For use where no pre-existing Salesforce org

Data Processing Addendum

This Data Processing Addendum ("**Addendum**") is entered into on the Effective Date by and between:

(1) **SIRENUM LIMITED**, a company incorporated in England and Wales with company no. 08749533, whose registered office is at First Floor, Winston House, 349 Regents Park Road, London, United Kingdom, N3 1DH ("**Sirenum**"); and

(2) **the Client** (as defined in Clause 1 below),

each a "**Party**" and collectively the "**Parties**".

Introduction

A. Sirenum and the Client have entered into an agreement under which Sirenum provides certain staff management software-as-a-service to the Client using Sirenum's platform hosted on a salesforce org.

B. The Client is a Controller of Client Personal Data. Sirenum Processes Client Personal Data as a Processor in connection with its performance of the Agreement.

C. The Parties have entered into this Addendum to ensure that the Processing of Client Personal Data is in accordance with Data Protection Laws and Regulations.

Agreement

The Parties hereby agree that the terms and conditions set out below shall apply to the Processing of Client Personal Data in connection with the performance of the Agreement.

1. DEFINITIONS

In this Addendum the following words and expressions have the following meanings:

"Agreement" means the agreement entered into either prior to or at or around the Effective Date under which Sirenum contracts to provide to the Client certain staff management software-as-service to the Client alongside certain ancillary configuration, set-up and support services.

"**Authorised Affiliate**" means any of Client's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement, but has not signed its own agreement with Sirenum and is not a "Client" as defined under this Addendum.

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, and its implementing regulations.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"**Client**" means the Client together with its Affiliates (for so long as they remain Affiliates) which have signed the Agreement and/or any order form pursuant to the Agreement.

"Client Personal Data" means any Client Data (as described in Schedule One of this Addendum (Introduction) that is Personal Data and that is processed by Sirenum on behalf of the Client in the course of performing the Services, as described in more detail in Schedule One. Client Personal Data excludes Personal Data with respect to which Sirenum is a data controller (such as, but not limited to, business contact information relating to the Client's personnel and representatives used for the purposes of entering into and performing the Agreement, communicating with the Client in connection with the Agreement, setting up Accounts and invoicing and receiving payments of the Fees);

"Data Protection Laws and Regulations" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom and the United States and its states, applicable to the Processing of Personal Data under the Agreement.

"Data Subject" means the identified or identifiable person to whom Personal Data relates.

"Effective Date" means that the date that the Client signs this Addendum, or 10 business days after this Addendum is sent to the Client (in each case as indicated in Sirenum's records), whichever is the earlier;

"**GDPR**" means the 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).

"Personal Data" means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Client Personal Data.

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

"Processor" means the entity which Processes Personal Data on behalf of the Controller, including as applicable any "service provider" as that term is defined by the CCPA.

"Salesforce Processor BCR" means SFDC's processor binding corporate rules for the Processing of Personal Data, the most current version of which is available on SFDC's website, currently located at https://www.salesforce.com/company/privacy, which govern transfers of Personal Data to third countries to and between members of the Salesforce Group, and to third-party Sub-processors.

"Security, Privacy and Architecture Documentation" means SFDC's Security, Privacy and Architecture Documentation applicable to the specific Services purchased by Client, as updated from time to time, and accessible via SFDC's Trust and Compliance webpage at https://trust.salesforce.com/en/trust-and-compliance-documentation/ (also accessible via http://www.salesforce.com/company/legal/agreements under the "Trust and Compliance Documentation" link), or as otherwise made reasonably available by SFDC.

"Services" means any services that Sirenum provides to the Client, or has an obligation to provide to the Client, under the Agreement.

"SFDC" means Salesforce UK Limited (f/k/a salesforce.com EMEA Limited), a company registered in England and Wales.

"SFDC Group" means SFDC and its Affiliates engaged in the Processing of Personal Data.

"Standard Contractual Clauses" means the standard contractual clauses adopted pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection (as published here: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0087&from=en or such other location from time to time.

"Sub-processor" means any Processor engaged by Sirenum.

"**Supervisory Authority**" means an independent public authority which is established by an EU Member State pursuant to the GDPR.

"**User**" means individuals authorised by the Client or the Client's clients or their affiliates to access and use the Services.

"**Withdrawal Agreement**" means the Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community between the United Kingdom and European Union dated 19 October 2019.

2. EFFECT OF THIS ADDENDUM

2.1 This Addendum supplements the Agreement and shall form a binding part of the Agreement with effect from the Effective Date.

2.2 This Addendum shall apply to all Processing of Client Personal Data that Sirenum carries out as a Processor in connection with the performance of the Agreement. Sirenum shall not have any obligations under this Addendum in relation to any Client Personal Data in respect of which Sirenum is or becomes a Controller.

2.3 Except as modified in this Addendum, the Agreement shall remain in full force and effect.

2.4 The provisions of this Addendum shall extinguish and replace any provisions contained in the Agreement

relating to the Processing of Client Personal Data.

2.5 In the event of any conflict or inconsistency between the provisions of this Addendum and the Agreement, the provisions of this Addendum shall prevail with regard to the Parties' obligations, rights and liability in connection with the Processing of Client Personal Data.

3. PROCESSING OF PERSONAL DATA

3.1 **Roles of the Parties.** The parties acknowledge and agree that with regard to the Processing of Client Personal Data, Client is the Controller, Sirenum is the Processor and that Sirenum will engage Sub-processors pursuant to the requirements set forth in Paragraph 5 (Sub-processors) below. The Client acknowledges and agrees that SFDC is Sirenum's primary Sub-processor and the majority of Client Personal Data is processed in the course of the Services by SFDC. This Addendum therefore provides appropriate detail relating to SFDC's Processing but the Client acknowledges that this Processing is carried out as Sirenum's Sub-processor and not as a direct Processor of the Client.

3.2 **Client's Processing of Client Personal Data.** Client shall, in its use of the Services, Process Client Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including any applicable requirement to provide notice to Data Subjects of the use of Sirenum as Processor. For the avoidance of doubt, Client's instructions for the Processing of Client Personal Data shall comply with Data Protection Laws and Regulations. Client shall have sole responsibility for the accuracy, quality, and legality of Client Personal Data and the means by which Client acquired Client Personal Data. Client specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Client Personal Data, to the extent applicable under the CCPA (if applicable). Sirenum shall notify the Client as soon as practicable if Sirenum considers that an instruction from the Client infringes applicable Data Protection Laws and Regulations.

3.3 **Sirenum's Processing of Personal Data.** Sirenum shall treat Client Personal Data as Confidential Information and shall Process Client Personal Data on behalf of and only in accordance with Client's documented instructions for the following purposes: (i) Processing in accordance with the Agreement; (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Client (e.g., via email) where such instructions are consistent with the terms of the Agreement. Notwithstanding anything else in this Addendum, the Client acknowledges and agrees that Sirenum may Process the Client Personal Data otherwise than in accordance with the Client's instructions if and to the extent that it is required by any applicable law to which it is subject to Process the Client Personal Data otherwise than in accordance with the Client's instructions, provided that Sirenum informs the Client of that legal requirement before carrying out such Processing unless prohibited by that law from doing so.

3.4 **Details of the Processing.** The subject-matter of Processing of Client Personal Data by Sirenum is the performance of the Services pursuant to the Agreement. The nature and purpose of the Processing, the types of Client Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule One to this Addendum. The duration of the Processing is for the duration of the Agreement.

3.5 **Assistance**. Sirenum shall assist the Client in ensuring compliance with the obligations relating to the security of processing of personal data, the notification of personal data breaches to the supervisory authority, the communication of personal data breaches to the data subject, data protection impact assessments and prior consultation in relation to high-risk processing under the Data Protection Laws and Regulations in respect of the Client Personal Data to the extent Client does not otherwise have access to the relevant information, and to the extent such information is available to Sirenum. Sirenum may charge the Client at its standard time-based charging rates for any work performed by Sirenum at the request of the Client pursuant to this Paragraph 3.5, except where such work is necessitated by a breach by Sirenum of its obligations under this Addendum.

3.6 **General compliance with data protection laws.** Without prejudice to Paragraph 3.2, each party shall comply with the Data Protection Laws and Regulations with respect to the processing of the Client Personal Data and other Personal Data obtained in connection with the Agreement.

3.7 **Changes to data protection laws.** If any changes or prospective changes to the Data Protection Laws and Regulations result or will result in one or both parties not complying with the Data Protection Laws and

Regulations in relation to processing of Client Personal Data carried out under the Agreement, then the parties shall use their best endeavours promptly to agree such variations to the Agreement as may be necessary to remedy such non-compliance.

4. RIGHTS OF DATA SUBJECTS

Data Subject Request. Sirenum shall, to the extent legally permitted, promptly notify Client if Sirenum receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making, each such request being a "**Data Subject Request**". Taking into account the nature of the Processing, Sirenum shall assist Client by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Client's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, Sirenum shall upon Client's request provide commercially reasonable efforts to assist Client in responding to such Data Subject Request, to the extent Sirenum is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Sirenum may charge the Client at its standard time-based charging rates for any work performed by Sirenum at the request of the Client in connection with responding to such requests where Sirenum makes automated tools available to the Client via the Services that enable the Client to respond to such requests itself.

5. SIRENUM PERSONNEL

5.1 **Confidentiality.** Sirenum shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Sirenum shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

5.2 **Reliability.** Sirenum shall take commercially reasonable steps to ensure the reliability of any Sirenum personnel engaged in the Processing of Personal Data.

5.3 **Limitation of Access.** Sirenum shall ensure that Sirenum's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

5.4 **Data Protection Officer.** Sirenum has appointed a manager with responsibility for data protection. The appointed person may be reached at privacy@sirenum.com.

6. SUB-PROCESSORS

6.1 **Appointment of Sub-processors.** Sirenum must not engage any third party to process the Client Personal Data without the prior specific or general written authorisation of the Client**.** The Client acknowledges and agrees that Sirenum may engage third-party Sub-processors in connection with the provision of the Services in accordance with this Paragraph 5. Sirenum shall ensure that each third party Sub-processor it engages to process Client Personal Data is engaged pursuant to a written agreement containing obligations no less protective as those imposed on Sirenum by this Addendum with respect to the protection of Client Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor.

6.2 **List of Current Sub-processors and Notification of New Sub-processors**:

6.2.1 **Sirenum-appointed Sub-processors**: Paragraph 5 of Schedule One of this Addendum contains the current list of Sub-processors engaged by Sirenum. Sirenum shall inform the Client at least 14 days in advance of any intended changes concerning the addition or replacement of any third party Sub-processor after the Effective Date.

6.2.2 **SFDC-appointed Sub-processors:** the current list of Sub-processors engaged by SFDC are set out here: https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/misc/salesforce-infrastructure-and-subprocessors.pdf. Client may find on Sirenum's Trust and Compliance webpage (also accessible via http://www.salesforce.com/company/legal/agreements.jsp under the "Trust and Compliance Documentation" link) the Infrastructure and Sub-processor Documentation as well as a mechanism to subscribe to notifications of new Sub-processors for each applicable Service; Sirenum will subscribe to this service and Sirenum will relay to the Client details of any new Sub-

processor(s) proposed by SFDC.

6.3 **Objection Right for New Sub-processors.** Client may object to Sirenum's or SFDC's use of a new Sub-processor by notifying Sirenum promptly in writing within ten (10) business days after receipt of Sirenum's notice in accordance with the mechanism set out in Section 6.2. In the event Client objects to a new Sub-processor, as permitted in the preceding sentence, then the parties will discuss the objection and attempt to agree a mutually acceptable resolution in good faith.

6.4 **Liability.** Sirenum shall be liable for the acts and omissions of its Sub-processors to the same extent Sirenum would be liable if performing the services of each Sub-processor directly under the terms of this Addendum, except as otherwise set forth in the Agreement.

7. SECURITY

7.1 **Controls for the Protection of Client Personal Data.** Sirenum shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorised or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorised disclosure of, or access to, Client Personal Data), confidentiality and integrity of Client Personal Data. Further details are set out in Paragraph 4 of Schedule One of this Addendum. Sirenum regularly monitors compliance with these measures. Sirenum will not materially decrease the overall security of the Services during a subscription term.

7.2 **Third-Party Certifications and Audits.**

7.2.1 **In relation to Sirenum:** Sirenum shall allow for and contribute to audits, including inspections, conducted by the Client or another auditor mandated by the Client in respect of the compliance of Sirenum's processing of Client Personal Data with the Data Protection Laws and Regulations and this Addendum.

7.2.2 **In relation to SFDC:** SFDC has obtained the third-party certifications and audits set forth in the Security, Privacy and Architecture Documentation. Upon Client's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Sirenum shall make available to Client that is not a competitor of SFDC (or Client's independent, third-party auditor that is not a competitor of SFDC) a copy of SFDC's then most recent third-party audits or certifications, as applicable.

7.2.3 Sirenum may charge the Client at its standard time-based charging rates for any work performed by Sirenum at the request of the Client pursuant to this Paragraph 7.2, providing that no such fees shall be levied where the request to perform the work arises out of any breach by Sirenum of the Agreement or any security breach affecting the systems of Sirenum.

8. CLIENT PERSONAL DATA INCIDENT MANAGEMENT AND NOTIFICATION

Sirenum maintains security incident management policies and procedures (and which in respect of SFDC are specified in the Security, Privacy and Architecture Documentation) and shall notify Client without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Client Personal Data, including Personal Data, transmitted, stored or otherwise Processed by Sirenum or its Sub-processors of which Sirenum becomes aware (a "**Client Personal Data Incident**"). Sirenum shall make reasonable efforts to identify the cause of such Client Personal Data Incident and take those steps as Sirenum deems necessary and reasonable to remediate the cause of such a Client Personal Data Incident to the extent the remediation is within Sirenum's reasonable control. The obligations herein shall not apply to incidents that are caused by Client or Users.

9. ACCESS AND DELETION OF CLIENT PERSONAL DATA

9.1 Return and deletion of Client Personal Data (within the context of Client Data) will be governed by the provisions of the Agreement. If no such provisions exist, then upon termination of the Agreement the following Client Personal Data deletion provisions shall apply:

9.1.1 Sirenum will permit the Client to access Client Personal Data held within the Services for 30 days [(subject to clause 9.2)]. During that time, the Client may obtain, copy and delete that Client Personal Data itself. If the Client so requests, Sirenum will assist the Client with obtaining, copying

or deleting that Client Personal Data, provided that if the Client is able to do this itself using tools made available by Sirenum via the Services, Sirenum may charge the Client for such assistance at its standard time-based charging rates;

9.1.2 After 30 days, the Client will no longer be able to access or use the Services but will be able to export the Client Personal Data using its admin account for as long as the Client has an active Salesforce org.

9.2 The Client acknowledges and agrees that Sirenum will be under no obligation to renew any Salesforce org following termination of the Agreement even if such renewal is due to occur within 30 days of termination and the Client has not accessed and copied the Client Personal Data by such renewal date. Sirenum will however notify the Client in advance of any renewal date which is due to occur within 30 days of termination.

10. AUTHORISED AFFILIATES

10.1 **Contractual Relationship.** The parties acknowledge and agree that, by executing the Agreement, Client is acting on its own behalf and also, in relation to this Addendum only, in the name and on behalf of its Authorised Affiliates, thereby establishing a separate data processing agreement between Sirenum and each such Authorised Affiliate subject to the provisions of this Addendum. Each Authorised Affiliate agrees to be bound by the obligations under this Addendum. For the avoidance of doubt, an Authorised Affiliate is not and does not become a party to the Agreement as a whole. All access to and use of the Services by the Client and any Authorised Affiliate must comply with the terms and conditions of this Addendum and any violation of the terms and conditions of this Addendum by the Client or an Authorised Affiliate shall be deemed a violation by Client.

10.2 **Rights of Authorised Affiliates.** Where an Authorised Affiliate becomes a party to this Addendum with Sirenum, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this Addendum, subject to the following:

10.2.1 Except where applicable Data Protection Laws and Regulations require the Authorised Affiliate to exercise a right or seek any remedy under this DPA against Sirenum directly by itself, the parties agree that (i) solely the Client itself shall exercise any such right or seek any such remedy on behalf of the Authorised Affiliate, and (ii) the Client shall exercise any such rights under this Addendum not separately for each Authorised Affiliate individually but in a combined manner for itself and all of its Authorised Affiliates together (as set forth, for example, in Section 9.2.2, below).

10.2.2 the Client shall, when carrying out an on- site audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on Sirenum and its Sub-Processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of itself and all of its Authorised Affiliates in one single audit.

11. LIMITATION OF LIABILITY

To the extent permitted by law, the Client acknowledges and agrees that Sirenum's liability arising out of or related to this Addendum will be limited to Sirenum only, and its Sub-processors (including SFDC and its Affiliates) will not have any liability directly to Client or any Authorised Affiliates.

12. DATA TRANSFERS

12.1 **Transfer mechanisms for data transfers.** The Client hereby instructs Sirenum to transfer Client Personal Data outside the United Kingdom ("**UK**") and European Economic Area ("**EEA**") in the circumstances, and subject to the Transfer Mechanisms, set out in Paragraph 6 of Schedule One.

12.2 **Transfer mechanism – UK as a third country**. If the Client is established in a European Union or EEA member state, the provisions of this Paragraph 11.2 shall take effect at the end of the transition period agreed between the United Kingdom and European Union under the Withdrawal Agreement ("**transition period**"):

12.2.1 if there is no adequacy decision under Article 45 of the GDPR in favour of the United Kingdom that applies to the Provider ("adequacy decision") in effect on the date upon which the transition period expires (the "relevant date"), the Standard Contractual Clauses (incorporating the relevant details from Schedule One) shall come into effect and form a part of the Agreement on the relevant date;

12.2.2 if the Standard Contractual Clauses come into effect pursuant to Paragraph 12.2.1:

(a) the Client agrees to be bound by the Standard Contractual Clauses as the data exporter and comply with the obligations applicable to the data exporter under the Standard Contractual Clauses as if it had signed the Standard Contractual Clauses;

(b) Sirenum agrees to be bound by the Standard Contractual Clauses as the data importer and comply with the obligations applicable to the data importer under the Standard Contractual Clauses as if it had signed the Standard Contractual Clauses;

(c) the Client acknowledges and agrees that the authorisation to engage third party processors granted pursuant to Paragraph 6.1 above shall constitute the Client's prior written consent to sub-processing for the purposes of clauses 5(h) and 11(1) of the Standard Contractual Clauses and that Sirenum's compliance with its obligations under Paragraph 6 above shall constitute compliance with its obligations under clauses 5(h) and 11(1) of the Standard Contractual Clauses in respect of obtaining the Client's prior written consent to sub-processing;

(d) the Client agrees that the copies of the sub-processor agreements that must be provided by Sirenum to the Client pursuant to clause 5(j) of the Standard Contractual Clauses may have all commercial and confidential information and clauses unrelated to the Standard Contractual Clauses removed by Sirenum prior to being provided to the Client, and that such copies will be provided by Sirenum in a format determined by Sirenum only upon the Client's request;

(e) the Standard Contractual Clauses shall automatically terminate and no longer form a part of the Agreement if an adequacy decision under Article 45 of the GDPR in favour of the United Kingdom is made, with termination of the Standard Contractual Clauses taking effect on the date upon which the adequacy decision comes into effect;

12.2.3 if there is an adequacy decision in effect on the relevant date, the Standard Contractual Clauses shall not take effect and shall not form a part of the Agreement.

13. General

13.1 Notwithstanding anything to the contrary in the Agreement, the Client shall not claim that this Addendum is not a valid and legally binding variation to the Agreement.

13.2 This Addendum is for the benefit of the Parties, and is not intended to benefit or be enforceable by any third party. The exercise of the Parties' rights under this Addendum is not subject to the consent of any third party.

13.3 If a provision of this Addendum is determined by any court or other competent authority to be unlawful and/or unenforceable, the other provisions will continue in effect. If any unlawful and/or unenforceable provision of this Addendum would be lawful or enforceable if part of it were deleted, that part will be deemed to be deleted, and the rest of the provision will continue in effect.

13.4 This Addendum shall be governed by and construed in accordance with the laws of England and Wales. Any disputes relating to this Addendum shall be subject to the exclusive jurisdiction of the courts of England.

For use where no pre-existing Salesforce org

This Addendum is entered into and becomes a binding part of the Agreement with effect from the Effective Date.

SIGNED for and on behalf of SIRENUM LIMITED	**SIGNED for and on behalf of the CLIENT**
……..	**(as per Name and Date as recorded in the electronic signature system operated by Sirenum for this Addendum)**
	……..
Name: ……	
Title: ……	

SCHEDULE ONE

Data Processing Details

Introduction – nature and subject matter of the processing of Client Personal Data

"**Client Data**" means all data, works and materials:

- uploaded to or stored on the Platform by the Client;
- transmitted by the Platform at the instigation of the Client;
- supplied by the Client to Sirenum for uploading to, transmission by or storage on the Platform; or
- generated by the Platform as a result of the use of the Services by the Client (but excluding Aggregated Data)

As the Services are workforce management software designed to help Sirenum's clients manage their mobile workers, much of the Client Data will be Personal Data relating to their workers. Client Data that is Personal Data is Client Personal Data.

Sirenum will process Client Personal Data in the following circumstances:

- when Sirenum staff access or perform operations on Client Personal Data held within the Client's Salesforce org in the course of providing Services;
- when the Sirenum platform transmits, stores or otherwise processes Client Personal Data at the instigation of the Client;
- when the Client uploads or stores Client Personal Data on the Sirenum platform;
- when the Sirenum platform performs automated operations on Client Personal Data as a result of the use of the Services by the Client;
- when the Platform generates Client Personal Data as a result of the use of the Services by the Client.

1. Categories of data subject

The workers, including management staff, employees, consultants, individual contractors and temporary staff, of the Client and its Affiliates.

2. Types of Personal Data

Names

Email addresses

Home address

Phone numbers

Device IDs and IP addresses

Geolocation data

Job roles

Salary/wage/payment rate information

Shift details

Records of shifts attended, accepted and rejected

Bank and payment details

PAYE details, tax and NI records

Other information as included within the Services from time to time

3. Purposes of processing

To provide the Services in accordance with the Agreement.

4. Security measures for Personal Data

Sirenum security measures

The Sirenum Platform is built on Salesforce, whose robust security and privacy programs meet the highest standards in the industry. The Client accesses and uses the Sirenum platform and Services via the Client's own Salesforce org on the Salesforce platform. Sirenum is a Salesforce ISV (independent services vendor) partner, which means it is subjected to regular security reviews ensuring that the platform and Services are compliant with Salesforce's high standards.

Sirenum's Security Information Sheet https://sirenum.com/download/12598/ describes the security measures applied to the Salesforce platform and the Sirenum platform.

Salesforce

SFDC's security measures are as set forth in the Security, Privacy and Architecture Documentation.

Client security measures

The Client shall use reasonable security measures to ensure that no unauthorised person gains access to the Subscription Services using an Account, including ensuring that its Users do not share login details or passwords with others.

Salesforce and Sirenum may from time to time provide Client with instructions concerning its Salesforce Org settings. Failure by the Client to follow such instruction or any adjustment of Salesforce org settings which are done by any User other than in accordance with Salesforce or Sirenum instructions or documentation will be at the Client's own risk and Sirenum shall have no liability for any events occurring due to any such failure or adjustment.

5. Authorised sub-processors of Client Personal Data

The Client authorises sub-processing by the following third party service providers used by Sirenum in connection with providing the Services to the Client:

SFDC

SFDC provides the Salesforce org on which the Sirenum platform and Services are built.

Atlassian Pty Limited (Atlassian)

Atlassian provides the Jira Software, Jira Service Desk and Jira Core that Sirenum uses to manage and provide support services to users of the Sirenum platform.

Atlassian also provides the Bitbucket software that Sirenum uses to develop its code base for the Sirenum platform.

For clarity, the following third parties are **not** sub-processors engaged by Sirenum under the Agreement and do not require authorization by the Client:

Third party providers of integrated services

The Sirenum platform and Services integrate with third party provider services using APIs made available on the Salesforce platform in accordance with the Client's requirements. The Client contracts directly with these such third party providers, which means that those third parties are processors directly engaged by the Client and are **not** sub-processors engaged by Sirenum under the Agreement. The Client should refer to its agreements with the third party providers of the services integrated into the Client's Salesforce org to understand those providers' processing and use of sub-processors.

6. Authorised international transfers of Client Personal Data

The Client authorises any international transfer of Client Personal Data that results from the use of the authorised sub-processors described in section 5 above, provided that Sirenum shall ensure there is a Transfer Mechanism in place in respect of each such sub-processor.

Transfers to and within Salesforce are subject to the following Transfer Mechanisms in order of priority:

a) Salesforce Processor Binding Corporate Rules

b) SFDC's EU-U.S. and Swiss-U.S. Privacy Shield Framework self-certifications listed in SFDC's Notice of Privacy Shield Certification, which SFDC makes available online at https://www.salesforce.com/company/privacy/ (the "Privacy Shield Services")

c) Standard Contract Clauses

Further details on each of the above can be found here: https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/Agreements/EU-Data-Transfer-Mechanisms-FAQ.pdf

Transfers to Atlassian (Australia) are subject to the Privacy Shield Framework or Standard Contract Clauses.

The Client shall be responsible for ensuring that there is a Transfer Mechanism in place in respect of any transfers to the third party providers of the integrated services under its direct contracts with those other third parties.