Data Processing Agreement

1 Purpose and scope

This DPA shall govern all the Personal Data Processing conducted by Quorum Software Norway A.S. (including affiliates) ("Quorum", “Supplier" or "Data Processor") on customer's (and the organization(s) customer represent, including affiliates) ("Customer" or "Data Controller") behalf as specified and agreed under applicable Processing Specification Form referring to this DPA.

The Customer and the Supplier may also be referred to as a "Party" or as the "Parties", as the case may be. Any reference to "Customer" or "Supplier" shall be construed as referring to any Party or Parties acting in such capacity from time to time.

1.1 Structure of the agreement

The Parties shall specify the Processing activities conducted under this DPA in accordance with a Processing Specification Form, which – in executed format – shall be an integral part of this DPA; provided, however, that in the event of conflict, the provisions of the Processing Specification Form shall prevail.

The DPA shall regulate the Processing of Personal Data by the Supplier on behalf of the Customer under agreement(s) to which a Processing Specification Form is referring and/or applicable to for the provision of Services as defined under the applicable agreement(s) ("Main Agreement"). This DPA shall form an integral part of the Main Agreement, meaning that applicable parts of the Main Agreement (including its provisions on governing law and dispute resolution) shall apply also to this DPA. In the event of conflict, the provisions of this DPA shall prevail.

In the absence of a signed Processing Specification Form or separate data processing agreement between the Customer and the Supplier, the Supplier shall nevertheless act in accordance with this DPA when processing Customer Personal Data, if so required by the Laws.

1.2 Appendices

The DPA includes these Appendices, which apply in the following order:

1 **Defined terms**

Where applicable, capitalized terms used under this DPA shall have the meaning ascribed to them in Appendix 1. Unless and to the extent the context otherwise requires, any use of the singular includes plural and vice versa.

2 **Technical and organisational security measures**

3 **Standard Contractual Clauses template**

4 **DaWinci Processing Specification Form**

5 **Energy Components Processing Specification Form**

2 Rights and obligations of the Parties

2.1 General

In connection with the Processing, the Customer shall be regarded as Data Controller and the Supplier shall be regarded as Data Processor.

Both Parties shall be responsible to ensure that the Processing is made in accordance with the Laws which apply to each Party as well as good data processing practices.

2.3 Rights and obligations of the Data Controller

The Data Controller shall

1. give the Data Processor documented and comprehensive instructions on the Processing, which instructions shall comply with the Laws;
2. have the right and obligation to specify the purpose and means of Processing of Personal Data;
3. represent that all the data subjects of the Personal Data have been provided with all appropriate notices and information and establish and maintain for the relevant term the necessary legal grounds for transferring the Personal Data to the Data Processor and allowing the Data Processor to perform the Processing contemplated hereunder;
4. represent that if the Data Controller represents its Affiliates or third parties under this DPA, it has the legal grounds to enter into this DPA with the Data Processor and allow the Data Processor to process the Personal Data according to the terms of this DPA and the Main Agreement; and
5. confirm that:
   - the Processing stipulated under this DPA meets the Data Controller's requirements including, but not limited to, with regard to intended security measures, and
   - it has provided the Data Processor with all necessary information in order for the Data Processor to perform the Processing in compliance with the Laws.

2.4 Rights and obligations of the Data Processor

The Data Processor shall

1. perform the Processing only on and as per the documented, legitimate and reasonable instructions from the Data Controller unless required to do otherwise by Laws, in which latter case the Data Processor shall inform the Data Controller of such deviating legal requirement (provided the Laws do not prohibit such notification). For the avoidance of doubt, the Data Controller shall at all times be deemed to have instructed the Data Processor to provide the Service as defined and agreed under the Main Agreement;
2. ensure that persons authorised to perform the Processing hereunder have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality as further stated under this DPA;
3. take all security measures required to be taken by data processors under the Laws as further stated under this DPA;
4. respect the conditions referred to under Laws for engaging any Sub-Processor as further stated under this DPA;
5. insofar as this is possible and taking into account the nature of the Processing, assist the Data Controller by appropriate technical and organisational measures for the

fulfilment of the Data Controller's obligation to respond to requests for exercising the data subject's rights laid down in under the Laws;

6. assist the Data Controller in ensuring compliance with its legal obligations, such as, data security, data breach notification, data protection assessment and prior consulting obligations, as required of the Data Processor by the Laws, taking into account the nature of Processing and the information available to the Data Processor;
7. maintain necessary records and make available to the Data Controller all information necessary to demonstrate compliance with the obligations of the Data Processor, as laid down in the Laws, and allow for and contribute to audits, including inspections, conducted by the Data Controller or any auditor mandated by the Data Controller as further agreed under this DPA; and
8. at the Data Controller's instructions, delete or return to the Data Controller all the Personal Data after the end of the provision of the Services relating to Processing, and delete existing copies unless applicable laws require storage of the Personal Data. Deletion and return methods may be further agreed between the Parties;

Unless otherwise agreed, the Data Processor shall have the right to invoice any costs resulting from the above assistance under 5-6 above in accordance with the Data Processor's prevailing price list.

3 Security of Processing

3.1 Security measures

The Data Processor shall implement and maintain appropriate technical and organisational measures to protect the Personal Data, taking into account:

1. the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, and
2. the risks that are presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Personal Data transmitted, stored or otherwise processed.

3.2 Details on security measures

The principles of the security measures taken for the applicable Processing by the Data Processor under this DPA are described in **Technical and organisational security measures** and may be further specified and amended in the relevant Processing Specification and/or the Main Agreement.

Such measures include, inter alia as appropriate:

1. the pseudonymisation and encryption of the Personal Data;
2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
3. the ability to restore the availability and access to the Personal Data in a timely manner in the event of a physical or technical incident; and
4. a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

3.3 Information about security measures

The Data Controller is responsible for ensuring that the Data Processor is informed of all issues (including but not limited to risk assessment and the inclusion of special categories of Personal Data) related to the Personal Data provided by the Data Controller which affect the technical and organizational measures employed under this DPA.

3.4 Changes to security measures

Changes in security measures shall be handled in accordance with change management process of the Main Agreement.

4 Sub-Processors

4.1 Use of Sub-Processors

The Data Processor may from time to time use Sub-Processors to process the Personal Data hereunder. Sub-Processor(s) used in the provision of Services are listed in the Processing Specification Form and/or the Main Agreement.

Such use will be under written contract and the Data Processor will require the Sub-Processor to comply with the data protection obligations applicable to the Data Processor under this DPA or obligations which provide for the same level of data protection.

The Data Processor will be liable for its Sub-Processor’s actions as for its own.

4.2 Consent

The Data Controller agrees that the Data Processor has a general consent to use the Data Processor’s Affiliates as Sub-Processors when Processing Personal Data. At the effective date of this DPA, the following Affiliates are engaged by the Data Processor:

Office	Location
Quorum Software Norway AS (Branch office Australia)	Australia
Octaserv IT Brasil Servicos Tecnologicos Ltda	Brazil
Octaserv IT Canada Inc	Canada
Octagon IT Czech s.r.o.	Czech
Quorum Software Norway AS (Branch office Finland)	Finland
Octaserv IT Malaysia Sdn Bhd	Malaysia
Octaserv IT Netherlands B.V.	Netherlands
Octagon IT UK Limited	United Kingdom
Aucerna	Affiliates listed https://aucerna.com/about-us/contact/
Quorum	Affiliates listed https://www.quorumsoftware.com/locations

4.3 Changes to Sub-Processors

The Data Processor will inform the Data Controller in advance on any intended changes concerning the addition or replacement of Sub-Processors.

If the Data Controller does not accept an intended change, the Data Controller may terminate such part of the Main Agreement which the sub-processing would be related to by way of thirty (30) days' prior written notice.

5 Transfer of Personal Data

5.1 Customer's consent to transfer data outside of Approved Jurisdictions

The Data Processor will only transfer Personal Data out of the territory of the member states of the European Union, the European Economic Area, or other countries which the European Commission has found to guarantee an adequate level of data protection (collectively, the "Approved Jurisdictions") with the Data Controller's prior written consent. For purpose of clarity, such consent must be clearly indicated in the Processing Specification Form or the Main Agreement.

5.2 Data protection during data transfer

Subject to Data Controller's consent under 5.1 above, the Data Processor shall enter into relevant contractual arrangements with required parties for the lawful transfer of Personal Data from the Approved Jurisdiction to third countries.

Such contractual arrangements shall be carried out in accordance with the standard data protection clauses adopted or approved by the European Commission attached herein ("Standard Contractual Clauses"). As an alternative to entering into the Standard Contractual Clauses, the Data Processor may rely upon an alternative transfer safeguard permitting and providing for the lawful transfer of Personal Data outside of the Approved Jurisdictions, provided that such safeguard is in compliance with applicable legislation.

Subject to Data Controller's consent under 5.1 above, the Data Controller authorizes the Data Processor to enter into and sign **Standard Contractual Clauses** in the name and on behalf of the Data Controller, unless otherwise agreed. The duly signed Standard Contractual Clauses document is available for Data Controller's review upon request.

5.3 Order of application

In case of conflict between the Standard Contractual Clauses or any other alternative transfer safeguard permitting the lawful transfer of Personal Data outside the Approved Jurisdictions and the DPA, the Standard Contractual Clauses or such alternative framework shall always take precedence over the Main Agreement and this DPA.

6 Notification of Personal Data Breach

6.1 Personal Data Breach notification process

The Data Processor shall without undue delay notify the Data Controller if it, or one of its Sub-Processors, becomes aware of a Personal Data Breach. Information shall be provided to the contact person named by the Data Controller, if not otherwise agreed between the Parties.

6.2 Personal Data Breach notification content

The Data Processor shall without undue delay inform the Data Controller of the circumstances giving rise to the Personal Data Breach, and any other related information reasonably requested by the Data Controller and available to the Data Processor.

Additionally, to the extent it is available, the Data Processor shall provide to the Data Controller the following information:

1. a description of the nature of the Personal Data Breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;
2. a description of the likely consequences of the personal data breach; and
3. a description of the measures taken or proposed to be taken by the Data Processor to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

The Parties may agree on a more detailed breach notification process in separate.

7 Auditing

7.1 General

The Data Controller shall be entitled to audit the Data Processor's performance of its Processing obligations under this DPA ("Audit").

7.2 How auditing is performed

The Data Controller is obligated to use external auditors who are not competitors of the Data Processor, to conduct such an Audit.

The Parties shall agree well in advance on the time and other details relating to the conduct of such Audits.

The Audit shall be conducted in such a manner that the Data Processor's undertakings towards third parties (including but not limited to the Data Processor's customers, partners and vendors) are in no way jeopardized. All the Data Controller's representatives or external auditors participating in the Audit shall execute customary confidentiality undertakings towards the Data Processor.

7.3 Authorities' right to audit

The Data Processor shall always allow any relevant regulatory authority supervising the Data Controller's business to conduct Audits of the Data Processor's operations, in which case relevant parts of the Parties' agreement hereunder shall apply.

7.4 Cost of auditing

The Data Controller shall bear all Audit expenses, and compensate the Data Processor for any and all costs incurred as a result of the Audit.

However, if the Audit reveals material deficiencies in the Data Processor's performance, the Data Processor shall bear its own costs for the Audit.

8 Confidentiality

8.1 Data Processor's undertakings

The Data Processor shall

1. keep any Personal Data received from the Data Controller confidential;
2. ensure that persons authorized to process the Personal Data have committed themselves to confidentiality; and
3. ensure that Personal Data is not disclosed to third parties without the Data Controller's prior written consent, unless the Data Processor is obliged by mandatory law or decree to disclose such information.

8.2 Disclosure

In case data subjects or governmental authorities make a request concerning Personal Data, the Data Processor shall, as soon as reasonably possible, inform the Data Controller about such requests before providing any response or taking other action concerning the Personal Data.

In case any applicable authority prescribes an immediate response to a disclosure request, the Data Processor shall inform the Data Controller as soon as reasonably possible, unless the Supplier is prohibited by mandatory law or authority order to disclose such information.

9 Limitation of liability

9.1 General

The limitations of liability set out under the Main Agreement shall apply also to this DPA.

9.2 Liability

The Parties agree that the general principle of division of responsibilities between the Parties relating to administrative fines imposed by any relevant supervisory authority or claims by data subjects under this DPA is based on the principle that the respective Party needs to fulfil its own obligations under the Laws. Hence, any administrative fines imposed or damages ordered should be paid by the Party that has failed in its performance of its legal obligations under the Laws, as decided by the relevant supervisory authority or competent court authorized to impose such fines or damages.

10 Term and Termination

10.1 General

This DPA shall enter into force at the last signature date of Processing Specification Form referring to this DPA. This DPA shall be in effect for the term of an applicable Processing Specification Form.

10.2 Surviving clauses

All provisions which by nature are intended to survive the termination of this DPA shall remain in full force and effect regardless of the termination of this DPA.

10.3 Changes and amendments

The Supplier has the right to change this DPA from time to time. However, the version of the DPA which was applicable at the time the relevant Processing Specification Form entered into force shall govern the Processing between the Parties until terminated as set out under this DPA and relevant Processing Specification Form. The Supplier will upkeep change history of the DPA. Customer is also encouraged to download this DPA when signing the Processing Specification Form.

Appendix 1: Defined terms

Affiliate: any legal entity which is directly or indirectly owned or controlled by a Party or directly or indirectly owning or controlling a Party or under the same direct or indirect ownership or control as a Party for so long as such ownership or control lasts. Ownership or control shall exist through direct or indirect ownership of more than fifty (50%) per cent of the nominal value of the issued equity share capital or of more than fifty (50%) per cent of the voting rights entitling to vote for the election of directors or persons performing similar functions or right by any other means to elect or appoint directors or persons who collectively can exercise such control.

Data Controller: the Customer, who determines the purposes and means of the Processing.

Data Processor: the Supplier, who processes Personal Data on behalf of the Data Controller.

Laws: EU Data Protection Regulation (2016/679) and the data protection laws under the governing law of the Main Agreement applicable to the Processing hereunder from time to time. The Parties acknowledge and agree that in the time period prior to the EU Data Protection Regulation (2016/679) becoming applicable (expected on 25 May 2018), interpretation of this DPA shall be based on applicable data protection laws under the governing law of the Main Agreement.

Personal Data: any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed hereunder.

Processing: any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, of Personal Data.

Processing Specification Form: the DPA appendix specifying processing activities under the DPA or other specifying appendix agreed between the Parties.

Services: any services provided under or in connection with the Main Agreement.

Sub-Processor: a processor contracted by the Data Processor to perform Processing hereunder, in part or in whole, on the Data Processor's behalf.

Appendix 2: Technical and organisational security measures

The purpose of this document is to describe the principles of the technical and organisational data security measures of Quorum Software Norway A.S. ("Quorum"), which Quorum provides for all Customers as a standard in Quorum's products and services as required by the Regulation (EU 2016/679), the General Data Protection Regulation ("GDPR").

Quorum implements appropriate technical and organisational data security measures which are designed to meet the data protection principles in an effective manner, and ensures that appropriate safeguards are integrated into the personal data processing in order to meet the requirements of the GDPR and to protect the rights of data subjects as described below.

Product level security descriptions are available upon request if not agreed to be part of the agreement governing the processing of personal data. Customer specific security measures are agreed separately.

1 Data protection risk assessment

Quorum executes and documents risk assessment for each Quorum product or service. Data protection and security risks are registered and monitored in the Quorum risk databases.

Quorum executes the data protection risk assessment in order to decide which data security measures shall be implemented. The aim is to define the appropriate level of data security measures for each product or service. In all cases, Quorum has implemented at least the security measures described in chapter 3 below.

2 Security measures

As a part of the Information Security Management System (ISMS) Quorum has public security and privacy policies, which are available for customers on request. The policies are supported with wide range of mandatory rules on different aspects of data protection and information security. Documents are subject to regular internal review process as well as an external third party verification on their appropriateness as well as the review process.

Quorum has certified its relevant operations utilizing the following international standards ISO 27001, ISO 9001 and ISO 14001.

With regard to physical and environmental controls in data processing facilities and security management, an external third party audit utilizing ISAE 3402 Type 2 standard is conducted annually. The annual report of the audit can be delivered to Quorum customer upon request. If agreed, Quorum can also provide a customer specific infrastructure ISAE 3402 Type 2 assurance report.

2.1 Security of personal data

Quorum is implementing the following measures based on requirements set out in "Security of processing" (article 32 of the GDPR):

(a) the pseudonymisation and encryption of personal data

Quorum is utilizing encryption and/or pseudonymization in its operations to mitigate data protection risks where appropriate. Encryption and pseudonymization techniques may vary between services upon the service requirements and data protection risk assessment. Details of the used measures are available upon request.

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services

Protection of the personal data requires implementation of multiple security controls. Standard operational processes follow good industry practice framework ITIL. Standardized processes help to secure quality of service and safeguards personal data processing.

Quorum has a centralized system to manage administrative access to customer environments. To access a customer system, the employee must have a valid reason and access is only approved by utilizing a jointly agreed process with the customer. At minimum all access to customer environments requires an encrypted tunnel within Quorum network. Connections to customer environments are logged to provide full audit trail on administrative operations in customer environments. All remote access to Quorum services requires an encrypted connection and other possible measures (e.g. strong authentication) as required by the data protection risk assessment.

Unauthorized persons are prevented from gaining physical access to data processing facilities. Personal data is protected against accidental and unlawful destruction utilizing physical and environmental controls. Physical and environmental security controls in data processing facilities are subject to an annual independent third party ISAE 3402 Type 2 audit.

Quorum controls, monitors and audits all administrative connections, 3rd party access and file transfers which are deployed within Quorum infrastructure.

Quorum executes a framework for planning, executing and controlling customer business related operations. The organisational structure assigns roles and responsibilities to provide for adequate staffing and efficiency of operative capabilities. Quorum management established authority and appropriate lines of reporting for key personnel. As a part of the hiring processes education verification and background checks are conducted based on employee's position and level of access to Quorum processing facilities and systems.

Quorum maintains and controls the execution of the Quorum security policy, provides security training to employees, and performs application security reviews. These reviews assess the confidentiality, integrity, and availability of data, as well as conformance to the Quorum information security policy.

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

To restore the availability and access to personal data in a timely manner in the event of a physical or technical incident Quorum has backup and business continuity management processes and strategies which ensure rapid restoration of business critical systems as and when necessary.

Quorum has defined continuity and disaster recovery plans for Quorum infrastructure supporting Quorum service delivery to Customers. These plans are regularly updated and tested and are subject to third party auditing. Customer specific continuity plans and procedures are agreed separately between Quorum and the Customer.

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

Quorum emergency processes, plans and systems are regularly tested to assess and evaluate the effectiveness of technical and organisational measures for ensuring the security of the personal data processing. Customer specific disaster recovery testing is agreed separately.

Quorum operations follow defined processes and are subject to internal and independent third party audits as a part of quality and security management certification (ISO 9001 and 27001). Quorum conducts internal security testing and vulnerability scanning. For high risk environments Quorum utilize third party security testing services including penetration testing.

Appendix 3: Standard Contractual Clauses template

Example of Standard Contractual Clauses (SCCs) – processor

Standard Contractual Clauses (SCCs) - processor

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

	Data exporting organization (the data exporter)	**Data importing organization (the data importer)**
Name		
Address		
Business ID		
Tel.		
Fax		
E-mail		
Other information needed to identify the organization		
	each a '**party**'; together '**the parties**'	

The parties have agreed on the following **Contractual Clauses (the Clauses)** in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1 - Definitions

For the purposes of the Clauses:

a) '**personal data**', '**special categories of data'**, '**process/processing'**, '**controller**', '**processor'**, '**data subject**' and '**supervisory authority**' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

b) '**the data exporter**' means the controller who transfers the personal data;

c) '**the data importer**' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;EN L 39/10 Official Journal of the European Union 12.2.2010

d) '**the sub-processor**' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data

[1] Parties may reproduce definitions and meaning contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone

exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

e) ‘**the applicable data protection law**’ means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

f) ‘**technical and organisational security measures**’ means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2 - Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3 - Third-party beneficiary clause

1 The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2 The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3 The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub- processor shall be limited to its own processing operations under the Clauses.

4 The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4 - Obligations of the data exporter

The data exporter agrees and warrants:

a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter’s behalf and in accordance with the applicable data protection law and the Clauses;EN 12.2.2010 Official Journal of the European Union L 39/11

c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

e) that it will ensure compliance with the security measures;

f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub- processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5 - Obligations of the data importer[2]

The data importer agrees and warrants:

a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;EN L 39/12 Official Journal of the European Union 12.2.2010

d) that it will promptly notify the data exporter about:

i.) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

ii.) any accidental or unauthorised access; and

iii.) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements

independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6 - Liability

1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2 If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses;EN 12.2.2010 Official Journal of the European Union L 39/13.

Clause 7- Mediation and jurisdiction

1 The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2 The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8 - Cooperation with supervisory authorities

1 The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9 - Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely please add.

Clause 10 - Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11 - Sub-processing

1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses[3]. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2 The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3 The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely please add.

4 The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12 - Obligation after the termination of personal data-processing services

1 The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2 The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

[3] This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision

Example of Standard Contractual Clauses (SCCs) – processor

On behalf of the data exporter:

Name (written out in full)

Position

Address

Other information necessary in order
for the contract to be binding (if any)

(stamp of organization)

Signature

On behalf of the data importer:

Name (written out in full)

Position

Address

Other information necessary in order
for the contract to be binding (if any)

(stamp of organization)

Signature

Personal data specified

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter	Data importer
(Please specify briefly your activities relevant to the transfer):	(Please specify briefly your activities relevant to the transfer):

Data subjects	The personal data transferred concern the following categories of data subjects (please specify):		
	☐ Employees including volunteers, agents, temporary and casual workers	☐ Customer and clients	☐ Suppliers
	☐ Healthcare and welfare data subjects	☐ Personal data included, but types not specified due to the nature of the processing (such as capacity services).	
	☐ Other:		
Categories of data	The personal data transferred concern the following categories of data (please specify):		
	☐ **Customer details** such as name, title, home address, telephone and mobile numbers, email address, date of birth, sex, customer number, purchase and/or service use history and details.		
	☐ **Corporate customer, partner and vendor details** such as name, title, home address, telephone and mobile numbers, email address, date of birth, sex, service use history and details.		
	☐ **Financial and transactional details** such as income, salary, assets and investments, payments, items purchased, loans, benefits, grants, bank account number, payment transaction information, credit card number, insurance details and pension information		
	☐ **Employment and human resources details** such as name, addresses, contact details, age, sex, and date of birth, national identification number, details relating to the employment of the data subject, including career history, recruitment and termination details, employee assessments, training and security records.		
	☐ **IT management details** such as details of equipment data related to the services provided including technical identifiers, user name, location, contact details, communication data and metadata and technical events related to the services provided including system and application logs.		

□ **Security details** such as security log information, facility and system surveillance information and security incident information.

□ **Personal data** included, but types not specified due to the nature of the processing (such as capacity services).

□ **Other**

Special categories of personal data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

□ racial or ethnic origin	□ political opinions	□ religious or philosophical beliefs
□ trade union membership	□ processing of genetic data, biometric data for the purpose of uniquely identifying a natural person	□ data concerning health
□ data concerning a natural person's sex life or sexual orientation	□ criminal convictions and offences or related security measures	

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

□ Provision of IT -services to data exporter	□ Provision of consultancy and development services

The provision of above services may result in processing of data exporter's personal data in at least the following manner (without limitation):

□ Collection	□ Storage	□ Recoding	□ Organising
□ Making available	□ Combining	□ Erasure and deletion	□ Analysing
□ Statistical use	□ Other:		

Data importer will not access, process, transfer or use in any way, directly or indirectly, any personal data under or in connection with the agreement, except (i) where required under the agreed service delivery model or for the performance of the services, as amended from time to time in accordance with the agreement, and (ii)as directed in good faith by data exporter, in any event subject to applicable law and the agreement. The details of the processing activities, the transfer and onward transfer of personal data are stipulated in the agreement and the services delivery model.

Appendix 1 to Standard Contractual Clauses (SCCs) - processor

Data exporter

Name

Authorised signature

Data importer

Name

Authorised signature

Appendix 2 to Standard Contractual Clauses (SCCs) - processor

Technical and organisational security measures

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

❑ As agreed between the data exporter and the data importer.

Appendix 4: DaWinci Processing Specification Form

This **Processing Specification Form** is made under the DPA defined hereunder as Exhibit I of the Main Agreement:

This PSF specifies the Personal Data Processing, which the Data Processor performs on behalf of the Data Controller as part of the services defined below (Services) and is an integral part of the DPA.

The terms relating to Personal Data Processing set out herein are agreed in Exhibit I (DPA) of the < > Agreement No. < > (Main Agreement) between the parties. This PSF is part of the DPA and in case of conflict between the DPA and the PSF, the DPA shall prevail to the extent of the conflict.

The Parties agree the following:

Data Controller(s)	Organisation number Website
Data Processor	**Quorum Software Norway A.S.** Organisation number: 927028387
Services	The following Services are covered by this PSF subject to a Service Order for such Services being executed under Hosting Service Addendum 6 and/or the Main Agreement: • DaWinci Subscriptions • DaWinci related Professional Services
	The processing of Personal Data in the Services is based on the Main Agreement and legitimate interests where the purpose of the Processing is to enable Data Controller's follow up requirements for travel to and from licensed Operation(s), the execution of personnel and cargo transportation, managing the stay on the licensed Operation(s), as well as accessing necessary information in an emergency situation and related system hosting including logging and analytics, service requests, support & maintenance and development where the data subjects' rights have been deemed not to override those interests. Data Controller has approved the DaWinci Privacy Notice attached as Annex A and understands that performance of the DaWinci Subscriptions is subject to the data subjects having been informed about the processing of Personal Data as described in the notice. For MyDaWinci users an electronic read confirmation is currently automatically created as a condition for usage of DaWinci. For personnel not having a MyDaWinci account, the Data Controller is responsible for having a copy of the privacy notice signed and uploaded on the personnel record in DaWinci.
Approved Sub-processors	The Data Controller consents that the Services may utilize Sub-processors that process Personal Data as subcontractors of the Data Processor, as further described on www.quorumsoftware.com/dawinci-data-processing (once the Service is up and running) **Error! Hyperlink reference not valid.**and depending on the ordered Services. At the effective date of this PSF, the following Sub-processors are used by the Data Processor: • **DaWinci Maintenance & Support (incl. Professional Services)** ○ Atlassian (Jira, Confluence) ○ Microsoft 365 (Collaboration tools including e-mail, office applications, messaging services, etc.)

	○ Oracle (Technical support of database; Data Processor may need to send logs to Oracle in case of support issues) ○ Yellowfin (optional Reporting and Analytics tool in DaWinci; Data Processor may need to send logs to Yellowfin in case of support issues) ○ Amazon Web Services (Hosting and infrastructure provider; any test and development environments hosted within Data Processors platform on AWS) • **DaWinci Cloud Services** (in addition to the Sub-processors mentioned above): ○ Amazon Web Services (Hosting and infrastructure provider) ○ Datadog (monitoring of infrastructure) • **Data Processor affiliates** participating in performing the Services ordered by the Data Controller.
Support model and geographic location of Personal Data	The mutually agreed Personal Data geographic storage locations are agreed only in Exhibit M of the Main Agreement. The Data Controller consents that Data Processor and its Sub-processors may process Personal Data (remotely accessed or hosted) as detailed under in the DPA.
Changes	The Data Processor may update or change the Sub-processors in accordance with Exhibit I of the Contract and Hosting Services Addendum 6. Any intended changes concerning the addition or replacement of Sub-processors and their access locations must be announced in advance with a 90 days prior written notice to Customer. Customers subscribing to updates on www.quorumsoftware.com/dawinci-data-processing (once the Service is up and running), will receive automatic notifications of changes. If the Data Controller does not accept an intended change, it must contact Data Processor within 90 days from Processor's written notice of anticipated change.
Categories of data subjects	The categories of data subjects whose Personal Data are processed consist of the following: ☒ Employees including volunteers, agents, temporary and casual workers ☒ Customer and clients ☒ Suppliers ☐ Healthcare and welfare data subjects ☐ Personal data included, but types not specified due to the nature of the processing (such as capacity services). ☐ Other:
Types of Personal Data	At the effective date of this PSF, the following basic Personal Data attributes may be registered by Data Controller, either in the DaWinci application itself or in Service-related internal tools: • UserID • Username • First name last name • Title • Phone numbers • Address • E-mail • Customer company information • Location and language • Attributes listed in the DaWinci Privacy Notice • IT management details, such as log information and journal tables, facility and system surveillance details, information related to the incident tickets or service requests raised by the Data Controller and its authorized DaWinci users. Furthermore, information may be obtained about authorized users' use of the Services and the Data Processors related websites through "cookies" which enables easier use of certain parts of the services. When entering Services hosted by Data Processor, information about authorized users' computer, IP address, operating system and browser type may for example be collected. This information generally comprises data which does not allow individual identification of information related to a specific user.
	During the term of the Services, the registered attributes may change but will remain within the following types of Personal Data:

	☒	**Customer details** such as name, title, home address, telephone and mobile numbers, email address, date of birth, sex, customer number, purchase and/or service use history and details.
	☒	**Corporate customer, partner and vendor details** such as name, title, home address, telephone and mobile numbers, email address, date of birth, sex, service use history and details.
	☐	**Financial and transactional details** such as income, salary, assets and investments, payments, items purchased, loans, benefits, grants, bank account number, payment transaction information, credit card number, insurance details and pension information
	☒	**Employment and human resources details** such as name, addresses, contact details, age, sex, and date of birth, details relating to the employment of the data subject, including career history, recruitment and termination details, employee assessments, training and security records.
	☒	**IT management details** such as details of equipment data related to the services provided including technical identifiers, user name, location, contact details, communication data and metadata and technical events related to the services provided including system and application logs.
	☒	**Security details** such as security log information, facility and system surveillance information and security incident information.
	☐	**Personal data** included, but types not specified due to the nature of the processing (such as capacity services).
	☐	**Other** •

Special categories of Personal Data (if applicable)	The Personal Data transferred concern the following special categories of data:					
	☐	racial or ethnic origin	☐	political opinions	☐	religious or philosophical beliefs
	☐	trade union membership	☐	processing of genetic data, biometric data for the purpose of uniquely identifying a natural person	☐	data concerning health
	☐	data concerning a natural person's sex life or sexual orientation	☐	criminal convictions and offences or related security measures		

Processing operations	The Personal Data may be subject to the following basic processing activities (please specify):							
	☒	Provision of IT -services to data exporter	☒	Provision of consultancy and development services				
	The provision of above services may result in processing of data exporter's Personal Data in at least the following manner (without limitation):							
	☒	Collection	☒	Storage	☐	Recoding	☒	Organising
	☒	Making available	☒	Combining	☒	Erasure and deletion	☒	Analysing
	☒	Statistical use	☐	Other:				

Term and data retention instructions	This PSF shall enter into force at the effective date of Hosting Service Addendum 6 and remains in force as long as the Services are provided under the Main Agreement unless otherwise agreed between the Parties. DaWinci offers the ability for clients to configure data retention periods and automatic deletion and/or anonymization of Personal Data. Unless otherwise agreed in the DPA or separately, the data retention periods and principles in Annex B applies and the

	authorized users Personal Data will not be stored for longer than for the term of the Services and 90 days thereafter..

Annex A - Privacy Notice for the DaWinci Personnel Logistics Solution

1.1 General

This privacy notice contains information about why and how personal data registered in the DaWinci Personnel Logistics Solution (DaWinci) is processed.

1.2 What is personal data

Personal data is personal information that identifies you as a physical person, as well as corresponding information related to the processing of you as a person.

1.3 What does processing of personal data imply

In this context, processing of personal data involves collecting, checking, storing, maintaining and making available information. This process involves a Data Controller. For DaWinci, it is the oil companies that use the solution for personnel transport and personnel on board (POB) administration who is the Data Controller at all times. Quorum Software Norway A.S. holds the role as a Data Processor, which is conducted in accordance with instructions from the oil companies.

1.4 Legal basis and purpose of data processing

The processing of data in DaWinci is based on contracts between the Data Controller and the Data Processor and legitimate interests where the purpose of the data processing is to enable follow up requirements for travel to the installations, the execution of personnel transportation, managing the stay on the installations, as well as accessing necessary information in an emergency situation as well as system hosting, maintenance and development where your interests and fundamental rights as data subject have been deemed do not override those interests.

1.5 Information being processed

No sensitive personal data is stored or processed in DaWinci, only data required for the undertaking of the personnel logistics and the onboard management of the oil and gas installations.

The personal data that may be registered and processed are:

Category	**Data**	**Purpose**
Personnel details	Name, gender, date of birth, national ID, marital status, phone and e-mail	Enabling identification of correct person
Next of kin / emergency contact	Name, relation, address and phone	For use in an emergency preparedness situation
Certificates	Health certificate and other certificates required and/or deemed necessary for travel to and work onboard installations	Enabling validation of travel requirements
Employment	Position and job category Company	Information needed as part of POB (personnel on board) management.

Travel and accommodation information	Transportation reservations and information about work and accommodation installation (incl. cabin, bed and life boat) Information about travel constraints	Enabling POB (personnel on board) management (including outcome of validation of travel requirements.
Misc. Information	Passport details, survival suit details and shoulder width	Passport is not mandatory to register, but may be used in conjunction with visa and/or work/residence permit information.

Furthermore, information may be obtained about your use of DaWinci and the Data Processors related websites through "cookies" which enables easier use of certain parts of the services. When you enter DaWinci, information about your computer, IP address, operating system and browser type, may for example be collected. This information generally comprises data which does not allow individual identification of information related to a specific user.

Aggregated data such as statistical or demographic data may also be collected, used and shared for any purpose. Aggregated data may be derived from your personal data but is not considered personal data by law as this data does not directly or indirectly reveal your identity. For example, your usage data may be aggregated to calculate the percentage of users accessing a specific feature. However, if such aggregated data is combined or connected with your personal data so that it can directly or indirectly identify you, the combined data will be treated as personal data which will be used only in accordance with this privacy notice.

1.6 Sharing of data

Sharing data with third parties may be done to comply with regulatory requirements or to accommodate contractual or legitimate interests. Examples of such sharing are:

- reporting to the authorities
- electronic mustering / tracking
- handling of survival suits
- emergency preparedness
- system hosting and maintenance
- usage analytics

Only personal data that is necessary to fulfill the purposes stated above will be provided to these third parties. All third-party providers must follow this privacy notice and applicable written data processor agreements and any other agreements that are in place with such third-party providers and must implement appropriate technical and organizational measures for the protection of the personal data.

1.7 Where is your data processed?

Your personal data is primarily processed on servers within the EU/EEA or such other geographical locations as agreed with the Data Controller.

However, there may be a need to transfer your data from the agreed data locations. As the level of information protection in countries outside the EU/EEA may be lower than that offered within the EEA, appropriate measures under the EU General Data Protection Regulation (2016/679) will be implemented to ensure that your personal data remains protected and secure. A similar degree of protection is afforded by ensuring at least one of the following safeguards is implemented:

- personal data is only transferred to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission. For further details, see *European Commission: Adequacy of the protection of personal data in non-EU countries*.
- where service providers are used, specific contracts approved by the European Commission are used which give personal data the same protection it has in Europe. For further details, see *European Commission: Model contracts for the transfer of personal data to third countries*.

1.8 Securing personal data

Quorum Software Norway A.S., as Data Processor, ensures it will only process personal data for the purposes for which it was collected and as set out in this privacy notice, and that personal data will only be available to authorized persons holding a position that requires them to process personal data to perform their work. Quorum Software Norway A.S. has taken appropriate technical and organizational measures to keep your personal data secure to ensure that only authorized persons are given access to the personal data.

1.9 Storing of personal data

Your personal data will not be stored longer than is necessary to fulfill the purpose for which they were obtained, as well as to meet statutory requirements for the oil companies' activities.

1.10 Right to view, correct and delete personal data

You have the right to view the personal data we have registered on you and that we process. On the ‘My Page’ in MyDaWinci - you may download a report of all the personal data that have been registered.

It is important that the personal data registered are correct, and you have the right to have incorrectly registered data to be corrected.

You have the right to have your personal data deleted if you should wish to do so, and this will be done when the data are no longer required in order to comply with legitimate interests and statutory or regulatory requirements.

1.11 Changes

This privacy notice may change over time and we will inform you if significant changes are made.

1.12 Contact

Any questions may be directed to the oil company that is the operator of the installation you are travelling to:

< > **Email:** **Phone:**	**< >** **Email:** **Phone:**

< > **Email:** **Phone:**	For other operators you may contact: dpp@quorumsoftware.com

1.13

Read confirmation

For personnel registered as MyDaWinci users a read confirmation will be created upon the user having viewed this Privacy Notice. Personnel not having a MyDaWinci account will have to sign a hard copy version of this document, which in turn will be uploaded and stored on the personnel record in DaWinci.

____
Place/date

______________________________ __________________________
DaWinci-ID & name (capital letters) Signature

Data Controller Instructions

Annex B to PSF

Storage of personal data in DaWinci is required when a person will perform work for or on behalf of the Operator (Data Controller) using DaWinci to manage their Logistics Operation. This may be in the form of a Traveler registered to do work for, or a User managing the Logistics Operation on behalf of the Operator. Quorum Software Norway A.S. (Data Processor), a company part of the Quorum group, has in the role of owner and developer of the DaWinci application, implemented mechanisms requested by the Operator community to help govern personal data in a responsible way – aligned with the requirements of the General Data Protection Regulation (GDPR) of the European Union.

Read Receipt for Storing of Data

User

Any Person registered to work on behalf of the Operator as a User managing the Logistics Operation is currently required to be registered as a user in the Logistics Management application – DaWinci. This enables them to manage personnel and/or cargo logistics depending on which modules the Operator is using.

Traveler

Any Person registered to work for the Operator as a Traveller to and from the managed Operation(s) is currently required to be registered as a user in the Traveller application – MyDaWinci. This enables them to do pre-check-in, see information about their future travels and verify their personal data and certificates. In line with the request of the operators, DaWinci includes functionality for automatical creation of such user for all travelers immediately when they are created as Person (for potential future work on the managed Operation and/or Industry Hub) in the core Application DaWinci.

This point is controlled by the "Create MyDaWinci Traveler Automatically" configuration in the application, which the Operator can turn on / off.

Requirements for confirmation of the storage of personal data

User

Upon first login to DaWinci, which normally takes place in connection with the User starting its job assignment in the tool, the User will have to confirm having read the DaWinci Data Privacy Notice.

Traveler

Upon first login to MyDaWinci, which normally takes place in connection with the first travel for the Person, a Traveler will have to confirm having read the DaWinci Privacy Notice. This describes the data processing in DaWinci, as well as the opportunities the traveler has in connection with storing their data. The content of the Data Privacy Notice is governed by the Operator(s) using DaWinci, and adjustments are managed through the Monthly Tactical Meeting or Customer Forum (for Industry Hubs). The initial version of the DaWinci Privacy Notice is agreed in the Data Processing Agreement.

If the Traveler does not approve the DaWinci Privacy Notice in advance of their first departure, this will currently be indicated by the letter G in NB/Disp, and the Traveler will be prevented from checking in. This badge is visible to those involved in the booking and check-in process of the Person concerned and can be handled by the Traveler being asked to log in to MyDaWinci to confirm reading the DaWinci Privacy Notice.

Alternatively, the Traveler can fill out a manual form entered into the application as part of the heliport process. In order not to prevent the flow of traffic, a choice is made available in the tool which allow the Traveler to be checked in manually at the terminal before the document is physically uploaded in DaWinci (note that it is stated to have been received).

This element is governed by the configuration ”Require that Privacy Statement is read”, and the corresponding ”Get confirmation that Privacy Statement is read”.

Duration of data storage and automatic data obfuscation

User

The Data Controller is responsible for disabling and potentially removing a User in the system upon them no longer using the DaWinci tool as part of their job.

Traveler

At the request of the Operators, DaWinci includes a functionality for automatical anonymization of personal data for Persons who have not had activity on the managed Operation and/or Industry Hub in the last 10 years.

Anonymization of the data means that it can no longer be traced back to the Person, but the data will still be listed for analysis and KPIs historically in anonymized form. This section is controlled by the configuration called ”The maximum number of years we keep person”.

The right to know what is stored about itself

User

Because the data stored about a User is limited to basic personal data, they have insight into what is stored about them directly in the application and can also contact the Operator on the contact details provided in the tool to request to get it exported by email.

Traveler

If a Person wants information about the data stored about them in DaWinci, they can send a request for this using the MyDaWinci application and then have a report sent to their registered email address.

The right to be forgotten

User

Users are normally inactivated or removed as part in the employee no longer going to work in DaWinci. Should the individual User want to be forgotten then this is handled by contacting the Operator on the contact details provided in the tool.

Traveler

If a Person wishes to exercise their right to be forgotten, a request can be made directly from the MyDaWinci application. In such a case, the Operator has decided that historical data shall be retained for 5 years after the last activity on the managed Operation and/or Industry Hub (i.e. in the application), and that data about the Person older than this will be obfuscated.

This section is controlled by the configuration called ”Minimum number of years we keep person”.

Administration

Traveler

DaWinci also includes a functionality for identification of Persons who have travel in the future but not given their read confirmation to the DaWinci Privacy Notice in the screen ”Travels with Deviations” for effective handling.

Appendix 5: Energy Components Processing Specification Form

Processing Specification Form

This **Processing Specification Form** (PSF) is made under the (DPA):

This PSF specifies the Personal Data processing, which the Data Processor performs on behalf of the Data Controller as part of the services defined below (Services) and is an integral part of the DPA.

The terms relating to Personal Data processing are agreed in the Master Licensing and Support Agreement for Energy Components No. 77001753 (Main Agreement) between the parties. This PSF is part of the DPA referred to in clause 10 of the Main Agreement and in case of conflict between the DPA and the PSF, the DPA shall prevail to the extent of the conflict.

The Parties agree the following:

Data Controller(s)	**NAME** Organisation number: XXXXX WEBSITE
Data Processor	**QUORUM SOFTWARE NORWAY A.S.** Organisation number: 927028387
Services	The following Services are covered by this PSF subject to an Order for such Services being executed under the Main Agreement: • Energy Components (EC) Maintenance • EC Application Support • EC as a Service (ECaaS) • EC Smart • EC related Professional Services
	The processing of Personal Data in the Services is based on contract(s) between the Data Controller and the Data Processor, and legitimate interests where the purpose of the data processing is to enable provisioning of the Services requested by the Data Controller including Personal Data required for access management, logging and analytics related to system hosting, service requests, support and service development where the data subjects' rights have been deemed not to override those interests. The Personal Data shall only be processed for the term of the Services and as otherwise agreed between the Parties. Subject-matter, nature and purpose of the Processing are defined in more detail under the respective Orders and in the Main Agreement.
Approved Sub-processors	The Data Controller consents that the Services may utilize Sub-processors that process Personal Data as subcontractors of the Data Processor, as further described on the EC Community Portal located at www.quorumsoftware.com/energy-components-data-processing (or any successor location design designated by the Data Processor) and depending on the ordered Services. At the effective date of this PSF, the following Sub-processors are used by the Data Processor: • **EC Maintenance and/or Support Services** o Atlassian (Jira, Confluence, Bitbucket) o Microsoft 365 (Collaboration tools including e-mail, office applications, messaging services, etc.)

	○ Oracle (Technical support of database; Data Processor may need to send logs to Oracle in case of support issues) ○ ServiceNow (for Service Desk related tasks when applicable) ○ Yellowfin (Reporting and Analytics tool in EC; Data Processor may need to send logs to Yellowfin in case of support issues) • **ECaaS and EC Smart** (in addition to the Sub-processors mentioned above): ○ Amazon Web Services (Hosting and infrastructure provider) ○ Datadog (monitoring of infrastructure) • All Data Processor Affiliates participating in performing the Services ordered by the Data Controller.
Geographic location of Personal Data	The mutually agreed Personal Data geographic storage location(s) are agreed under the respective Orders and/or applicable Service Description. The Data Controller consents that Data Processor and its Sub-processors process and remotely access or process Personal Data as detailed on the EC Community Portal and in accordance with this PSF and the Main Agreement.
Changes	The Data Processor may update or change the Sub-processors. Except for emergency changes, any intended addition or replacement of Sub-processors and/or change in their access or processing locations will be announced in advance with 30 days prior written notice. Data Processor will provide a subscription feature that enables Data Controller to subscribe to updates to the Sub-processor information on the EC Community Portal or from the relevant About page on the respective EC application deployment. Receipt of such notices requires that Data Controller has opted to receive the updates. Until this is in place, Data Processor will send updates to the list of Sub-processors to Data Controller prior to each main release.
Transfer of Personal Data	The Data Controller hereby authorizes the Data Processor to transfer Data Controller's Personal Data to Data Processor's Affiliates and Sub-processors outside of the EU/EEA, subject to appropriate safeguards as described in GDPR Art. 46. The Data Processor group of companies is authorized by the Data Controller to execute and enter into the Standard Contractual Clauses (SCC) with the relevant required parties as data exporter. The currently valid EU Commission's SCCs are provided under https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02010D0087-20161217. Following the Schrems II ruling and until further guidance from authorities is made available, Data Processor cannot provide final conclusion whether the SCCs and implemented safeguards with specific Sub-processors are considered sufficient or not. Additional information and/or adjustment to the PSF will be provided as soon as possible and when available. The Parties agree that, if the SCCs are in the future amended or replaced, the Data Processor shall also have the right to enter into the new data transfer arrangement with relevant Sub-processors in accordance with this PSF.

Categories of data subjects	The categories of data subjects whose Personal Data are processed consist of the following:		
	☒ Employees including volunteers, agents, temporary and casual workers	☒ Customer and clients	☒ Suppliers
	□ Healthcare and welfare data subjects	□ Personal data included, but types not specified due to the nature of the processing (such as capacity services).	
	□ Other:		
Types of Personal Data	At the effective date of this PSF, the following basic Personal Data attributes are registered by Data Controller, either in the EC application itself or in Service-related internal tools: • UserID • User name • Phone numbers • E-mail • Customer company information • Department • Location and language		

	• IT management details, such as log information and journal tables, information related to the incident tickets or service requests raised by the Data Controller, Data Processor and/or their authorized EC users. Furthermore, information may be obtained about authorized users' use of the Services and the Data Processors related websites through "cookies" which enables easier use of certain parts of the services. When entering Services hosted by Data Processor, information about authorized users' computer, IP address, operating system and browser type may for example be collected. This information generally comprises data which does not allow individual identification of information related to a specific user. Aggregated data such as statistical or demographic data may also be collected, used and shared for any purpose. Aggregated data may be derived from authorized users' Personal Data but is not considered Personal Data by law as this data does not directly or indirectly reveal an authorized user's identity. For example, usage data may be aggregated to calculate the percentage of users accessing a specific feature. However, if such aggregated data is combined or connected with authorized users' Personal Data so that it can directly or indirectly identify a data subject, the combined data will be treated as Personal Data which will be used only in accordance with this PSF.		
	During the term of the Services, the registered attributes may change but will remain within the following types of Personal Data:		
	☒ **Customer details** such as name, title, home address, telephone and mobile numbers, email address, date of birth, sex, customer number, purchase and/or service use history and details.		
	☒ **Corporate customer, partner and vendor details** such as name, title, home address, telephone and mobile numbers, email address, date of birth, sex, service use history and details.		
	☐ **Financial and transactional details** such as income, salary, assets and investments, payments, items purchased, loans, benefits, grants, bank account number, payment transaction information, credit card number, insurance details and pension information		
	☐ **Employment and human resources details** such as name, addresses, contact details, age, sex, and date of birth, national identification number, details relating to the employment of the data subject, including career history, recruitment and termination details, employee assessments, training and security records.		
	☒ **IT management details** such as details of equipment data related to the services provided including technical identifiers, user name, location, contact details, communication data and metadata and technical events related to the services provided including system and application logs.		
	☒ **Security details** such as security log information, facility and system surveillance information and security incident information.		
	☐ **Personal data** included, but types not specified due to the nature of the processing (such as capacity services).		
	☐ **Other** •		
Special categories of Personal Data (if applicable)	The Personal Data transferred concern the following special categories of data: N/A		
	☐ racial or ethnic origin	☐ political opinions	☐ religious or philosophical beliefs
	☐ trade union membership	☐ processing of genetic data, biometric data for the purpose of uniquely identifying a natural person	☐ data concerning health
	☐ data concerning a natural person's sex life or sexual orientation	☐ criminal convictions and offences or related security measures	
Processing operations	The Personal Data may be subject to the following basic processing activities (please specify):		
	☒ Provision of IT -services to data exporter	☒ Provision of consultancy and development services	
	The provision of above services may result in processing of Data Controller's Personal Data in at least the following manner (without limitation):		

☒	Collection	☒	Storage	☒	Recording	☒	Organising
☒	Making available	☒	Combining	☒	Erasure and deletion	☒	Analysing
☒	Statistical use	☐	Other:				

The Data Processor will not access, process, transfer or use in any way, directly or indirectly, any Personal Data under or in connection with the agreement, except
(i) where required for the performance of the Services, as amended from time to time in accordance with the Main Agreement, and
(ii) as directed in good faith by the Data Controller, in any event subject to applicable law and the Main Agreement.

Term and data retention instructions	This PSF shall enter into force at the date of signature below and remains in force as long as the Services are provided under the Main Agreement unless otherwise agreed between the Parties. Disabling and removing authorized users in EC is Data Controller's responsibility. In self-hosted solutions Data Controller is further responsible by itself for configuring appropriate data retention periods. When the Services are hosted by Data Processor, authorized users' Personal Data will, unless otherwise agreed, be stored no longer than for the term of the Services and 90 days thereafter, with audit logs for the cloud infrastructure being retained for maximum three (3) years. However, Data Processor may thereafter also process usage data that has been aggregated and/or anonymized (for clarity does not allow a third party to identify Data Controller as the source of the information) in order to develop new services and features and to promote Data Processor's services for example via analyses of patterns and trends regarding used functionalities.
Signatures	This PSF has been executed in two (2) counterparts, each Party taking one. Any signed and electronically exchanged copy shall have the same effect as the original signed document.
	place & date
	Quorum Software Norway A.S.
	name & title
	place & date
	COMPANY's NAME
	name & title