloud environment) has no backup overnight. Because we work with automated deployment towards the Azure Cloud environments from a development perspective, the roll-out of the latest version in the event of calamities is secured. During the deployment of the TMS, the application will also be configured fully automatically.

When we have to roll out to another data center of the Azure Cloud environment during calamities, only a few parameters of deployment will have to be adjusted, after which the application can also be rolled out automatically to the fallback possible.

Database

The database is encrypted via Azure Transparent Data Encryption. Databases are backed up every night and can be restored via the restore function. When we have to move to another data center during calamities, we can load the backup file to restore the database with the data from the previous night.

Access provisioning policy

Within the TMS, the areas of the programming are technically separated from each other. Within the TMS we know the following areas:

- Candidate Area: this is the area where the candidate makes the analysis
- Feedback Area: This is the area where the feedback givers without an account based on a token give feedback
- Customer Area: this is the area where the customer of TMA B.V. can carry out all customer-related matters.
- Documentation Area: this is the area where the developers keep the documentation about the TMS and where customers and ICT partners can read the documentation.
- Administration Area: this is the area where the service desk of TMA B.V. can carry out all administrative matters related to the application
- Application Area: this is the area where the monitoring dashboards of the TMS are located

To access each of the above areas, people must be explicitly authorized by the service desk of TMA B.V.,with the exception of the feedback area, which works on the basis of tokens. Without the correct authorization, it is not possible to gain access to a specific area of the TMS or to the data associated with the area.
For each customer, we look at which areas access is provided. This does not alter the fact that organizations that have access to the TMS are responsible for actually authorizing people within the assigned areas.

Rights for users

The TMS works with roles. Specific roles have been defined for each area.

Rights for platform accounts

By dividing the TMS into various areas and assigning its own roles for each area, we have made a split in the various functionalities. Due to this split, it is not possible to have access to another area and the data associated with this area without the necessary roles.

Authorizations are always set by the people of the service desk of TMA B.V. with the exception of the Customer area. Within the Customer area it is possible for a customer to create users based on various roles within their own area and within their own data domain.

Security & privacy

Policy-compliance-checks TMS

The Security of the TMS is checked at least 1 time per year with a penetration test. A report is made of a penetration test.

Policy-compliance-checks hosting

When there are fundamental changes on the hosting platform that have a major impact on compliance, the changes are investigated.

Improvements

When improvement proposals emerge from the policy compliance checks and are implemented in the TMS, these improvements will, provided that they are not sensitive, be included in the release notes of the TMS. If the improvement proposals have a sensitive character, the improvement proposals will be included in an internal system.

Technical Auditing

Within the development environment of the TMS, CodeIt .Right is used to automatically perform automated scans over the entire source code during development. Furthermore, During development, CodeIt.Right gives the developer tips and makes the developer aware of certain things.

Logging incidents

Incidents related to the TMS are recorded and recorded in a system so that there is an overview of what has been received and when they are resolved and in which version. External notifications are logged in the same system and may lead to a hotfix/interim release or be included in a regular release. Furthermore, a report will be made of each report with the necessary data to test which solution has been implemented and in which release it will be delivered.

Within the TMS we have different types of logging:

- Application Error logging
- Authentication logging (success/failure)
- Performance logging (speed of each call to the application)

When our logging mechanisms fail, this means for the TMS that the entire application is offline. The logging mechanism is part of the application and is interwoven in it. The only exception to this is the logging of the hosting environment. This can be accessed via a separate interface.

Depending on the type of logging, the TMS has a retention period for its logging, see below per type of logging what the retention period is.

- Application Error Logging: Application error logging is stored for 3 months.
- Authentication logging: Authentication logging is stored for 3 months.
- Performance logging: Performance logging is stored for 1 month.

The TMS uses a database to log. Only the application administrator has access to this database and can delete logs.

TMA's service desk has a live view of all the above-mentioned logs and checks the authentication logs for suspicious circumstances. If necessary, action will be taken based on information from one of the log files. This action will be logged in the release/incident system of the TMS.

Means of access provision

In the TMS, customers are created via the service desk of TMA B.V. This results from a signed contract with which the identity of these customers is established. After creating the customer administrator, it is the responsibility of the customer which users he adds to the system. The identity check lies with the customer for her own environment of the TMS.

Within the ASP.Net Identity Model used by the TMS, the passwords are stored one-way by using a hashing in combination with a salt. Passwords can only be compared but can never be returned to the original characters.

Authentication means

The TMS has a username-password combination to grant access. If an incorrect combination is entered here, access to the TMS will not be granted. In addition, based on roles, it is examined whether the correct access to a specific area can be granted. If the correct roles for a specific area are not associated with the user, access to the area is not provided. In the TMS, 2-step verification can be used to access the system. This setting can be activated by the service desk of TMA B.V. Furthermore, the functionalities are determined by the roles in the TMS. The functionalities can be set per TMS implementation together with the service desk of TMA B.V.

Identity and access management

The TMS supports the complete lifecycle of accounts, by which we mean:

- Request
- Give
- Modify
- Retract/suspend/remove

The TMS logs when a user is created. This allows us to see exactly when a user has gained access to our system. For the activities related to granting access to our systems, both the successful and the unsuccessful actions are logged.

The customers and/or calling systems are responsible for blocking an account. We provide them with an interface to block accounts. When it concerns a customer or a calling system, the service desk of TMA B.V. blocks the account.

The TMS sets requirements for the identification/authentication (mechanisms) to enforce sufficiently strong passwords.'

To prevent login details from being entered incorrectly too often, the TMS blocks an account after 5 attempts for 5 minutes. Within these 5 minutes it is not possible to log in with this account. After these 5 minutes, the account will be active again. TMA has taken this measure to increase the security of the TMS. These measures make login attempts by means of automated methods (e.g. Brute-force attack) more difficult.

New releases TMS

New releases of the TMS are rolled out at the set times of the release calendar. A release is only executed and brought to production when the steps of Development, Test and Acceptance have been completed.

Incident fixes

Incident fixes for which there is no workaround will, after they have been thoroughly tested, be implemented on the production environment. This procedure is followed to keep the nuisance to a minimum.

Validation of the input on the server

All input on the portal is validated both client-side and server-side. Validation notifications are communicated to the user. This is the first step before any of the final code is executed. Validation messages are contained in the response of the call and can be used by the calling system to inform the user. Within the TMS we use Anti Forgery tokens in combination with Request Validation. This allows us to trace whether the call is also authentic and comes from our server. Within the TMS we have enabled Request Validation, which makes it impossible to send risky characters to the server, unless this is explicitly tolerated for a certain field.

Privacy-promoting techniques

The TMS is designed in accordance with the privacy by design principles. Where possible, personal data is anonymized or pseudonymized.

Encryption or hashing of sensitive data in databases and files

The TMS uses encryption or hashing of sensitive data in the database and files.

Cryptographically strong session-identifying cookies

The TMS uses cryptographically strong session-identifying cookies.

Communication encryption

All communication with the TMS is done over TLS 1.2. The ICT security guidelines for Transport Layer Security have been applied in the TMS.

Generate and store reports and dashboards

In the TMS, users gain insight into the results of the TMA analyses and instruments completed by participants via the reports and dashboards module. All visible output is generated when an authorized user opens a report or dashboard when logged into the TMS. These reports and dashboards are not stored in the TMS database but are regenerated each time. After generating, the TMS automatically deletes it. However, as long as access to the TMS exists and users have access to certain reports and dashboards, it is possible to download them as a PDF file and save them at their own location (e.g.. on your own PC or in a cloud storage such as Google drive). This downloaded pdf document can also be printed. The TMS and the content of the TMA Method may change on the one hand and on the other hand the data available about a participant may change(e.g. because he has completed or redacted another analysis or the standard scores of an analysis have changed) so that in both cases the dashboards and reports can change over time. The reports and dashboards are therefore always a snapshot. A user is responsible if he downloads a document from the TMS in order to store it in a safe environment. The TMS does not store these pdf documents in the TMS database. Partly to prevent privacy-sensitive documents directly from the TMS database from unauthorized third parties.

TMS information

Comment lines are not carried over to a release executable/binary during compilation. For code that is not compiled but interpreted, the comment will be removed as much as possible.   The TMS has recorded sensitive configuration in the Azure configuration for the Web Role in which the application runs. This data is dynamically and securely added to the configuration by the Azure system. Within the TMS, command and query texts are built by the Microsoft Entity Framework. This framework (developed and maintained by Microsoft) ensures that no SQL injection can take place. This framework is therefore maintained by Microsoft and at the beginning of each release it will be checked whether there is a newer version. If this is the case, these components will be upgraded. The query texts are compiled using LINQ. Within the TMS, the input of data is captured and validated.

Development and improvement of the TMS

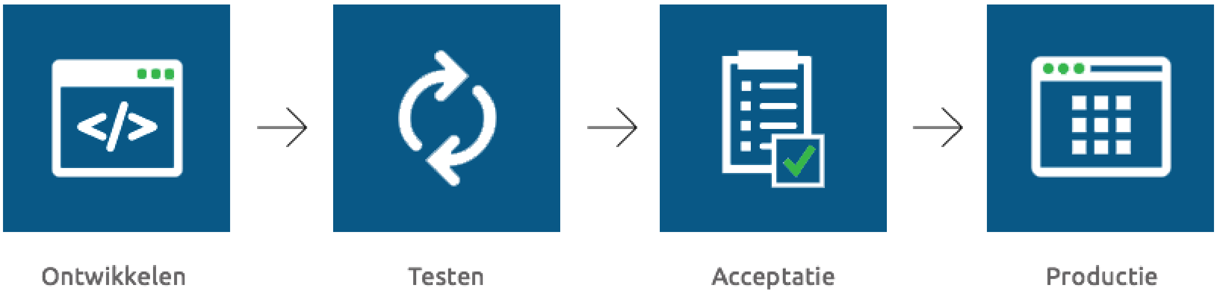
The development of the TMS is done by TMAB.V. and partly outsourced. TMA B.V. is in control and leads the development of the TMS. TMA is the owner and has 24/7 access to the latest version of the programming code. During the development, TMA places high demands on the security and possible processing of personal data. Insofar as the development takes place by another party, contractual agreements have been made about the security and processing of personal data.

The development of the TMS is done by means of the OTAP method.
There are 4 different environments that an update in the code has togo through.

The environments that are passed are:

- Develop (in which the TMS is developed with fictitious data)
- Test (TMA tests new releases on this environment with fictitious data)
- Acceptance (Here TMA tests the deploy of the TMS as if it were live.)
- Production (This is the environment where all TMS implementations that are online are located)

Agreements have also been made about the publication of new releases. Every 2nd Thursday of the month, a release is published when it has passed the test procedure. So-called "hotfixes" may be published more quickly as described earlier in the topic "logging incidents".



When data is migrated at the request of the customer, it will first be transferred to the acceptance environment. When the customer agrees that the correct data has been migrated, the migration is only implemented to the production environment.

During the development process, the developers adhere to the OWASP development principle (more information about this can be found on https://www.owasp.org). From the start of the development of the TMS, privacy by design has already played an important role. During the development, there is constant thinking about privacy-enhancing measures. In addition, the principle of data minimization (processing as little personal data as possible) is always kept in mind.

TMS sessions

Within the TMS, sessions that are not used for 20 minutes are automatically terminated. When a user still has an existing session, it is recognized by the system and the user can access it without creating a

new session. When a new session is created, the old one is automatically terminated. Within the TMS, the user has the possibility to end his/her session via a menu item.
Within the TMS, it is not possible to gain access to closed parts of the application or to data within the application after the end of a session. Users are always referred to the login screen of the application to request a new session here.

Web protocols

Settings related to the http-requests validation are recorded in the configuration of the TMS. These configurations are validated at the web server level so that the http requests will not execute code from the TMS.

Within the TMS, all endpoints that can be called are secured by means of authorizations. These authorizations are validated before an http-request code can execute. If there is no appropriate authentication or authorization, this results in the appropriate http status code.

For the TMS, only the GET, POST and OPTIONS http request methods are activated. Other http request methods are blocked in the configuration. Within the portal of the TMS, no use is made of the http headers other than the standard necessary ones.

The TMS never gives the error and the error text in an http response. This makes it possible to contact the Service desk of TMA B.V. The employees of the Service desk can use this number to find out the error and start the appropriate action / procedure.

Web server

Within the TMS configuration, the flags 'secure' and 'HTTP Only' are set for all cookies and are enforced at web server level.

The headers 'Content-Security-Policy: frame-ancestors' and (temporarily) 'X-Frame-Options' are included to prevent the screens of the TMS from being loaded within another application (for example within a frame). This is by overruling us by adding the authorized applications to these settings.

Pen tests

TMA B.V. has included in its ISMS that pen tests are periodically carried out on the acceptance environment. This acceptance environment provides a good representation of the production environment. The degree of security, the code and settings are equal to a TMS in the production environment. Customer data is never compromised when performing a pen test. Findings from the report of the pen test will be resolved within the recommended period. TMA therefore tries to keep the security of the TMS at a high level so that your data is safe. If a critical security problem occurs, TMA B.V. will make a 100% commitment to remedy the problem immediately.

Error handling

The capture of errors is a basic form of security. By means of detailed errors, a malicious person can deduce a lot from a server or software. This information can be used for a potentially targeted attack on a potentially weak component of the server or software. TMA B.V. therefore only shows custom error notification with an ID whose meaning is only known to TMA B.V. and its developers. The actual error message is safely stored in a database. TMA has taken all possible precautions to handle the error in the best possible and safe way. The collected error messages are used to improve the TMS.

Technical means for identification, authentication and authorisation

The TMS is developed on the Microsoft.NET platform. Within this platform, Microsoft provides identification, authentication and authorization components, called Microsoft ASP.NET Identity. The TMS implements these components that are supplied to and maintained by Microsoft. This gives the TMS the certainty that safety issues related to these components will be resolved by Microsoft. With each release, we look at whether an update of these components is available. If an update is available, this update will be implemented.

Uniformity and flexibility of authentication mechanisms

The TMS uses 'Microsoft ASP.NET Identity'. This set of components implements various open standards. This set of components gives access to different ways of authentication in a uniform way. Due to this flexible set-up, various authentication sources can be unlocked by means of developed add-ons.

Passwords

The TMS has the following requirements regarding passwords.

- Password must be at least 8 characters long
- Password must contain both uppercase and normal letters
- Password must contain at least a special character or a numeric character.

It is possible for the user to change his password himself. The use of 2-wayauthentication can be configured per TMS implementation.

Implemented security measures

In the implementation of security measures, the following points have in any case been taken into account.

- Information security policy documents
- Assigning responsibilities regarding access to personal data
- Assigning responsibilities regarding information security
- TMA asset security and management
- Secure areas
- Access security
- Supplier management and reviews
- Continuity management
- Registration and handling of incidents/data leaks
- Have pen tests carried out
- Logging and auditing of logs
- Security awareness
- Monitoring and measuring
- Risk analyses
- Risk treatment plan
- Management reviews
- Management
- Implementing procedures, for example
  - Change of function
  - Change of staff
  - Safe staff
  - Granting rights SaaS application
  - Data breach notification
  - Access office space TMA

- In use ICT resources
- Change in systems
- Verification of the authenticity of means of identification

- Backup policy
- Drawing up competency profiles for TMA staff
- Version control on documents
- Confidentiality clauses in employee contracts

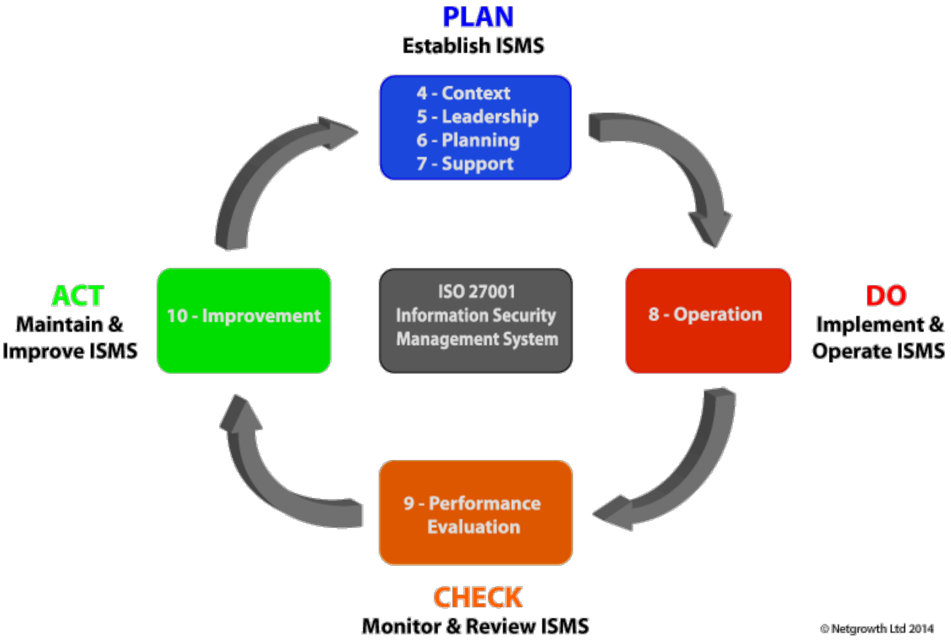
In the context of the ISO 27001 certification of TMA, all security measures and policy documents have been reviewed.

Key material and certificates.

The TMS has as its only key material the TLS Certificate for the encryption of the data traffic between client and server to encrypt over the http(s) protocol. Requesting a TLS Certificate and generating the password for the private key is done by the management authorized system administrator of TMA B.V. During the (re)installation, the system administrator (or an authorized replacement) will enter the password of the key material. In addition to the system administrator, there is always at least one extra person within TMA B.V. who knows the password. The key material of the TLS Certificate is stored by the system administrator of TMA B.V. in a safe place. The place where this material is stored is (in addition to the system administrator of TMA B.V.) known to the management of TMA B.V.

ISO 27001:2013 Certification TMA

Below is a schematic representation of the ISMS (Information Security Management System) set up by TMA.



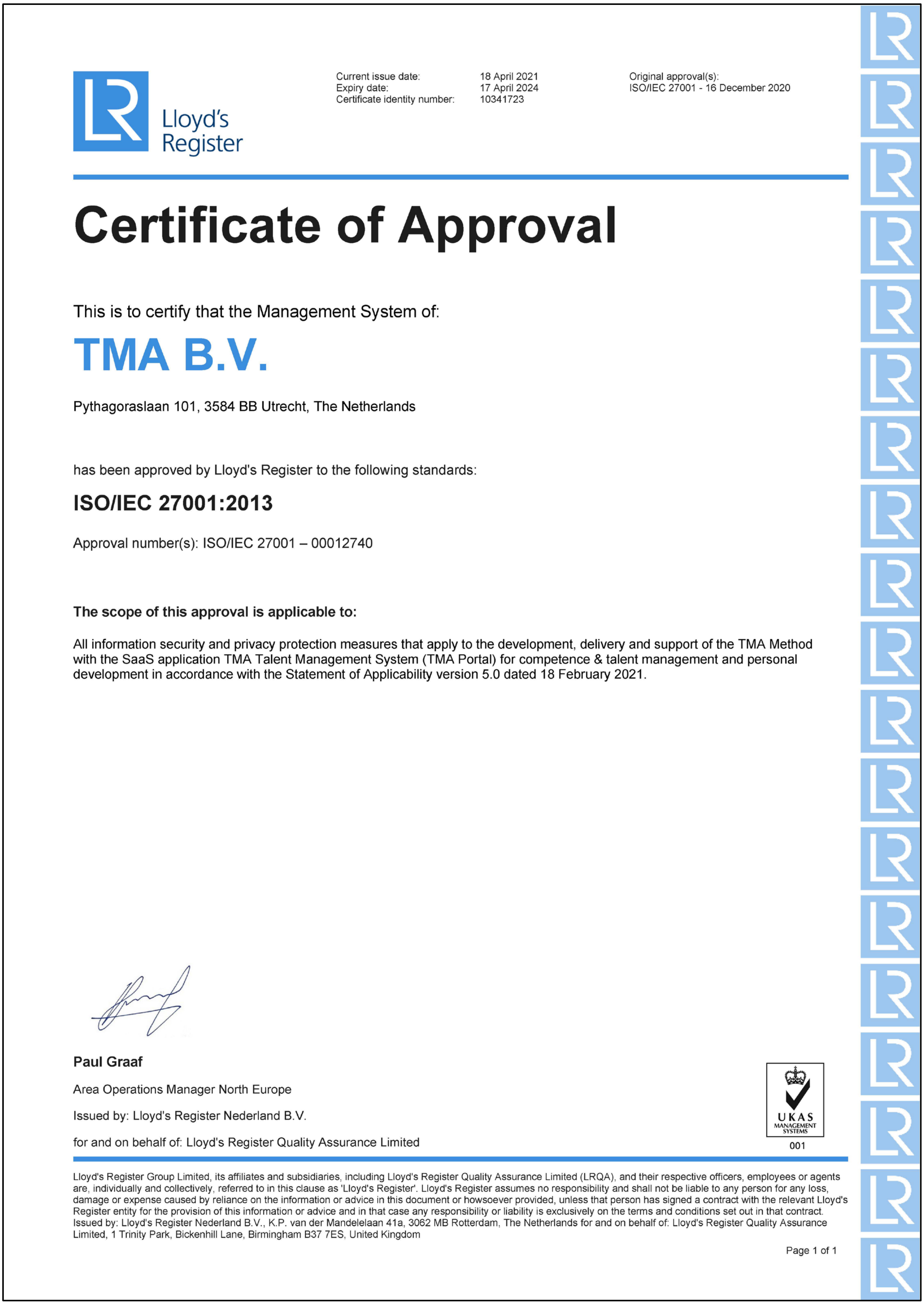
Based on the ISMS used by TMA, the ISO 27001 certificate has been obtained. Every year, TMA B.V. performs an external audit by Lloyd's Register to remain ISO 27001 certified.

The process

The ISO 27001 certification ensures that TMA B.V. as an organization continues to think carefully about the data protection in the TMS and the way in which (personal) data should be handled within the organization.

TMA has set up an ISMS in which the plan, do, check, act method is constantly applied. This method ensures that ISMS is constantly monitored and improved. In order not to let the ISMS grow into an uncontrollable system, the ISMS is divided into various documents. Consider, for example, the information security policy. This policy consists of 2 separate documents, namely the General Information Security Policy and the Technical Information Security Policy. Information security is central to both documents.

TMA's Data Protection Officer (DPO)/Privacy & Security Officer conducts internal audits at scheduled times. These internal audits are a testing moment for TMA to see whether TMA still complies with the rules and security guidelines on which it has obtained the certification. The SPO monitors on a daily basis whether TMA complies with the provisions as described in the ISMS and which are legally anchored in the GDPR.



Lloyd's Register

Current issue date: 18 April 2021
Expiry date: 17 April 2024
Certificate identity number: 10341723

Original approval(s):
ISO/IEC 27001 - 16 December 2020

Certificate of Approval

This is to certify that the Management System of:

TMA B.V.

Pythagoraslaan 101, 3584 BB Utrecht, The Netherlands

has been approved by Lloyd's Register to the following standards:

ISO/IEC 27001:2013

Approval number(s): ISO/IEC 27001 – 00012740

The scope of this approval is applicable to:

All information security and privacy protection measures that apply to the development, delivery and support of the TMA Method with the SaaS application TMA Talent Management System (TMA Portal) for competence & talent management and personal development in accordance with the Statement of Applicability version 5.0 dated 18 February 2021.

Paul Graaf

Area Operations Manager North Europe

Issued by: Lloyd's Register Nederland B.V.

for and on behalf of: Lloyd's Register Quality Assurance Limited

UKAS MANAGEMENT SYSTEMS
001

Lloyd's Register Group Limited, its affiliates and subsidiaries, including Lloyd's Register Quality Assurance Limited (LRQA), and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'Lloyd's Register'. Lloyd's Register assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant Lloyd's Register entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.
Issued by: Lloyd's Register Nederland B.V., K.P. van der Mandelelaan 41a, 3062 MB Rotterdam, The Netherlands for and on behalf of: Lloyd's Register Quality Assurance Limited, 1 Trinity Park, Bickenhill Lane, Birmingham B37 7ES, United Kingdom

Page 1 of 1

Definitions

API

An application programming interface (API) is a set of definitions that allow a computer program to communicate with another program or component (usually in the form of libraries).

Cloud

The term cloud is actually a bit misleading. The cloud is really just the internet. Like a cloud, the internet is not tangible. A cloud server is actually a server that is connected to the internet. Data can be accessed via various devices or places. The hardware with which and the location from which the server is connected plays less important role than in the past. A connection to the Internet is the most important thing to connect to the cloud server.

Code for information security

The Code for Information Security describes standards and measures that are important for achieving an adequate level of information security. The Code for Information Security consists of two parts of the standard (ISO 27001) and a 'code of practice' (ISO 27002). Certification is done against the standard. The 'code of practice' provides guidelines for the implementation of measures in the organization

Hashing

Encryption method. A hash function is a function in computer science that converts input from a broad domain of values into a (usually) smaller range, usually a subset of integers. The output is called the hash, hash code, or digest of the input. It is a form of pseudonymization.

IP address

The abbreviation IP stands for Internet Protocol. Every computer or network connected to the Internet has an IP address. This is a number that makes it visible to all other computers on the Internet. You can compare an IP address with a telephone number. To make it possible for computers to find and identify each other, they need their own number. That's the IP address. An IP address is under the protocol version IPv4 32bit and under the protocol version IPv6 128bit. The IPv4 version is the most well-known and has a format of, for example, 192.168.1.0 (this example is often found on an internal network)

IIS

Internet Information Services. This is a collection of server services developed by Microsoft intended for windows machines on the Internet. A windows machine running IIS becomes a web server through this collection of services.

Information security

Information security is the set of preventive, detection, repressive and corrective measures and procedures and processes that guarantee the availability, exclusivity and integrity of all forms of information within an organization. The aim is to guarantee the continuity of information and the provision of information and to limit the possible consequences of security incidents to an acceptable, predetermined level.

ISMS

Information Security Management System. This is an information security management system. The ISMS consists partly of IT components, but in addition, employee behavior, standard procedures and company guidelines are discussed.

ISO

An ISO standard sets requirements that an organization must meet when it wishes to obtain an ISO certificate. In order to meet the standard requirements, the organization must critically assess its existing management system in order to adapt existing processes and procedures accordingly, if necessary.

ISO 27001

ISO 27001 is a standard for information security. The standard specifies requirements for the implementation of security measures adapted to the needs of individual organizations or parts thereof. The ISMS is designed to ensure the choice of adequate and proportionate security measures that protect the information and provide trust to interested parties.

Personal data

Personal data is any data about an identified or identifiable natural person. This means that information can be traced back to a person either directly or indirectly. The fact that it must be a natural person means that data of deceased persons or of an organization are not personal data.

SaaS application

Software as a Service. The TMS (formerly TMA Portal) is a SaaS application

Salt

In salting, random data is added to a hash function.

TLS

Transport Layer Security (TLS) and its predecessor Secure Sockets Layer (SSL), are encryption protocols that secure the communication between computers (for example on the Internet).

TMS

Talent Management System / SaaS application / Portal

Web application

Web application is a term used for a program that runs on a web server, and can be accessed via the web browser.

Web Roles

Web roles are configured to be capable of running a Web application programmed for IIS.

Sources: kader-advies.nl; wikipedia; TMA technical policy; TMA general policy; NEN; Dutch Data Protection Authority

Appendix 1: Privacy statement TMA B.V. attn. TMS

TMA B.V. operates a web application called the 'Talent Management System' (TMS) and issues it online as a SaaS (Software as a Service) service. Organizations can license the use of their own TMS implementation.

TMA B.V. processes personal data and wants to clearly inform users (data subjects) and using organizations of the TMS about this.

Organisatiegegevens

TMA B.V.
Pythagoraslaan 101
3584 BB Utrecht
Netherlands

KvK No.: 30174292
Internet: www.tma.nl

Contact details Security & Privacy Officer

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

Rights with regard to personal data

If users have any questions or want to know what personal data we have about them, they can contact us. Data subjects have the following rights:

- Get an explanation about the personal data we process and what we do with it.
- Access to your personal data.
- Correcting justified mistakes.
- Deleting outdated data.
- Withdrawal of consent.
- Object to a particular use.
- Transferring your data to a third party.

In principle, we will refer requests from users about their personal data to the organization that uses a TMS implementation in which the relevant personal data of the user is located. That organization is the controller and TMA B.V. is only the processor that may only act on behalf of the controller.

If users feel that they are not being helped in the right way, they have the right to file a complaint with the above contact person or the Dutch Data Protection Authority.

Whose personal data TMA B.V. processes

TMA B.V. processes in the TMS (personal) data of people who have been provided by the organizations that use a TMS implementation and have a license for it.

If an organization that uses the TMS directly or indirectly provides personal data of users to TMA B.V., this organization must inform the persons concerned about this.

Which personal data are processed

The following personal data of the user are processed if present:

- First name, prefix and last name
- Gender
- Email
- Date of birth
- Education
- Function name of the user
- Scores that give an indication of a user's motives, talents, cognitive abilities, professional interests and competencies. This data is only processed if a user completes and completes one or more analyses or if feedback providers and/or assessors complete one or more feedback or assessment analyses about a user.
- Reports and dashboards with written and visualized output based on the scores, texts and personal data available about a user in the TMS / TMA portal
- Texts about the user that arise from the completed questions and the written conclusions or comments. This data will only be processed if a user, feedback providers and/or assessors have written these texts and placed them in the TMS / TMA Portal

The following personal data of the user are only processed by TMA B.V. This personal data is used to correct error messages, log the activities of users in the TMS, support users in the use of the TMS and improve the security and user experience of the TMS:

- The IP address of the user
- The location of the user based on IP address
- The operating system the user is using
- The browser the user is using
- The time of a user's login

The following personal data of the user can optionally be processed **anonymously** by TMA B.V. in addition to the personal data described above if provided for the purpose of scientific research and remuneration research:

- User salary level
- Percentage of employment (full-time/part-time)
- Working and thinking level
- Training
- Nationality

Why personal data are processed

TMA B.V. processes this personal data in order to implement the agreements concluded with the organizations that have taken a license to the TMA Method and the associated TMS.

For organizations that use the TMS and thus want to gain insight into the talents, motives, professional interests, cognitive capacities and competencies of their (potential) employees and / or interns and students, TMA B.V. offers various analyses, instruments with resulting reports and dashboard via the TMS . In order to make it possible for users to complete analyses and generate reports and dashboards, TMA B.V. needs a number of personal data. Why an organization that has a license to the TMS uses personal data determines the organization in fact. We therefore refer users to them if they have questions about this.

Retention period

The personal data that TMA B.V. processes are carefully stored. The retention period is determined by the organization that has a license to the TMA Method and the TMS. At the moment that this organization indicates that certain personal data must be deleted or as soon as the license for the use of the TMS with an organization has been terminated, TMA B.V. destroys all personal data with the exception of anonymized personal data for scientific and reward research.

If an individual user wishes to effect the removal of his personal data from the TMS, he must submit a request to the organization that has the license for the use of the TMS. If the user nevertheless makes this request to TMA B.V., he will be referred to the organization that has the license for the use of the TMS.

Who has access to the personal data.

The authorized employees of TMA B.V. and the processors listed in the Register of Processors have access to the personal data in addition to the organization that has a license to use its own TMS implementation. Processors may only process personal data if they have taken appropriate measures with at least the same level of security as TMA offers and this organization contractually guarantees confidentiality of the personal data.

Annex 2: Register of workers

Software development

Certigon B.V.
Sutton 15
7327AB Apeldoorn
Netherlands

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