PwC's processing of personal data in its role as a Personal Data Processor – Personal Data Processor Agreement, comprising an integrated part of the Engagement Letter

1. The Client's commitments
The client comprises the Personal Data Controller for the processing of personal data PwC executes within the framework of the assignment and is, therefore, responsible for ensuring that such processing takes place according to applicable legislation. This implies that the Client is responsible for ensuring that it has the right to transfer the data in question to PwC and to allow PwC to process the data within the framework of the assignment.

The Engagement Letter and Attachment 1 and Attachment 2 include a more detailed description of the processing PwC is expected to execute and the terms and conditions for such processing. This description comprises the Client's instructions to PwC.

For those cases in which the Client wishes to change or present new instructions implying a significant change in relation to the previous instructions, where the Client takes measures beyond the normal limitations implied by the data protection legislation in effect, or where the Client breaches the applicable law and professional standards to which PwC is to comply, then, PwC incurs the right to terminate the Engagement including this Personal Data Processor Agreement with immediate effect. The Client shall claim no damage in such a situation. PwC's commits to inform the Client in the case instructions are in conflict with applicable data protection legislation.

2. PwC's general commitments
Within the framework of the assignment, PwC shall process personal data to the degree and in the manner stated in the Client's instructions, that is, in accordance with what is stated in the Engagement Letter and sub-appendixes to this Personal Data Processor Agreement and Engagement Letter.

3. Security measures
PwC will undertake the applicable technical and organizational measures to ensure a security level which is appropriate in relation to the risks involved and in order to protect the personal data we process from personal data breaches. Only those personnel in PwC requiring access to the personal data in order to execute the assignment will have access to the data. These individuals are, in addition, subject to an obligation of confidentiality which is no less in scope that the obligation stipulated in the Engagement Letter. A more detailed description of PwC's security measures can be found in Attachment 3.

In the case of a personal data breach, PwC, as soon as it has become aware of such incident, will, and without undue delay, inform the Client in writing of such breach. PwC will, in this context, and as soon as possible, provide the Client with a description of the nature and category of the incident and of the number of registered individuals affected, as well as providing information regarding the categories and number of personal data items impacted, the probable consequences of the personal data breach and a description of the measures which we, as applicable, have already undertaken or intend to undertake in order to address the personal data breach and/or in order to limit its possible negative effects.

4. Contracting of a sub-processor
As stipulated in the Engagement Letter and/or the attached General Terms & Conditions, PwC has the right to contract sub-suppliers, sub-consultants and other third parties (”Sub-processors”) in order to process personal data on behalf of the Client. PwC has entered into

Personal Data Processor Agreements with these Sub-processors. The Sub-processors meet the requirements of the applicable data protection legislation. PwC is fully responsible vis á vis the Client for the obligations of the Sub-processors.

5. Transfer of personal data to a third country
PwC has the right to transfer personal data belonging to the Client to a third country (a country which is not a member of EU or is not a member of EEA), on the premise that (i) the third country, in accordance with a decision announced by the EU Commission, is regarded as a country that ensures an adequate level of protection for personal data, (ii) PwC ensures that there are appropriate safeguards in place according to the applicable personal data legislation, for example, standardized data protection measures adopted by the EU Commission, which address the transfer and processing of personal data; or (iii) any other exception according to the applicable personal data legislation in place, addressing the processing of personal data.

6. The rights of the registered individual
The Client is responsible for assessing whether a registered individual's request to execute its rights is legitimate in relation to the laws in effect and for providing instructions to PwC as regards the support the Client wishes to receive to meet the request of the registered individual. PwC is prepared to provide the information required by the Client in conjunction with a request from a registered individual on the premise that PwC has access to such information. PwC is, furthermore, prepared, in conjunction with a request for rectification, erasure, limitation on processing and data portability, assist the Client in a helpful manner, and to the degree possible, in undertaking such measures.

PwC shall, without undue delay, inform the Client of complaints and present other information which PwC receives from a registered individual. The Client is, subsequently, responsible for the handling of the case and is the entity providing information to or being responsible for undertaking measures in relation to the registered individual.

7. The Client's right to information in terms of impact assessments and advance consultations
At the request of the Client, PwC shall assist the Client with the necessary information to which PwC has access in order for the Client to fulfill its obligations to execute an impact assessment and an advance consultation with the authorities involved as regards the processing of personal data as addressed in the Personal Data Processor Agreement.

8. Return of personal data
The Client has the right, with termination of the Engagement Letter, to request the erasure or return of the personal data PwC processes in its role as a Personal Data Processor. Note, however, that the personal data in PwC's working papers will be stored, both in order that the supervisory authorities can review executed assignments within the framework of quality controls and in response to potential reports to the supervisory authorities, and also in order for PwC to determine, enforce or defend itself from legal claims. The personal data will be erased after eleven (11) years. As regards such measures, PwC comprises, alone, the Personal Data Controller.

9. Responsibilities
The terms stipulating responsibilities in the Engagement Letter are to equally apply to this Personal Data Processor Agreement.

10. Review
The Client has the right to perform an inspection of the technical and organizational measures undertaken by PwC in order to fulfill its obligations according to the personal data legislation in effect. For the avoidance of doubt, such an inspection shall only address such information necessary for the Client to determine if PwC has taken the appropriate

technical and organizational measures to fulfill PwC's obligations according to this commitment and the inspection should, under no circumstances, include other information regarding PwC's operations which is not significant to PwC's processing of the personal data on behalf of the Client. The inspection is to be performed by a third party jointly appointed by both parties. The third party shall sign a confidentiality agreement covering all information to which it receives access within the scope of the inspection. In the case the Client wishes to utilize its right to an inspection, the Client shall inform PwC in writing at least thirty (30) days in advance. The Client assumes the costs for the work of the third party and for out-of-pocket expenses. In general, the parties assume their respective costs arising in conjunction with an inspection.

Attachment 1

DESCRIPTION OF PROCESSING OF PERSONAL DATA WITHIN THE FRAMEWORK OF THE ASSIGNMENT

Categories of Registered Individuals	Categories of Personal Data	Purpose of the Processing	Processing of Personal Data	Location	Preservation of Personal Data
Employees	Employment and salary details. Name, personal identity number, address, salary, compensation, bonuses, bank account, position.	In order to perform a statutory/contractual audit in accordance with the Engagement Letter and generally accepted auditing practice. Personal data will be used to the degree such data is relevant in validating and analyzing financial transactions and financial positons, as well as to assess the Board of Directors' and management's administration of the company.	Information, including personal data is compiled from files received from the Client. For this purpose, the systems Connect or MFT2GO are used. As an alternative, a storage medium is agreed upon together with the Client. Transactions are validated in the systems, Halo and/or ACL. Microsoft Excel is used for certain calculations. Temporary storage takes place on PwC's servers with TeleComputing and in shared work spaces in Google Drive. The final result is documented in PwC's auditing system, Aura, which is maintained and operated by PwC Germany.	Personal	Personal data in PwC's working papers will be stored during a period of eleven (11) years, partly in order that the supervisory authorities can examine executed assignments after the completion of the assignment and on the basis of quality controls, and after any possible claims, and partly in order that PwC can determine, enforce or defined itself against legal claims. Personal data in other documentation will, in accordance with the Client's instructions, be erased or returned at the end of the assignment.
Suppliers/Consultants	Details related to the sale and delivery of goods and services to the company: Name, personal identity number, address, bank account, quality assessment.	See above.	See above.	See above.	See above.
Clients	Details referring to the purchase of goods and services from the company: Name, personal identity number, address, credit status, bank accounts, purchase history.	See above.	See above.	See above.	See above.

Attachment 2

LIST OF SUB- PROCESSORS

Sub-Processor	Duties of the Sub-Processor	Location
Telecomputing Sweden AB	Provider of IT operations	Kista, Sweden
PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, Germany	DEvelopment, operations and maintenance of auditing system, Aura	Frankfurt am Main, Germany
Google Inc, Mountain View, California, USA	Provision of e-mail and calendar services and work tools	EU/EES and third countries https://www.google.com/about/datacenters/inside/locations/index.html

Attachment 3

Technical and Organizational Security Measures

1. Information Security Policy

PwC Sweden (referred to herein as ”PwC”) complies with the PwC network’s global policy for information security - ”PwC Information Security Policy” – which is supplemented with approximately 250 detailed controls. These regulations are based on ISO/IEC 27002:2013. A global group within the PwC network - PwC Network Information Security (NIS) – is responsible for the framework and executes annual compliance controls in the national PwC firms.

The global framework is supplemented locally with the policy documents, “Information Security Policy for PwC Sweden” and “Daily Information Security”.

2. Organization of Information Security

PwC has a ”Chief Information Security Officer (CISO)” who is responsible for information security within the firm and who regularly reports to the Chief Operating Officer (COO) and to the Risk Management Partner within PwC. In addition, there are ongoing reconciliations with the firm’s internal legal function,”Office of General Counsel (OGC)”. The role of Personal Data Representative is executed by the General Counsel.

3. Personnel Security

To the degree allowed by Swedish legislation, background controls are made of all personnel prior to their employment. This also applies to personnel provided by a third party.

All new personnel are informed of their responsibility for security and confirm in writing that they commit to comply with all applicable guidelines and routines, as well as with PwC’s requirements of confidentiality.

At least once a year, all employees and consultants complete a program for security awareness and security training.

For sub-suppliers, the document ”PwC’s third party suppliers - Guidelines for information security” is an integrated part of the agreement.

4. Physical and Environmental Security

Server locations are properly protected from unallowed entry, theft, fire, water damage, electricity disruption and other hazards. Physical access to server locations is limited to a minimum of personnel.

Physical access to office premises is limited to PwC personnel. Visitors are welcomed in an external area. Personnel, as well as visitors, carry ID badges.

PwC has a Clean Desk Policy.

Secured storage is available for handling and destruction of sensitive paper documentation.

5. Operations and Communications security

PwC has appropriate segregation between its development, testing and production environments.

Proper firewalls and IDS (Intrusion Detection Systems) are in place, as well as procedures for log follow-up.

All personal computers are equipped with hard disk encryption according to the most recent standards, password protected screen savers, personal firewalls, anti-virus software and VPN. Adequate patching procedures are in place.

Only PwC equipment can access the PwC network.

Solutions for the secure sharing of information with Clients are available. PwC prohibits the use of services such as Dropbox, Box, Drive, etc.

PwC has procedures for the secure erasure of data media. Erasure of client information is undertaken according to the agreements with Clients and on the basis of legal requirements

6. Access Controls

Access to information is based on the user's role and responsibilities. Authorization is provided according to the principle that only individuals needing access to the information in order to execute their work duties within the framework of an assignment are to to be provided with access. All user accounts refer to a single individual.

Decisions on access are taken by the information owners (for Client information this is the Client and/or the Engagement Leader). User accounts are subject to review by the information owner, at least once a year.

PwC has formal procedures for the addition, changing or removal of user accounts and in order to change logical access where work duties are changed. Inactive user accounts are blocked automatically. Furthermore, there is a procedure for the withdrawal of physical and logical access for personnel and consultants terminating their work with PwC.

The number of user accounts with high authorization, such as system administrators, and the equivalent, have been reduced to a minimum. Personnel with access to such user accounts use separate accounts when executing their regular work.

Systems support is enabled for mandatory changes of passwords, the requirement of password structure and with lock out after unsuccessful access attempts.

7. Incident Management

PwC has a formal incident management process. The process defines responsibilities and how reporting, classification and escalation is to take place. Should an incident occur in which laws, regulations or contractual obligations are breached, there are risk and/or damage reducing procedures for investigation and, as applicable, for reporting to Clients and supervisory authorities.

PwC's mandatory training within security includes training in the manner in which a breach of security or incident (including personal data incident) is to be identified and who is, in such a case, to be contacted.

8. Business Continuity

PwC has a continuity plan for its operations. The plan is communicated to all involved personnel and is updated annually. In addition, there are disaster recovery plans for PwC's IT environment. These plans are updated annually.

9. Compliance

The control of compliance with the above descripted framework, including ongoing follow-ups, is executed by NIS. Compliance audits are also initiated by PwC in Sweden, for example, self-assessments, audits executed by PwC's internal audit unit, technical security audits, security penetration tests, risk analyses of new solutions, etc. The reporting of information security issues takes place to NIS, Risk Management and the COO.