Data Processor Agreement

Between

Customer

(the "**Controller**")

and

Fingerprint Cards AB (FPC)

(the "**Processor**")

PREAMBLE

BY PROVIDING FPC WITH PERSONAL DATA (AS DEFINED BY APPLICABLE DATA PROTECTION LAWS), YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT, WITHOUT ANY FURTHER ACKNOWLEDGEMENT ON YOUR PART. IF YOU DO NOT AGREE WITH THE TERMS AND CONDITIONS OF THIS AGREEMENT, YOU MAY NOT PROVIDE ANY PERSONAL DATA TO FPC.

1. BACKGROUND AND PURPOSE

1.1 The purpose of this Agreement is to regulate the Parties' rights and obligations that accompany the task of processing personal data, in order to ensure that personal data are processed in accordance with the provisions arising from at that time applicable data protection laws, including the General Data Protection Regulation, EU 2016/679, (GDPR) and any subsequent legislation replacing or supplementing them.

1.2 The parties have entered into a supply, licensing and/or support agreement in relation to FPC's provison of biometric solutions (the "**Main Agreement(s)**"). This Agreement governs the processing of Personal Data provided by the Controller and/or as the Processor is granted within the framework of the Parties' cooperation under the Main Agreement(s). THE CONTROLLER ACKNOWLEDGES AND AGREES THAT BY PROVIDING PROCESSOR WITH ANY PERSONAL DATA UNDER THE MAIN AGREEMENT(S), SUCH PERSONAL DATA WILL BE TREATED IN ACCORDANCE WITH THIS AGREEMENT.

1.3 The parties wish to supplement the terms and conditions of the Main Agreement(s) and to formalize the terms and conditions that will be applicable to the Processing of Personal Data that takes place in the context of the Main Agreement(s). The purpose is to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of the Data Subjects.

1.4 In the event of inconsistency between the other terms of the Main Agreement(s) and the Data Processor Agreement, the Main Agreement(s) shall generally prevail, however this Data Processor Agreement shall prevail with respect to those terms and issues relating particularly to Processing of Personal Data.

2. DEFINITIONS

2.1 Words, abbreviations and expressions shall have the meaning as ascribed to them in the Main Agreement(s), unless the context requires otherwise, or it is explicitly stated below:

2.2 "**Applicable Data Protection Law**": The at any time valid legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the Processing of Personal data applicable in the country in which the Controller is established and/or applicable in the jurisdiction in which the Processor or any Sub-processors are established including the General Data Protection Regulation, EU 2016/679, (GDPR) and any subsequent legislation replacing or supplementing them;

2.3 "**Personal Data**", "**Processing**", "**Controller**", "**Processor**", "**Data Subject**", "**Biometric Data**" and "**Supervisory Authority**" shall have the same meaning as in the General Data Protection Regulation (EU 2016/679) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data;

2.4 "**Clauses**": The standard contractual clauses for the transfer of personal data to data processors established in third countries, laid down by the EU Commission decision of 5 February 2010;

2.5 "**EEA**": The European Economic Area;

2.6 "**Sub-processor**": Any processor (subcontractor) engaged by the Processor who Processes Personal Data on behalf of the Processor in accordance with his instructions, the terms of this Agreement and the terms of the written subcontract;

2.7 "**Technical and Organisational Security Measures**": Those measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing.

3. PURPOSE OF THE PROCESSING

3.1 Processor will have access to Controller's data containing Personal Data, such as Biometric Data, in order to ensure the functionality of the Processor's products (such as both short term and long term product improvement) or in order to answer specific questions concerning one of the Processor's products.

3.2 Categories of data subjects and categories of personal data that may occur in the Processing of Personal Data are set out in Annex 1 to this Data Processor Agreement.

4. GENERAL OBLIGATIONS OF THE CONTROLLER

4.1 The Controller shall ensure that its own organisation abides to Applicable Data Protection Law. That includes:

- That the data has been collected in accordance with Applicable Data Protection Law and that there is a legal ground (e.g. relevant consent) for Processing, including the right to transfer the Personal Data to a third party, in accordance with the Purposes outlined in 3.1,
- That there are procedures and processes set in place in order for the data subject to be able to exercise its rights in accordance with Applicable Data Protection Law, and
- It has a procedure in place in order to report Data Protection Breaches to the relevant data protection authority.

5. GENERAL OBLIGATIONS OF THE PROCESSOR

5.1 The Processor shall, when Processing Personal Data in the context of the Main Agreement(s), comply with Applicable Data Protection Law.

5.2 The Processor shall further adhere to those routines and instructions for such Processing as communicated by the Controller from time to time, provided that such routines and instructions will not cause disproportionate costs and inconvenience to the Processor. The Processor is entitled to refrain from adhering with such routines or instructions if it would involve Processing of Personal Data in conflict with Applicable Data Protection Law.

5.3 The Processor shall not Process Personal Data given access to or generated in the context of the Main Agreement(s) for any purpose other than as to perform its obligations pursuant to the Main Agreement(s) and in accordance with sections 3.1 and 3.2 of this Data Protection Agreement.

5.4 Without limiting the generality of the foregoing, the Processing activities shall be limited to the categories of Personal Data and the categories of the Data Subjects as specified in Annex 1 to this Data Processor Agreement, unless otherwise is instructed in writing by the Controller.

6. USE OF SUB-PROCESSORS

6.1 The Processor may only subcontract any of its Processing operations under this Data Processor Agreement with the approval of the Controller, not to be unreasonably withheld. Any pre-approved Sub-processors are listed in Annex 1.

6.2 Where the Processor subcontracts its obligations under this Data Processor Agreement with the approval of the Controller, it shall do so only by way of a written agreement with the Sub-processor which requires the Sub-contractor to abide to the same obligations as the Processor in accordance with this Data Processor Agreement and imposes adequate data protection obligations on the Sub-processor (including provisions adequately safeguarding the rights of the Data Subjects).

6.3 The Processor shall upon request make available to the Controller a copy of any Sub-processor agreement, however commercial terms and terms not concerning Processing of Personal Data may be redacted.

6.4 Clause 3 applies similarly if any approved Sub-processor wishes to further subcontract any of its Processing operations.

7. INTERNATIONAL DATA TRANSFER

7.1 The Processing activities (including storage) shall take place on the location(s) set out in Annex 1. Personal Data shall not be transferred outside such location, including to other countries/states, without the prior written consent of the Controller.

7.2 Provided that consent is given in accordance with section 7.1, any transfer from an EU/EEA country to a non-EU/EEA country performed by the Processor shall satisfy the requirements laid down in Applicable Data Protection Law, such as enter into an agreement incorporating the Clauses.

7.3 If an approved Sub-processor is established or otherwise Processes Personal Data outside the EU/EEA, and if required in order to comply with Applicable Data Protection Law, the Processor shall enter into an agreement with such Sub-processor that incorporates the Clauses. In such instance, the Processor is given proxy by the Controller to enter into the agreement in the name and on behalf of the Controller, and in line with this Data Processor Agreement.

8. TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

8.1 The Processor shall implement and maintain throughout the term appropriate Technical and Organisational Security Measures to protect the Personal Data against unauthorized or unlawful Processing and against accidental or unlawful destruction or accidental loss, damage, alteration, unauthorised disclosure or access. These measures shall ensure a level of security appropriate to the risk presented to the Processing and the nature of the Personal Data to be protected (including the harm which might result from any accidental or unlawful destruction or accidental loss, damage, alteration, unauthorised disclosure or access to the Personal Data) having regard to the state of the art and the cost of their implementation.

8.2 The Processor shall only allow access to the Personal Data to personnel on a need-to-know basis. The Processor shall ensure that all personnel having access to the Personal Data are subject to adequate secrecy obligations. The secrecy obligations shall survive the termination of employment/engagement of the personnel and the termination of the Main Agreement(s).

8.3 The Processor shall document its Technical and Organisational Security Measures. Such documentation shall be made available to the Controller upon reasonable request, so that the Controller is able to fulfil his responsibility as Controller as set forth in Applicable Data Protection Law.

9. AUDITS

9.1 The Controller is entitled to (and may allow the Supervisory Authority to) access and conduct an audit of the data-processing facilities of the Processor. The Processor shall provide all necessary assistance in that respect. The Controller shall endeavour to perform such audit without causing significant interruptions to the Processor's regular operations. The audit shall be preceded by a minimum of four week's notice, the notice to be sent by email to the Contact Person and only upon confirmation of receipt should the audit be scheduled for at least four week in the future.

9.2 The Parties may agree on periodic security audits. The purpose of such audits shall be to demonstrate the adequacy of the Technical and Organisational Security Measures employed by the Processor and any Sub-processor. Such audits may include inspection of systems, operations and relevant Technical and Organisational Security Measures, walk-through of routines, random sampling, more comprehensive on-site controls and other suitable controls.

9.3 The audit shall not grant the Controller access to trade secrets or proprietary information unless required to comply with Applicable Data Protection Law. The Controller shall ensure its personnel conducting such audit are subject to adequate secrecy obligations. Provided that the adequate security obligations shall be documented by means of contracts with the personnel and shall be made available to the Processor on request.

9.4 If the parties agree that an audit is to be performed by external auditors, such external auditor is to be appointed by the Controller. The Processor may only oppose the appointment if such auditor is a competitor of the Processor. Upon security audits performed by an external auditor, both Parties shall be entitled to receive a copy of the audit report.

9.5 If the audit reveals inadequate Technical and Organisational Security Measures or other non-compliance with this Data Processor Agreement, the Processor shall (and, if relevant, shall procure that the relevant Sub-processor shall) without undue delay remedy such inadequacy or non-compliance. The Controller may require whole or parts of the Processing activities to temporarily cease until successful remedy is confirmed.

9.6 Each party shall cover its own costs associated with an audit. However, if the time the Processor spends to support the Controller with the Audit exceeds 15 hours during a single audit, then it is agreed that the Processor is entitled to compensation for the actual costs. Additionally, if the audit reveals deviations from the obligations set out in this Data Processor Agreement, the costs of the audit shall be borne by the Processors, limited to reasonable and documented out-of-pocket expenses of the Controller (such as payment to a third party engaged in the audit).

9.7 The Processor shall procure that the Controller is similarly entitled to conduct audits in respect to the Sub-processors.

10. DATA BREACHES

10.1 Deviations to this Data Processor Agreement (including, without limitation, accidental or unlawful destruction or accidental loss, damage, alteration, unauthorised disclosure or access) and/or Processing in conflict with Applicable Data Protection Law (a "Data Breach") shall be promptly notified to the Controller in writing.

10.2 The notification referred to in Clause 10.1 must at least (if relevant):

(a) Describe the Data Breach including the categories and amount of the Data concerned, and the categories, number, and, where feasible, names of the Data Subjects concerned;

(b) Describe the circumstances of the Data Breach, including the date and time of the incident;

(c) Communicate the identity and contact details of the data protection officer or other contact point where more information may be obtained;

(d) Recommend measures to mitigate the possible adverse effects of the Data Breach;

(e) Describe the likely consequences and potential risk to the Data Subjects due to the Data Breach;

(f) Describe the measures proposed or taken to address the data breach, including to re-establish the situation and to prevent the recurrence of the Data Breach;

(g) Include any other information required in order for Controller to comply with Applicable Data Protection Law.

10.3 The Processor shall document any Data Breaches. This documentation must enable the Supervisory Authority to verify compliance with this Data Processor Agreement, including without limitation the Technical and Organisational Security Measures and Applicable Data Protection Law. The documentation shall only include information necessary for that purpose.

10.4 The Controller is responsible for notifying the relevant Supervisory Authority about the Data Breach when applicable. The Processor shall promptly assist the Controller with all information requested and cooperate with the Supervisory Authority. If the Data Breach is material, and the Processor is not capable if remedying it with reasonable notice, the Controller is entitled to terminate the Data Processor Agreement. If a Sub-processor causes the Data Breach, the Controller is correspondingly entitled to require the termination of the subcontract with such Sub-processor.

11. LIABILITY AND LIMITATIONS OF LIABILITY

11.1 Unless otherwise agreed in the Main Agreement(s), the party in breach of this Data Processor Agreement shall be liable for documented and relevant damages suffered by the other party. However, neither party shall be liable for indirect or consequential damages (loss or reconstruction of data shall be considered direct damages).

11.2 The limitation of liability set out in clause 11.1 shall not apply if the breach is caused by intent or gross negligence.

12. INDEMNIFICATION

12.1 The Processor shall indemnify and hold the Controller harmless from reasonable costs, losses and liabilities arising from third party claims from Data Subjects or Supervisory Authorities that the Processing operations under this Data Processor Agreement is in breach of Applicable Data Protection Laws, provided that:

(a) the Controller notifies the Processor of a claim without undue delay;

(b) the Processor is given the possibility to cooperate with the Controller in the defence and settlement of the claim;

(c) the Controller does not agree on a settlement or similar payment arrangement with the third party without the Processor's prior written approval; and

(d) the Controller uses reasonable endeavours to limit its costs, losses and liabilities caused by the claim.

13. GENERAL NOTIFICATIONS

13.1 The Controller shall without undue delay notify the Processor in writing of:

(a) Any changes to the rights to use Personal Data that the Controller imposes on its web site(s), for instance a change in legal grounds for processing, which do or may reasonably be expected to have an adverse effect on the Processor’s or the Sub-processors ability or willingness to process the Personal Data in accordance with this Data Processor Agreement.

13.2 The Processor shall without undue delay notify the Controller in writing of:

(a) Any changes in the Technical and Organisational Security Measures or other aspects of the Processor or the Sub-processors, which do or may reasonably be expected to have an adverse effect on the Processor’s or the Sub-processors ability or willingness to process the Personal Data in accordance with this Data Processor Agreement;

(b) Any request or complaint from a Data Subject. The Processor shall not respond to that request or complaint, unless it has been otherwise authorised to do so; and

(c) Any request from any Supervisory Authority requiring access to or information regarding the Processor’s and/or the Sub-processor' Processing of Personal Data covered by this Data Processor Agreement, including any legally binding request for disclosure of the Personal Data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

14. TERM AND TERMINATION

14.1 This Data Processor Agreement will stay in force as long as the Processor processes or has access to Personal Data on behalf of the Controller in the context of the Main Agreement(s).

14.2 Upon expiration or termination, the Processor and any Sub-processors shall, at the choice and request of the Controller, return all the Personal Data and the copies thereof to the Controller or shall destroy all the Personal Data and certify to the Controller that it has done so, unless legislation imposed upon the Processor prevents it from returning or destroying all or part of the Personal Data. In that case, the Processor warrants that it will guarantee the confidentiality of the Personal Data and will not actively Process the Personal Data anymore.

15. GOVERNING LAW AND LEGAL VENUE

15.1 Unless otherwise agreed in the Main Agreement(s), this Data Processor Agreement shall be governed by Swedish law. The parties agree on Stockholm as the legal venue.

Annex 1

This Annex forms part of the Data Processor Agreement.

Data Subjects

The Personal Data to be processed concerns the Data Subjects:

Controller's employees and/or end-users.

Categories of Personal Data

The following categories of Personal Data will be Processed:

Biometric data such as fingerprints, facial images and retina images.

Pre-approved Sub-processors (if any)

The following Sub-processors are pre-approved by the Controller:

FPC's affiliates.

Processing location

The Processing will take place, and the Personal Data will be stored, in the following location (country/state):

For the Processor and pre-approved Sub-processor(s): Personal Data will be stored in Copenhagen, Denmark. Personal Data will be processed by various FPC offices/affiliates globally with which FPC has signed agreements on adequate protection.