



Master International A/S

Independent auditor's ISAE 3000 report on the design and implementation of selected controls applicable to the EU General Data Protection Regulation as per 6 February 2018

EXCERPT

ISAE 3000 REPORT GDPR COMPLIANCE – EXCERPT

- Section 1 - Signed assertion by Master International
- Section 2 - Signed independent auditor's report by Deloitte

For security reasons, this excerpt does not include the detailed technical description of the system and security setup, or the details of the individual controls performed by the auditor. The full audit report is available for data controllers and data processors using the platform and services provided by Master International, after signing a non-disclosure agreement.

1. Assertion by Master International A/S

Master International deliver systems that processes personal data for our customers who are data controllers under 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, and repealing Directive 95/46/EC (General Data Protection Regulation) ".

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. Master International confirms that:

a) The accompanying description in section 3 fairly presents the Metis platform (the system) for processing personal data for data controllers covered by the General Data Protection Regulation as of 6 February 2018. The criteria used in making this statement were that the accompanying description:

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

- The types of services provided, including the type of personal data processed;
- The processes in both IT and manual systems that are used for initiating, registering, processing and, if necessary, correcting, deleting and restricting the processing of personal data;
- The processes used to ensure that the data processing was carried out under contract, instruction or agreement with the data controller;
- The processes which ensure that the persons authorised to process personal data have committed themselves to confidentiality or are subject to appropriate statutory confidentiality;
- The processes which, on termination of data processing, ensure that, after the data controller's choice, deletion or retrieval of all personal data is transferred to the data controller, unless law or regulation prescribes the retention of personal data;
- The processes which, in the event of a personal data breach, support the data controller in reporting to the supervisory authority and notifying the data subjects of the breach;
- The processes which ensure appropriate technical and organisational security measures for the processing of personal data, taking into account the risks involved in processing, in particular by accidental or illegal destruction, loss, alteration, unauthorised disclosure or access to personal data transmitted, stored or otherwise processed;
- Controls which we, referring to the Metis platform, assumed would be designed and implemented by the data controller and, if necessary to achieve the control objectives set forth in the description, which are identified in the description;
- Other aspects of our control environment, risk assessment process, information system (including associated business processes) and communication, control activities and monitoring controls that have been relevant to the processing of personal data;

- (ii) Contains relevant information about changes in the data processor's Metis platform for processing personal data made as per 6 February 2018;
- (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 individual data controller had to consider important according to their particular circumstances;
- b) The controls associated with the control objectives listed in the accompanying description were appropriately designed and operating effectively as per 6 February 2018. 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 used consistently as designed and that manual controls were performed by persons with appropriate competence and skills as per 6 February 2018;
- c) Appropriate technical and organisational measures have been established and maintained to fulfil the agreements with the data controller, good data processing practice and relevant data processing requirements under the General Data Protection Regulation.

Norbert Mörtl

CEO

26 April 2018

Bregnerødvej 144C, 3460 Birkerød



Jesper Starch

CTO

26 April 2018

Bregnerødvej 144C, 3460 Birkerød



2. Independent auditor's report

Independent auditor's ISAE 3000 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 have been engaged to report on Master International A/S's systems description of the Metis platform in section 3 and the related control objectives and control descriptions in section 4 regarding the processing of personal data on behalf of data controllers covered by 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, and repealing Directive 95/46/EC (General Data Protection Regulation)" as of 6 February 2018, and on the design and the implementation of controls associated with the control objectives specified 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 sub-processor. This report does not cover customers with specific process and security requirements.

Master's responsibility

Master is responsible for the preparation of the description and the accompanying statement as provided in section 3 and the related control objectives and control descriptions in section 4, including the completeness, accuracy and method of presentation of the description and the assertion; providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Our independence and quality assurance

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

Deloitte applies the International Standard on Quality Control (ISQC) 1 and, accordingly, maintains a comprehensive quality control system, including documented policies and procedures for ensuring compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Our responsibility

Our responsibility is to express an opinion on Masters' description and on the suitability of the design and implementation of the controls described therein to meet the selected control objectives, based on our procedures.

Our engagement was conducted in accordance with International Standard on Assurance Engagements (ISAE) 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by The International Auditing and Assurance Standards Board (IAASB) and, accordingly, included procedures that we considered necessary in the circumstances. Those Standards require that we plan and perform our audit to obtain reasonable assurance about whether, in all material respects,

1. The description is fairly presented, based on the description criteria;
2. The controls were appropriately designed and implemented to meet the selected control objective criteria as of 6 February, 2018.

An assurance engagement to report on the description and design of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its system, and the design of controls. The procedures selected depend on the service auditor's judgement, including the assessment that the description is not fairly presented, and that controls are not appropriately designed. An assurance engagement of this type also includes evaluating the overall presentation of the description, the appropriateness of the control objectives stated therein, and the suitability of the criteria specified by the service organisation and described on pages 3-4.

As noted above, we did not perform any procedures regarding the operating effectiveness of the controls included in the description and, accordingly, do not express an opinion thereon.

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

Inherent Limitations

Master International's description has been prepared to meet the general needs of a wide range of data controllers and may therefore not include every aspect of the Metis platform that the data controllers may consider important to its own particular needs. Because of their nature and inherent limitations, controls at a service organisation may not always operate effectively to meet the selected control objectives. Further, the projection to future periods of any evaluation of the fairness of the presentation of the description or conclusions on the suitability of the design or implementation of the controls to meet the selected control objectives is subject to the risk that the system may change or that the controls at a service organisation may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the description criteria identified in Master International's statement and the selected control objectives:

- (a) The description fairly presents the controls as they were designed and implemented as per 6 February 2018, and
- (b) The controls stated in the description were appropriately designed to provide reasonable assurance that the selected control objectives would be met if the controls were designed and implemented as of 6 February 2018.

Description of the testing of controls

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

Restricted Use

This report and the description of tests of controls in section 4 are intended solely for the information of and use by Master International and the data controllers and data processors who are using the described services as well as their auditors as of 6 February, who have a sufficient understanding of the following:

- The nature of the service provided by Master International;
- Internal control and its limitations;
- The risks that may threaten the fulfilment of the selected control objectives and how controls address those risks.

This report is not intended for and should not be used by anyone other than the parties specified above.


Copenhagen, 26 April 2018

Deloitte

Statsautoriseret Revisionspartnerselskab
Business Registration No 33 96 35 56



Thomas Kühn
State-Authorised Public Accountant



Jesper Due Sørensen
Partner

EXCERPT