infosrevision

Master International A/S

Bregnerødvej 144
3460 Birkerød

ISAE 3000, type 2

Independent auditor's ISAE 3000 assurance report on the description of controls aimed at information security and processing of personal data throughout the period from 1st March 2020 to 28th February 2021

CVR.NR. 10 02 80 86

1. Assertion by Master International A/S

Master International A/S deliver systems that processes personal data for our customers who are data controllers with reference to the data processing agreements.

The accompanying description has been prepared for customers who have used the Metis platform and their auditors who have a sufficient understanding to consider the description along with other information, including information about controls operated by the customers themselves, when assessing whether the requirements of the EU Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter "the Regulation") have been complied with.

Master International A/S confirms that:

a) The accompanying description in section 2 fairly presents the Metis platform (the system) for processing personal data for data controllers covered by the Regulation throughout the period from 1st March 2020 to 28th February 2021. The criteria used in making this statement were that the accompanying description:

(i) Presents how the system was designed and implemented, including:

- The types of services provided, including the type of personal data processed;
- The procedures, within both information technology and manual systems, used to initiate, record, process and, if necessary, correct, delete and restrict processing of personal data;
- The procedures used to ensure that data processing has taken place in accordance with contract, instructions or agreement with the data controller;
- The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality;
- The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation;
- The procedures supporting in the event of breach of personal data security that the data controller may report this to the supervisory authority and inform the data subjects;
- The procedures ensuring appropriate technical and organisational safeguards in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- Controls which we, referring to the Metis platform, have assumed would be implemented by the data controllers and which, if necessary in order to achieve the control objectives stated in the description, are identified in the description;
- Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to the processing of personal data;

(ii) Contains relevant information about changes in the data processor's Metis platform in the processing of personal data in the period from 1st March 2020 to 28th February 2021;

(iii) Does not omit or distort information relevant to the scope of the Metis platform described for processing personal data, taking into consideration that the description was prepared to meet the general needs of a wide range of data controllers and therefore cannot include any aspect of the Metis platform that the individualdata controller had to consider important according to their particular circumstances;

b) The controls related to the control objectives stated in the accompanying description were suitably designed and implemented throughout the period from 1st March 2020 to 28th February 2021. The criteria used in making this statement were that:

(i) The risks threatening the achievement of the control objectives listed in the description were identified;

(ii) The controls identified would, if carried out as described, provide a high level of assurance that the risks involved did not prevent the achievement of the control objectives stated; and

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority throughout the period from 1st March 2020 to 28th Februar 2021.

c) Appropriate technical and organizational safeguards were established and maintained to comply with the agreements with the data controllers, sound data processing practices and relevant requirements for data processors in accordance with the Regulation.

Birkerød, 23rd April 2021
Master International A/S

Jesper Broberg Nielsen
CEO

Uffe Dejligbjerg
CTO

2. Systems description (the Metis platform)

Introduction

The accompanying description has been prepared for customers who have used the Metis platform and their auditors who have a sufficient understanding to consider the description along with other information, including information about controls operated by the customers themselves, when assessing whether the requirements of the General Data Protection Regulation are complied with.

Digital Test and Assessment Platform

Master International A/S develops, supports, and operates the Master Assessment Platform (Metis) and supplies a broad range of tests and assessment solutions on the platform. Access is provided to customers as software-as-a-service (SaaS), using a subscription-based model, and the components, features and tests available to each customer depend on license terms and contract.

The customer uses Metis to invite employees and job candidates to take online tests and make assessments. The customer also uses Metis for the workflow of the assessment process and for the analysis and reporting of response and test results.

The customer is the data controller for all data collected and generated, and Master International A/S and its employees do not access or handle personal data collected by the customer directly or in a personally identifiable format. As a data processor, Master International makes the platform available to the customer. The configuration and use of the software serve as instructions for the data processing on the platform, and the data stored on the platform is the responsibility of the customer, being the data controller. The types of data which are being processed and the nature of the processing are defined in the Data Processing Agreement. The platform has features to support the data controller's obligations, including, but not limited to, the following areas:

- Transparency in handling and using personal data
- Handling requests for correction or deletion of personal data
- Limiting the collection and processing of personal data to intended and legitimate purposes
- Limiting the storage time of personal data.

When personal data is processed and stored on the platform, data is always protected through appropriate security through technical and organizational measures, and Master International A/S stays committed to meet every requirement of the EU General Data Protection Regulation.

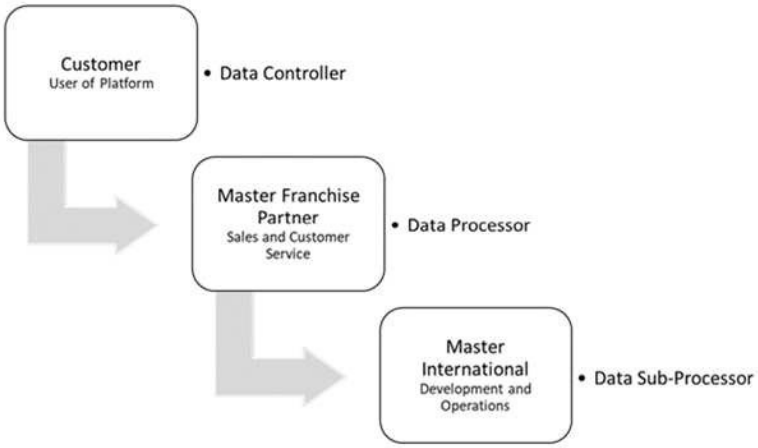
Scope

The description includes the services delivered by Master International and focuses on control objectives relevant to the internal controls that relate to the EU General Data Protection Regulation. The description includes the business processes that Master International has identified as important to the companies using Master International as their data processor or data sub-processor from an information security perspective. The management of Master International is responsible for identifying control objectives and for the manual and automated controls put into operation to achieve these objectives. This includes the information technology and infrastructure supported by Master International's operating organization.

The description is intended to cover the companies using Master International as their data processor or data sub-processor. Therefore, focus will be on the processes and controls which are used in the common processes.

The platform is Software-as-a-Service (SaaS) and is most often provided to the end-user company (customer) through franchise partners having a GDPR Data Processing Agreement (DPA) with Master International. The end-user company is the Data Controller, thus entering a DPA with the franchise partner and becoming responsible for the test takers they administer through the platform. The test takers are the data subjects in a GDPR context.

The delivery of the SaaS can be illustrated as follows:



Master International also has direct customers with no franchise partners involved. For them, Master International serves as Data Processor, and the customer enters a DPA with Master International directly.

All processing of personal data on the platform, and all related procedures and tasks, are governed by strict policies and principles of the Master International Security and GDPR Compliance Guide and by legally binding Data Processing Agreements between Master International and its partners, and between partners and customers. The Data Processing Agreements between partners and customers are not subject to this assurance engagement. The Security and Compliance guide is maintained by Master International's CTO function to ensure continuous compliance checking and consistency with the technical and operational aspects of the platform. All employees working with the platform and with the test solutions delivered on the platform are audited and have signed the Master Trusted Employee Policy, covering conduct, compliance, procedures, and confidentiality.

Data collected from assessments on the platform are always persisted in an anonymous form. Personal data are stored in a different storage system with a separate authentication system and only kept per agreement with the data controller. To ensure cleaning of data, the platform implements a notification system that can notify the data controller when personal data is due for deletion and implements a process for the actual deletion of personal data.
All security policies, procedures, internal controls, data processing agreements and compliance objectives are a primary focus of Master International, with the CEO assuming final responsibility and signing off on correctness and internal compliance. To make sure that all security policies and processes are implemented throughout the organization, annual internal review and approval by area managers complement the Master Trusted Employee policies signed by all employees.

Risk Assessment

Master International maintains a thorough risk assessment concerning threats relevant to each area of the platform which may constitute a target or a vulnerability. The risk assessment is completed and maintained by the CTO function following best practices and with due regard to current threat levels and the overall security landscape. It covers risks for personal data and for service continuity and recovery, and other types of risks and failures. Types of threats covered include cybercrime, misuse, service interruptions, physical events and accidents, technical errors and unauthorized access, and the separate areas covered include communication, storage, software, and physical locations and assets.

For all risks identified, the hypothetical scenario and its possible consequences from a general perspective as well as a GDPR perspective were identified, and an analysis of impact and probability was conducted. Finally, for each risk, the countermeasure taken to protect the platform and the data stored has been described and approved as a valid means of minimizing or removing the risk concerned.

The risk assessment is part of the Master International Security and Compliance Guide governing all security measures concerning the platform and is approved and reviewed yearly.

Control measures

Procedures and controls have been developed in the following main areas, which refer to the Data Protection Regulation:

- Procedures and controls are followed to ensure that processing of personal data is performed according with the principles and instructions in the Data Processing Agreement.
- The data processor has implemented technical measures to safeguard relevant security of processing.
- The data processor has implemented organizational measures to safeguard relevant security of processing.
- Procedures and controls are complied with to ensure that personal data can be deleted or returned if arrangements are made with the data controller.
- Procedures and controls are complied with to ensure the data processor will only store personal data in accordance with the agreement with the data controller.
- Procedures and controls are complied with to ensure that only approved sub-data processors are used.
- Procedures and controls are complied with to ensure that the data processor will only transfer personal data to third countries in accordance with the agreement with the data controller.
- Procedures and controls are complied with to ensure that the data processor can assist the data controller in handling out, correcting, deleting or restricting information.
- Procedures and controls are complied with to ensure that any personal data breaches may be responded to in accordance with the data processing agreements.

Reference is also made to section 4, where the specific control activities are described.

Encryption

To secure data beyond access control, the platform implements different encryption strategies on multiple levels: Transport, Code and Storage.

All communication between our services and clients are secured by a 2048-bit encryption certificate issued to Master International A/S by GlobalSign. The encryption is implemented on all our services and supports HTTPS/TLS1.2+1.3 on all domains and endpoints used by the platform.

To ensure the integrity of our application, we use code-signing certificate issued by GlobalSign for all distributed applications. This digital signature preserves the integrity of the application and ensure that the application code is not altered with unapproved changes after release.

The platform utilized multiple database technologies. All of them implements encryption on a service level. This means, that all databases perform real-time encryption and decryption of data, backups and transaction logs using the AES256 standard. Encryptions keys are managed and rotated in compliance with the internal security policy and the root key is protected by an internal secret store.

Complementary controls for the data controllers

As part of the delivery of the services, there are controls that are assumed to have been implemented by the data controllers. These controls are essential to achieve the control objectives stated in the description. The data controllers have the following obligations:

- Ensure that the personal data is up to date.
- Ensure that the instruction is always legal in relation to the privacy law.
- Ensure that the instruction is appropriate, with respect to the data processing agreement and the principal service.
- Ensure that the data controller's users are up to date.
- It is the data controllers' responsibility to ensure that the test taker (data subject) has given their consent to the processing of their personal data.
- It is the data controllers' responsibility to ensure that they only perform legal processing of personal data.

- Franchise partners (data processor) are responsible for ensuring a data processing agreement with the data controller.
- It is the data controllers' responsibility to ensure that the test taker (data subject) is informed about relevant processing of personal data and the subject's rights.
- Franchise partners (data processor) are responsible for ensuring a data processing agreement with thedata controller.
- It is data controllers' responsibility to ensure a process for responding to queries from the data subject in a timely manner.
- Franchise partners (data processor) are responsible for ensuring a data processing agreement with thedata controller.
- It is the data controller's responsibility to delete or rectify personal data.
- Franchise partners (data processor) are responsible for ensuring a data processing agreement with thedata controller.
- It is the data controller's responsibility to ensure that the data controller's employees have restricted access to personal data and to delete or rectify personal data on request.
- It is the data controller's responsibility to ensure that the correction of personal data has been done correctly and without undue delay.
- Franchise partners (data processor) are responsible for ensuring a data processing agreement with the data controller.
- The data controller is responsible for providing the data subject with an extract file of personal data on request.
- It is the data controllers' responsibility to ensure that only authorized employees at the data controller have access to personal data.
- Franchise partners (data processor) are responsible for ensuring a data processing agreement with the data controller.
- Franchise partners (data processor) are responsible for ensuring a data processing agreement with the data controller.
- It is the data controller's responsibility to observe and examine the user's activities in relevant audit logs.

3. Independent auditor's assurance report on the description of controls related to data protection and processing of personal data

To the management of Master International and Master International's franchise partners and customers

Scope
We were engaged to provide assurance about Master International A/S's systems description of the Metis platform in section 2 for processing personal data in accordance with the data processing agreement with the data controllers throughout the period from 1st March 2020 to 28th February 2021 ("the Description") and about the design and operating effectiveness of controls related to the control objectives stated in the Description.

The description and, accordingly, our report only deal with shared processes, controls involved in those processes and the security baselines generally applicable to companies using Master International as a data processor or data subprocessor. This report does not cover customers with specific process and security requirements.

We express reasonable assurance in our conclusion.

Master International responsibility
Master International A/S is responsible for: preparing the Description and the accompanying statement in section 1, including the completeness, accuracy, and the method of presentation of the Description and statement, providing the services covered by the Description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Auditor's independence and quality control
We have complied with the independence and other ethical requirements of the Code of Ethics for Professional Accountants issued by FSR - Danish Auditors (Code of Ethics for Professional Accountants), which are based on the fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional conduct.

Inforevision is subject to the International Standard on Quality Control (ISQC 1) and accordingly uses and maintains a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Auditors responsibility
Our responsibility is to express an opinion on Master International A/S' Description and on the design and operating effectiveness of controls related to the control objectives stated in that Description, based on our procedures.

We conducted our engagement in accordance with International Standard on Assurance Engagements 3000, "Assurance Engagements Other than Audits or Reviews of Historical Financial Information", and additional requirements under Danish audit regulation, to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls are appropriately designed and operating effectively.

An assurance engagement to report on the Description, design, and operating effectiveness of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's description of its system and about the design and operating effectiveness of controls. The procedures selected depend on the auditor's judgment, including the assessment of the risks that the Description is not fairly presented, and that controls are not appropriately designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the Description, the appropriateness of the objectives stated therein, and the appropriateness of the criteria specified by the data processor and described in section 1.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of controls at a data controller
Master International A/S' Description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of the Metis platform that the individual data controllers may consider important in their particular circumstances. Also, because of their nature, controls at a data processor may not prevent or detect personal data breaches. Furthermore, the projection of any evaluation of the operating effectiveness to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

Opinion
Our opinion has been formed on the basis of the matters outlined in this auditor's report. The criteria we used in forming our opinion were those described in Management's statement section. In our opinion, in all material respects:

(a) The Description of the controls, as they were designed and implemented throughout the period from 1st March 2020 to 28th February 2021, is fairly presented
(b) The controls related to the control objectives stated in the Description were appropriately designed throughout the period from 1st March 2020 to 28th February 2021; and
(c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved, operated effectively throughout the period from 1st March 2020 to 28th February 2021.

Description of the testing of controls
The specific controls tested and the nature, timing, and results of those tests are listed in section 4.

Intended users and purpose
This report and the description of tests of controls are intended only for customers who have made use of Master International A/S's Metis platform and the auditors of these customers, who have a sufficient understanding to consider it along with other information, including information about controls operated by customers themselves, in assessing whether the requirements of the General Data Protection Regulation have been complied with.

Søborg, 23rd April 2021

inforevision
statsautoriseret revisionsaktieselskab

John Richardt Søbjærg
State Authorized Public Accountant

Simon Okkels
IT Auditor, CISA

4. Control objectives, control activities, tests and results thereof

4.1 Objective and scope

Our work has been performed in accordance with ISAE 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information.*

Our test of the design and implementation of the controls has included the control objectives and associated control activities selected by the management, which are stated in section 4.2. Any other control objectives, associated controls and controls at Master International A/S' customers are not covered by our tests.

4.2 Tests Performed

The tests performed to evaluate design and implementation of controls are mentioned below:

Method	Description
Inspection	Review and assessment of policies, procedures and documentation regarding the execution of controls
Inquiries	Inquiries of appropriate staff at the company, regarding controls
Observation	Observation of how controls are performed
Re-execution of control	We have repeated or observed the performance of the control in order to verify that the control are working as assumed.

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registereret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

John Richardt Søbjærg
Statsautoriseret revisor
Serienummer: CVR:19263096-RID:1265358432438
IP: 93.165.xxx.xxx
2021-04-23 12:55:28Z
NEM ID

Jesper Broberg Nielsen
CEO
Serienummer: PID:9208-2002-2-616599340531
IP: 85.184.xxx.xxx
2021-04-23 12:55:52Z
NEM ID

Simon Okkels
IT-Revisor, CISA
Serienummer: CVR:19263096-RID:63988234
IP: 93.165.xxx.xxx
2021-04-26 06:54:48Z
NEM ID

Uffe Dejligbjerg
CTO
Serienummer: PID:9208-2002-2-319695137229
IP: 152.115.xxx.xxx
2021-04-26 08:31:01Z
NEM ID