Findmyshift - Data Processing Agreement

Last updated: 23/06/2022

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 Regulation (EU) 2016 of the European Parliament and of the Council from 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 the repeal of Directive 95/46/EC ("General Data Protection Regulation" or "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laws in any Member State of the European Union or, to the extent applicable, in any other country, as amended, repealed, consolidated or replaced from time to time.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. ‘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).

1.10. ‘Personal Data’, Personal Data Breach, Processing, Processor and Supervisory Authority have the meaning assigned to that term by the applicable Data Protection Regulation;

1.11. ‘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.

1.12. ‘Standard Contractual Clauses’ means the clauses attached hereto as Annex 1 pursuant to the European Commission’s decision (C(2021) 3972) of 4 June 2021 on Standard Contractual Clauses for the transfer of personal data between a Controller and Processor and where one Party (or both) is established in a third country which does not ensure an adequate level of data protection.

1.13. ‘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;

1.14. ‘Subscription Service’ means all web-based applications, mobile applications, and software developed, operated, and maintained by Findmyshift.

1.15. ‘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 Customer requests the Subscription Services of Findmyshift. In the context of performing the Subscription Services, it is possible that Findmyshift will processes Personal Data on behalf of the Customer. 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 Subscription Service 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 Subscription Services, Customer shall be solely responsible for complying with all of its obligation as set out in the Data Protection Laws, including ensuring compliance with the principles relating to the Processing of Personal Data as laid down in Article 5 of the GDPR and in particular regarding the disclosure and transfer of Personal Data to Findmyshift. For the avoidance of doubt, Customer's Instructions for the Processing of Personal Data shall comply with Data Protection Laws.

3.2. The Customer is solely responsible for determining the purposes of the Processing and is responsible for establishing the documented instructions according to which Findmyshift has the right to process Personal Data during the term of the DPA. 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 provisions on the Processing of Personal Data or related to the Customer Data communicated to Findmyshift.

3.4. If necessary, the Customer introduces Technical and Organisational Measures, and will continue to introduce them, to protect Personal Data from accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access. These measures must ensure an adequate level of protection, taking into account the state of the art, the costs of the implementation of the measures and risks associated with the Processing. If Findmyshift is required to take such Technical and Organisational Measures, the Customer must check and approve these Technical and Organisational Measures before Processing starts (see clause 4.2).

---

4. Obligations of Findmyshift as Processor

4.1. Compliance with Instructions

Findmyshift shall Process Personal Data only within the scope of Customer's Instructions or insofar as this would be necessary to be able to execute the Subscription Services.

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, unless the law forbids disclosure of this information for important reasons of public interest.

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.

4.1.4. Findmyshift guarantees that the persons in its organisation who are authorised to Process Personal Data, have committed themselves to observe confidentiality or are bound by an appropriate statutory confidentiality obligation.

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 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.

4.2.7. Depending on the types of services delivered by Findmyshift and mentioned in the Agreement, the specific measures stated in Annex 3 shall apply, unless otherwise agreed between Parties. Findmyshift listed the minimum technical and organisational measures to be taken by the Findmyshift in Annex 3. Additional measures (if any) can be agreed upon in mutual consent in the concerned Agreement. Findmyshift shall be entitled to invoice Customer for any additional requested technical and organisational measures (other than those agreed upon in Annex 3 and/or the concerned Agreement) in the event Customer requires stricter technical and organisational measures as a consequence of Customer's policies,

guidelines, regulations, or laws, etc. applicable to Customer. By signing this DPA the Customer accepts the technical and organisational measures, as set out in Annex 3, as appropriate and must notify the Data Processor immediately in the event these technical and organisational measures would not be sufficient. Any deviations or additions that result from a specific request of the Customer shall be added in Annex 3.

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.

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 of the Customer. 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. Findmyshift shall inform the Customer of all requests that it receives from Data Subjects with regard to the Processing. Findmyshift shall forward the questions/requests in time so that this will not result in the Customer being unable to fulfil its obligation to respond to Data Subjects' requests in accordance with the GDPR. The Customer is responsible for handling and responding to such requests. Findmyshift is entitled to compensation for such assistance, based on its hourly rates, which shall be made available to Customer upon request.

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 in relation to (i) the security of the Processing, (ii) notification of a Personal Data Breach to the Supervisory Authority of the Data Subject as set out in clause 4.4 (iii) the performance of a data protection impact assessment and the prior notification of the Supervisory Authority. The Processor is entitled to compensation for such assistance based on the hourly rates of Findmyshift, which shall be made available to Customer upon request.

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 9 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). It is possible that Findmyshift will not be able to guarantee continuous delivery of the Subscription Services in case of disagreements regarding a Subprocessor, and

Findmyshift cannot be held liable for such implementation delays due to discussions related to the Subprocessor.

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 the transfer shall only take place in accordance with the principles set out in the GDPR.

In the event Findmyshift transfers Personal data outside the EEA to another party, the following will apply. The Customer grants Findmyshift to transfer Personal Data to a third country or to an international organisation as set out in Annex 4 and/or Agreement. Any change or addition to the list as stated in the Annex 4, as proposed, or required by Findmyshift, will be communicated to the Customer before such transfer takes place. The Customer has the right to object to such transfer within thirty (30) days of notification of the change. The Parties agree on whether or not to proceed with the transfer and the consequences thereof for the provision of the Subscription Services in terms of scope, timing and budget. Following this section 4.8, Findmyshift will guarantee the adequate level of protection of the Personal Data to a country outside the European Economic Area, by signing of the European Commission Standard Clauses.

In the event that one of the Parties (the Controller or Processor) is located outside the EEA and thus Personal data is transferred outside the EEA, either directly or via onward transfer to any country not recognized by the European Commission as providing an adequate level of protection of Personal Data, Parties shall guarantee the adequate level of protection by engaging the European Commission Standard Clauses for Controller-Processor with the inclusion of necessary supplementary measures to ensure that the transfer of Personal Data is subject to appropriate safeguards. The European Commission Standard Clauses for Controller-Processor (SCC's) is found in Annex 1 and shall be directly binding between the Parties when signing this DPA.

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.

4.9.3. Findmyshift may keep copies if the storage of Personal Data is required for legal or regulatory reasons.

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. Findmyshift 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. Liability

6.1. Findmyshift can only be held liable for an infringement of this DPA that is directly attributable to them, or the provisions that apply directly to the Processor on the basis of the applicable Data Protection Law insofar as the Customer has complied with its own obligations as set out in this DPA and the applicable Data Protection Law.

6.2. The liability provision set out in the Agreement is fully applicable. In the event no limitation of liability was agreed in the Agreement, the total liability that Findmyshift may incur in the provision of the Subscription Services shall be limited to the value of the Agreement.

---

7. General Provisions

7.1. Precedence

7.1.1. In case of any conflict, this DPA shall take precedence over the Agreement.

7.1.2. 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.

7.2. 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.

7.3. 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 as included in the Agreement and failing that to the court in the district where Findmyshift is located, with the exception of the conflict of law rules.

7.4. Prior agreements

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

---

8. Parties to this DPA

8.1. 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 this DPA.

8.2. 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

Purpose and scope

a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of data to a third country.

b. The Parties:

   i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

   ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

   have agreed to these standard contractual clauses (hereinafter: 'Clauses').

c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

ii. Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

iii. Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

iv. Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

v. Clause 13;

vi. Clause 15.1(c), (d) and (e);

vii. Clause 16(e);

viii. Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

a. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

b. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing

copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

b. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another

third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

a. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

b. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

c. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

d. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

e. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

a. GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-

processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

c. The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

d. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

e. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

a. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

b. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

   i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

   ii. refer the dispute to the competent courts within the meaning of Clause 18.

d. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the

conditions set out in Article 80(1) of Regulation (EU) 2016/679.

e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

b. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

c. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

d. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

e. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

f. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

g. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

a. [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

b. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

Clause 14

Local laws and practices affecting compliance with the Clauses

a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

   i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

   ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

   iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an

application of such laws in practice that is not in line with the requirements in paragraph (a).

f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g., technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

   i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

   ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are

reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

Clause 16

Non-compliance with the Clauses and termination

a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

   i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

   ii. the data importer is in substantial or persistent breach of these Clauses; or

   iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

   In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is

without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of where the data importer is located.

Clause 18

Choice of forum and jurisdiction

a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

b. The Parties agree that those shall be the courts of where the data importer is located.

c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

d. The Parties agree to submit themselves to the jurisdiction of such courts.

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.

A. LIST OF PARTIES

Data exporter(s):

The Customer, as defined in the Findmyshift Terms and Conditions.

Data importer(s):

Name:	Findmyshift B.V.
Address:	Panamalaan 5H, 1019AS, Amsterdam, Noord Holland, Netherlands
Contact details:	gdpr@findmyshift.com
Activities relevant to the data transferred under these Clauses:	The data importer provides the Subscription Services to the data exporter in accordance with the Agreement.
Role (Controller/Processor):	Processor

B. DESCRIPTION OF TRANSFER

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 Personal 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.

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis)

Data is transferred on a continuous basis during normal use of the services.

Purpose(s) of the data transfer and further processing

See section 2.5 of the Data Processing Agreement to which the Clauses are attached.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

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

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

See Annex 4 of the Data Processing Agreement to which the Clauses are attached.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13.

The Supervisory Authority where the data exporter is located is the competent Supervisory Authority.

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 8.6 (or document/legislation attached):

The data importer currently abides by the security standards in this Annex 3. 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

According to section 4.7 of the DPA and Clause 9 of the Standard Contractual Clauses, the Customer has authorised the use of the following sub-processors:

Company	Activities	Location of sub-processor
Amazon Web Services, Inc.	Hosting, data storage	Ireland
Google, Inc.	Site analytics, customer support	United States of America
Twilio, Inc.	Customer support, SMS message delivery	United States of America
FrontApp.com, Inc.	Customer support	United States of America
Slack Technologies, Inc.	Customer support	United States of America
Stripe, Inc.	Payment processing	United States of America
Clickatell Ltd.	SMS message delivery	Ireland

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.