

Findmyshift - Data Processing Agreement

Last updated: 25/01/2021

Data Processing Agreement (DPA)

This Data Processing Agreement (“DPA”) is between Findmyshift B.V. (“Findmyshift”) and Customer to reflect the Parties’ agreement with regard to the Processing of Personal Data of Customer, in accordance with the requirements of Data Protection Laws. The DPA forms part of the Agreement between Findmyshift B.V. and Customer as defined below. Terms not otherwise defined herein shall have the meaning as set forth in the Agreement.

Together, Findmyshift and Customer are referred to as the “Parties”.

1. Definitions

- 1.1. ‘Agreement’ means the Terms and Conditions of Findmyshift and all materials referred or linked to therein.
- 1.2. ‘Contact’ means a single individual (other than a User) whose Contact Information is stored by a User in the Subscription Service.
- 1.3. ‘Contact Information’ means the name, email address, telephone number, and similar information uploaded by a User to the Subscription Service.
- 1.4. ‘Customer Data’ means all information that a User submits or collects via the Subscription Service.
- 1.5. ‘Customer’ means the person or entity using the Subscription Service and identified in the applicable account record, billing statement or online subscription process as the Customer.
- 1.6. ‘Controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
- 1.7. ‘Data Protection Laws’ means all applicable legislation relating to data protection and privacy including without limitation the EU Data Protection Directive 95/46/EC and all local laws and regulations which amend or replace any of them, including the GDPR, together with any national implementing laws in any Member State of the European Union or, to the extent applicable, in any other country, as amended, repealed, consolidated or replaced from time to time. The terms “process”, “processes” and “processed” will be construed accordingly.
- 1.8. ‘Data Subject’ means the individual to whom Personal Data relates.

- 1.9. 'GDPR' means the General Data Protection 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.
 - 1.10. 'Instruction' means the written, documented instruction, issued by Controller to Processor, and directing the same to perform a specific action with regard to Personal Data (including, but not limited to, depersonalising, blocking, deletion, making available).
 - 1.11. 'Personal Data' means any information relating to an identified or identifiable individual where such information is contained within Customer Data and is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws.
 - 1.12. 'Personal Data Breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
 - 1.13. 'Processing' means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data.
 - 1.14. 'Processor' means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.
 - 1.15. 'Restricted Transfer' means a transfer of Personal Data from Controller to Processor; or an onward transfer of Personal Data from a Processor to a Sub-Processor, in each case where such transfer would be prohibited by Data Protection Laws in the absence of Standard Contractual Clauses.
 - 1.16. 'Standard Contractual Clauses' means the clauses attached hereto as Annex 1 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.
 - 1.17. 'Subprocessor' means any person appointed by or on behalf of the Processor to Process Personal Data on behalf of Controller in connection with the Agreement;
 - 1.18. 'Subscription Service' means all web-based applications, mobile applications, and software developed, operated, and maintained by Findmyshift.
 - 1.19. 'User' means the person or entity who uses the Customer's Subscription Service.
-

2. Details of the Processing

2.1. Parties to the Processing

For the purposes of the DPA and with regard to Personal Data, the Parties acknowledge and agree that Customer is the Controller of Personal Data and Findmyshift is the Processor of that data.

2.2. Categories of Data Subjects

Customer's Users and Contacts.

2.3. Types of Personal Data

Contact Information, the extent of which is determined and controlled by the Customer in its sole discretion, shift times, pay rates, salaries and other Personal Data such as navigational data (including website usage information), email data, system usage data, application integration data, and other electronic data submitted, stored, sent, or received by Users via the Subscription Service.

2.4. Subject-Matter and Nature of the Processing

The provision of the services to the Customer under the Agreement may involve the Processing of Personal Data. The subject-matter of such Processing of Personal Data by Findmyshift is set out in the Agreement. Personal Data will be subject to those Processing activities as may be specified in the Agreement.

2.5. Purpose of the Processing

Personal Data will be Processed for purposes of providing the services set out and otherwise agreed to in the Agreement.

2.6. Duration of the Processing

Personal Data will be Processed for the duration of the Agreement, subject to Section 4 of this DPA.

3. Controller Responsibility

3.1. Within the scope of the Agreement and in its use of the services, Customer shall be solely responsible for complying with the Controller's statutory requirements relating to data protection and privacy, in particular regarding the disclosure and transfer of Personal Data to Findmyshift and the Processing of Personal Data. For the avoidance of doubt, Customer's Instructions for the Processing of Personal Data shall comply with Data Protection Laws.

3.2. This DPA is to be considered as a complete Instruction by Customer to Findmyshift in relation to the Processing of Personal Data under the Agreement and the DPA. Any additional Instructions outside the scope of the DPA shall require prior written agreement between the Parties. Other Instructions may be specified in the Agreement and may, from time to time thereafter, be amended, amplified or replaced by Customer in separate Instructions.

3.3. Customer shall inform Findmyshift without undue delay and comprehensively about any errors or irregularities related to statutory provisions on the Processing of Personal Data or related to the Customer Data communicated to Findmyshift.

4. Obligations of Findmyshift as Processor

4.1. Compliance with Instructions

Findmyshift shall Process Personal Data only within the scope of Customer's Instructions.

- 4.1.1. If Findmyshift believes that an Instruction of the Customer infringes the Data Protection Laws, it shall immediately inform the Customer without delay.
- 4.1.2. If Findmyshift cannot process Personal Data in accordance with the Instructions due to a legal requirement under any applicable European Union or Member State law, Findmyshift will promptly notify the Customer of that legal requirement before the relevant Processing to the extent permitted by the Data Protection Law; and cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as the Customer issues new instructions with which Findmyshift is able to comply. If this provision is invoked, Findmyshift will not be liable to the Customer under the Agreement for any failure to perform the applicable services until such time as the Customer issues new instructions in regard to the Processing.
- 4.1.3. If Findmyshift has reasons to suspect the Instructions involve a Restricted Transfer, it shall immediately notify Customer of this suspicion and Findmyshift shall only perform the Instruction upon Customer guaranteeing that the Instruction does not concern a Restricted Transfer.

4.2. Security

Findmyshift shall take the appropriate technical and organisational measures to adequately protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data, described under Appendix 2 to the Standard Contractual Clauses. Such measures include, but are not be limited to:

- 4.2.1. the prevention of unauthorised persons from gaining access to Personal Data Processing systems,
- 4.2.2. the prevention of Personal Data Processing systems from being used without authorisation,
- 4.2.3. ensuring that persons entitled to use a Personal Data Processing system gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights, and that, in the course of Processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorisation,
- 4.2.4. ensuring that Personal Data cannot be read, copied, modified or deleted without authorisation during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified,
- 4.2.5. ensuring that Personal Data is Processed solely in accordance with the Instructions,
- 4.2.6. ensuring that Personal Data is protected against accidental destruction or loss.

4.3. Confidentiality

Findmyshift shall ensure that any personnel whom Findmyshift authorises to process Personal Data on its behalf is subject to confidentiality obligations with respect to that Personal Data. The undertaking to confidentiality shall continue after the termination of the Processing activities as defined in the Agreement.

4.4. Personal Data Breaches

Findmyshift will notify the Customer as soon as practicable after it becomes aware of any of any Personal Data Breach affecting any Personal Data. At the Customer's request, Findmyshift will promptly provide the Customer with all reasonable assistance necessary

to enable the Customer to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if Customer is required to do so under Data Protection Laws.

4.5. Data Subject Requests

Findmyshift will provide reasonable assistance, including by appropriate technical and organisational measures and taking into account the nature of the Processing, to enable Customer to respond to any request from Data Subjects seeking to exercise their rights under Data Protection Laws with respect to Personal Data (including access, rectification, restriction, deletion or portability of Personal Data, as applicable), to the extent permitted by the law. If a Data Subject request is made directly to Findmyshift, Findmyshift shall inform the Customer and comply with such a request as soon as possible. If Findmyshift is unable to comply with the request it will advise Data Subjects to submit their request to the Customer in which case Customer shall be solely responsible for responding to any Data Subjects' requests.

4.6. Assistance

Taking into account the nature of processing and the information available to the processor, Findmyshift will facilitate Customer's compliance with the Controller's obligation to implement security measures with respect to Personal Data (including if applicable Controller's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR), by implementing and maintaining the security measures described under Annex 3, complying with the terms of Section 4.4 (Personal Data Breaches); and (iii) providing the Customer with information in relation to the Processing in accordance with Section 5 (Audits).

4.7. Subprocessors

Findmyshift shall be entitled to engage Subprocessors to fulfil Findmyshift's obligations defined in the Agreement only with Customer's written consent. For these purposes, Customer consents to the engagement as Subprocessors of the third parties listed in Annex 4. For the avoidance of doubt, the above authorisation constitutes Customer's prior written consent to the sub-Processing by Findmyshift for purposes of Clause 11 of the Standard Contractual Clauses.

4.7.1. If Findmyshift intends to instruct Subprocessors other than the companies listed in Annex 4, Findmyshift will notify the Customer thereof in writing (email to the email address(es) on record in Findmyshift's account information for Customer is sufficient) and will give the Customer the opportunity to object to the engagement of the new Subprocessors within 30 days after being notified. The objection must be based on reasonable grounds (e.g. if the Customer proves that significant risks for the protection of its Personal Data exist at the Subprocessor). If Findmyshift and Customer are unable to resolve such objection, either party may terminate the Agreement by providing written notice to the other party. Customer shall receive a refund of any prepaid but unused fees for the period following the effective date of termination.

4.7.2. When instructing Subprocessors other than the companies listed in Annex 4, and before that Subprocessor first Processes Customer Personal Data, Findmyshift agrees to carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Personal Data required by the Agreement.

4.7.3. Where Findmyshift engages Subprocessors, Findmyshift will enter into a contract with the Subprocessor that imposes on the Subprocessor the same obligations that apply to Findmyshift under this DPA. Where the Subprocessor fails to fulfil its data protection obligations, Findmyshift will remain liable to the Customer for the performance of such Subprocessors obligations.

4.7.4. Where a Subprocessor is engaged, the Customer must be granted the right to monitor and inspect the Subprocessor's activities in accordance with this DPA and Data Protection Laws, including to obtain information from Findmyshift, upon written request, on the substance of the contract and the implementation of the data protection obligations under the sub-Processing contract, where necessary by inspecting the relevant contract documents.

4.7.5. The provisions of this Section 4.6 shall mutually apply if Findmyshift engages a Subprocessor in a country outside the European Economic Area (“EEA”) not recognised by the European Commission as providing an adequate level of protection for personal data. If, in the performance of this DPA, Findmyshift transfers any Personal Data to a sub-processor located outside of the EEA, Findmyshift shall, in advance of any such transfer, ensure that a legal mechanism to achieve adequacy in respect of that processing is in place.

4.8. Data Transfers

Customer acknowledges and agrees that, in connection with the performance of the services under the Agreement, Personal Data will be transferred to Findmyshift in the EEA. Parties will not engage in Restricted Transfers. Should Personal Data be transferred outside the EEA to any country not recognised by the European Commission as providing an adequate level of protection for Personal Data (as described in Data Protection Laws), Parties will ensure that a legal mechanism to achieve adequacy is in place. Annex 1 of the present DPA provides Standard Contractual Clauses to that effect, which will apply with respect to Personal Data that is transferred outside the EEA, either directly or via onward transfer to any country not recognised by the European Commission as providing an adequate level of protection for Personal Data.

4.9. Deletion or Retrieval of Personal Data

Other than to the extent required to comply with Data Protection Laws, following instruction from the Customer;

4.9.1. Findmyshift will delete all Personal Data (including copies thereof) processed pursuant to this DPA. If Findmyshift is unable to delete Personal Data for technical or other reasons, Findmyshift will apply measures to ensure that Personal Data is blocked from any further Processing.

4.9.2. Customer shall, upon termination or expiration of the Agreement and by way of issuing an Instruction, stipulate, within a period of time set by Findmyshift, the reasonable measures to return data or to delete stored data. Any additional cost arising in connection with the return or deletion of Personal Data after the termination or expiration of the Agreement shall be borne by Customer.

5. Audits

5.1. Without prejudice to Sections 5.2 to 5.6, Customer may, prior to the commencement of Processing, and at regular intervals thereafter, audit the technical and organisational measures taken by Findmyshift. For such purpose, Customer may, e.g.,

5.1.1. obtain all information necessary to demonstrate compliance with this DPA from Findmyshift,

5.1.2. request Findmyshift to submit to Customer an existing attestation or certificate by an independent professional expert.

5.2. Customers who can identify and show legitimate concerns as to Findmyshift’s compliance with Data Protection Laws, may, upon reasonable and timely advance agreement, without interrupting Findmyshift’s business operations, order an (on-site) audit or inspection of Findmyshift’s business operations. Findmyshift may refuse such a request if it considers the request to be disproportionate or unfounded. This audit or inspection shall be conducted by a qualified third party auditor. Customer shall reimburse Findmyshift for any time expended for audits at the Findmyshift’s then-current rates, which shall be made available to

Customer upon request. Before the commencement of any (on-site) audit or inspection, Customer and Findmyshift shall mutually agree upon the scope, timing, and duration of the audit in a separate Annex to this DPA (Annex 5), in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Findmyshift.

- 5.3. The previous Section also applies if Customer is required or requested to carry out an audit or inspection by Data Protection Laws, a data protection supervisory authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory, provided that the Customer ordering an audit or inspection has identified the relevant requirement or request in its notice to Findmyshift of the audit or inspection.
- 5.4. Customer may only mandate an auditor for the purposes of Section 5.1.3 if the auditor is identified in the list set out in Annex 5 to this DPA, as that list is amended by agreement between the Parties in writing from time to time. Findmyshift shall not unreasonably withhold or delay agreement to the addition of a new auditor to that list.
- 5.5. Customer need not give access to its premises for the purposes of an audit or inspection under Section 5.2:
 - 5.5.1. to any individual unless he or she produces reasonable evidence of identity and authority;
 - 5.5.2. outside regular business hours adopted by Findmyshift; and
 - 5.5.3. for the purposes of more than [one] audit or inspection in any [calendar year].
- 5.6. If an audit or inspection exceeds the scope, timing and/or duration of the audit agreed upon by both Parties under Section 5.1.3 and set out in Annex 5, Customer shall compensate Findmyshift for all damages or losses that such excessive audit or inspection may have caused.
- 5.7. Findmyshift shall, upon Customer's written request and within a reasonable period of time, provide Customer with all information necessary for such audit, to the extent that such information is within Findmyshift's control and Findmyshift is not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party.
- 5.8. Customer shall, upon completion of any (on-site) audit, promptly notify Findmyshift with information regarding any non-compliance discovered during the audit, and shall use commercially reasonable efforts to address any confirmed non-compliance.

6. General Provisions

6.1. Precedence

- 6.1.1. In case of any conflict, this DPA shall take precedence over the Agreement.
- 6.1.2. Upon the incorporation of this DPA into the Agreement, the parties indicated in Section 7 below (Parties to this DPA) are agreeing to the Standard Contractual Clauses (where and as applicable) and all appendixes attached thereto. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses in Annex 1, the Standard Contractual Clauses shall prevail.

6.2. Severability

Where individual provisions of this DPA are invalid or unenforceable, the validity and enforceability of the other provisions of this DPA shall not be affected.

6.3. Applicable law

Effective 25 May 2018 Findmyshift will process Personal Data in accordance with the GDPR requirements contained herein which are directly applicable to Findmyshift's provision of the Subscription Services.

6.4. Governing law and jurisdiction

This DPA and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by, and construed in accordance with, the laws of England and Wales and shall be under the exclusive jurisdiction of the competent courts of England and Wales.

6.5. Prior agreements

If Customer has previously executed a data processing addendum with Findmyshift, this DPA supersedes and replaces such prior Data Processing Addendum.

7. Parties to this DPA

7.1. This DPA is an amendment to and forms part of the Agreement. Upon the incorporation of this DPA into the Agreement Customer and Findmyshift are each a party to this DPA.

7.2. The legal entity agreeing to this DPA as Customer represents that it is authorised to agree to and enter into this DPA for, and is agreeing to this DPA solely on behalf of, the Customer.

Annex 1 - Standard Contractual Clauses (Processors)

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

The Customer, as defined in the Findmyshift Terms and Conditions (the "data exporter")

And

Findmyshift B.V., Panamalaan 5H, 1019AS, Amsterdam, Noord Holland, Netherlands (the "data importer"),

each a 'party'; together 'the parties',

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

Clause 1

Definitions

For the purposes of the Clauses:

- a. 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- b. 'the data exporter' means the controller who transfers the personal data;
- c. 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- d. 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- e. 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- f. 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1)

and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

- a. that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- b. that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- c. that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- d. that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- e. that it will ensure compliance with the security measures;
- f. that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- g. to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

- h. to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- i. that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- j. that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

- a. to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- b. that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- c. that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- d. that it will promptly notify the data exporter about:
 - i. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
 - ii. any accidental or unauthorised access; and
 - iii. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- e. to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- f. at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- g. to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is

- unable to obtain a copy from the data exporter;
- h. that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
 - i. that the processing services by the subprocessor will be carried out in accordance with Clause 11;
 - j. to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - a. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
 - b. to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

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

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by

the law of the Member State in which the data exporter is established.

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

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

Annex 2 - Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is the Customer, as defined in the Findmyshift Terms and Conditions ("Agreement").

Data importer

The data importer is Findmyshift B.V., a provider of online employee scheduling software (on a software-as-a-service basis).

Data subjects

Categories of data subjects set out under Section 2.2 of the Data Processing Agreement to which the Clauses are attached.

Categories of data

Categories of personal data set out under Section 2.3 of the Data Processing Agreement to which the Clauses are attached.

Special categories of data (if appropriate)

Neither party anticipates the transfer of data relating to special categories.

Processing operations

The processing activities set out under Section 2.4 of the Data Processing Agreement to which the Clauses are attached, and in the Agreement.

Annex 3 - Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses.

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

The data importer currently abides by the security standards in this Appendix 2. The data importer may update or modify these security standards from time to time provided such updates and modifications will not result in a degradation of the overall security of the Services during the term of the Service Agreement.

Encryption of data in transit:	The data importer ensures that all interactions between Users and the Subscription Service are done using the Secure Socket Layer (SSL) or Transport Layer Security (TLS) standard cryptographic protocols.
Encryption of personal data at rest:	The data importer ensures that all personal data is encrypted when recorded within its Subscription Service.
Encryption of backed up data:	The data importer ensures that all data backups are encrypted before being replicated for redundancy.
Two-factor access controls:	The data importer offers Users the option to enable two-factor authentication on their account.
Network security:	The data importer provides a high level of network security with intrusion detection, active server monitoring, rate limiting, firewalls, dynamic IP blacklists and mandatory SSL.
Staff conduct:	The data importer ensures that all personnel with access to personal data are aware of security and social engineering threats and conduct themselves in a manner consistent with its documented guidelines regarding security and confidentiality.

Annex 4 - List of Sub-Processors

1. Google, Inc.
2. Amazon Web Services, Inc.
3. Twilio, Inc.
4. FrontApp.com, Inc.
5. Slack Technologies, Inc.
6. Stripe, Inc.
7. Clickatell Ltd.
8. Livestorm SAS.
9. Tinify B.V.

10. Hotjar Ltd.
 11. Any other wholly-owned Findmyshift B.V. subsidiary organisations
-

Annex 5 - Audit rights

This Annex 5 forms part of the Data Processing Agreement (DPA) between Findmyshift and Customer and sets out the Audit rights of the Customer with regard to audits or inspections.

Scope, timing and duration of the audit

The scope, timing and duration of the audit will be defined by Findmyshift and Customer prior to the commencement of the audit.

Authorised third-party auditors

A list of authorised, third-party auditors will be provided by Findmyshift on request from Customer.