

PERSONAL DATA PROCESSOR AGREEMENT

("the Personal Data Processor Agreement")

BETWEEN:

- (1) **AFA TRYGGHETSFÖRSÄKRINGSAKTIEBOLAG**, 516401-8615, Klara Södra Kyrkogata 18, SE-111 52 Stockholm, Sweden ("the Personal Data Processor"); and
- (2) **THE USER COMPANY(COMPANIES)/ORGANISATION(S) THAT HAS (HAVE) ENTERED INTO THE ACCESS AGREEMENT**, ("the Personal Data Controller");

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

BACKGROUND:

- A The Personal Data Processor and the Personal 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, (3) Data Distribution for the IA companies' occupational health and safety information system, (4) Service Level Agreement and (5) Information for contact persons about personal data processing ("**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 Personal Data Processor will process personal data for which the Personal Data Controller is responsible, as specified in more detail in Appendix 1. This Personal Data Processor Agreement sets out the terms and conditions on how the Personal Data Processor shall process personal data on behalf of the Personal Data Controller.
- C Should any conflict arise between a clause in this Personal Data Processor Agreement and a clause in the Access Agreement, the provisions in this Personal Data Processor Agreement shall take precedence wherever the provision in this Personal Data Processor Agreement provides greater protection for the Personal Data being processed.

1. DEFINITIONS

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

"**Processing**", "**Personal Data Controller**", "**Personal Data**", "**Personal Data Processor**", "**Personal Data Incident**", 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**");

"**Personal Data Processor Agreement**" is this Personal Data Processor 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 Personal Data Processor and the Personal 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 Personal Data Processor and the Personal Data Controller, including legislation, regulations and directives within the meaning of Directive 95/46/EC and, from 25 May 2018, the GDPR; and

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

2. RESPONSIBILITIES OF THE PERSONAL DATA CONTROLLER

- 2.1 The Personal Data Controller determines the purpose and means of the Processing the the Personal Data and is therefore responsible for the Processing. The Personal Data Processor carries out processing of the Personal Data on behalf of the Personal Data Controller and is therefore to be regarded as a personal data processor.
- 2.2 The Personal Data Controller is 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 Personal 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 Personal Data Controller.

3. OBLIGATIONS OF THE PERSONAL DATA PROCESSOR

- 3.1 The Personal Data Processor undertakes to process personal data only in compliance with the Personal Data Controller's documented instructions and the provisions contained in this Personal Data Processor Agreement and in the Access Agreement. The Personal Data Processor must not process personal data for which the Personal Data Controller is a Personal Data Controller for any other purposes.
- 3.2 Should the Personal Data Controller present new instructions that go beyond the provisions contained in this Personal Data Processor Agreement or the Access Agreement, the Personal Data Processor shall be entitled to remuneration in accordance with the Personal Data Processor Agreement's price list in force at the time, or as agreed between the Parties.
- 3.3 Notwithstanding what is stated in paragraph 3.1 above, the Personal Data Processor may process personal data to the extent required to enable the Personal Data Processor to meet its obligations as the Personal Data Processor and which apply under Applicable Legislation in force at the time. However, it is the responsibility of the Personal Data Processor to inform the Personal Data Controller of the legal obligation, unless the Personal 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 Personal Data Processor Agreement.

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

4. SECURITY MEASURES

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

- 4.1.1 The Personal Data Processor takes appropriate technical and organisational measures to ensure that the Personal Data that are processed are protected from Personal Data Incidents. 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 for personal data security is in place.
- 4.1.2 Furthermore, the Personal Data Processor must, if so requested, assist the Personal Data Controller with information necessary to enable the Personal Data Controller, as applicable, to be able to meet its obligations to carry out an impact analysis and pre-consultation discussion meetings with relevant supervisory authorities concerning the Processing of Personal Data that are subject to the terms of this Personal Data Processor Agreement. If the Personal Data Controller requests the Personal Data Processor to assist with an impact analysis, even though there is no obligation under Applicable Personal Data Legislation to carry out an impact analysis, the Personal Data Processor shall be entitled to remuneration as set out in the price list in force at the time.
- 4.1.3 The Parties agree that at least the technical and organisational measures specified in Appendix 2 must be implemented.

4.2 Personal Data Incident

- 4.2.1 Should a Personal Data Incident occur, the Personal Data Processor must notify the Personal Data Controller in writing of the breach without undue delay after the Personal Data Processor has become aware of the Personal Data Incident.
- 4.2.2 If it is not unlikely that a Personal Data Incident poses a risk to the privacy of the Data Subjects, the Personal Data Processor must, immediately after it has become aware of the Personal Data Incident, take all appropriate steps to prevent or minimise the potential negative consequences of the Personal Data Incident.
- 4.2.3 If requested by the Personal Data Controller, the Personal Data Processor shall provide:
- 4.2.3.1 a description of the Personal Data Incident's nature, categories of and the number of Data Subjects affected, and categories of and the number of personal data items affected;
 - 4.2.3.2 the likely consequences of the Personal Data Incident; and
 - 4.2.3.3 a description of the measures that the Personal Data Processor, where appropriate, has already taken or intends to take to correct the

Personal Data Incident and/or to minimise the potential negative consequences of the Personal Data Incident.

Should it not be possible for the Personal Data Processor to provide the information in one go, the information may be provided in batches without any further undue delay. The Personal Data Processor shall be entitled to compensation for any expenses incurred as a result of the Personal Data Processor providing information as set forth in this paragraph 4.2.3.

4.3 Access to Personal Data, etc.

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

4.3.2 The Personal Data Processor must give the Personal Data Controller access to all information necessary to show that the Personal Data Processor has met its obligations set forth in Article 28 of the General Data Protection Regulation. Furthermore, the Personal Data Processor must enable and assist with reviews, including inspections performed by the Personal Data Controller. To avoid misunderstandings, such an inspection must only extend to information that is absolutely essential to enable the Personal Data Controller to be able to determine whether the Personal Data Processor has met its obligations set forth in Article 28 of the General Data Protection Regulation and must, under no circumstances, extend to any other information concerning the business activities of the Personal Data Processor, which have no relevance to the Personal Data Processor's processing of personal data on behalf of the Personal 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 Personal Data Controller. The Personal 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 paragraph 5.6 below.

4.3.3 Neither Party has the right to represent itself as an agent of the other Party to the Swedish Data Protection Authority (Datainspektionen) or to any other third party.

5. HIRING SUBCONTRACTORS

5.1 The Personal Data Processor may hire subcontractors, consultants or other third parties for the Processing of Personal Data on behalf of the Personal Data Controller ("**Subcontractor**").

5.2 If the Personal Data Processor hires a Subcontractor, the Personal Data Controller consents to the Personal Data Processor entering into a Personal Data Processor Agreement directly with the Subcontractor. The obligations under such Personal Data Processor Agreement with the Subcontractor shall be equal to and no less restrictive than those under this Personal Data Processor Agreement. The Personal Data Controller accepts that the Personal Data Processor and the Subcontractor enter into the Subcontractor's standard agreement for personal data processing when circumstances so require, on condition that such a standard agreement meets the requirements stipulated in Applicable Personal Data Protection Legislation.

5.3 Should the Personal Data Processor hire a Subcontractor, the Personal Data Processor must notify the Personal Data Controller in writing without undue delay of the following:

- 5.3.1 The Subcontractor's identity (including details of the company's name, organisation number and address);
 - 5.3.2 the type of service performed by the Subcontractor; and
 - 5.3.3 at which location the Subcontractor will be Processing Personal Data on behalf of the Personal Data Controller.
- 5.4 With respect to hiring new Subcontractors, the Personal Data Controller is entitled to make objections to the hiring of the Subcontractor.
- 5.5 At the request of the Personal Data Controller, the Personal Data Processor must provide, in addition to the information stated in paragraph 5.3 above, a copy of the personal data processing agreement that the Personal Data Processor has entered into with the Subcontractor as stated in paragraph 5.2 above.
- 5.6 The Personal Data Processor is liable to the Personal Data Controller for the Subcontractor's Processing of Personal Data and on its own behalf.

6. CONFIDENTIALITY

- 6.1 Without prejudice to the application of any obligations of confidentiality in the Access Agreement, the Personal Data Processor agrees to keep all Personal Data that is processed on behalf of the Personal Data Controller strictly confidential. Accordingly, the Personal Data Processor will not, either directly or indirectly, divulge, disclose or communicate any Personal Data to any third party without the prior written consent of the Personal Data Controller, unless the Personal Data Processor has an obligation under Applicable Legislation or a decision by a court or authority to provide the Personal Data, or where this is necessary in the fulfilment of the requirements of the Access Agreement or this Personal Data Processor Agreement. The Personal Data Processor shall notify the Personal Data Controller if Personal Data is provided to a third party, unless prevented from so doing by Applicable Legislation or a decision by a court or authority.
- 6.2 The Personal Data Processor accepts that the obligation of confidentiality as defined in paragraph 6.1 shall remain in force even following the termination of the Personal Data Processing Agreement and until all Personal Data have been provided to the Personal Data Controller or, following a written request from the Personal Data Controller, have been securely and irreversibly destroyed or anonymised as defined in paragraph 9 below.
- 6.3 The Personal Data Controller agrees to keep all information that the Personal Data Controller receives about the Personal 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 Personal Data Processor or its Subcontractors. The Personal Data Controller may only disclose such information that the Personal Data Controller is required to disclose under Applicable Legislation or under the terms of the Access Agreement or this Personal Data Processor Agreement. The Personal Data Controller accepts that this obligation of confidentiality remains in force even after this Personal Data Processor Agreement is terminated or otherwise ceases to be in effect.

7. LIABILITY

- 7.1 The Personal Data Processor shall indemnify the Personal Data Controller against any and all liability, loss, claim or expenses that it incurs which has been caused by the Personal Data

Processor, either intentionally or through gross negligence, processing personal data in breach of the terms of the Access Agreement or Applicable Personal Data Protection Legislation.

7.2 The liability of the Personal Data Processor as defined in paragraph 7.1 is, however, limited to liability for direct loss or damage to a sum per incident and year equal to the base amount set by the Swedish Social Insurance Code (Socialförsäkringsbalken) that applies at the time of the incident.

7.3 The Personal Data Controller shall hold the Personal Data Processor harmless from any and all liability, loss, claim or expenses that the Personal Data Processor incurs as a result of the Personal Data Controller Processing Personal Data in breach of the terms of the Access Agreement or Applicable Personal Data Protection Legislation.

8. RIGHTS OF DATA SUBJECTS

The Personal Data Processor shall, to the extent possible, assist the Personal Data Controller by taking all and any technical and organisational measures that are necessary to enable the Personal Data Controller to meet its obligation to respond to a request for the exercise of a Data Subject's right according to the rights of data subjects as required by the Applicable Personal Data Protection Regulation. The Personal Data Processor shall be entitled to compensation for any expenses that such assistance incurs at the rates stated on the price list in force at the time.

9. RETURN OF PERSONAL DATA

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

10. TRANSFERS TO AND PROCESSING OF PERSONAL DATA IN A THIRD COUNTRY

10.1 The Personal Data Processor may not transfer personal data that belongs to the Personal Data Controller to a Third Country without the prior written consent of the Personal Data Controller.

10.2 Should the Personal Data Controller's affiliates 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 Personal Data Controller obtains access in any other way to the Personal Data in a Third Country, the Personal Data Controller understands and accepts that the Personal Data Controller is transferring the Personal Data to a Third Country. The Personal Data Controller must therefore, in such a case, ensure adequate protection is in place by, for example, including standard data protection clauses adopted by the European Commission together with the receiving party. To avoid any misunderstanding, the Personal Data Processor is not liable for transfers, in accordance with this paragraph 10.2, being allowed under Applicable Personal Data Legislation.

11. TERM AND TERMINATION OF THE AGREEMENT

11.1 This Personal Data Processor Agreement shall become effective upon signing and shall remain effective throughout the term of the Access Agreement or throughout the longer period

in which the Personal Data Processor processes personal data on behalf of the Personal Data Controller.

- 11.2 The Personal Data Processor Agreement shall be effective even if the Access Agreement terminates or ceases to be in effect, and shall remain effective until the Personal Data Processor (and Subcontractor(s) hired by the Personal Data Processor) cease to process personal data on behalf of the Personal Data Controller.

12. TRANSFERS

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

13. AMENDMENTS AND ADDITIONS

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

14. APPLICABLE LAW AND LITIGATION

The provisions relating to applicable law and litigation set forth in the Access Agreement shall apply correspondingly to this Personal Data Processor Agreement.

Appendix 2.1

DESCRIPTION OF THE PROCESSING OF PERSONAL DATA THAT ARE SUBJECT TO THE TERMS OF THE PERSONAL DATA PROCESSING AGREEMENT

This Appendix 2.1 shall be deemed to form an integral part of the Personal Data Processor Agreement.

<i>Categories of Data Subjects</i>	<p>The following categories of Data Subjects are affected by the Processing of Personal Data that are subject to the terms of the Personal Data Processor Agreement:</p> <ul style="list-style-type: none">• Persons with occupational injuries• Contact Persons• Users of the service
<i>Categories of Personal Data</i>	<p>The following categories of personal data are processed:</p> <ul style="list-style-type: none">• Contact information for persons with occupational injury, contact person and users• Information about occupational injury incident
<i>Purpose of the Processing</i>	<p>The Personal Data is processed for the following purposes:</p> <ul style="list-style-type: none">• to provide the Services set forth in the Access Agreement;• to meet other obligations that the Personal Data Processor has under the terms of the Access Agreement and this Personal Data Processor Agreement
<i>Processing of Personal Data</i>	<p>The Personal Data will be processed as follows:</p> <ul style="list-style-type: none">• Collection• Storage• Erasure
<i>Storage of Personal Data</i>	<p>The personal data will be retained according to the timetables specified by the Data protection administrator in the service</p>