SwipedOn data processing addendum (visitor / employee data)

1 APPLICATION OF THIS ADDENDUM

1.1 This Data Processing Addendum, including its Schedules, (**Addendum**) applies to the Processing (as defined below) of Visitor or Employee Data (as defined in the SwipedOn Terms of Service).

1.2 This Addendum forms part of the SwipedOn Terms of Service (together, the **Terms**) between us and you (as defined in the Terms) and sets out the parties' agreement in relation to the processing of Visitor or Employee Data in accordance with the requirements of Applicable Data Protection Laws.

1.3 We are located in New Zealand, which the European Commission has determined provides adequate protection within the meaning of Article 45 of the GDPR. However, to provide you with additional assurance as to our data protection commitments, this Addendum also includes EU Standard Contractual Clauses (as defined below), which are pre-signed by us. If you would like to opt in to the EU Standard Contractual Clauses, please complete the necessary details, countersign the EU Standard Contractual Clauses, and return a counter-signed copy to us at **privacy@swipedon.com**.

1.4 Except as varied in this Addendum (including the EU Standard Contractual Clauses, if applicable) all terms and conditions set out in the Terms continue to apply.

1.5 For the purposes of the CCPA, we certify that we understand and will comply with our obligations under this Addendum.

2 INTERPRETATION

2.1 Unless the context requires otherwise:

a capitalised terms used, but not defined, in this Addendum will have the meanings given to them in the Applicable Data Protection Laws (or, if not defined in the Applicable Data Protection Laws, the Terms);

b the rules of interpretation set out in the Terms apply to this Addendum; and

c references to *clauses* are references to the clauses in this Addendum.

2.2 In this Addendum:

Applicable Data Protection Laws means any applicable data protection or privacy laws of any country, including, if applicable, EU/UK Data Protection Laws, the CCPA and the NZ Privacy Act

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

Data Subject has the meaning given in EU/UK Data Protection Laws and includes an *individual* as defined in the NZ Privacy Act, a *consumer* as defined in the CCPA and any other identified or identifiable natural person to whom any information relates

EU/UK Data Protection Laws means all laws and regulations, including laws and regulations of the European Union, its member states and the United Kingdom, that apply to the Processing of Visitor or Employee Data, including (where applicable) the GDPR and the equivalent laws of the United Kingdom

EU Standard Contractual Clauses means the standard contractual clauses set out in Schedule 3, as may be amended under clause 12.1

GDPR means the European Union General Data Protection Regulation 2016/679

Instruction means the instructions set out in clause 3.4 or agreed under clause 3.5

NZ Privacy Act means the New Zealand Privacy Act 2020

Processing means any operation or set of operations which is performed upon Visitor or Employee Data, whether or not by automated means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. *Process* has a consistent meaning

Sub-Processor means any person appointed by us or on our behalf to Process Visitor or Employee Data on your behalf in connection with the Terms.

2.3 If there is any conflict between any of the following, they will have precedence in the descending order of priority set out below:

a the EU Standard Contractual Clauses;

b this Addendum; and

c the Terms.

3 PROCESSING OF VISITOR OR EMPLOYEE DATA

3.1 With respect to the Processing of Visitor or Employee Data under the Terms:

a for the purposes of EU/UK Data Protection Laws:

i you act as the Data Controller; and

ii we act as the Data Processor;

b we are acting as your agent for the purposes of the NZ Privacy Act;

c we are acting as the service provider (and not a third party) for the purposes of the CCPA; and

d subject to clause 6, we may engage the Sub-Processors listed in Schedule 2.

3.2 We will comply with all Applicable Data Protection Laws that apply to our Processing of Visitor or Employee Data on your behalf, including, if applicable, all EU/UK Data Protection Laws that apply to Data Processors.

3.3 You must, when using the Service, comply with all Applicable Data Protection Laws that apply to your Processing of Visitor or Employee Data, including, if applicable, all EU/UK Data Protection Laws that apply to Data Controllers.

3.4 You instruct us to Process Visitor or Employee Data and in particular, subject to clause 6, transfer Visitor or Employee Data to any country or territory:

a as reasonably necessary to provide the Service in accordance with the Terms;

b as initiated through the use of the Service by you, your Personnel and other end users you allow to use the Service; and

c to comply with any further instruction from you (including by email or through our support channels) that is consistent with the Terms and this Addendum.

3.5 This Addendum and the Terms are your complete and final instructions for the Processing of Visitor or Employee Data as at the time this Addendum takes effect. Any additional or alternate instructions must be agreed between us and you separately in writing.

3.6 We will not Process Visitor or Employee Data other than on your Instructions unless required by any law to which we are subject, in which case we will to the extent permitted by applicable law inform you of that legal requirement before we Process that Visitor or Employee Data.

3.7 As required by Article 28(3) of the GDPR, if applicable, and, if applicable, equivalent requirements of other Applicable Data Protection Laws, the nature and purpose of the Processing, the types of Visitor or Employee Data and categories of Data Subjects Processed under this Addendum are set out in Schedule 1. We may amend Schedule 1 from time to time on written notice to you as we reasonably consider necessary to meet the requirements of Applicable Data Protection Laws (including, if applicable, the GDPR).

3.8 The duration of Processing is limited to the duration of the Terms and the 6 month period following termination of the Terms. Our obligations in relation to Processing will continue until the Visitor or Employee Data has been properly deleted or returned to you in accordance with clause 10 of this Addendum.

3.9 You are solely responsible for ensuring that your Instructions comply with Applicable Data Protection Laws. It is also your responsibility to enter into data processing agreements with other relevant Data Controllers in order to allow us and our Sub-Processors to Process Visitor or Employee Data in accordance with this Addendum.

3.10 If, in our reasonable opinion, an Instruction infringes Applicable Data Protection Laws, we will notify you as soon as reasonably practicable.

3.11 We will not:

a sell (as that term is defined in the CCPA) Visitor or Employee Data;

b retain, use, or disclose Visitor or Employee Data for any purpose other than the specific business purpose of providing the Service, including retaining, using, or disclosing such information for a commercial purpose other than providing the Service; and

c retain, use, or disclose such Visitor or Employee Data outside of our direct business relationship with you.

4 DATA SUBJECT REQUESTS

4.1 To the extent permitted by law, we will notify you promptly if we receive a request from a Data Subject to exercise the Data Subject's rights under Applicable Data Protection Laws relating to any Visitor or Employee Data (**Data Subject Request**).

4.2 Taking into account the nature of the Processing, we will assist you by implementing appropriate technical and organisational measures, to the extent possible, to fulfil your obligation to respond to a Data Subject Request under Applicable Data Protection Laws.

4.3 To the extent you do not have the ability to address a Data Subject Request, we will, on your written request, provide reasonable assistance in accordance with Applicable Data Protection Laws to facilitate that Data Subject Request. You will reimburse us for the costs arising from this assistance.

4.4 We will not respond to a Data Subject Request except on your written request or if required by applicable law.

5 OUR PERSONNEL

5.1 We will:

a take reasonable steps to ensure the reliability of any of our Personnel engaged in the Processing of Visitor or Employee Data;

b ensure that access to Visitor or Employee Data is limited to our Personnel who require that access as strictly necessary for the purposes of exercising our rights and performing our obligations under the Terms;

c ensure that our Personnel engaged in Processing Visitor or Employee Data are subject to confidentiality undertakings or professional or statutory obligations of confidentiality; and

d ensure that our Personnel engaged in Processing Visitor or Employee Data are informed of the confidential nature of the Visitor or Employee Data and receive appropriate training on their responsibilities.

5.2 We have appointed a data protection officer who can be contacted at privacy@swipedon.com.

6 SUBPROCESSESORS

6.1 You acknowledge and agree that we may engage third party Sub-Processors in connection with the provision of the Service.

6.2 We have entered into (and will, for any new Sub-Processor, enter into) written agreements with each Sub-Processor containing data protection obligations which offer at least the same level of protection for Visitor or Employee Data as set out in this Addendum and that meet the requirements

of Article 28(3) of the GDPR and/or equivalent requirements of other Applicable Data Protection Laws, as applicable to the nature of the services provided by that Sub-Processor.

6.3 You may request copies of our written agreements with Sub-Processors (which may be redacted to remove confidential information not relevant to this Addendum).

6.4 A list of current Sub-Processors for the Services as at 26 May 2022 is set out in Schedule 2. We may update the list of Sub-Processors from time to time and, subject to clause 6.5, we will give prior written notice of any new Sub-Processor [*(**Change Notice**)*].

6.5 We may engage Sub-Processors as needed to serve as an Emergency Replacement to maintain and support the Services. *Emergency Replacement* means a sudden replacement of a Sub-Processor where a change is outside our reasonable control. In this case, we will inform you of the replacement Sub-Processor as soon as reasonably practicable.

6.6 *You may object to any new Sub-Processor on reasonable grounds by notifying us within 10 days of receipt of a Change Notice. Your notice of objection to any new Sub-Processor must explain the reasonable grounds for your objection. The parties must discuss your concerns about the new Sub-Processor in good faith with a view to resolve the objection to the use of the new Sub-Processor in a commercially reasonable manner. If it is not possible to resolve the objection, and we do not revoke the Change Notice before the date the Change Notice takes effect, you may, despite anything to the contrary in the Terms, terminate the applicable Service under the Terms that cannot be provided to you without that new Sub-Processor. If you do not terminate the relevant Service under the Terms in accordance with this clause, you are deemed to have agreed to the new Sub-Processor.*

6.7 We are liable for the acts and omissions of our Sub-Processors to the same extent we would be liable if performing the services of each Sub-Processor directly under the terms of this Addendum, except as otherwise set out in this Addendum.

7 SECURITY

We will maintain technical and organisational measures to protect the confidentiality, integrity and security (including protection against unauthorised or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorised disclosure of, or access to, Data) of Visitor or Employee Data, and to manage data security incidents affecting Visitor or Employee Data, in accordance with Annex II of the EU Standard Contractual Clauses.

8 SECURITY BREACH MANAGEMENT

8.1 We will comply with all applicable laws requiring notification to you of any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Visitor or Employee Data Processed by us or our Sub-Processors of which we become aware (**Breach Incident**).

8.2 We will make reasonable efforts to identify the cause of that Breach Incident, notify you within a timely manner to allow you to meet your obligations to report a Breach Incident, cooperate with you in good faith and provide any assistance reasonably necessary for you to comply with your obligations under Applicable Data Protection Laws with respect to a Breach Incident, including any obligations you have under Applicable Data Protection Laws to report, notify or investigate a Breach Incident, and take steps we consider necessary and reasonable to remediate the cause of the Breach Incident, to the extent remediation is within our reasonable control.

9 AUDIT AND COMPLIANCE

9.1 Upon your written request, we will, at your cost, submit to your audits and inspections, and provide you all information necessary, to demonstrate that both you and we are complying with our respective obligations under Applicable Data Protection Laws (including our respective obligations under Article 28 of the GDPR).

10 DATA PROTECTION IMPACT ASSESSMENT

Upon your written request, we will provide you with reasonable assistance needed to fulfil your obligations under Applicable Data Protection Laws to carry out a data protection impact assessment relating to your use of the Service, to the extent you do not otherwise have access to the relevant information.

11 RETURN AND DELETION OF VISITOR OR EMPLOYEE DATA

11.1 Subject to clauses 11.2 and 11.3, following termination of the Terms we will delete all Visitor or Employee Data within 6 months from termination of the Terms.

11.2 Subject to clause 11.3, you may submit a written request to us within 10 working days of the termination of the Terms requiring us, within 20 working days of your written request, to:

a return a complete copy of all Visitor or Employee Data by secure file transfer in a common format; and

b delete all other copies of Visitor or Employee Data Processed by us or any Sub-Processor.

11.3 We, or each Sub-Processor, may retain Visitor or Employee Data to the extent that it is required by applicable laws, provided that we ensure the confidentiality of all such Visitor or Employee Data and ensure that such Visitor or Employee Data is only processed as necessary for the purposes required under applicable laws requiring its Processing and for no other purpose.

11.4 With the exception of visitor photos and signatures (which must, where deletion is required under this clause 11, be completely and permanently deleted), you agree that we may satisfy any requirement to delete Visitor or Employee Data under this clause 11 by anonymising the Visitor or Employee Data so that it is no longer Personal Data.

12 CHANGES IN DATA PROTECTION LAWS

12.1 We may on prior written notice to you from time to time, make any variations to this Addendum (including to the EU Standard Contractual Clauses), which we consider (acting reasonably) are required as a result of any change in, or decision of a competent authority under, Applicable Data Protection Laws, to allow transfers and Processing of Visitor or Employee Data to continue without breach of Applicable Data Protection Laws. You must do any further thing and sign any document required to give effect to this clause 12.1.

12.2 If you object to any variation under clause 12.1 on reasonable grounds, you may, despite anything to the contrary in the Terms, terminate these Terms and your right to access and use the Service without penalty on written notice, provided your notice of termination is received by us before the effective date of our notice. If you do not terminate these Terms and your right to access and use the Service in accordance with this clause, you are deemed to have agreed to the variation.

13 LIMITATION OF LIABILITY

The liability of each party to the other party under or in connection with this Addendum is subject to the limitations and exclusions set out in the Terms, and any reference in the Terms to the liability of a party means the aggregate liability of that party under the Terms and this Addendum together.

14 GENERAL

If any provision of this Addendum is, or becomes unenforceable, illegal or invalid for any reason, the relevant provision is deemed to be varied to the extent necessary to remedy the unenforceability, illegality or invalidity. If variation is not possible, the provision must be treated as severed from this Addendum without affecting any other provisions of this Addendum.

SCHEDULE 1

DETAILS OF PROCESSING

Nature and Purpose of Processing

We will Process Visitor or Employee Data as necessary to provide the Service in accordance with the Terms, as further specified in our online documentation relating to the Services, and as further instructed by you and your Personnel and other end users you allow to use the Service through the use of the Service.

Duration of Processing

Subject to clause 11 of this Addendum, we will Process Visitor or Employee Data for the duration of the Terms and for a period of not more than 6 months after termination of the Terms, unless otherwise agreed upon in writing.

Categories of Data Subjects

You may submit Visitor or Employee Data to the Service, the extent of which is determined and controlled by you in your sole discretion, and which may include, but is not limited to, Visitor or Employee Data relating to the following categories of data subjects:

- your Personnel who are natural persons
- visitors to your premises, including customers, suppliers, business partners, contractors and your Personnel's personal visitors (including family and friends) who are natural persons

Type of Visitor or Employee Data

You may submit Visitor or Employee Data to the Service, the extent of which is determined and controlled by you in your sole discretion, and which may include, but is not limited to, the following categories of personal data:

- first and last name
- title
- employer
- contact information (company, email, phone, physical business address)
- vehicle registration
- photographs
- time and date of visit
- person visiting

SCHEDULE 2

LIST OF SUB-PROCESSORS AS AT 28 SEP 2022

Third party / service vendor	Purpose	Location of subprocessor	Policy pages
Aircall	Calling system	USA, EU	https://aircall.io/privacy/
Apple	Mobile Push Notifications	USA	https://www.apple.com/privacy/
AWS Amazon	Cloud Services, data storage, content delivery, SMS and email sending, push notifications, networking	USA, AUS, GER, CAD, SNG, UK	https://aws.amazon.com/privacy/
Github	Issue tracking and source code management	USA	https://help.github.com/en/github/site-policy/github-privacy-statement
Google	Cloud services, push notifications, analytics	USA	https://policies.google.com/privacy?hl=en&gl=nz
HotJar	Analytics	USA	
HubSpot	Marketing and sales software	USA	https://legal.hubspot.com/privacy-policy
Intercom	Customer messaging platform	USA	https://www.intercom.com/terms-and-policies#eu-us
Mailgun	Email service provider	USA	https://www.mailgun.com/privacy-policy
Nexmo	SMS service provider	USA	https://www.nexmo.com/gdpr
Linear	Product management tool	USA	https://linear.app/privacy
Profitwell	Retention and Analytics tool	USA	
Sentry	Error tracking tool	USA	https://sentry.io/privacy/#eu-us-privacy-shield

Slack	Team communication platform	USA	https://slack.com/gdpr
Stripe	Payment gateway	USA	https://stripe.com/nz/privacy
Windcave	Payment gateway	NZ	https://www.windcave.com/privacy-policy
Xero	Accounting platform	USA	https://www.xero.com/nz/about/terms/privacy/

SCHEDULE 3

EU STANDARD CONTRACTUAL CLAUSES (CONTROLLER TO PROCESSOR)

SECTION I

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) ([1]) 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.

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

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 8.1b, 8.9a, c, d and e;

iii Clause 9a, c, d and e;

iv Clause 12a, d and f;

v Clause 13;

vi Clause 15.1c, d and e;

vii Clause 16e;

viii Clause 18a and b.

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: [not used]

SECTION II – OBLIGATIONS OF THE PARTIES

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 14e 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 14a.

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 ([2]) (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 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 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

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

writing of any intended changes to that list through the addition or replacement of sub-processors at least 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. ([3]) 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.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

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 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.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

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 ([4]);

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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 16d 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 14e 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 14e.

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.

SECTION IV – FINAL PROVISIONS

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 14f.

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 one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of *the Republic of Ireland*.

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 *the Republic of Ireland*.

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.

APPENDIX

ANNEX I

A LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

[*Customer to complete the details below*]

Name: _____

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses:

_____

_____

Signature and date: _____

Role (controller/processor): controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*]

Name: Swiped On Limited (**SwipedOn**)

Address: L1, 115 The Strand, Tauranga, 3110, New Zealand

Contact person's name, position and contact details: Alex Alvarez Cubitt, Data Protection Officer, privacy@swipedon.com

Activities relevant to the data transferred under these Clauses:

SwipedOn provides a cloud based visitor management solution (**Service**), that its customer can use to register and manage onsite visitors and employees. The provision of the Service is governed by the terms set out at https://www.swipedon.com/terms-of-service (**Terms**) and the Data Processing Addendum to which these clauses are attached (**DPA**, and together with the Terms the **Agreement**).

Signature: 

Role (controller/processor): processor

B DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As set out in Schedule 1 of the DPA.

Categories of personal data transferred

As set out in Schedule 1 of the DPA.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The data exporter may submit personal data to the Service, the extent of which will be determined and controlled by the data exporter in the data exporter's sole discretion, and which is for the sake of clarity is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

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

Continuous.

Nature of the processing

As set out in Schedule 1 of the DPA.

Purpose(s) of the data transfer and further processing

As set out in the Agreement.

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

As set out in the Agreement.

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

As set out in Schedules 1 and 2 of the DPA.

C COMPETENT SUPERVISORY AUTHORITY

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

The Data Protection Commission of the Republic of Ireland

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Details of SwipedOn's security measures can be found here:
https://www.swipedon.com/support/data-protection-and-security-1

ANNEX III

LIST OF SUB-PROCESSORS

As set out in Schedule 2 of the DPA.