DATA PROCESSING AND DATA SECURITY AGREEMENT (Version 1:2019)

Notice:

This Data Processing Agreement ("**DPA**") creates the legal framework, between the data controller and the data processor, for processing of personal data in a manner compliant with *EU General Data Protection Regulation 2016/679 (GDPR)*.

The data controller is using a subscribed (licensed) service (SaaS) and the data processor will, on behalf of the data controller, process Personal Data selected, collected and submitted by the data controller, and/or third parties designated by the data controller, and stored and used within the service. The terms of this DPA only apply to data controller with an active subscription to the service.

By agreeing to be bound by this DPA the data controller (you, the entity or company that you represent) is unconditionally consenting to be bound by and is becoming a party to this DPA with the data processor; Comlink AB, co. reg. no. 556514-0190, Energigatan 10B, SE-434 37 Kungsbacka, Sweden. If the data controller does not unconditionally agree to all terms of this DPA the use of the service is strictly prohibited, other than for internal validation and testing purposes.

Should European Parliament and/or the Council pass new regulations and/or issue any guidelines which contains terms that conflict with those used in this DPA, such terms in this DPA shall be changed or otherwise interpreted and applied strictly in accordance with any such new regulation and guideline.

Please contact info@comlink.se **with any questions**

1. DEFINITIONS

All capitalized terms used in this DPA shall have the meanings given to them below:

"**Cloud Entity**" means entities added to the Data Controller's account to which Personal Data may be associated and/or processed.

"**Data Controller**" has the meaning given in GDPR (and, for the purpose of this DPA, means the party licensing and using the Service).

"**Data Processor**" has the meaning given in GDPR (and, for the purposes of this DPA, COMLINK AB, co. reg. no. 556514-0190, Energigatan 10B, SE-434 37 Kungsbacka, Sweden).

"**Data Security Breach**" has the meaning set forth in Section 4.2(3).

"**Data Subject**" means an individual who is the subject of Personal Data.

"**Data Subject Request**" has the meaning set forth in Section 4.2(6).

"**Data Transfer**" means a transfer of Personal Data from the Data Controller to the Data Processor, or an onward transfer of Personal Data from the Data Processor to a Sub-Processor, or between two establishments of a Data Processor; in each case, where such transfer would be prohibited by EU Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of EU Data Protection Laws).

"**DPA**" means this Data Processing and Data Security Agreement together with its annexes, as supplemented and amended from time to time.

"**EEA**" means the European Economic Area.

"**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each member state and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR.

"**GDPR**" means EU General Data Protection Regulation 2016/679.

"**JDCA**" means the joint data controller agreement set forth in **Exhibit C**, between a Data Controller and a third part data controller (whom is also bound by this DPA), creating the legal framework for the access delegation and shared use of Cloud Entities and the joint use and processing of (same) Personal Data. Access to and right to use each delegated Cloud Entity is conditioned upon the prior acceptance of the JDCA.

"**Joint Data Controller**" has the meaning given in GDPR (and, for the purposes of this DPA, the Data Controller and such third party (each a joint data controller) that under a JDCA and by sharing the use of Cloud Entities are jointly determining the purposes and means of Processing of Personal Data in and for the Service).

"**Party**" means either Data Controller or Data Processor.

"**Parties**" means Data Controller and Data Processor.

"**Personal Data**" means any information relating to an identified or identifiable natural person, where 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.

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

"**Service**" mean the Data Processor's proprietary Software-as-a-Service and (as applicable) Cloud Sourcing services that are ordered by Data Controller through a link or via an order form and made available online by Data Processor, via the applicable subscriber login link and other web pages designated by Data Processor or Data Processor's reseller/channel partner.

"**Service Data**" means electronic data, text, messages, communications or other materials submitted to and stored within the Service by Data Processor, its agents and end-users in connection with Data Controller's access and use of the Service, including, without limitation, Personal Data.

"**Sub-Processor**" means any third party data processor engaged by Data Processor who receives Personal Data from Data Processor or Data Controller for Processing on behalf of Data Controller.

"**Subscription Agreement**" means the agreement and terms and conditions under which the Data Controller is subscribing and granted licensing rights to use the Service.

"**Supervisory Authority**" means any Data Protection Supervisory Authority with competence over Data Controller, Joint Controllers, Data Processor and any Sub-Processor Processing of Personal Data.

"**Third Party Services**" means any services, products, devices, equipment, gateways, links or other functionality and any third-party content and materials that may be included in or linked to the Service and that allows the user to access third party services, for example connectivity- and mobile network services.

2. PURPOSE

2.1 The Data Controller has entered into a Subscription Agreement pursuant to which Data Controller is granted a license to access and use the Service, and the Data Processor will, on behalf of the Data Controller, Process Personal Data selected, collected and submitted by the Data Controller, and/or third parties designated by the Data Controller with whom Data Controller transacts using the Service, and such Personal Data is stored and used within the Service. For the avoidance of doubt, the terms of this DPA shall only apply to the Data Controller with an active subscription to the Service.

2.2 The Parties are entering into this DPA to ensure that the Processing by the Data Processor of Personal Data, within the Service, is done in a manner compliant with GDPR and its requirements regarding the collection, use and retention of Personal Data.

2.3 To the extent that any terms of the Subscription Agreement conflict with the substantive terms of this DPA (as they relate to the protection of Personal Data and the Parties' respective obligations and liabilities), the terms of this DPA shall take precedence.

3. OWNERSHIP OF THE SERVICE DATA

As between the Parties, all Service Data Processed under the terms of this DPA and the Subscription Agreement shall remain the property of the Data Processor. Under no circumstances will the Data Processor act, or be deemed to act, as a data controller (or equivalent concept such as joint data controller) of the Service Data Processed within the Service under GDPR.

4. OBLIGATIONS OF DATA PROCESSOR

4.1 The Parties agree that the subject-matter and duration of Processing performed by the Data Processor under this DPA and the Subscription Agreement, including the nature and purpose of Processing, the type of Personal Data, and categories of Data Subjects, shall be as described in **Exhibit A** of this DPA.

4.2 As part of the Data Processor providing the Service to the Data Controller under the Subscription Agreement, Data Processor shall comply with the obligations imposed upon it under *GDPR Articles 28 - 32* and agrees and declares as follows:

(1) The Data Processor shall process Personal Data in accordance with the instructions set forth in this DPA;

(2) the Data Processor shall ensure that all staff and management of the Data Processor are fully aware of their responsibilities to protect Personal Data in accordance with this DPA and have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality in accordance with *GDPR Article 28(3)(b)*;

(3) the Data Processor shall implement and maintain appropriate technical and organizational measures to protect Personal Data in accordance with *GDPR Article 32* against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access (a "**Data Security Breach**"), provided that such measures shall take into account 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, so as to ensure a level of security appropriate to the risks represented by the Processing and the nature of the Personal Data to be protected, including data security consistent with the Security Standards described in **Exhibit B**, ,

(4) the Data Processor shall notify the Data Controller in accordance with *GDPR Article 33(2)*, without undue

delay but in any event within 48 hours, in the event of a confirmed Data Security Breach affecting the Data Controller's Service Data and to cooperate with the Data Controller as necessary to mitigate or remediate the Data Security Breach. Further, the Data Processor shall cooperate with the Data Controller and take such commercially reasonable steps as are directed by the Data Controller to assist in the investigation, mitigation and remediation of any such Data Security Breach under *GDPR*;

(5) the Data Processor shall comply with the requirements of Section 5 when engaging a Sub-Processor;

(6) taking into account the nature of the Processing, the Data Processor shall assist the Data Controller (including by appropriate technical and organizational measures), insofar as it is commercially reasonable, to fulfil Data Controller's obligation to respond to requests from Data Subjects to exercise their rights under *GDPR* (a "**Data Subject Request**"). In the event the Data Processor receives a Data Subject Request directly from a Data Subject, it shall (unless prohibited by law) direct the Data Subject to the Data Controller. However, in the event the Data Controller is unable to address the Data Subject Request, taking into account the nature of the Processing and the information available to the Data Controller, the Data Processor, shall, on the Data Controller's written request and the Data Controller's instruction to the Data Processor, and at the Data Processor's reasonable expense (scoped prior to the Data Processor's response to the Data Subject Request), address the Data Subject Request, as required under *GDPR*;

(7) upon request, the Data Processor shall provide the Data Controller with commercially reasonable information and assistance, taking into account the nature of the Processing and the information available to the Data Processor, to help the Data Controller to conduct any data protection impact assessment or Supervisory Authority consultation it is required to conduct under *GDPR*;

(8) upon termination of the Data Controller's access to and use of the Service, the Data Processor shall comply with the requirements of Section 10;

(9) the Data Processor shall comply with the requirements of Section 6 in order to make available to the Data Controller information that demonstrates the Data Processor's compliance with this DPA; and

(10) the Data Processor shall appoint a security officer who will act as a point of contact for the Data Controller, and coordinate and control compliance with this DPA.

4.3 The Data Processor shall immediately inform the Data Controller if, in its opinion, the Data Controller's processing instructions infringe any law or regulation. In such event, the Data Processor is entitled to refuse Processing of Personal Data that it believes to be in violation of any law or regulation.

5. USE OF SUB-PROCESSORS

5.1 The Data Controller hereby confirms its general written authorisation for the Data Processor's use of the Sub-Processor(-s) listed in accordance with *GDPR Article 28*, to assist it in providing the Service and Processing Personal Data provided that such Sub-Processor(-s),

(1) agree to act only on the Data Processor's instructions when Processing the Personal Data (which instructions shall be consistent with the Data Controller's Processing instructions to the Data Processor), and

(2) agree to protect the Personal Data to a standard consistent with the requirements of this DPA, including by implementing and maintaining appropriate technical and organizational measures to protect the Personal Data they Process consistent with the Security Standards set forth in **Exhibit B**.

5.2 The Data Processor agrees and warrants to remain liable to the Data Controller for the Processing services of any of its Sub-Processor(-s) under this DPA. The Data Processor shall maintain an up-to-date list of the names and locations of all Sub-Processor(-s) used for the Processing of Personal Data under this DPA at www.comlink.se. The Data Processor shall update the list on its website of any Sub-Processor to be appointed at least 30 days prior to the date on which the Sub-Processor shall commence processing Personal Data. The Data Processor may sign up to receive email notification of any such changes. (The details of the sign-up process are as detailed in the aforementioned URL.)

5.3 In the event that the Data Controller objects to the Processing of its Personal Data by any newly appointed Sub-Processor, as described in this Section 5, the Data Controller shall inform the Data Processor within 30 days following the update of its online policy above. In such event, the Data Processor will instruct the Sub-Processor to cease any further processing of the Data Controller's Personal Data and this DPA shall continue unaffected.

5.4 In addition, and as stated in the Subscription Agreement, the Service requires integrations and combinations with Third Party Services. If the Data Controller elects to enable, access or use such Third Party Services, its access and use of such Third Party Services is governed solely by the terms and conditions and privacy policies of such Third Party Services, and the Data Processor does not endorse, is not responsible or liable for, and makes no representations as to any aspect of such Third Party Services, including, without limitation, their content or the manner in which they handle Service Data (including Personal Data) or any interaction between the Data Controller and the provider of such Third Party Services. The Data Processor is not liable for any damage or loss caused or alleged to be caused by or in connection with the Data Controller's enablement, access or use of any such Third Party Services, or the Data Controller's reliance on the privacy practices, data security processes or other policies of such Third Party Services. A provider of a Third Party Service shall not be deemed a Sub-Processor for any purpose under this DPA.

6. AUDIT

6.1 Subject to this Section 6, the Data Processor shall make available to the Data Controller on request all

information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, by the Data Controller or an auditor mandated by the Data Controller in relation to the Processing of Personal Data by the Data Processor and any Sub-Processor.

6.2 Information and audit rights of the Data Controller only arise under Section 6.1 to the extent that the DPA does not otherwise give them information and audit rights meeting the relevant requirements of *GDPR*.

7. INTERNATIONAL DATA TRANFERS

7.1 The Data Controller acknowledges that Services Data Processor and its Sub-Processors may maintain Processing operations in countries that are outside of the EEA. As such, both Data Processor and its Sub-processors may Process Personal Data in non-EEA countries. This will apply even where Data Controller has agreed with Data Processor to host Personal Data in the EEA, if such non-EEA countries Data Transfer and Processing is necessary to host, provide and develop the Service, and access and support-related or other services requested by Data Controller.

7.2 If Personal Data processed in the Service and under this DPA is transferred from a country within the EEA to a country outside the EEA, the Data Processor shall ensure that the Personal Data are adequately protected. To achieve this, the Data Processor shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of Personal Data.

8. OBLIGATIONS OF DATA CONTROLLER

As part of the Data Controller receiving the Service under the Subscription Agreement, the Data Controller agrees to abide by its obligations under *GDPR* and declares and warrants as follows.

(1) That the Data Controller is solely responsible for the means by which Personal Data is acquired and used by the Data Controller, including instructing Processing by the Data Controller in accordance with the provisions of the Subscription Agreement and this DPA, is and shall continue to be in accordance with all the relevant provisions of *GDPR*, particularly with respect to the security, protection and disclosure of Personal Data,

(2) that if collection by Data Processor involves any 'special' or 'sensitive' categories of Personal Data (as defined in *GDPR*), the Data Controller is acquiring and transferring such Personal Data in accordance with GDPR,

(3) that that Data Controller will inform its Data Subjects (if applicable);

(a) about its general use of data processors to Process their Personal Data, including the Data Processor, and

(b) that their Personal Data may be Processed outside of the EEA,

(4) that, upon instructions from the Data Processor, it shall respond in reasonable time and to the extent reasonably practicable to enquiries by Data Subjects regarding the Processing of their Personal Data by the Data Processor, and to give appropriate instructions to the Data Processor in a timely manner,

(5) that, upon instructions from the Data Processor, it shall respond in a reasonable time to enquiries from a Supervisory Authority regarding the Processing of relevant Personal Data by Data Processor, and

(6) that the Data Controller is solely responsible for any arrangement in the event of the Data Controller becomes a Joint Data Controller as further specified in Section 9.

9. JOINT CONTROLLERS

9.1 Subject to the Subscription Agreement, the Data Controller may appoint and delegate access to and share use of Cloud Entities with (another) third party data controller whom is also bound by this DPA. The Data Controller and the third party data controller are then, as Joint Data Controllers, subject to *GDPR Article 26*, jointly determining the purposes and means of processing of (same) Personal Data related to the (same) Cloud Entity.

9.2 By registration and by becoming a Data Controller under the Service, and in all events before granting access to and right to use any delegated Cloud Entities, the delegating Data Controller and the third party data controller, being delegated to, accepts to be bound by the JDCA in **Exhibit C**, to ensure that the Joint Data Controllers comply with the requirements relating to Joint Data Controllers pursuant to *GDPR Article 26*. The JDCA determines the Joint Data Controllers' respective responsibilities for compliance with the obligations under the *GDPR*, in particular as regards the exercising of the rights of the Data Subject and their respective duties to provide the information as set forth in *GDPR*. I.e. the delegating Data Controller and the third party data controller (being delegated to) accepts the DPA and the JDCA when accepting the terms and conditions for the Service (during registration) and are then automatically becoming Joint Data Controllers by delegation, upon which the JDCA shall come into full effect between the Joint Data Controllers.

9.3 The JDCA includes a confirmation that the appointed third party joint controller (i) has accepted and agreed to be bound by terms and conditions of this DPA, (ii) and has accepted the appointment of the Data Processor under the DPA for Processing of relevant Personal Data for each of the Joint Data Controllers.

9.4 Each Joint Data Controller is responsible for its own Personal Data Transfers, including for ensuring that a legal basis for joint data controlling exists and that *GDPR Article 26* has been fully observed and adhered to.

9.5 The Data Controller delegating access to and right to share the use of Cloud Entities is legally solely responsible and liable for ascertaining the creation of a JDCA and the Data Controller acknowledges that the Data Processor's only responsibility in this respect is to adhere to this DPA and to inform the Data Controller of the

legal requirements under *GDPR* pertaining to joint data controlling and that the JDCA is provided by the Data Processor solely as a service.

10. RETURN AND DESTRUCTION OF PERSONAL DATA

Upon the termination of the Data Controller's access to and use of the Service, the Data Processor will up to 30 days following such termination at the choice of the Data Controller either (a) permit the Data Controller to export its Service Data, at its expense; or (b) delete all Service Data in accordance with the capabilities of the Service in accordance with *GDPR Article 28(3)(g)*. Following such period, the Data Processor shall delete or anonymize all Service Data stored or Processed by the Data Processor on behalf of the Data Controller in accordance with the Data Processor's deletion policies and procedures. The Data Controller expressly consents to such action.

11. DURATION

This DPA will remain in force for as long as the Data Processor Processes Personal Data on behalf of the Data Controller under the Subscription Agreement and for the Service.

12. LIMITATION ON LIABILITY

12.1 As between the Data Controller and the Data Processor this DPA shall be subject to the limitations of liability set forth in this Section below, and in applicable Subscription Agreement for the Service subscribed by the Data Controller.

12.2 The Data Processor does not accept any liability under this DPA or GDPR for any Third Party Services, including acts and omissions.

12.3 The Data Processor does not accept any liability under this DPA or GDPR due to the Data Controller's breach of its obligations to create a Joint Data Controller arrangement as set forth in Section 9.

12.4 The limitation of liability set forth in this Section 12 shall not be construed as limiting the liability of either Party with respect to claims by Data Subjects.

13. MISCELLANEOUS

13.1 This DPA may not be amended or modified except by a writing signed by both Parties hereto. This DPA may be executed in counterparts, provided however that the Data Processor shall be entitled to from time to time make non-material functional changes and updates to the DPA (not changing the Parties' respective rights and responsibilities in this DPA) by giving the Data Controller 30 days' notice. Also, should European Parliament and/or the Council pass new regulations and/or issue any guidelines which contains terms that conflict with those used in this DPA, the Parties hereby agree that such terms in this DPA shall primarily be changed or secondarily be interpreted and applied strictly in accordance with any such new regulation and guideline.

13.2 The terms and conditions of this DPA are confidential and each party agrees and represents, on behalf of itself, its employees and agents to whom it is permitted to disclose such information that it will not disclose such information to any third party; provided, however, that each party shall have the right to disclose such information to its officers, directors, employees, auditors, attorneys and third party contractors who are under an obligation to maintain the confidentiality thereof and further may disclose such information as necessary to comply with an order or subpoena of any administrative agency or a court of competent jurisdiction or as reasonably necessary to comply with any applicable law or regulation.

13.3 Subject to the foregoing restrictions, this DPA will be fully binding upon, inure to the benefit of and be enforceable by the Parties and their respective successors and assigns.

13.4 This DPA and the Subscription Agreement constitute the entire understanding between the Parties with respect to the subject matter herein, and shall supersede any other arrangements, negotiations or discussions between the Parties relating to that subject-matter.

14. GOVERNING LAW AND JURISDICTION

This DPA and the rights and obligations of the Parties pursuant thereto will be governed by the laws of Sweden, without regard to conflicts of law principles. The Parties irrevocably agree that, subject as provided below, the courts of Sweden shall have exclusive jurisdiction in relation to any claim, dispute or difference concerning this DPA (including the right to possible appeal), and any matter arising therefrom and irrevocably waive any right that they may have to object to an action being brought in those courts, or to claim that the action has been brought in an inconvenient forum, or that those courts do not have jurisdiction.

***

PROCESSING, PERSONAL DATA AND DATA SUBJECTS

(DATA CONTROLLER'S INSTRUCTIONS)

Terms defined in the DPA shall have the same meaning in this Exhibit.

1. DATA PROCESSOR (WHERE APPLICABLE)

The Data Processor (where applicable) operates a Software-as-a-Service and (as applicable) Cloud Sourcing services for asset management and the operation and administration of attached equipment including the identification of users e.g. for entry into doors and gates via mobile phones.

Further information can be found online at www.comlink.se.

2. DATA CONTROLLER

The Data Controller is the subscriber and user of the Service and will collect and process Personal Data for registering persons and users for access-controlling attached equipment.

3. DURATION OF PROCESSING

The processing of Personal Data shall endure for the duration of the subscription term in the relevant Subscription Agreement for the Service.

4. DATA SUBJECTS

The Data Controller may, at its sole discretion, collect and submit Personal Data to the Service, which may include, but is not limited to, the following categories of Data Subjects (all of whom are natural persons) of the Data Controller and any natural person(s) authorized by the Data Controller to use the Service:

1. Employees	2. Relatives of employees	3. Customers	4. Prospective customers
5. Service providers	6. Business partners	7. Vendors	8. Advisors
9. Subscribers of the Service	10. Users of Data Controller provided services		

5. CATEGORIES OF PERSONAL DATA

The Data Controller may, at its sole discretion, submit Personal Data to the Service which may include, but is not limited to, the following categories of data:

1. First name	2. Last name	3. Title	4. Email address
5. Telephone number	6. Address	7. Other contact details	8. Contractual relations/matters
9. Support communications	10. Customer service information	11. Customer history	12. Restrictions or grants
13. Information provided to third parties (e.g. credit reference agencies, public directories	14. Cloud Entity usage		

6. SPECIAL CATEGORIES OF DATA

Not applicable.			

7. PROCESSING OPERATIONS AND COOKIES

The subject matter of the Processing of the Personal Data:

The Data Processor (where applicable) will host and process Personal Data obtained by the Data Controller using or third party using the Service, in the course of and as a technical prerequisite for the Data Processor to provide the

Service, the Software-as-a-Service and (as applicable Cloud sourcing services, including;

1. Collection of Personal Data	2. Storage of Personal Data	3. Compilation of Personal Data	4. Administration of Personal Data
5. Organisation of Personal Data	6. Disclosure by forwarding Personal Data	7. Utilisation of Personal Data	8. Communication with users regarding the Service.
9. Cookies, as further detailed in this Section below.			

The Data Processor uses cookies. Anyone user who visits the Data Processor's website or the Service shall receive information that the website and/or Service contains cookies and the purpose of using the cookies. The Data Processor uses two types of cookies on its website and in the Service; so called durable cookies, which are a text file stored on a visiting computer and so called temporary cookies or session cookies, which are only stored temporarily on a visiting computer and disappear when the user shuts down the browser on the visiting computer. The Data processor uses these two types of cookies partly to optimize the data Processor's website and the function of Service, and partly to analyse statistics so that the Data processor in its contacts with users of the Service should be able to provide the best possible level of Service and Service-offers. The user will be given the opportunity to consent to or decline that cookies be stored on the user's computer, however in order to be granted access to the Service, the user must approve the Data Processor's cookies. By using the Service, the user agrees that the Data Processor uses cookies to offer the user the best possible experience of the Service.

Service Data and Personal Data which relates to Data Subjects and constitutes personal data in accordance with GDPR, collected for or on behalf of the Data Controller and its users via cookies, shall be treated as Personal Data under this DPA.

8. RESTRICTIONS

Processing shall take place exclusively within the European Union or in another contracting state of the agreement of the EEA.

Any transfer of Personal Data outside of the EEA requires the prior approval of the Data Controller and shall be in accordance with the DPA and relevant parts of the *GDPR*.

9. CONTACT DETAILS

For Personal Data queries arising from or in connection with this Processing and this DPA, the Controller and Data Subjects shall contact the following:

DATA PROCESSOR:

COMLINK AB (Co. reg. no. 556514-0190)

Adress: Energigatan 10B, SE-434 37 Kungsbacka, Sweden

Web: www.comlink.se

Email: info@comlink.se

Tel: +46 (0)31-208600

Appointed Contact person Peder Kierkemann

Email: peder@comlink.se

Tel: +46 31-208600

***

DATA SECURITY STANDARDS

As of the Effective Date of the DPA, the Data Processor, when Processing Personal Data on behalf of the Data Controller in connection with the Service, the Data Processor shall implement and maintain the following technical and organizational security measures for the Processing of such Personal Data ("**Security Standards**").

Terms defined in the DPA shall have the same meaning in this Exhibit.

1. PHYSICAL ACCESS CONTROLS

The Data Processor shall take reasonable measures to;

(a) prevent physical access, such as security personnel and secured buildings, and

(b) prevent unauthorized persons from gaining access to Personal Data or ensure third parties operating data centres on its behalf are adhering to such controls.

2. SYSTEM ACCESS CONTROLS

The Data Processor shall take reasonable measures to prevent Personal Data from being used without authorization. These measures shall vary based on the nature of the Processing undertaken and may include, among other;

(a) controls,

(b) authentication via passwords and/or two-factor authentication,

(c) documented authorization processes,

(d) documented change management processes, and/or,

(e) logging of access on several levels.

3. DATA ACCESS CONTROLS

The Data Processor shall take reasonable measures to provide that;

(a) Personal Data is accessible and manageable only by properly authorized staff,

(b) direct database query access is restricted, and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the Personal Data to which they have privilege of access, and

(c) Personal Data cannot be read, copied, modified or removed without authorization in the course of Processing.

4. TRANSMISSION CONTROLS

The Data Processor shall take reasonable measures to ensure that it is possible to check and establish to which entities the transfer of Personal Data by means of data transmission facilities is envisaged so Service Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport.

5. INPUT CONTROLS

5.1 The Data Processor shall take use commercial best efforts to provide that it is possible to check and establish whether and by whom Service Data has been entered into data processing systems, modified or removed.

5.2 The Data Processor shall take reasonable measures to ensure that;

(a) the Personal Data source is under the control of the Data Controller; and

(b) Personal Data integrated into the Service is managed by secured transmission from the Data Controller for interactions with Data Processor's User Interface ("**UI**") or Application Programming Interface ("**API**").

6. DATA BACKUP

Back-ups of the databases in the Service are taken on a regular basis, are secured, and encrypted to ensure that Personal Data is protected against accidental destruction or loss.

7. LOGICAL SEPARATION

Personal (Service) Data from different data controller's and their respective users is logically segregated on systems managed by the Data Processor to ensure that Personal Data that is collected by different data controllers is segregated from one another.

***

JOINT DATA CONTROLLER AGREEMENT

(Version 1:2019)

Notice:

This Joint Data Controller Agreement ("**JDCA**") shall apply to each data controller (each delegating data controller) who is using a subscribed (licensed) service (SaaS) and who also to another data controller delegates access and shared use of cloud entities within the service, or part thereof, being joint data controllers jointly determining the purposes and means of processing of (same) personal data, pursuant to *Article 26 of the EU General Data Protection Regulation 2016/679 (GDPR)*. In the event there is no such joint data control this JDCA shall not apply.

This JDCA defines the relationship between two joint data controllers and creates the legal framework for the joint data controllers in a manner compliant with *GDPR*. This JDCA determines the joint data controllers' respective responsibilities for compliance with the obligations under the *GDPR*, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information.

By accepting this JDCA the Joint Data Controllers (the delegating joint data controller and the data controller being delegated to) are unconditionally consenting to be bound by and is becoming parties to this JDCA. If both joint data controllers do not unconditionally agree to all terms of this JDCA there will be no access to and right to use any delegated rights to the licensed service.

By delegation of a Cloud Entity the delegating Data Controller and the third party data controller being delegated to (receiver) are automatically becoming Joint Data Controllers under *GDPR* regarding the Personal Data related to the shared Cloud Entity, and also the JDCA accepted by the Joint Data Controllers shall come into full effect and shall apply between the Joint Data Controllers. The JDCA can be terminated at any time; by the delegating Data Controller by retracting the delegation, or by the receiving data controller by deleting the Cloud Entity from the receiving account.

In connection with an audit or a complaint or part of a complaint by a data subject, the joint data controllers must notify the essence of or provide access to this JDCA as in effect between the joint data controllers.

Should European Parliament and/or the Council pass new regulations and/or issue any guidelines which contains terms that conflict with those used in this JDCA, such terms in this JDCA shall be changed or otherwise interpreted and applied strictly in accordance with any such new regulation and guideline.

DEFINITIONS

All capitalized terms used in this JDCA shall have the meanings given to them below:

"**Cloud Entity**" means entities added to the Data Controller's account to which Personal Data may be associated and/or processed.

"**Data Controller**" has the meaning given in GDPR (and, for the purpose of this DPA, means the party licensing and using the Service).

"**Data Processor**" has the meaning given in GDPR (and, for the purposes of this JDCA, COMLINK AB, co. reg. no. 556514-0190, Energigatan 10B, SE-434 37 Kungsbacka, Sweden).

"**Data Security Breach**" means accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access of Personal Data.

"**Data Subject**" means an individual who is the subject of Personal Data.

"**DPA**" means the Data Processing and Data Security Agreement together with its annexes, as supplemented and amended from time to time, as in effect between each of the Joint Data Controllers and the Data Processor.

"**EEA**" means the European Economic Area.

"**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each member state and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR.

"**GDPR**" means EU General Data Protection Regulation 2016/679.

"**JDCA**" means this joint data controller agreement between the Data Controller and each third part data controller (whom is also bound by the DPA), creating the legal framework between such Joint Data Controllers for delegated access to and shared use of Cloud Entities and the joint use and processing of (same) Personal Data.

"**Joint Data Controller**" has the meaning given in GDPR (and, for the purposes of this JDCA, the Data Controller and such third party (each a joint data controller) that under an arrangement are jointly determining the purposes and means of Processing of Personal Data in and for the Service).

"**Personal Data**" means any information relating to an identified or identifiable natural person, where 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.

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

"**Service**" mean the Data Processor's proprietary Software-as-a-Service and (as applicable) Cloud Sourcing services that are ordered by Data Controller through a link or via an order form and made available online by Data Processor, via the applicable subscriber login link and other web pages designated by Data Processor or Data Processor's reseller/channel partner.

"**Subscription Agreement**" means the agreement and terms and conditions under which the Data Controller is subscribing and granted licensing rights to use the Service.

"**Supervisory Authority**" means any Data Protection Supervisory Authority with competence over Data Controller, Joint Controllers, Data Processor and any sub-processor Processing of Personal Data.

1. GENERAL TERMS AND CONDITIONS

1.1 Subject to *GDPR Article 26*, where two or more Data Controllers jointly determine the purposes and means of Processing, they shall be Joint Data Controllers.

1.2 Joint Data Controllers shall determine their respective responsibilities for compliance with the obligations under GDPR, in particular as regards the exercising of the rights of the Data Subject and their respective duties to provide the information referred to in *GDPR Articles 13 and 14*, by means of an arrangement between the Joint Data Controllers unless, and in so far as, the respective responsibilities of the controllers are determined by Union or member state law to which the controllers are subject.

1.3 The arrangement referred to in Section 1.2 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.

1.4 Irrespective of the terms of the arrangement between the Joint Data Controllers, the data subject may exercise his or her rights under *GDPR* in respect of and against each of the Joint controllers.

1.5 The 'internal' distribution of responsibilities in the Joint Data Controller arrangement does not prevent the supervisory authority from exercising its powers vis-à-vis each of the Joint Data Controllers.

2. GENERAL DISTRIBUTION OF RESPONSIBILITIES AND LIABILITIES

2.1 The Joint Data Controllers agree that in connection with the use of the Service and Personal Data, they are Joint Data Controllers. The assessment shall take into account:

(a) All relevant Data Subjects that the Joint Data Controllers have access to and use for the Service and Personal Data

(b) In connection with the Joint Data Controllers' access to the Service and Personal Data, they have access to Personal Data of all relevant Data Subjects.

2.2 The Joint Data Controllers agree on the following joint rules and guidelines for the Joint Data Controllers' use of the Personal Data, including, as applicable, access restrictions for certain types of Personal Data.

2.3 The Joint Data Controllers acknowledge that they are bound by the DPA and that they have accepted the Data Processor (Comlink AB) for Processing of the Joint Data Controllers Service Data and Personal Data.

2.4 The Joint Data Controllers shall each have one designated contact point for Data Subjects, always provided that Data Subjects can exercise their rights under the *GDPR* vis-à-vis each individual Joint Data Controller.

2.5 The Joint Data Controllers are each responsible for the Data Subjects with whom the individual Joint Data Controller collects Personal Data, including the responsibility to inform the Data Subject of the Processing and the rights of the Data Subject;

(a) to ensure that the necessary authority exists for the Processing of the registered Personal Data, including the obtaining of consent, and

(b) that Personal Data is erased when they are no longer necessary.

2.6 Each Joint Data Controller who obtains specific data from sources other than the Data Subject is responsible for informing the Data Subject accordingly.

3. PRINCIPLES AND AUTHORITY TO PROCESS DATA

3.1 Each Joint Data Controller who obtains specific or sensitive data is responsible for ensuring that there is a valid legal ground for Processing and for documenting this to both Supervisory Authority and the Data Subject.

3.2 Each Joint Data Controller is responsible for compliance with the principles for the Processing, insofar as the

rules apply to the individual Joint Data Controller's areas of responsibilities.

4. RIGHTS OF THE DATA SUBJECTS

4.1 Each Joint Data Controller is responsible for ensuring the rights of the Data Subjects in accordance with the provisions of the *GDPR*, this JDCA and the DPA, including but not limited to;

(a) duty of disclosure when collecting Personal Data from the Data Subject,

(b) duty of disclosure if Personal Data are not collected from the Data Subject,

(c) right of access by the Data Subject,

(d) right to rectification,

(e) right to erasure (the right to be forgotten),

(f) right to restriction of Processing,

(g) notification obligation regarding rectification or erasure of Personal Data or restriction of Processing,

(h) right to data portability (but not for public authorities), and

(i) right to object to Processing.

4.2 If one of the Joint Data Controllers receives a request or inquiry from a Data Subject regarding matters covered by another Joint Data Controller's responsibilities, see above, the request is forwarded to such Joint Data Controller without undue delay.

4.3 Each Joint Data Controller is responsible for assisting each other to the extent this is relevant and necessary in order for both parties to comply with their obligations to the Data Subjects.

5. SECURITY OF PROCESSING AND PROOF OF COMPLIANCE WITH THE GDPR

5.1 Taking into account the nature, scope, context and purposes of Processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, each Joint Data Controller must implement appropriate technical and organisational measures and appropriate data protection policies to ensure and to be able to demonstrate that Processing is performed in accordance with the *GDPR*, DPA and the JDCA. Those measures must be reviewed and updated where necessary (*GDPR Article 24*). Each Joint Data Controller shall must have appropriate procedures for the handling of security breaches, requests for access and compliance with the duty of disclosure, in accordance with the *GDPR*, DPA and the JDCA.

5.2 The Joint Data Controllers are jointly responsible for compliance with the provision on data protection by design and by default in *GDPR Article 25*.

5.3 Each Data Controller is responsible for compliance with the requirement for security of Processing in *GDPR Article 32*. This involves that, taking into account 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, the Joint Data Controllers must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Consequently, each Joint Data Controller must make (and be able to document) a risk assessment, and subsequently implement measures to mitigate the risks identified.

6. USE OF DATA PROCESSORS AND SUB-PROCESSORS

The Data Controllers shall not be entitled to use other data processors and/or sub-processors than the Data Processor in connection with the use of the Service.

7. RECORDS

7.1 Each Joint Data Controller is responsible for compliance with the requirement for records of Processing activities in *GDPR Article 30*. Each Joint Data Controller shall prepare records of the Processing activities, for which the parties are Joint Data Controllers.

7.2 The Joint Data Controllers shall inform each other about the contents of the above records.

7.3 On the basis of the contents of each other's records, each Joint Data Controller shall prepare their own records of the Processing activities covered by this JDCA and the DPA.

8. NOTIFICATION OF A PERSONAL DATA BREACH TO THE SUPERVISORY AUTHORITY

8.1 Each Joint Data Controller is responsible for compliance with *GDPR Article 33* on notification of a Personal Data breach to the Supervisory Authority.

8.2 The Joint Data Controller with whom a Personal Data Breach was committed or from whom the reason for the breach originates is responsible for notifying the Personal Data Breach to the Supervisory Authority.

8.3 Immediately after having become aware of a Data Security Breach, the Joint Data Controller must inform the other Joint Data Controller of the breach. The other Joint Data Controller must be kept informed of the process after the discovery of the Personal Data breach and will receive a copy of the notification to the Supervisory Authority.

8.4 If the reason for the breach is not immediately attributable to one of the Joint Data Controllers, the (delegating)

Data Controller is responsible for notifying the Data Security Breach to the Supervisory Authority.

9. COMMUNICATION OF A PERSONAL DATA BREACH TO THE DATA SUBJECT

9.1 Each Joint Data Controller is responsible for compliance with *GDPR Article 34* on communication of a Personal Data breach to the Data Subject.

9.2 If a Personal Data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Joint Data Controller with whom the Personal Data Breach was committed, or from whom the reason for the breach originates is responsible for communicating the Personal Data Breach to the Data Subjects affected.

9.3 If the reason for a Personal Data Breach is not directly attributable to one of the Joint Data Controllers, and the breach is likely to result in a high risk to the rights and freedoms of natural persons, (original) Data Controller (being party to the DPA) is responsible for communicating the Personal Data Breach to Data Subjects affected.

10. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

10.1 Each Joint Data Controller is responsible for compliance with the requirement in *GDPR Article 35* on data protection impact assessment. Where a type of Processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the Processing, is likely to result in a high risk to the rights and freedoms of natural persons, the Joint Data Controllers must, prior to the Processing, carry out an assessment of the impact of the envisaged Processing operations on the protection of Personal Data.

10.2 Likewise, the Joint Data Controllers are obliged to comply with the requirement in *GDPR Article 36* on prior consultation of the Supervisory Authority when this is relevant.

11. TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

11.1 The Joint Data Controllers may decide that Personal Data can be transferred to third countries or international organisations.

11.2 Each Joint Data Controllers are responsible for compliance with the requirements in *GDPR Chapter V* if Personal Data are transferred to third countries or international organisations.

11.3 Each Joint Data Controller is responsible for its own Personal Data transfers to third countries, including for ensuring that a legal basis for transfer exists and that *GDPR Chapter V* has been observed.

12. COMPLAINTS

12.1 Each Data Controller is responsible for the handling of any complaints from Data Subjects if the complaints relate to the infringement of provisions in the *GDPR*, for which the Data Controller is responsible as given by this JDCA.

12.2 If one of the Joint Data Controllers receives a complaint which should rightfully be handled by the other Joint Data Controller, the complaint is forwarded to such Joint Data Controller without undue delay.

12.3 If one of the Joint Data Controllers receives a complaint, part of which should rightfully be handled by the other Joint Data Controller, such part is forwarded for reply by the Joint Data Controller without undue delay.

12.4 In connection with the forwarding of a complaint or part of a complaint to the other Joint Data Controller, the Data Subject must be notified about the essence of this JDCA between the Joint Data Controllers.

12.5 Generally, the Joint Data Controllers inform each other about all complaints received.

13. INFORMATION OF THE OTHER PARTIES

The Joint Data Controllers shall inform each other about matters of the essence to the joint Processing, this JDCA and the DPA.

14. COMMENCEMENT AND TERMINATION

14.1 The JDCA (agreement) shall enter into force at the time of both Joint Data Controllers' acceptance by means acceptable to the parties.

14.2 The JDCA shall be in force as long as relevant Personal Data for the Cloud Entity is being jointly processed, or until the arrangement is replaced by a new arrangement determining the distribution of responsibilities in connection with Processing.

14.3 The JDCA is terminated either by the delegating Data Controller by retracting the delegation or recipient by deleting the Cloud Entity from their account.

15. GOVERNING LAW AND JURISDICTION

15.1 This JDCA (agreement) shall be governed by the laws of the country within the EEA where the delegating Data Controller is registered or incorporated, and in the absence of such a country the substantive laws of Sweden shall apply, and the parties irrevocably submit to the exclusive jurisdiction of the courts of such jurisdiction and any court of appeal therefrom.

15.2 For the avoidance of doubt, this Section shall not be construed or interpreted as limiting Data Subjects rights to enforce their rights under the *GDPR*, such as to bring actions in other jurisdictions.

***