ISAE 3000 ASSURANCE REPORT AT 15 DECEMBER 2018 ON TECHNICAL AND ORGANISATIONAL MEASURES AND THEIR DESIGN RELATING TO PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION AND THE DANISH ACT ON SUPPLEMENTARY PROVISIONS

Saville Consulting Danmark A/S

CONTENT

AUDITOR'S REPORT

INDEPENDENT AUDITOR'S ISAE 3000 REPORT AT 15 DECEMBER 2018 ON TECHNICAL AND ORGANISATIONAL MEASURES AND THEIR DESIGN RELATING TO PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION AND THE DANISH ACT ON SUPPLEMENTARY PROVISIONS

To: The Management of Saville Consulting Danmark A/S

Scope

We have examined the accompanying Statement by Saville Consulting Danmark A/S (the Processor) describing that technical and organisational measures (controls) were suitably designed and implemented at 15 December 2018 to provide reasonable assurance that the Processor fulfils the agreements with the clients (the Controller), good practices for the processing of data, and relevant requirements in relation to processors in accordance with the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the EU General Data Protection Regulation) and the Danish Act on Supplementary Provisions.

The Processor's Responsibilities

The Processor is responsible for providing processing of personally identifiable data and designing and implementing technical and organisational measures (controls) to provide reasonable assurance that the requirements of the EU General Data Protection Regelation and the Danish Act on Supplementary Provisions were achieved. When preparing the Statement, the Processor is responsible for completeness, accuracy, and method of presenting the Statement as well as stating control objectives and designing and implementing 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 FSR - "Code of Ethics for Danish Professional Accountants" which is based on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional conduct.

We are subject to the international standard on quality control, ISQC 1, and apply and maintain a comprehensive system for quality control, including documented policies and procedures for complying with rules of ethics, professional standards and applicable requirements according to legislation and other regulation.

Auditor's Responsibilities

Our responsibility is to express an opinion on the Processor's Statement.

We conducted our engagement in accordance with ISAE 3000, Assurance Reports Other Than Audits or Reviews of Historical Financial Information. That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the Processor's Statement is fairly presented.

An assurance engagement to report on the Processor's Statement involves obtaining an understanding of the Processor's processing of personally identifiable data and related technical and organisational measures (controls), testing and evaluating the design and implementation of controls, and performing such other procedures as we considered necessary in the circumstances. The procedures selected depend on the auditor's judgment, including the assessment of the risks that controls are not suitably designed and implemented.

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

Limitations of Controls at a Processor

Because of their nature, controls at a Processor may not prevent or detect all breaches of the personal data security.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report.

In our opinion, in all material respects, the Processor's Statement that technical and organisational measures (controls) were suitably designed and implemented at 15 December 2018 to provide reasonable assurance that the Processor fulfils the agreements with the Controllers, good practices for the processing of data, and relevant requirements in relation to processors in accordance with the EU General Data Protection Regulation and the Danish Act on Supplementary Provisions, is fairly stated.

Intended Users and Purpose

This report is intended for the Controllers, who need assurance about the Processor's technical and organisational measures (controls) related to the EU General Data Protection Regulation and the Danish Act on Supplementary Provisions. This report is not to be used for other purposes.

Copenhagen, 21 December 2018

BDO Statsautoriseret revisionsaktieselskab

Per Sloth
Partner, Head of Risk Assurance
Registered Public Accountant

STATEMENT BY SAVILLE CONSULTING DANMARK A/S

Saville Consulting Danmark A/S (hereafter SCDK) is responsible for processing of personal data of our clients, who are Controllers according to the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the EU General Data Protection Regulation) and Danish Act on Supplementary Provisions.

SCDK is a value-added reseller for Towers Watson Software Ltd certifying people in online assessment tools in the form of psychometric assessments and related reports aimed at the business sector for the purpose of recruitment, development and selection of employees.

SCDK has suitably designed and implemented technical and organisational measures (controls) at 15 December 2018 to provide reasonable assurance that SCDK fulfils the agreements with the Controllers, good practices for the processing of data, and relevant requirements in relation to processors in accordance with the EU General Data Processing Regulation and the Danish Act on Supplementary Provisions.

The description at pages 5 to 8 identifies SCDK’s handling of personally identifiable data for Controllers subject to the EU General Data Protection Regulation and the related technical and organisational measures (controls) at 15 December 2018 covered by this Statement.

Nærum, 21 December 2018

Saville Consulting Danmark A/S

Birte Møller

Birte Møller, Partner

SAVILLE CONSULTING DANMARK A/S' DESCRIPTION

About Saville Consulting Danmark

SCDK sells online assessment tools developed by Saville Assessment Ltd., a subsidiary of Towers Watson Software Ltd., company number 3318544, residing in England (Saville Assessment Ltd. and Towers Watson Software Ltd. is collectively called "TWSA"). TWSA owns all intellectual property rights of the assessment tools and test administration platform Oasys, including IT security responsibility related to this.

Personal data is processed by SCDK in connection with clients' participation on test certification training courses, clients' use of Bureau Service (SCDK handles all test administration on behalf of the client) and in connection with consultancy services.

Personal Data - Personal Information Processed by SCDK

Personal information is included in the following:

Test Administration Platform, Oasys: SCDK is data processor for clients regarding Bureau Service and test certification training course participation. We ensure that candidate data is anonymized at the beginning of each month. The data storage period specified and agreed with TWSA for SCDK's Oasys platform is 6 months. However, as anonymization is done at the beginning of each month candidate data can be in the system up to a maximum of 7 months. For the sake of "Disaster Recovery" (DR), backup databases are maintained for 35 days.

Hard Copy Reports and Notes: If assessment reports or other personal data are stored as part of any consultancy service, for example in development settings, data is kept as long as necessary for SCDK to be able to deliver the agreed services to the client.

Client Portal: Portal hosted by UnoEuro containing SCDK's training course materials, sample reports, articles, etc. to which test certified users are granted access. Test certified users are created with registration number, name, email address, and information about assessment tools in which they are certified. Furthermore, test certified users can download their test certificates from the Client Portal. All users of the Client Portal receive unique registration number and self-chosen password. If a test certificated user wants to be deleted from the Client Portal, this can be done by sending an e-mail to SCDK, where after it will be done within 2 business days.

Client Databases: An excel file containing the following data about test certified users: Names, email addresses, company in which they are employed, dates for test training course participation, and registration number at SCDK. In addition, an excel file is stored containing: Overview of primary contacts and clients' super users of Oasys test administration platform (super users are designated by the client company as experts in the use of Oasys).

Risk Assessment

SCDK takes initiatives that reflect the risks associated with SCDKs processing of personal data so that the security measures are appropriate, and the risk of security breaches is reduced to an appropriate level.

SCDK makes an ongoing assessment of the level of safety that is appropriate. The assessment takes into account the risks posed by the treatment, in particular by accidental or illegal destruction, loss, alteration, unauthorised disclosure or access to personal data transmitted, stored or otherwise processed.

As a basis for updating the technical and organisational measures, an overall risk assessment is carried out annually. The assessment should highlight the likelihood and consequences of incidents that may threaten the protection of personal data, including random, intentional and unintentional incidents.

Data Protection Agreements

Data Processing Agreements are made for all client companies. The Data Processing Agreement contains a description of the basis for processing personal data.

Data Processing Agreements have been gathered from sub-data processors. For each data processing agreement, control has been carried out based on an assessment of the risks associated with each individual sub-data processor.

Employees' Confidentiality

All employee contracts contain information regarding confidentiality.

Technical and Organisational Security Measures

Physical security

Willis Towers Watson in Nærum has alarm system and access control installed. Entrances are locked, and access cards must be used, including code to enter. The reception can, however, be entered during the manning period. All sections of the building are closed 24/7 and access cards must be used to move around the building. The property is patrolled every night to make sure everything is closed, and alarm connected. The building has an automatic fire system.

External devices

External devices (such as USB and CD-Rom) not owned by SCDK must not be connected to SCDK's PCs. USB owned by SCDK is not used for storing documents with personal data.

Access Security

All employees' PCs are password protected, and all SCDK's systems/accounts that can be accessed via Internet make use of two factors authentication. Login and password procedures are managed through LastPass with a Security Score at minimum 95%.

If an employee leaves their PC, the employee ensures that the computer is being locked or turned off. Password is then needed to reopen it. For this, the PC's sleep function is used.

Virus Attacks

All PCs are equipped with virus scanner and anti-theft protection. If an employee suspects a PC to be infected with virus, they immediately stop using the PC and contacts IT assistance immediately (ESET DK Anti-Virus and Internet Security Solutions). The employee does not attempt to remove viruses themselves.

Communication

SCDK has its own network at Willis Towers Watson with password not available to anyone other than SCDK's employees.

SCDK makes use of Microsoft Office365 and communicates internally as well as internally through this. This communication is encrypted.

Mails sent through Office365 are encrypted through TLS 1.2, and thus is in compliance with the Danish Data Protection Authorities' requirements.

Storage and Backup of Data, including Emergency Plans

As regards SCDK's website, www.savilleconsulting.dk, data is stored in data centers in Europe. Backup is taken daily and saved for 21 days. Data may be recovered by contacting DanDomain Customer Service.

For Office 365, data is stored in Europe. If a document is to be recreated, this can be done via www.office.com by SCDK's own employees or through support from DanDomain.

In addition, backup is taken of SCDK's share drive on an external hard drive, which is stored for 30 days and kept in a locked cabinet.

No personal data (such as assessment reports) is stored directly on the employees' local drive or the PC's desktop. Everything is in the cloud. If an employee prepares a test feedback/interview, notes and candidate report are stored in locked cabinets until test feedback/interview takes place. After completion of test feedback interview, all personal data is shredded.

Remote Workplaces

When working from home, the same employer-paid laptop is used as in the workplace. All employees use secure network connection when working from home with access to SCDKs SharePoint in the cloud.

Hence, when working from home, the same guidelines apply for protection of personal data that apply to SCDK's company address. Since all electronic data is in the cloud, it is the same work process, regardless of where the work is done.

All employees have access to locked drawers and/or cabinets at home, if printed documents containing personal data are to be stored.

Repair and Disposal of PCs, Mobile Phones and Other IT Equipment

As stated, data is solely on SCDK's secure server located in the cloud and encrypted. In case of repair, no data is stored directly on the employees' PC or mobile phones. In case of disposal of PCs and mobile phones, these are destroyed.

Education and Awareness

All employees are thoroughly trained in this security policy and handling of data streams.

Erasure of Personal Information

Hard copy documents with personal data

Personal data gathered in connection with delivery of consultancy services listed in hard copy documents are stored in locked cabinets. This information is shredded within 6 months after consultancy service has been delivered, unless longer storage is required for SCDK to deliver the agreed services to the client who has given consent.

Assessment reports used on test certification training courses are shredded immediately after training course and stored in locked cabinets in the intermediate period.

Emails

Received emails with candidate data regarding Bureau Service are stored in a folder in the cloud and no later than the 15th of each month, data older than 6 months is permanently deleted.

Received emails with candidate data regarding other Support are stored in the cloud and no later than the 15th of each month, data older than 6 months is permanently deleted.

Received emails with data regarding personality test training course follow-up are stored in the cloud and no later than the 15th of every month, data older than 6 months is permanently deleted.

Sent mails with candidate data regarding Bureau Service are stored in the cloud and no later than the 15th of each month, mails older than 6 months are permanently deleted.

Assessment reports

Downloaded reports from Oasys are not stored. Assessment reports sent from clients prior to participation on test certification training courses are stored in folder in the cloud. Only reports generated on real assessment candidates will be stored as long as necessary to deliver the agreed services to clients.

If individuals (candidates and clients) report that personal data is to be anonymised, this will take place within one month. In addition, it is ensured that request for anonymisation also is forwarded to any relevant sub-data processor. It is ensured that the withdrawal of personal data and the description of how personal data will be processed, is being updated and approved annually in January. Responding to requests from registered (candidates and clients) are handled in a timely manner, and it is ensured that sub-data processors also have handled this in a timely manner.

Handling Security Breaches

In case of breach of data security regarding SCDK's processing of personal data, SCDK will without unnecessary delay inform clients after being aware of this and in accordance with signed data processing agreements. The notification will include a description of:

- The nature of the breach of personal data security
- The likely consequences of the breach of personal data security
- The measures taken or proposed by SCDK to deal with the breach of personal data protection, including and where appropriate, measures to limit its possible harmful effects

Complementing Controls at the Clients

Controls at SCDK are designed to supplement the client’s (data controller) own controls to ensure compliance with the EU General Data Protection Regulation (GDPR) and the Danish Data Protection Act.

According to the data protection legislation, the data controller is as a minimum to implement the following procedures, instructions and controls in relation to SCDK’s handling of personally identifiable data:

1. General instruction to all users on processing and destruction of personal data and use of Oasys.
2. Procedure for administration of users in Oasys, including creation, change and deletion of users and granting of user rights in accordance with the roles created in Oasys.
3. Control of granted user rights.
4. Instruction for change of access codes (password) of users created in Oasys.

BDO Statsautoriseret revisionsaktieselskab

Havneholmen 29
DK-1561 Copenhagen V
CVR no. 20 22 26 70