Assurance report

Master International A/S

Independent auditor's ISAE 3000 type 2 assurance report on information security and measures pursuant to the data processing agreement with customers using the Master People Platform throughout the period from 1 January 2025 to 31 December 2025

March 2026

Grant Thornton | www.grantthornton.dk
Lautrupsgade 11, 2100 København Ø
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

Penneo document key: A0EXE-2J80B-PAMJ1-CFKYO-B16VC-FA7

Section 1: Master International A/S' statement

The accompanying description has been prepared for data controllers, who has signed a data processing agreement with Master International A/S, and who has a sufficient understanding to consider the description along with other information, including information about controls operated by the data controllers themselves in 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 uses the sub-processor: Microsoft. This statement does not include control objectives and related controls at Master International A/S' sub-processor. Certain control objectives in the description can only be achieved, if the sub-processor's controls, assumed in the design of our controls, are suitably designed and operationally effective. The description does not include control activities performed by sub-processors.

Some of the control areas, stated in Master International A/S' description in Section 3 of delivery of the Master People Platform, can only be achieved if the complementary user entity controls with the data controllers are suitably designed and operationally effective with Master International A/S' controls. This assurance report does not include the appropriateness of the design and operational effectiveness of these complementary user entity controls.

Master International A/S confirms that:

a) The accompanying description, Section 3, fairly presents how Master International A/S has processed personal data for data controllers subject to the Regulation throughout the period from 1 January 2025 to 31 December 2025. The criteria used in making this statement were that the accompanying description:

   (i) Presents how Master International A/S' processes and controls were 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 that we, in reference to the scope of Master International A/S, 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

Penneo document key: A0EXE-2J80B-PAMJ1-OFKYO-JB4I6-WCFA7

(ii) Includes relevant information about changes in the data processor's delivery of the Master People Platform in the processing of personal data during the period from 1 January 2025 to 31 December 2025;

(iii) Does not omit or distort information relevant to the scope of delivery of the Master People Platform being described for the processing of personal data while acknowledging that the description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of delivery of the Master People Platform that the individual data controllers might consider important in their particular circumstances.

b) The controls related to the control objectives stated in the accompanying description were, in our view, suitably designed and operated effectively throughout the period from 1 January 2025 to 31 December 2025 if relevant controls with sub-processors were operationally effective and data controller has performed the complementary user entity controls, assumed in the design of Master International A/S' controls throughout the period from 1 January 2025 to 31 December 2025. The criteria used in making this statement were that:

(i) The risks that threatened achievement of the control objectives stated in the description were identified

(ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and

(iii) The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period from 1 January 2025 to 31 December 2025.

c) Appropriate technical and organisational 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, 16 March 2026
Master International A/S

Jesper Broberg
CEO

Penneo document key: A0EXE-2J80B-PAMJ1-OFKYO-JB4I6-WCFA7

Section 2: Independent auditor's ISAE 3000 assurance report with reasonable assurance on information security and measures pursuant to Master International A/S' data processing agreements with data controllers during the period from 1 January 2025 to 31 December 2025

To: Master International A/S and their customers

Scope

We were engaged to provide assurance about Master International A/S' description, Section 3 of delivery of the Master People Platform in accordance with the data processing agreement with data controllers throughout the period from 1 January 2025 to 31 December 2025 and about the design and operational effectiveness of controls related to the control objectives stated in the Description.

Master International A/S uses the sub-processor: Microsoft. This statement does not include control objectives and related controls at Master International A/S' sub-processor. Certain control objectives in the description can only be achieved if the sub-processor's controls, assumed in the design of our controls, are appropriately designed, and operating effectively. The description does not include control activities performed by sub-processor.

Some of the control objectives stated in Master International A/S' description in Section 3 of delivery of the Master People Platform, can only be achieved if the complementary user entity controls with the data controller have been appropriately designed and operating effectively with the controls with Master International A/S. The report does not include the appropriateness of the design and operational effectiveness of these complementary user entity controls.

Our opinion is based on reasonable assurance.

Master International A/S' responsibilities

Master International A/S is responsible for: preparing the Description and the accompanying statement, 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 for the design and implementation of operationally effective controls, to achieve the stated control objectives.

Grant Thornton's independence and quality control

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour and ethical requirements applicable to Denmark.

Grant Thornton applies International Standard on Quality Management 1, ISQM 1, requiring that we maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express an opinion on Master International A/S' Description and on the design and operational 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.

Penneo document key: A0EXE-2J80B-PAMJ1-OFKYO-JB4I6-WCFA7

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 delivery of the Master People Platform 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 processor

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 delivery of the Master People 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 are those described in the *Management's statement* Section 1. In our opinion, in all material respects:

(a) The description fairly presents how Master International A/S' delivery of the Master People Platform was designed and implemented throughout the period from 1 January 2025 to 31 December 2025.

(b) The controls related to the control objectives stated in the description were suitably designed and implemented throughout the period from 1 January 2025 to 31 December 2025 in all material respects, and

(c) The controls tested, which were the controls necessary for providing reasonable assurance that the control objectives in the description were achieved in all material respects, operated effectively throughout the period from 1 January 2025 to 31 December 2025.

Description of tests 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 in Section 4 are intended only for data controllers who have used Master International A/S' delivery of the Master People Platform who have a sufficient understanding to consider it along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the Regulation have been complied with.

Copenhagen, 16 March 2026

Grant Thornton
Godkendt Revisionspartnerselskab

Anders Holmgaard Christiansen
State Authorised Public Accountant

Andreas Moos
Partner, CISA, CISM

Penneo document key: A0EXE-2J80B-PAMJ1-OFKYO-JB4I6-WCFA7

Section 3: Master International A/S' description of processing activity for the delivery of the Master People Platform

The purpose of this description is to provide information to Master International A/S' customers and their stakeholders (including auditors) about compliance with the data processing agreements with customers.

Further, the purpose of this description is to provide information about the processing security, technical and organisational measures, and responsibilities between the data controller (our customers) and Master International A/S.

The nature of processing

Master International A/S' processing of personal data on behalf of the data controller is primarily: **General Personal data.**

Personal data

- **General personal data**, including identification such as name and contact information, year of birth, gender, country of origin, preferred language, level of highest education, current employment status, and current business function.
- Sensitive categories of personal data, including race and ethnic origin, political beliefs, religious or philosophical conviction, union memberships, genetic data, biometric data for unambiguous identification, health details, sexual relations, or sexual orientation.
- Other personal data, including information about criminal offences and CPR numbers.

The following categories of natural people are included in the data processing agreement:

- Customers

Instructions from the data controller

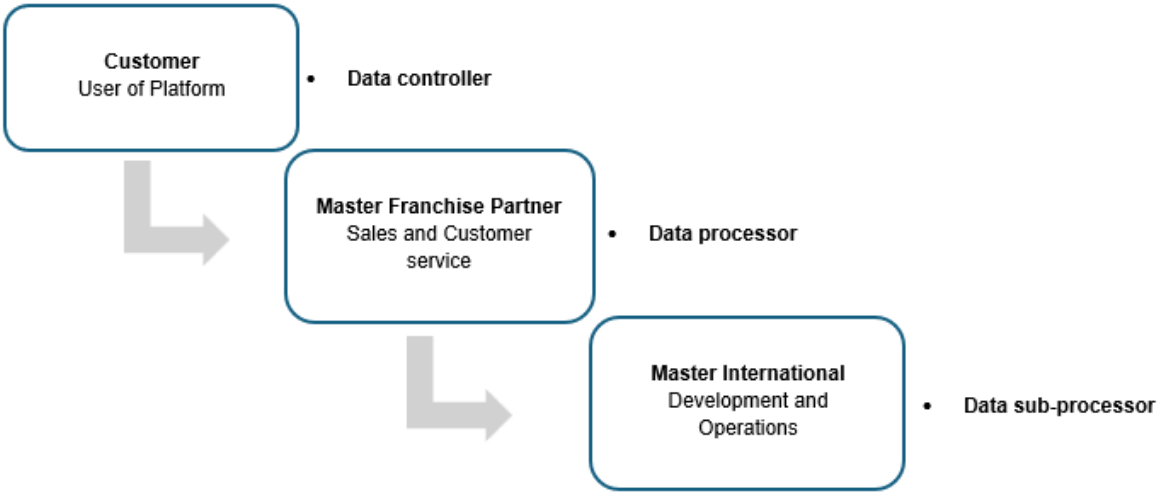
The description includes the services delivered by Master International and focuses on control objectives relevant to the internal controls that relate to the EU General Data Protection Regulation. The description includes the business processes that Master International has identified as important to 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 organisation.

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.

Penneo document key: A0EXE-2J80B-PAMJ1-OFKYO-JB4I6-WCFA7

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.

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 organisation, 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 unauthorised access, and the separate areas covered include communication, storage, soft- ware, 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 minimising 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.

Penneo document key: A0EXE-2J80B-PAMJ1-OFKYO-JB4I6-WCFA7

Instructions regarding processing of personal data

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.

Technical 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 to 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 organisational 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 being 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 is secured by a 2048-bit encryption certificate issued to Master International A/S by a trusted certificate authority. 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 ensures that the application code is not altered with unapproved changes after release.

The platform utilised multiple database technologies. All of them implement 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.

Penneo document key: A0EXE-2J80B-PAMJ1-OFKYO-JB4I6-WCFA7

Organisational measures

The Master Trusted Employee Policy ensures that all employees at all times work actively to protect personal data and information about test takers, customers, and partners, stored by users on the Master People Platform. It also covers personal information available in other formats or on other media, when the data or exposure to the data is related to Master International operating and supporting the Master People Platform.

Employees are authorised to perform work related tasks and required maintenance operations according to their individual role(s). The register of roles assigned to employees is called "Risk Register and User Access List". The employee is responsible for at all times to be aware of the roles that they can act in, and for escalating any doubts or uncertainties regarding roles and/or policies to the immediate manager.

Data Protection Officer (DPO)

Master International A/S does not have an internal DPO, as the nature of data processing is not sensitive and no systematic monitoring is involved.

Return and deletion of personal data

On termination of the provision of personal data processing services, Master International A/S will be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless Union or Member State law requires storage of the personal data.

The data processor commits to exclusively processing the personal data for the purposes and duration provided for by this law and under strict applicable conditions.

Storage of personal data

We are only storing data as agreed in the data processing agreement, and we are frequently verifying the location of servers and databases used by the system.

Use of sub processors

We ensure the following via frequent verifications:

- That we have data processing agreements with sub processors.
- That the requirements that we are subject to according to law or legislation, or by customers via contracts and data processing agreements, also are imposed on sub processors.
- That the data controllers are informed in case of changes / replacement of sub processors.

Transfer of personal data to third countries

We do not store personal/customer data outside the EU/EEA.

Rights of the data subjects

For all systems we have a procedure for how the data processor meets the data subject's rights. These may be obtained from our support, or our support can assist in solving the task.

Managing personal data breaches

We have a procedure for detecting and handling possible data breaches. Additionally, we have monitoring and alarms on critical systems. Data controllers are without undue delay informed about possible data breaches that may affect their data.

Penneo document key: A0EXE-2J80B-PAMJ1-OFKYO-JB4I6-WCFA7

Complementary user entity controls with the data controller

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 controller's responsibility to ensure that the test taker (data subject) has given their consent to the processing of their personal data.
- It is the data controller's responsibility to ensure that they only perform legal processing of personal data.
- Franchise partners (data processors) are responsible for ensuring a data processing agreement with the data controller.
- It is the data controller's responsibility to ensure that the test taker (data subject) is informed about relevant processing of personal data and the subject's rights.
- It is the data controller's responsibility to ensure a process for responding to queries from the data subject in a timely manner.
- It is the data controller's responsibility to delete or rectify personal data.
- 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.
- The data controller is responsible for providing the data subject with an extract file of personal data on request.
- It is the data controller's responsibility to ensure that only authorised employees at the data controller have access to personal data.
- It is the data controller's responsibility to observe and examine the user's activities in relevant audit logs.

Penneo document key: A0EXE-2J80B-PAMJ1-OFKYO-JB4I6-WCFA7

PENNEO

The signatures in this document are legally binding. The document is signed using Penneo™ secure digital signature. The identity of the signers has been recorded, and are listed below.

"By my signature I confirm all dates and content in this document."

Jesper Broberg Nielsen

Underskriver 1
Serial number: e327c0e2-38a5-4b7d-83c6-90567777e450
IP: 152.115.xxx.xxx
2026-03-16 14:05:31 UTC

Mit ID

Andreas Moos

Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 2
Serial number: 8ba4bf1c-2aac-4cbe-9a4b-48056ec67035
IP: 77.241.xxx.xxx
2026-03-16 14:41:14 UTC

Mit ID

Anders Holmgaard Christiansen

Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 3
Serial number: 8bbbd46c-7c17-4a94-90cc-be53fedff2e6
IP: 62.243.xxx.xxx
2026-03-16 19:23:36 UTC

Mit ID

Penneo document key: A0EXE-2J80B-PAMJ1-OFKYO-JB4I6-WCFA7

This document is digitally signed using **Penneo.com**. The signed data are validated by the computed hash value of the original document. All cryptographic evidence is embedded within this PDF for future validation.

The document is sealed with a Qualified Electronic Seal. For more information about Penneo's Qualified Trust Services, visit **https://eutl.penneo.com**.

How to verify the integrity of this document
When you open the document in Adobe Reader, you should see that the document is certified by **Penneo A/S**. This proves that the contents of the document have not been modified since the time of signing. Evidence of the individual signers' digital signatures is attached to the document.

You can verify the cryptographic evidence using the Penneo validator, **https://penneo.com/validator**, or other signature validation tools.