ICT infrastructure, privacy & security

Appendix 1: Privacy statement TMA B.V. with regard to TMS
Appendix 2: Register of processors

CERTIFIED ISO/IEC 27001

CERTIFIED NEN 7510

Version 1.5

Table of contents

Introduction

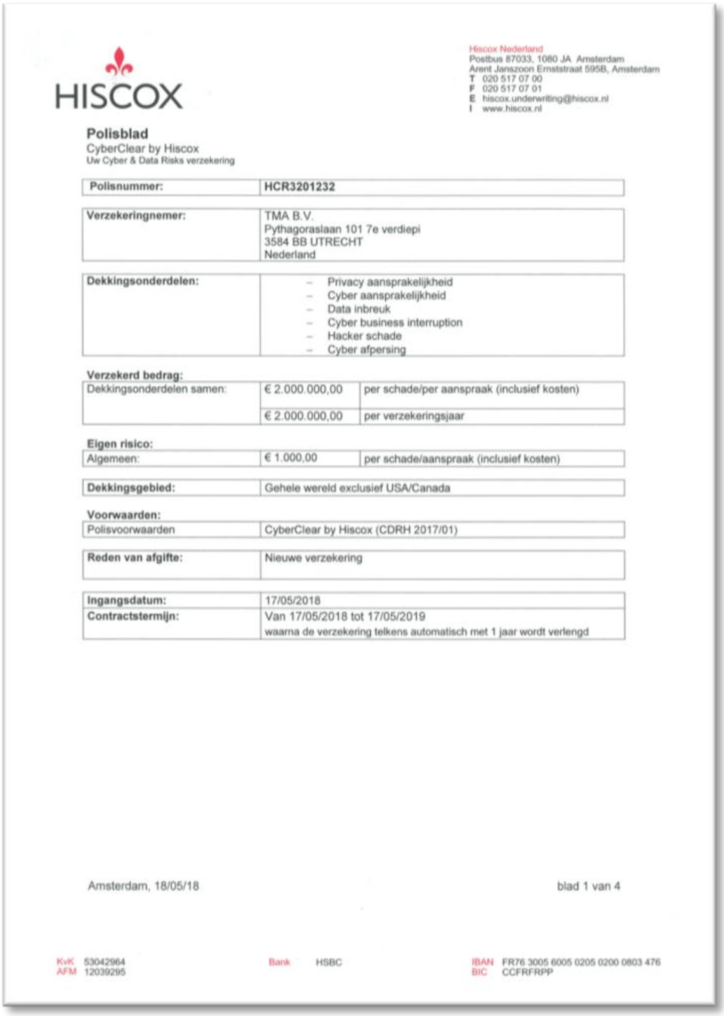
In this document the system requirements, IT infrastructure and the security measures for the Talent Management System (TMS) of TMA B.V. are listed.

The Talent Management System (TMS) is the modular platform with TMA Instruments and Content which are provided online by TMA B.V. as a SaaS (Software as a Service) service and where an organization gets one or more implementations if it has a license agreement with TMA B.V.

It is also described in this document how TMA B.V. takes the privacy of users into account. TMA is in possession of an ISO 27001 and NEN 7510 certification, which means that TMA is periodically checked to ensure that it also applies the guidelines in the correct manner according to the given standards. During these audits, organizational and technical security measures established by TMA B.V. are checked and tested for their implementation. In this document, we refer to the articles for the organizational and technical measures taken by TMA to secure personal data and data.

CERTIFIED ISO/IEC 27001 CERTIFIED NEN 7510

In the unlikely event of an incident in the field of data security and privacy, causing damage for which TMA B.V. is liable, TMA B.V. is insured up to an amount of 2 million Euro per year at 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 at least the following technical items to be able to use the TMS:

- A standalone Windows or Mac computer with Internet connection.
- A unique personal email address.
- At least the second to the latest version of one of the following browsers: Google Chrome, Apple Safari, Microsoft Internet Explorer, 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, Adobe Acrobat reader by Adobe must be available. This can be downloaded free of charge from the Adobe website or there should a comparable solution that can open PDF documents.
- The licensee's mail server(s) must be able to accept the e-mails from the TMS.

Organizational requirements

The organization that uses the TMS is responsible for the use of the personal data from the TMS and sets up conditions for the use of the personal data. It means, for example, that this organization shoul formalize the following prior to the use of the TMS:

- Indicate the goals 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. The way of using the personal data and the purpose of usage is also the responsibility of the organization that uses the TMS.
- Decide whether or not to explicitly request permission from users for the use of the personal data (a so-called opt-in function). This can be built into the TMS if the organization using the TMS indicates this.
- Decide whether or not to set up a so-called 'opt-out procedure' with which users can subsequently state that the personal data from the TMS may no longer be used.

ICT platform

The TMS uses the FIPS 140-2 certified Cloud from Microsoft Azure. The TMS is built on the Microsoft .NET framework. We only use components that are also included in the .NET Framework and are offered 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.

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. This party has access to the production network for releases and bug fixes 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, the main location is the location for Western Europe where the data center is located in Amsterdam. As an alternative location, the location was chosen in Northern Europe where the data center is located in Dublin. Under the alternative location we mean the location that we switch to if there is a major disruption in our main location. Furthermore, all backups that are made are stored at the Dublin location.

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 perform all maintenance on the infrastructure. When maintenance results are in downtime, we will inform the users of our platform about it. As an application provider, we also do not have access to the data centers and/or the infrastructure.

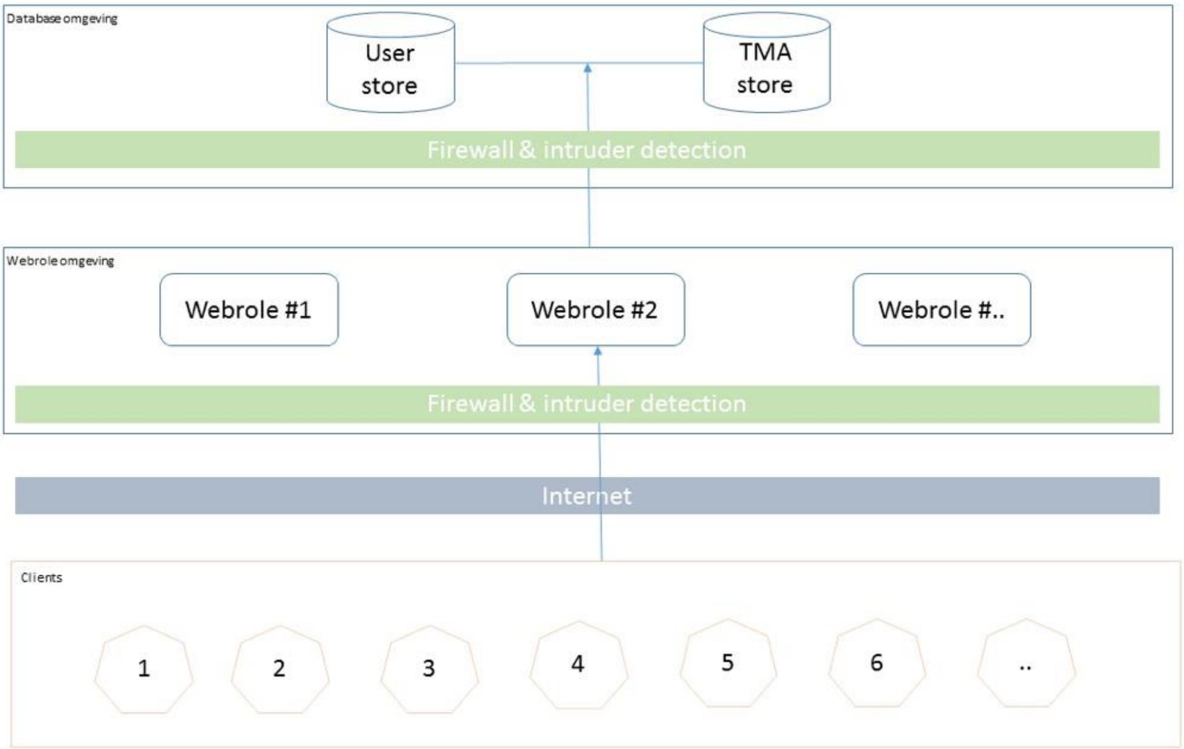
Operating system

The TMS is hosted on the Microsoft Cloud environment within the so-called 'Web roles' and the maintenance of the operating system is carried out by the Cloud supplier. Due to the use of the so-called 'Web role' we do not have access to the operating system, the maintenance of the operating system is carried out by the Cloud supplier, as a result. The Microsoft Azure Cloud is known for keeping the operating system well maintained with the latest updates.

Web servers

Since we make use of the aforementioned 'Web roles', the maintenance is the same as that of the operating system as described in the previous chapter. The 'Web roles' are set so that when the load of a web role exceeds 80%, the 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. This means we always have enough resources available at very busy times.

Visual layout of hosting environment



Database servers

The databases of the TMS are also hosted on Microsoft Azure as Azure SQL Databases. There is a firewall for each database where you can control access to the database. By default, everything is closed. By default, only the Web servers (Web roles) will have access to 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 for the execution of a release or bug fix, the firewall of the database is modified for this limited time so that the IP number from which 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 removed from the firewall of the databases.

TMS web role back-up

The TMS (installed in the Azure Cloud environment) is not backed up every night. Because we work from development with automated deployment to the environments of the Azure Cloud, the rollout of the latest version is made safe in emergencies. During the deployment of the TMS, the application will also be fully automated.

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

Database

Databases are backed up every night and can be restored via the restore function. When we have to switch to another data center during calamities, we can load the backup file to restore the database with the data from the previous night.

Access policy

Within the TMS, the areas of the program are technically separated. Within the TMS the following areas are represented:

- Candidate Area: this is the area where the candidate takes the assessment.
- Feedback Area: this is the area where the feedback providers without an account give feedback on the basis of a token.
- Customer Area: this is the area where the customer of TMA B.V. can execute 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 the administrative tasks concerning the application.
- Application Area: this is the area where the monitoring dashboards of the TMS are located.

To access each of the areas listed above, people must be explicitly authorized by the service desk of TMA B.V., with the exception of the feedback area that works on the basis of tokens. Without proper authorization it is not possible to gain access to a specific area of the TMS or to the data belonging to the area.
For each customer, we examine which areas are being accessed. It does not alter the fact that organizations that have access to the TMS are themselves responsible for actually authorizing people within the allocated areas.

User rights

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 specific roles for each area, we have made a split in the various functionalities. Because of this split, it is not possible to have access to another area and the data associated with this area without the roles required.

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

Security & privacy

TMS Policy compliance checks

The Security of the TMS is checked at least once a year with a penetration test. A report is made from the results of a penetration test.

Policy compliance checks hosting

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

Improvements

If proposals for improvement from the policy compliance checks are made and implemented in the TMS, these improvements will be included in the release notes of the TMS, if they are not essential. If the improvement proposals are essential, the improvement proposals will be included in an internal system.

Technical control function

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

Logging incidents

Incidents relating to the TMS are registered and recorded in a system so that there is an overview of what has happened and when it was solved and in which version. External reports are recorded in the same system and can result in a hotfix/interim release or are included in a regular release. Furthermore, a report for every message with the necessary data will be drawn up to test which solution has been implemented and in which release it will be delivered.

Within the TMS there are different types of logging:

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

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

Depending on the type of logging, the TMS has a retention period for it, see the retention period for each type of logging below.

- 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 kept for 1 month.

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

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

Access equipment

In the TMS, customers are created via the service desk of TMA B.V. This is the result of a signed contract that determines the identity of these customers. After creating the customer administrator, it is the responsibility of the customer which users have been added to the system. The control of identity lies with the customer for his own environment of the TMS.

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

Authentication tools

The TMS has a username-password combination to give access. If an incorrect combination is entered, access to the TMS is not granted. In addition, it is examined on the basis of roles whether proper access to a specific area can be granted. If the correct roles for a specific area are not linked to the user, access to the area is not provided. In the TMS, 2-step verification can be used for access to 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 implemented 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 that we mean:

- Request
- Assigning
- Modifications
- Revoking/suspension/deleting

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 surrounding access to our systems, both successful and unsuccessful actions are logged.

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

The TMS makes demands on identification/authentication (mechanisms) to enforce sufficiently strong passwords.

New releases of TMS

New releases of the TMS will be rolled out at the set times of the release calendar. A release will only be 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 be implemented in the production environment, after being thoroughly tested. This procedure is carried out to minimize the inconveniences.

Validation of the input on the server

All entries in the portal are validated both on the client side and server side. Validation notifications are sent to the user. This is the first step before anything of the final code is executed. Validation notifications are included in the response to the call and can be used by the calling system to inform the user. Within the TMS we use AnitForgery tokens in combination with Request Validation. This allows us to trace whether the call is authentic and comes from our server. Within the TMS we have enabled Request Validation so that it is not possible 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 are anonymized or pseudonymised.

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 on TLS 1.2. The ICT security guidelines for Transport Layer Security have been applied in the TMS.

Generating and storing reports and dashboards

In the TMS, users gain insight into the results of the TMA assessments 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 in to the TMS. These reports and dashboards are not stored in the database of the TMS but are generated over and over again. After generating the report, the TMS will delete it automatically. 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 to store them in their own location (e.g. on the 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 can change, on the one hand, and on the other hand, the data that are available about a participant can change (e.g. because he has completed another assessment or has done it again or the norm scores of an assessment have been changed) so in both cases the dashboards and reports may change over time. The reports and dashboards are therefore always a snapshot. A user is responsible if he downloads a document from the TMS and should keep it in a safe environment. The TMS does not store these PDF documents in the database of the TMS. It is done to partly prevent privacy sensitive documents from being directly downloaded by unauthorized third parties from the database of the TMS.

TMS information

Comment lines are not included during compilation to a release executable/binary. For the code that is not compiled but interpreted, the comment will be maximally removed. The TMS has defined sensitive configuration in the Azure configuration for the Web Role in which the application runs. This data is added dynamically and securely 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 maintained by Microsoft and at the beginning of each release it will be checked if there is a newer version. If this is the case, these components will be upgraded. The query texts are compiled by means of 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 TMA B.V. and partially outsourced. TMA B.V. is in control and runs the development of the TMS. TMA is 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 is performed by another party, contractual arrangements have been made about the security and processing of personal data.

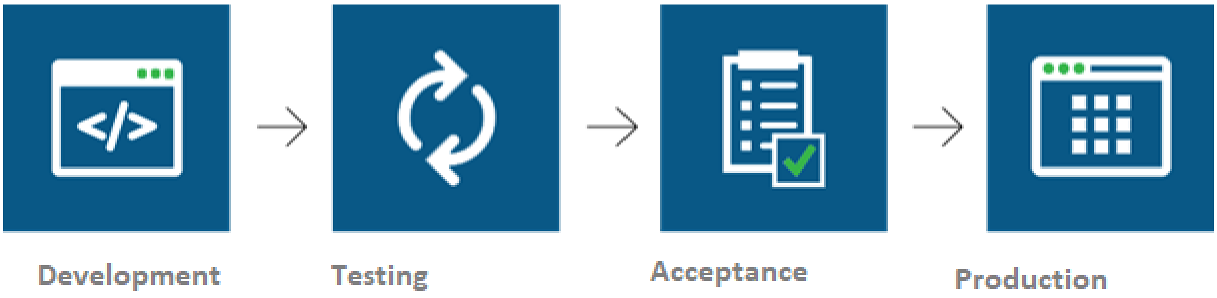
The development of the TMS is done by means of the OTAP method. There are 4 different environments that require an update in the code.

These environments are:

- Development (in this the TMS is developed with fictitious data)
- Testing (TMA tests new releases on this environment with fictitious data)

- Acceptance (Here TMA tests the deployment of the TMS as if it were live.)
- Production (This is the environment where all TMS implementations that are online).

Agreements have also been made about publishing new releases. Every second Thursday of the month a release is published when it has passed the test procedure. So-called "hotfixes" may be published faster, as described earlier in the subject "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 transferred to the production environment.

During the development process, the developers adhere to the OWASP development principle (more information can be found at 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 privacy-enhancing measures are constantly thought out. In addition, the basic 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 active for 20 minutes are automatically terminated. When a user has an existing session, it is recognized by the system and the user has access without creating a new session. If a new session is created anyway, 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 there.

Web protocols

Settings related to the http-request validation are recorded in the configuration of the TMS. These configurations are validated at the web server level, as a result of which the http requests will not execute a code from the TMS.

Within the TMS all possible endpoints to be called are protected by means of authorizations. These authorizations are validated before an http request code can be executed. 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 TMS portal, no other http headers than required by standards are used.

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 the error and start the appropriate action / procedure.

Web server

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

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

Pen tests

It is included in TMA B.V. ISMS that periodic pen tests are performed in the acceptance environment. This acceptance environment offers 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 jeopardized when performing a pen test. Findings from the report of the pen test are solved within the advised 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 arises, TMA B.V. is 100% committed to solve the problem immediately.

Handling errors

Capturing errors is a basic form of security. By means of detailed error descriptions, a malicious person can derive a lot from a server or software. This information can be used for a possible targeted attack on a potentially weak component of the server or software. TMA B.V. therefore only shows custom error messages with an ID the meaning of which 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 do the error handling in the best and the safest way possible. The collected error messages are used to improve the TMS.

Technical means for identification, authentication and authorization

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 delivered to and maintained by Microsoft. This gives the TMS the certainty that security issues relating to these components will be resolved by Microsoft. With each release it is checked 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 provides access to different ways of authentication in a uniform manner. Because of this flexible design, 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 capital letters and normal letters
- Password must contain at least one special character or one numeric character. It is possible for the user to change his password himself. The use of 2-way authentication can be configured per TMS implementation.

Implemented security measures

When implementing security measures, the following points are included in every case.

- Information security policy documents
- Assigning responsibilities with regard to access to personal data
- Assigning responsibilities with regard to information security
- Security and management of assets of TMA
- Secure areas
- Access security
- Suppliers management and assessments
- Continuity management
- Registration and handling of incidents/data leaks
- Performing pen tests
- Logging and checking of logs
- Security awareness
- Monitoring and measuring
- Risk assessments
- Risk treatment plan
- Management reviews
- Project management
- Implementing procedures for example o Modifying functions o Modifyng personnel o Personnel safety o Granting rights to SaaS application o Reporting data leak o Accessing

TMA office space o Using ICT resources o Changes in systems o Checking the authenticity of identification means

- Backup policy
- Drafting competency profiles
- Version management of documents
- Secrecy clauses in employee contracts

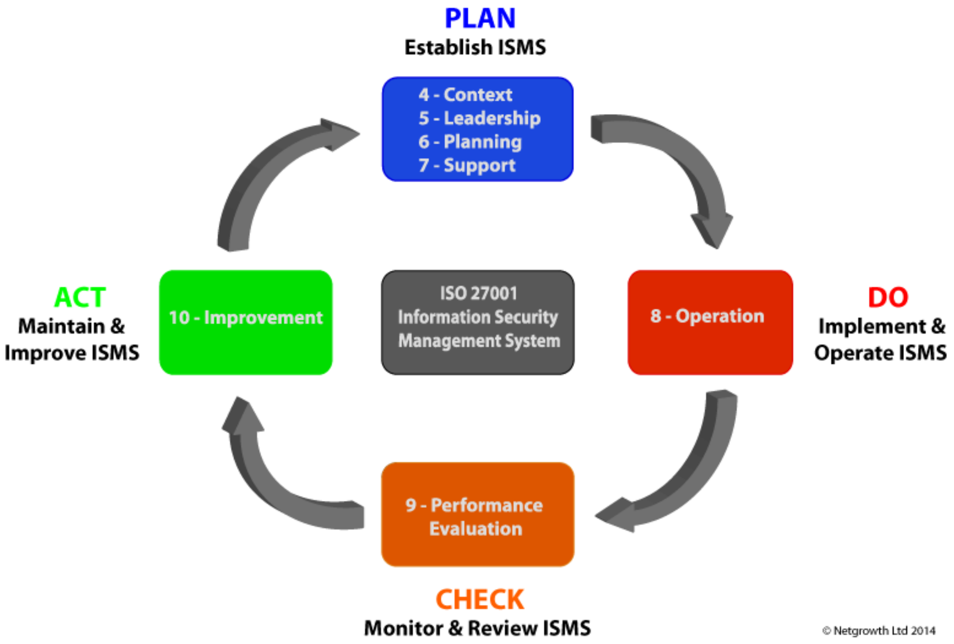
All the security measures and policy documents have been reviewed in the context of the ISO 27001 and NEN 7510 certification of TMA.

Key materials and certificates.

The TMS is the only key material to encrypt the TLS Certificate for the encryption of the data traffic between client and server 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 for the key material. In addition to the system administrator, TMA B.V. always has at least one extra person who knows the password. The key material of the TLS Certificate is provided by the system administrator of TMA B.V. stored in a safe place. The location 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 and NEN Certification of TMA

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



© Netgrowth Ltd 2014

The certificate was obtained based on the ISMS used by TMA, the ISO 27001 and NEN 7510.

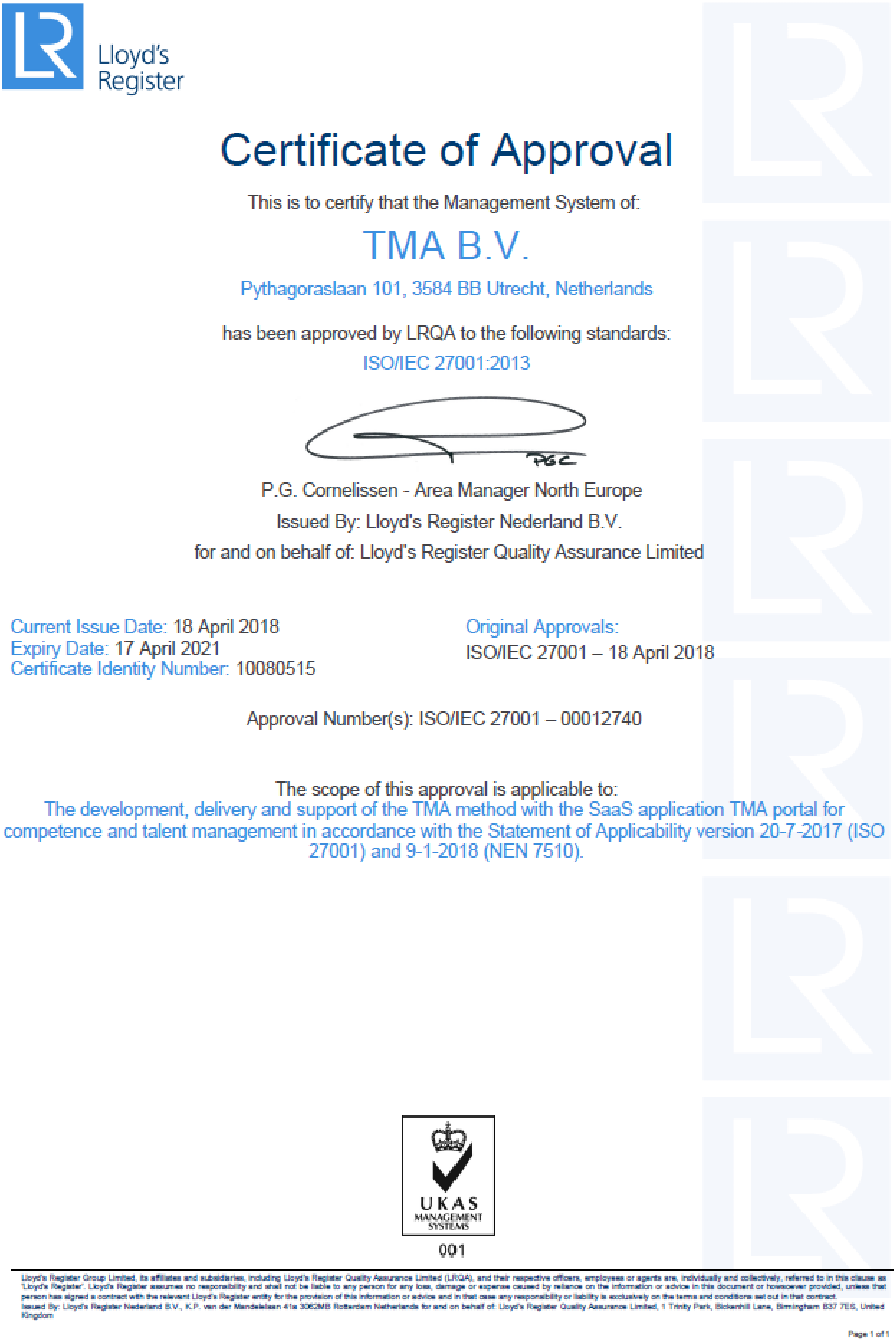
Every year an external audit is conducted at TMA B.V by Lloyd's Register to keep ISO 27001 and NEN 7510 certificates and to give its customers the assurance that TMA B.V. keeps handling (personal) data responsibly

The process

The ISO 27001 and NEN 7510 certification ensure that TMA B.V. as an organization continues to think carefully about the data protection in the TMS and the way (personal) data within the organization should be handled.

TMA has set up an ISMS that constantly applies the ‘plan-do-check-act method’. This method ensures that ISMS is constantly monitored and improved. In order not to expand the ISMS into an uncontrollable system, the ISMS is divided into various documents, for example, considering 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 in both documents.

The Security & Privacy Officer (SPO) of TMA carries out internal audits at scheduled times. These internal audits are a review moment for TMA to check whether TMA is still complying with the rules and security guidelines according to which it has been certified. The SPO monitors on a daily basis whether TMA complies with the provisions as described in the ISMS and legally anchored in the GDPR.



Lloyd's Register

Certificate of Approval

This is to certify that the Management System of:

TMA B.V.

Pythagoraslaan 101, 3584 BB Utrecht, Netherlands

has been approved by LRQA to the following standards:

ISO/IEC 27001:2013

PGC

P.G. Cornelissen - Area Manager North Europe

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

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

Current Issue Date: 18 April 2018
Expiry Date: 17 April 2021
Certificate Identity Number: 10080515

Original Approvals:
ISO/IEC 27001 – 18 April 2018

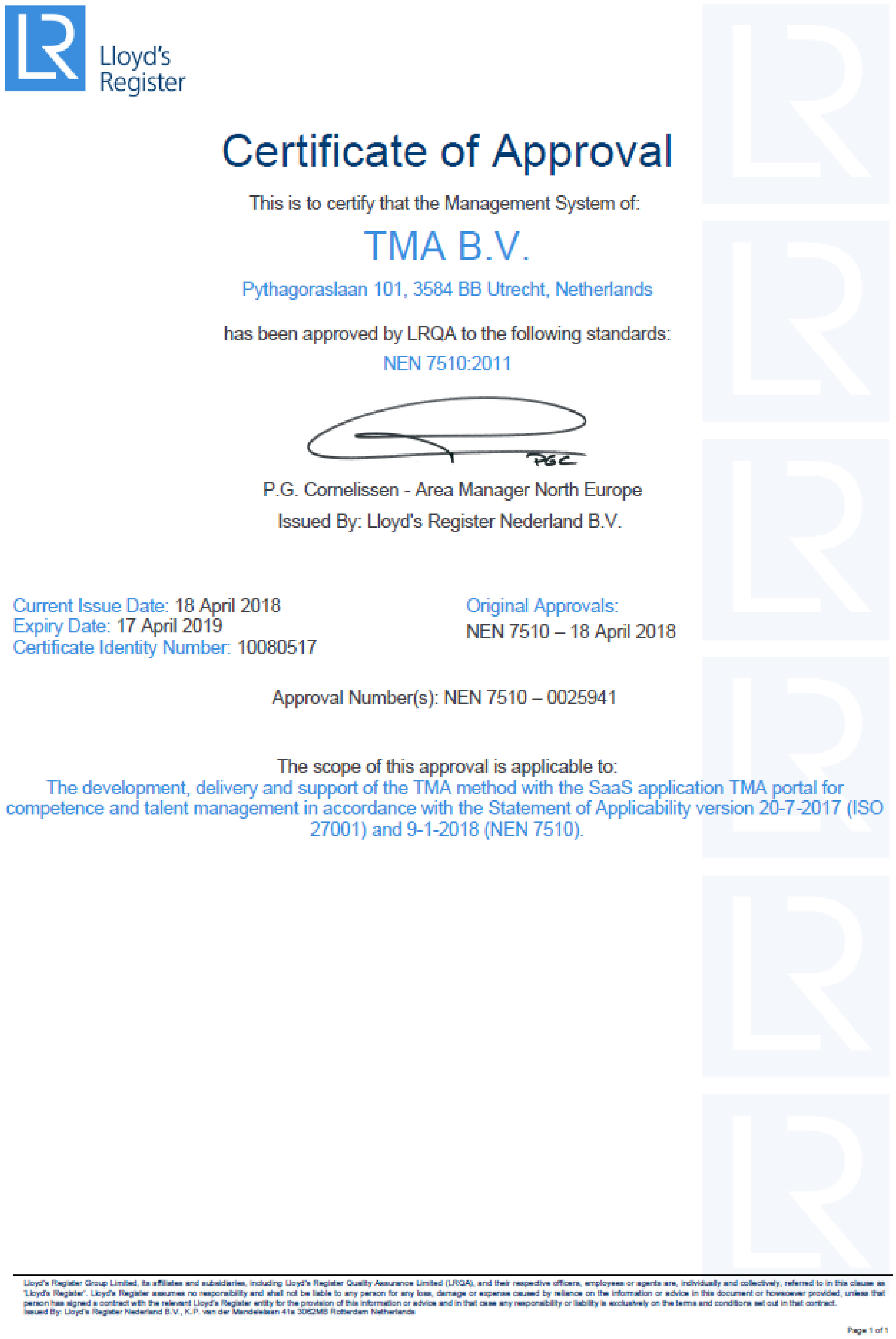
Approval Number(s): ISO/IEC 27001 – 00012740

The scope of this approval is applicable to:
The development, delivery and support of the TMA method with the SaaS application TMA portal for competence and talent management in accordance with the Statement of Applicability version 20-7-2017 (ISO 27001) and 9-1-2018 (NEN 7510).

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 3062MB Rotterdam 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



Lloyd's Register

Certificate of Approval

This is to certify that the Management System of:

TMA B.V.

Pythagoraslaan 101, 3584 BB Utrecht, Netherlands

has been approved by LRQA to the following standards:

NEN 7510:2011

PGC

P.G. Cornelissen - Area Manager North Europe

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

Current Issue Date: 18 April 2018
Expiry Date: 17 April 2019
Certificate Identity Number: 10080517

Original Approvals:
NEN 7510 – 18 April 2018

Approval Number(s): NEN 7510 – 0025941

The scope of this approval is applicable to:
The development, delivery and support of the TMA method with the SaaS application TMA portal for competence and talent management in accordance with the Statement of Applicability version 20-7-2017 (ISO 27001) and 9-1-2018 (NEN 7510).

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 3062MB Rotterdam Netherlands

Page 1 of 1

Definitions

API

An application programming interface (API) is a collection of definitions on the basis of which a computer program can communicate with another program or component (usually in the form of libraries).

Cloud

The term cloud is actually a bit misleading. The cloud is actually just the Internet. Just like a cloud, the Internet is not tangible. A cloud server is actually a server that is connected to the Internet. Data is accessible through various devices or places. The hardware with which and the location from which the connection is made with the server plays a 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 Information Security Code describes standards and measures that are important for achieving an adequate level of information security. The Code for Information Security consists of two parts: the standard (ISO 27001) and a 'code of practice' (ISO 27002). Certification is done within the norm. 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 wide domain of values into a (usually) smaller range, usually a subset of the 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 is 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 best 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 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 whole range of preventive, detective, 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 the 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 a management system for information security. The ISMS consists partly of IT components, but also the behavior of employees, standard procedures and company guidelines are discussed in ISO In an ISO standard, the requirements are set and an organization must comply to those if 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, if necessary, adapt existing processes and procedures accordingly.

ISO 27001

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

NEN 7510

NEN 7510 is a standard for information security for the healthcare sector in the Netherlands developed by the Dutch Standardization Institute. The standard is based on the Code for Information Security.

Personal data

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

SaaS application

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

Salt

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

TLS

Transport Layer Security (TLS) and its predecessor Secure Sockets Layer (SSL), are encryption protocols that protect the communication between computers (e.g. 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 suitable for running a web application that is programmed for IIS.

Sources: kader-advies.nl; Wikipedia; TMA technical policy; TMA general policy; NEN; Authority Personal Data

Appendix 1: Privacy statement TMA B.V. with regard to TMS

TMA B.V. operates a web application called 'Talent Management System' (TMS) and publishes 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 user organizations of the TMS.

Organizational data

TMA B.V.
Pythagoraslaan 101
3584 BB Utrecht
The Netherlands

CoC nr: 30174292
Internet: www.tma.nl

Contact details Security & Privacy Officer

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

Rights with regard to personal data

If users have questions or want to know what personal data we have from them, they can contact us. The persons involved have the following rights:

- Get an explanation about the personal data we process and what we do with it.
- The inspection of your personal data.
- Correcting justified errors.
- Deleting outdated data.
- Withdrawing permission.
- Object to a specific use.
- Transferring your data to a third party.

Requests from users about their personal data will in principle be referred to the organization that uses a TMS implementation where the personal data concerned are located by the user. That organization is in fact the controller and TMA B.V. is only the processor who is only allowed to 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 contact person above or the Dutch Data Protection Authority.

Whose personal data are processed by TMA B.V.

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

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

Which personal data will be processed

The following personal data of the user will be processed if present:

- First name, infix and last name
- Sex
- E-mail address
- Date of birth
- Education
- Function name of the user
- Scores that give an indication of the drives, talents, cognitive abilities, professional interests and competencies of a user. This data is only processed if a user takes and fills in one or more assessments or if feedback providers and/or assessors complete one or more feedback or assessment tests about a user

- Reports and dashboards with written and visualized output based on the scores, texts and personal data available to a user in the TMS/TMA portal
- Texts about the user that arise from the completed questionnaires and the written conclusions, such as comments. This data is only processed if a user, feedback providers and/or assessors have written these texts and placed them in the TMS/TMA Portal

Only the following personal data of the user are processed by TMA B.V. These personal data are 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 that the user uses
- The browser that the user uses
- The time of login of a user

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

- Salary level of the user
- Percentage of employment (full-time/part-time)
- Professional and intellectual abilities
- Education
- Nationality

Why personal data are processed

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

For organizations that use the TMS and therefore want to gain insight into the talents, drives, professional interests, cognitive capacities and competencies of their (potential) employees and/or trainees and students, TMA B.V. offers various assessments, instruments with resulting reports and dashboard via the TMS. In order to make it possible for users to fill in assessments and generate reports and dashboards, TMA B.V. need some personal data. Why an organization having a license on the TMS uses personal data is determined by the organization in question. We therefore redirect users to those organizations if they have any questions about it.

Storage period

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

If an individual user wishes to have his personal data removed from the TMS, he must submit a request to the organization that has the license to use the TMS. If the user sends this request to TMA B.V. he will be redirected to the organization that has the license to use the TMS.

Who has access to personal data

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

Appendix 2: Register of processors

Software development

Certigon B.V.
Sutton 15

7327AB Apeldoorn
The Netherlands

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