afa FÖRSÄKRING

Appendix 2

Data Processing Agreement
(the **”Data Processing Agreement”)**

Between:

(1) **Afa Försäkring tjänstepensionsaktiebolag** with company reg. no. 502033-0642, Klara Södra Kyrkogata 18, SE-111 52 Stockholm, Sweden (the **”Data Processor”**); and

(2) **THE USER COMPANY(COMPANIES)/ORGANISATION(S) THAT HAS (HAVE) ENTERED INTO THE ACCESS AGREEMENT, (**the **”Data controller”)**;

The Data Processor and the Data Controller are referred to separately as "**the Party**" and together as "**the Parties**".

Background:

A The Data Processor and the Data Controller have entered into an agreement for connection to the IA companies' occupational health and safety information system, including appendices (1) General Terms and Conditions (Appendix 1), Data Distribution Appendix (Appendix 3), Safety Appendix (Appendix 4) (the "**Access Agreement**"). This Agreement constitutes Appendix 2 of the Access Agreement.

B As part of its provision of Services under the terms of the Access Agreement, the Data Processor will Process Personal Data for which the Data Controller is responsible, as further specified in Appendix 2.1. This Data Processing Agreement sets out the terms and conditions on how the Data Processor shall Process Personal Data on behalf of the Data Controller

C Should any conflict arise between a clause in this Data Processing Agreement and a clause in the Access Agreement, the provisions in this Data Processing Agreement shall take precedence wherever the provision in this Data Processing Agreement provides greater protection for the Personal Data being Processed.

1. Definitions

In this Data Processing Agreement, the following definitions shall have the meaning set forth below:

"**Processing**", "**Data Controller**", "**Personal Data**", "**Data Processor**", **Personal Data Breach**", and "**Data Subject**" shall have the same meaning as in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ("**GDPR**");

"**Data Processing Agreement**" is this Data Processing Agreement and any appendices and annexes to it;

"**Applicable Legislation**" means legislation, regulations and directives in force at the time in the EU and in relevant Member States that are applicable to the Data Processor and the Data Controller; and

"**Applicable Personal Data Legislation**" means legislation, regulations and directives in force at the time, including directives notified by relevant supervisory authorities, with respect to the protection of privacy and fundamental rights and freedoms of individuals and, in particular, their right to the protection of their Personal Data with respect to the Processing of Personal Data applicable to the Data Processor and the Data Controller, including the GDPR; and

"**Third Country**" is a country outside the European Union (EU) or the European Economic Association (EEA).

2. Responsibilities of the Data Controller

2.1 The Data Controller determines the purposes and means of the Processing the Personal Data and is therefore responsible for the Processing. The Data Processor processes the Personal Data on behalf of the Data Controller and is therefore to be regarded as a data processor.

2.2 The Data Controller is *inter alia* responsible for ensuring that the Processing of the Personal Data is carried out in accordance with Applicable Legislation and that the Data Subjects are informed about the Processing.

2.3 The Data Processor does not have an obligation nor the technical means to check the accuracy or completeness of the Personal Data entered into the IA System. This obligation is the sole responsibility of the Data Controller.

3. Obligations of the Data Processor

3.1 The Data Processor undertakes to Process Personal Data only in accordance with the Data Controller's documented instructions and the provisions contained in this Data Processing Agreement and in the Access Agreement. The Data Processor shall not Process Personal Data for which the Data Controller is a Data Controller for any other purposes.

3.2 Should the Data Controller present new instructions that go beyond the provisions contained in this Data Processing Agreement or the Access Agreement and which are not necessary to comply with Applicable Legislation, the Data Processor shall be entitled to remuneration in accordance with the Data Processing Agreement's price list applicable from time to time, or as agreed between the Parties.

3.3 Notwithstanding what is stated in section 3.1 above, the Data Processor may Process Personal Data to the extent required to enable the Data Processor to fulfil its obligations under Applicable Legislation. However, the Data Processor is obligated to inform the Data Controller of the legal obligation, unless the Data Processor is prevented by Applicable Legislation from providing such information.

3.4 Notwithstanding the governing law provisions set forth in the Access Agreement, the Applicable Personal Data Legislation shall apply to the Processing of Personal Data that are subject to the terms of this Data Processing Agreement.

3.5 The Data Processor must notify the Data Controller if the Data Processor is unable to meet its obligations set forth in this Data Processing Agreement, or if the Data Processor considers that an instruction given by the Data Controller concerning the Processing of Personal Data would constitute a violation of Applicable Personal Data Legislation, unless the Data Processor is prevented by Applicable Legislation from providing such information to the Data Controller.

4. Security measures

4.1 Obligation to take technical and organisational measures to protect Personal Data

4.1.1 The Data Processor shall take appropriate technical and organisational measures to ensure that the Personal Data Processed are protected from Personal Data Breaches. The measures must ensure that at least the level of security required by Applicable Personal Data Legislation and by applicable regulations and guidelines of relevant supervisory authorities regarding data protection is in place.

4.1.2 Furthermore, the Data Processor must, if so requested, assist the Data Controller with information necessary to enable the Data Controller, as applicable, to be able to meet its obligations to carry out data protection impact assessments and prior consultations with relevant supervisory authorities concerning the Processing of Personal Data that are subject to the terms of this Data Processing Agreement. If the Data Controller requests the Data Processor to assist with a data protection impact assessment, even though there is no obligation under Applicable Personal Data Legislation to carry out such impact assessment, the Data Processor shall be entitled to remuneration as set out in the price list applicable from time to time.

4.1.3 The Parties agree that at least the technical and organisational measures specified in Appendix 4 of the Access Agreement (Security appendix IA system) must be implemented.

5. Personal Data Breach

5.1 Should a Personal Data Breach occur, the Data Processor must notify the Data Controller in writing of the breach without undue delay after the Data Processor has become aware of the Personal Data Breach.

5.2 If it is not unlikely that a Personal Data Breach poses a risk to the privacy of the Data Subjects, the Data Processor must, immediately after it has become aware of the Personal Data Breach, take all appropriate steps to prevent or minimise the potential adverse effects of the Personal Data Breach.

5.3 If requested by the Data Controller, the Data Processor shall provide:

5.3.1 a description of the Personal Data Breach’s nature, categories of and the number of Data Subjects affected, and categories of and the number of personal data affected;

5.3.2 the likely consequences of the Personal Data Breach; and

5.3.3 a description of the measures that the Data Processor, where appropriate, has already taken or intends to take to correct the Personal Data Breach and/or to minimise the potential adverse effects of the Personal Data Breach.

Should it not be possible for the Data Processor to provide the information in one go, the information may be provided in phases without any further undue delay. The Data Processor shall be entitled to compensation for any expenses incurred as a result of the Data Processor providing information as set forth in this section 5.3, if the Data Breach is due to circumstances over which the Data Processor had no control.

6. Access to information and the right to audit

6.1 The Data Processor shall continuously document the measures taken by the Data Processor in order to meet its obligations as set forth in this Data Processing Agreement. The Data Controller may request to see a copy of the latest version of such documentation.

6.2 The Data Processor must give the Data Controller access to all information necessary to show that the Data Processor has met its obligations set forth in Article 28 of the GDPR. Furthermore, the Data Processor must enable and assist with audits, including inspections performed by the Data Controller. For the avoidance of doubt, such an inspection shall only apply to information that is strictly necessary to enable the Data Controller to be able to determine whether the Data Processor has met its obligations set forth in Article 28 of the GDPR and must, under no circumstances, extend to any other information concerning the business activities of the Data Processor, which have no relevance to the Data Processor's Processing of Personal Data on behalf of the Data Controller. The Parties agree that an inspection must be carried out by a third party approved by both Parties and that inspection costs are the responsibility of the Data Controller. The Data Controller must ensure that such third party is bound by obligations of confidentiality in relation to all information acquired or received by the third party for the purposes of the inspection, and that such obligations of confidentiality are no less restrictive than the obligations of confidentiality in section 7.6 below.

6.3 Neither Party has the right to represent the other Party before the Supervisory Authority or before any other third party.

7. Engaging Sub-processors

7.1 The Data Processor may engage sub-processors for the Processing of Personal Data on behalf of the Data Controller ("**Sub-processors**").

7.2 If the Data Processor engages a Sub-processor, the Data Controller gives a general approval for the Data Processor to enter into a data processing agreement directly with the Sub-processor. The obligations under such data processing agreement with the Sub-processor shall be equal to and no less restrictive than those under this Data Processing Agreement. The Data Controller accepts that the Data Processor and the Sub-processor enter into the Sub-processor's standard agreement for processor of personal data when circumstances so require, provided that such a standard agreement complies with the obligations stipulated in Applicable Personal Data Legislation.

7.3 The Sub-processors that Process Personal Data on behalf of the Data Controller must be stated in https://www.iasystemet.se/en/sub-processors.

7.4 If the Data Processor intends to engage a new Sub-processor, the Data Processor must notify the Data Controller of this in writing without undue delay. Information about a new Sub-processor will be published on https://iasystemet.se/en/amendments-and-additions-to-the-access-agreements/ ninety (90) days before the change enters into force.

7.5 With respect to engaging new Sub-processors, the Data Controller is entitled to make objections to the engagement of the Sub-processor. The Data Processor also has the right to terminate the Access Agreement up and until the day on which the change of Sub-processor enters into force by notifying the Data Controller in writing. Continued use of the IA System after the change of the new Sub-processor has entered into force means that the change in Sub-processors is considered to have been accepted by the Data Controller.

7.6 The Data Processor shall remain liable to the Data Controller for the performance of the Sub-processor's obligations.

8. Confidentiality

8.1 Without prejudice to any confidentiality undertakings in the Access Agreement, the Data Processor agrees to keep all Personal Data that is Processed on behalf of the Data Controller strictly confidential. Accordingly, the Data Processor will not, neither directly nor indirectly, disclose any Personal Data to any third party without the prior written authorization of the Data Controller, unless the Data Processor has an obligation under Applicable Legislation or a decision by a court or authority to disclose the Personal Data, or if necessary to fulfil the obligations of the Access Agreement or this Data Processing Agreement. The Data Processor shall notify the Data Controller if Personal Data is disclosed to a third party, unless prevented from so doing by Applicable Legislation or a decision by a court or authority.

8.2 The Data Processor accepts that the confidentiality undertaking as defined in section 8.1 shall survive the termination of this Data Processing Agreement and remain in force until all Personal Data have been returned to the Data Controller or, upon the Data Controller's written request, have been securely and irreversibly destroyed or anonymised as defined in section 11 below.

8.3 The Data Controller agrees to keep all information that the Data Controller receives about the Data Processor's security measures, procedures, IT systems and any other information of a confidential nature strictly confidential and not to disclose to any third party any confidential information originating from or provided by the Data Processor or its Sub-processors. The Data Controller may only disclose such information that the Data Controller is required to disclose under Applicable Legislation or under the terms of the Access Agreement or this Data Processing Agreement. The Data Controller accepts that this confidentiality undertaking shall survive the termination of this Data Processing Agreement.

8.4 The Data Processor's duty of confidentiality in accordance with this section 8 includes both a confidentiality obligation and an obligation not to disclose any information received. The Data Processor shall ensure that all of the Data Processor's personnel who are authorized to access the Personal Data are bound by this confidentiality undertaking. The same obligation shall apply in cases where the Data Processor engages Sub-processors for the Processing of Personal Data.

9. Liability

9.1 The Parties are liable jointly and severally in relation to claims from data subjects relating to the Processing of the data subject's Personal Data. The Party compensating the data subject shall have a right to recourse in accordance with the provisions under Article 82 of the GDPR. The Data Processor's liability under this section 9.1 shall, however, be limited to a maximum amount of compensation in accordance with the Access Agreement.

9.2 The Parties acknowledge and agree that neither Party shall have an obligation to indemnify the other Party for any administrative fines imposed by a supervisory authority or court under Applicable Personal Data Legislation.

10. Rights of Data Subjects

The Data Processor shall, to the extent possible, assist the Data Controller by taking appropriate technical and organisational measures that are necessary for the fulfilment of the Data Controller's obligation to respond to requests for the exercise of a Data Subject's right as laid down by Applicable Personal Data Legislation. The Data Processor shall be entitled to compensation for such assistance according to the rates stated in the price list applicable from time to time.

11. Return of Personal Data

Upon termination of the Access Agreement, the Data Controller shall instruct the Data Processor in writing if the Personal Data that the Data Processor has Processed on behalf of the Data Controller for the purposes of this Data Processing Agreement shall be (i) returned to the Data Controller or (ii) irreversibly deleted. If the Data Controller does not provide such instructions within thirty (30) days of the termination or expiration of the Access Agreement, the Data Processor shall irreversibly delete the Personal Data without undue delay.

12. Transfers to and processing of Personal Data in a Third Country

12.1 The Data Processor has the right to transfer Personal Data belonging to the Data Controller to a Third Country only if any of the following conditions are met:

12.1.1 the Third Country guarantees an adequate level of protection for Personal Data according to a decision issued by the EU Commission;

12.1.2 there are appropriate safeguards in place in accordance with Applicable Personal Data Legislation, e.g. standard data protection clauses adopted by the EU Commission, covering the transfer and Processing of the Personal Data as well as other necessary protective measures required in the individual case; or

12.1.3 it is possible to rely on another exemption for the transfer of Personal Data under Applicable Personal Data Legislation

12.2 For the avoidance of doubt, Personal Data may not be transferred to or Processed in a Third Country if none of the conditions in section 12.1 above apply. Where data are transferred in accordance with section 12.1.3, the Personal Data may be transferred to the Third Country only to the extent that the applicable exemption covers the transfer and the Processing of Personal Data.

12.3 If the Data processor intends to transfer Personal Data to a third country, the Data Processor shall, before such transfer take place, inform the Data Controller of this.

12.4 Should the Data Controller's branches or Group companies outside the EU/EEA obtain access to Personal Data in the IA System as stated in the Access Agreement, or if the Data Controller obtains access in any other way to the Personal Data in a Third Country, the Data Controller understands and accepts that the Data Controller is transferring the Personal Data to a Third Country. The Data Controller must therefore, in such a case, ensure adequate protection for the Personal Data by, for example, entering into standard data protection clauses adopted by the EU Commission with the receiving party. For the avoidance of doubt, the Data Processor is not liable

for transfers, in accordance with this section 12.4, being allowed under Applicable Personal Data Legislation.

13. Terms and termination

13.1 This Data Processing Agreement shall become effective upon signing the Access Agreement and shall remain effective throughout the term of the Access Agreement or throughout the longer period in which the Data Processor Processes Personal Data on behalf of the Data Controller.

13.2 This Data Processing Agreement shall survive termination the termination of the Access Agreement and shall and shall remain effective until the Data Processor (and Sub-processor(s) hired by the Data Processor) cease to Process Personal Data on behalf of the Data Controller.

14. Non-assignment

Neither Party may assign, in full or in part, its rights or obligations under this Data Processing Agreement without the written consent of the other Party.

15. Amendments and additions

The provisions relating to amendments and additions set forth in the Access Agreement shall apply correspondingly to this Data Processing Agreement.

16. Governing law and dispute resolution

The provisions relating to governing law and dispute resolution set forth in the Access Agreement shall apply correspondingly to this Data Processing Agreement.

Appendix 2.1

Description of the processing of Personal Data Subject to this Data Processing Agreement

This Appendix 2.1 shall form an integral part of the Data Processing Agreement

Categories of Data Subjects	*The following categories of Data Subjects' Personal Data will be Processed under this Data Processing Agreement:* • *Individuals with occupational injuries* • *Contact persons* • *Users of the service*
Categories of Personal Data	*The following categories of Personal Data are processed:* • Personal id. no. of individuals with occupational injuries • Contact details of individuals with occupational injuries, contact persons and users • Information about occupational injury incident
Purpose of the Processing	*The Personal Data is processed for the following purposes:* • *to provide the Services set forth in the Access Agreement;* • *to meet other obligations that the Data Processor has under the terms of the Access Agreement and this Data Processing Agreement*
Processing of Personal Data	*The Personal Data will be Processed as follows:* • *Collection* • *Storage* • *Disclosure by transferring Personal Data to the Swedish Social Insurance Agency (Sw: Försäkringskassan) (LAF report)* • *Disclosure by transferring Personal Data to the Swedish Work Environment Authority (Sw: Arbetsmiljöverket) (LAF report, 3:3a)* • *Disclosure by transferring Personal Data to AFA Försäkring (TFA report)* • *Erasure*
Storage of Personal Data	The Personal Data will be retained according to the periods specified by the Data Controller in the service
Geographical location of processing	The Data Processor Processes the Personal Data in Sweden. The geographical location of any Sub-processor's Processing of Personal Data are described on https://www.iasystemet.se/en/sub-processors