**DATA PROCESSING ADDENDUM**

**for the use of Microblink technology and support services**

This **DATA PROCESSING ADDENDUM ("DPA")** is incorporated into and is subject to the terms and conditions of the agreement executed between Controller and Processor, as defined in Annex I (together "**the parties**"), terms of use or terms and conditions for using Processor's technology accepted by the Controller, governing Controller's use of Processor's technology or support services ("**Agreement**").

All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

When the Controller uses Processor's technology, both in the testing and production phase, or when Controller uses Processor's support services, Processor processes personal data (defined below). The parties agree to comply with the following provisions with regard to any processing of personal data and it is agreed as follows:

**SECTION I – GENERAL**

*Article 1*

***Definitions***

In this DPA, the following terms shall have the following meanings:

a. "**Controller**", "**Processor**", "**data subject**", "**personal data**", "**process**", and "**processing**" shall have the meanings given in European Data Protection Law;

b. "**European Data Protection Law**" means: (i) Regulation 2016/679 of the European Parliament and of the Council 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) (the "**EU GDPR**"); and (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**");

c. "**Applicable Data Protection Law**" means all worldwide data protection and privacy laws and regulations, to the extent applicable to the parties and the nature of the personal data processed under the Agreement, including, where applicable, European Data Protection Law, California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (collectively referred to as the **"CPRA"**), and any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with European Data Protection Law; in each case as may be amended or superseded from time to time;

d. "**personal data**" means, aside from the meaning given in European Data Protection Law, any information that identifies a person, that is scanned, uploaded and otherwise shared with the Processor using Processor's technology or pursuant to using support services by the Controller, Controller's affiliated companies, or by third parties acting on the Controller's behalf;

e. "**personal data breach**" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data disclosed and shared by the Controller and processed by Processor under this DPA;

f. "**restricted transfer**" means: (i) where the EU GDPR applies, a transfer of personal data from the European Union or European Economic Area to a country outside of the European Union or European Economic Area that has not been recognized by the European Commission as adequate pursuant to Article 45 of EU GDPR ("third country"); and (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to another country which is not based on adequacy regulations pursuant to Article 45 the UK GDPR;

g. "**adequacy decision**" means a formal decision made by the EU or UK which recognizes that another country, territory, sector, or international organisation provides an equivalent level of protection for personal data as the EU or UK does;

h. "**Standard Contractual Clauses**" or "**SCCs**" means the contractual clauses adopted by the European Commission in their *Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (available on the link: https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en)*;

i. "**Intra EU/EEA Standard Contractual Clauses**" or "**Intra EU/EEA SCCs**" means the contractual clauses adopted by the European Commission in their *Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council (available on the link: https://commission.europa.eu/publications/standard-contractual-clauses-controllers-and-processors-eueea_en);*

j. "**International Data Transfer Agreement**" or "**IDTA**" means the agreement issued by the Information Commissioner for Parties making Restricted Transfers under UK GDPR (available on the link: https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf);

k. **"Sub-Processor"** means any third-party Processor engaged by Processor to process any personal data on its behalf in connection with the technology or services provided to Controller.

*Article 2*

**Relationship of the parties**

1. Processor, as defined in Annex I of this DPA, will process personal data on behalf of Controller, as described in Annex II of this DPA. Where Microblink Ltd. (6th Floor, 9 Appold Street, London, United Kingdom, EC2A 2AP) or Microblink US (10 Grand Street, STE 2400, Brooklyn, NY 11249) is the signatory of the Agreement and Processor, Microblink LLC (Trg Drage Iblera 10, 10000, Zagreb, Republic of Croatia) will be deemed affiliated company and a Sub-Processor.

2. Each party shall comply with the obligations that apply to it under Applicable Data Protection Law.

*Article 3*

***Hierarchy***

1. In the event of a contradiction between this DPA and the provisions of related Agreements between the Parties existing at the time when this DPA is agreed or entered into thereafter, provisions of this DPA shall prevail.

2. Where applicable, provisions of SCCs or Intra EU/EEA SCCs or IDTA will supplement this DPA. In the event of a contradiction between this DPA and SCCs or Intra EU/EEA SCCs or IDTA, provisions of SCCs or Intra EU/EEA SCCs or IDTA

shall prevail.

3. If there is any conflict or inconsistency between this DPA and the Agreement, the provisions of the following documents (in order of precedence) shall prevail: (a) where applicable, SCCs or Intra EU/EEA SCCs or IDTA; then (b) this DPA; and then (c) the main body of the Agreement. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect.

4. This DPA applies to the processing of personal data as specified in Annex II.

5. Annexes I to IV are an integral part of this DPA.

*Article 4*

**Personal data processing under EU GDPR**

1. Where both parties are subject to EU GDPR and personal data is not transferred outside the European Union, Economic Area or countries without adequacy decisions under Article 45 of EU GDPR, Intra-EU/EEA SCCs apply completed as follows:

a. wherever there is an option to choose a regulation, Regulation (EU) 2016/679 shall apply;

b. the optional Clause 5 (Docking clause) shall apply;

c. in Clause 7.7. Option 2: General written authorization shall apply with a specified time period of thirty days;

d. Annex I of the Intra EU/EEA SCCs shall be deemed completed with the information set out in Annex I to this DPA;

e. Annex II of the Intra EU/EEA SCCs shall be deemed completed with the information set out in Annex II to this DPA;

f. Annex III of the Intra EU/EEA SCCs shall be deemed completed with the information set out in Annex III to this DPA; and

g. Annex IV of the Intra EU/EEA SCCs shall be deemed completed with the information set out in Annex IV to this DPA.

*Article 5*

**Processing under UK GDPR**

In relation to transfers of personal data protected by the UK GDPR, Intra-EU/EEA SCCs will apply with the following modifications:

a. wherever there is an option to choose a regulation, UK GDPR shall apply;

b. references to “EU”, “Union”, “Member State” and “Member State law” shall be replaced with references to “UK”, or “domestic law”;

c. references to the “competent courts” shall be replaced with references to the “competent courts of the UK”;

d. the optional Clause 5 (Docking clause) shall apply;

e. in Clause 7.7. Option 2: General written authorization shall apply with a specified time period of thirty days;

f. Annex I of the Intra EU/EEA SCCs shall be deemed completed with the information set out in Annex I to this DPA;

g. Annex II of the Intra EU/EEA SCCs shall be deemed completed with the information set out in Annex II to this DPA;

h. Annex III of the Intra EU/EEA SCCs shall be deemed completed with the information set out in Annex III to this DPA; and

i. Annex IV of the Intra EU/EEA SCCs shall be deemed completed with the information set out in Annex IV to this DPA.

*Article 6*

***International transfers***

**6.1. Restricted transfers under EU GDPR**

1. Where the transfer of personal data is considered a Restricted Transfer and EU GDPR requires that appropriate safeguards are put in place, such transfer shall be subject to the SCCs, which shall be incorporated by reference and form an integral part of this DPA. The applicable module of the SCCs shall be determined depending on the location of the Controller and Processor, and their roles as data exporter and data importer regarding the processed personal data.

2. In relation to personal data that is protected by the EU GDPR, when the Processor is located in the EU acting as data exporter and the Controller acting as data importer is located in the third country, the SCCs Module Four shall apply as follows:

a. the optional Clause 7 (Docking clause) shall apply;

b. In Clause 9, Option 2: General written authorization shall apply with a specified time period of thirty days;

c. In Clause 11, the option clause shall not apply;

d. In Clause 17, the governing law shall be the law of the Republic of Croatia;

e. In Clause 18, for resolving disputes arising from these Clauses shall be resolved by the courts of the Republic of Croatia;

f. Annex I.A and I.B of the EU SCCs shall be deemed completed with the information set out in Annex I and II to this DPA and Annex I.C shall have Croatian Personal Data Protection Agency as the competent supervisory authority;

g. Annex II of the EU SCCs shall be deemed completed with the information set out in Annex III to this DPA; and

h. Annex III of the EU SCCs shall be deemed completed with the information set out in Annex IV to this DPA.

**6.2. International transfers under UK GDPR**

1. Where UK GDPR applies to the processing, and where the Processor initiates and agrees on the transfer of personal data to a sub-processor outside of the UK or to a country without an adequacy decision, the Processor will sign an International Data Transfer Agreement with such Sub-Processor and will comply with the transfer rules.

2. Where UK GDPR applies to the Controller, the Controller remains responsible for all transfers of personal data they initiate or agree upon.

3. In relation to transfers of personal data protected by the UK GDPR, the parties acknowledge that the transfer where the Processor returns the processed personal data back to the Controller, provided that it has been initiated and agreed upon by the Controller, is not considered a Restricted Transfer under the UK GDPR.

**6.3. Onward transfers**

1. Processor shall not participate in (nor permit any Sub-Processor to participate in) any other Restricted Transfers of personal data (whether as an exporter or an importer of the personal data) unless the Restricted Transfer is made in compliance with Applicable Data Protection Law and provisions of this DPA.

2. Such measures may include (without limitation) transferring the personal data to a recipient in a country that the European Commission has decided provides adequate protection for personal data, to a recipient that has achieved binding corporate rules authorisation in accordance with Applicable Data Protection Law, or pursuant to SCCs implemented between the relevant exporter and importer of the personal data.

## SECTION II – OBLIGATIONS OF THE PARTIES

*Article 7*

***Description of processing(s)***

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the Controller, are specified in Annex II.

*Clause 8*

***Obligations of the Parties***

**8.1. Instructions**

1. The Processor shall process personal data only on documented instructions from the Controller, unless required to do so by applicable legal requirements to which the Processor is subject. In this case, the Processor shall inform the Controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the Controller throughout the duration of the processing of personal data. These instructions shall always be documented.

2. The Processor shall immediately inform the Controller if, in the Processor's opinion, instructions given by the Controller infringe provisions of Applicable Data Protection Law.

**8.2. Purpose limitation**

The Processor shall process the personal data, in accordance with the Controller's documented instructions, only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the Controller or if additional data processing documentation is signed between the parties.

**8.3. Duration of the processing of personal data**

Processing by the Processor shall only take place for the duration specified in Annex II.

**8.4. Security of processing**

1. The Processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (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 purposes of processing, and the risks involved for the data subjects.

2. The Processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing, and monitoring of the contract. The Processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Processor shall ensure that all authorized process personal data only as necessary for the Permitted Purpose.

**8.5. Sensitive data**

If the processing 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 offenses ("sensitive data"), the parties shall update categories of processed personal data in Annex II and Processor shall apply specific restrictions and/or additional safeguards.

**8.6. Documentation and compliance**

1. The Parties shall be able to demonstrate compliance with this DPA.

2. The Processor shall maintain records of processing activities performed under this DPA containing categories of data subjects involved in the processing and categories of personal data processed, nature, duration and purpose of processing, list of technical and organizational measures, and data protection impact assessment.

3. The Processor shall deal promptly and adequately with inquiries from the Controller about the processing of data in accordance with this DPA.

4. The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations that are set out in this DPA and stem directly from Applicable Data Protection Law. At the Controller's request, the Processor shall also permit and contribute to audits of the processing activities covered by this DPA, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the Controller shall take into account relevant certifications held by the Processor.

5. The Controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the Processor and shall, where appropriate, be carried out with reasonable notice, at least 30 days prior.

6. The Parties shall make the information referred to in this Article, including the results of any audits, available to the competent supervisory authority/ies on request.

**8.7. Use of Sub-Processors**

1. The Processor has the Controller's general authorisation for the engagement of Sub-Processors from an agreed list. The Processor shall specifically inform in writing the Controller of any intended changes to that list through the addition or replacement of Sub-Processors at least 30 days in advance, thereby giving the Controller sufficient time to be able to object to such changes prior to the engagement of the concerned Sub-Processor(s). The Processor shall provide the Controller with the information necessary to enable the Controller to exercise the right to object.

2. Where the Processor engages a Sub-Processor for carrying out specific processing activities (on behalf of the Controller), it shall do so by way of a contract which imposes on the Sub-Processor, in substance, the same data protection obligations as the ones imposed on the Processor in accordance with these clauses. The Processor shall ensure that the Sub-Processor complies with the obligations to which the Processor is subject pursuant to this DPA and to Applicable Data Protection Law.

3. At the Controller's request, the Processor shall provide a copy of such a Sub-Processor agreement and any subsequent amendments to the Controller. To the extent necessary to protect business secret or other confidential information, including personal data, the Processor may redact the text of the agreement prior to sharing the copy.

4. The Processor shall remain fully responsible to the Controller for the performance of the Sub-Processor's obligations in

accordance with its contract with the Processor. The Processor shall notify the Controller of any failure by the Sub-Processor to fulfill its contractual obligations.

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

**8.8. Notifications to the Controller**

1. In addition to other notifications envisaged by this DPA, Processor will inform the Controller, without undue delay, but no longer than five business days, if Processor becomes aware of:

a. Any non-compliance by Processor or its employees with the obligations under this DPA or the Applicable Data Protection Law requirements relating to the protection of personal data processed under this DPA;

b. Any legally binding request for disclosure of personal data by a law enforcement authority such as courts, tribunals, or administrative authorities, unless the Processor is otherwise forbidden by law to inform Controller (e.g. to preserve the confidentiality of an investigation by law enforcement authorities). Processor shall be able to provide information on the possible legally binding disclosure of personal data;

c. Any notice, inquiry, or investigation by a Supervisory Authority with respect to personal data shared by the Controller; or

d. Any complaint or request received directly from data subjects of Controller. Processor will not substantively respond to any such request without Controller's prior written authorization.

3. Before making any disclosures of personal data or providing other information regarding personal data, Processor shall consult with Controller unless in situations described in provision 1.b of this Article.

**8.9. Privacy by design and default**

Processor shall integrate privacy considerations into its processing activities from the outset, encompassing the design, development, implementation, and ongoing maintenance of its systems, applications, and services. Processor's default settings for systems, applications, and services shall prioritize the highest level of privacy protection, limiting the processing of personal data by default. Processor shall provide mechanisms that allow the Controller and data subjects to easily manage their privacy preferences and exercise their rights.

*Article 9*

***Assistance to the Controller***

1. The Processor shall assist the Controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing.

2. The Processor shall assist the Controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (1) and (2), the Processor shall comply with the Controller's instructions.

3. In addition to the Processor's obligation to assist the Controller pursuant to Clause 9.2, the Processor shall furthermore assist the Controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the Processor:

a. the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of

personal data (a 'data protection impact assessment'), where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons. The Processor shall provide assistance to the Controller to enable them to conduct the data protection impact assessment. When providing assistance, Processor may redact information to the extent necessary to protect business secret or other confidential information;

b. the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk;

c. the obligation to ensure that personal data is accurate and up to date, by informing the Controller without delay if the Processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

d. the obligations to implement and maintain appropriate technical and organisational measures to ensure a level of personal data security appropriate to the risk. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons and include as appropriate:

i. the pseudonymisation and encryption of personal data;

ii. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

iii. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

iv. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

4. The Parties shall set out the appropriate technical and organisational measures in Annex III by which the Processor is required to assist the Controller in the application of this Article as well as the scope and the extent of the assistance required. Controller acknowledges that the security measures are subject to technical progress and development and that Processor may update or modify the security measures from time to time, provided that such updates and modifications do not degrade or diminish the overall security of the processing.

*Clause 10*

***Notification of personal data breach***

In the event of a personal data breach, the Processor shall cooperate with and assist the Controller for the Controller to comply with its obligations under Applicable Data Protection Law, where applicable, taking into account the nature of processing and the information available to the Processor.

**10.1. Data breach concerning data processed by Controller**

In the event of a personal data breach concerning data processed by the Controller, the Processor shall assist the Controller:

a. in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the Controller has become aware of it, where relevant (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

b. in obtaining the following information which, shall be stated in the Controller's notification, and must at least include:

i. the nature of the personal data including where possible, the categories and approximate number of data subjects

concerned and the categories and approximate number of personal data records concerned;

ii. the likely consequences of the personal data breach;

iii. the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

c. in complying with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

**10.2. Data breach concerning data processed by Processor**

1. In the event of a personal data breach concerning data processed by the Processor, the Processor shall notify the Controller without undue delay after the Processor having become aware of the breach. Such notification shall contain, at least:

a. a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

b. the details of a contact point where more information concerning the personal data breach can be obtained;

c. its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

2. The Parties shall set out in Annex III all other elements to be provided by the Processor when assisting the Controller in the compliance with the Controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

## SECTION III – FINAL PROVISIONS

*Article 11*

***Non-compliance with this DPA and termination***

1. Without prejudice to any provisions of Applicable Data Protection Law, in the event that the Processor is in breach of its obligations under this DPA, the Controller may instruct the Processor to suspend the processing of personal data until the latter complies with this DPA or the Agreement is terminated. The Processor shall promptly inform the Controller in case it is unable to comply with this DPA, for whatever reason.

2. The Controller shall be entitled to terminate the Agreement insofar as it concerns the processing of personal data in accordance with this DPA if:

a. the processing of personal data by the Processor has been suspended by the Controller pursuant to provision 1. of this Article and if compliance with this DPA is not restored within a reasonable time and in any event within one month following suspension;

b. the Processor is in substantial or persistent breach of this DPA or its obligations under Applicable Data Protection Law;

c. the Processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to this DPA or Applicable Data Protection Law.

3. The Processor shall be entitled to terminate the Agreement insofar as it concerns processing of personal data under this DPA where, after having informed the Controller that its instructions infringe applicable legal requirements in accordance with Article 8.1.2, the Controller insists on compliance with the instructions.

4. Following termination of the Agreement, the Processor shall, at the choice of the Controller, delete all personal data processed on behalf of the Controller and certify to the Controller that it has done so, or, return all the personal data to the Controller and delete existing copies unless Applicable Data Protection Law requires storage of the personal data. Until the data is deleted or returned, the Processor shall continue to ensure compliance with this DPA.

*Article 12*

**Miscellaneous**

1. This DPA represents an integral part of the Agreement executed between the parties and becomes effective when both parties sign the Agreement.

2. If Applicable Data Protection Law or other applicable regulation requires the Controller to sign the DPA or to sign the SCCs, Intra-EU SCCs or IDTA applicable to a particular processing or restricted transfer of personal data to the Processor as a separate agreement, Processor will, on Controller's request, promptly execute such document.

3. The parties agree that this DPA shall replace any existing data processing agreement or similar document that the parties may have previously entered into in connection with the Processor's technology and services.

4. Notwithstanding anything to the contrary in the Agreement and without prejudice to Section 8.2 ("Purpose limitation"), Processor may periodically make modifications to this DPA as may be required to comply with Applicable Data Protection Law and to improve the level of security of personal data. Modifications to this DPA will be published on Processor's legal center (available on the link: https://microblink.com/dpa-for-the-use-of-microblink-technology-and-support-services/) and Processor will inform the Controller of any substantial changes to this DPA in writing.

**ANNEX I: LIST OF PARTIES**

**Controller:**

Name: Licensee

Address: As defined in the executed Agreement.

Contact person's name, position and contact details: As defined in the executed Agreement.

**Processor:**

Name: Microblink entity as defined in the executed Agreement.

Address: As defined in the executed Agreement.

Data protection Officer's contact details: privacy@microblink.com.

**ANNEX II: DESCRIPTION OF THE PROCESSING**

***Categories of data subjects whose personal data is processed***

Natural persons – Controller's end users, including, if applicable, Controller's affiliates' end users.

***Categories of personal data processed***

Name and last name, address, date, and place of birth, gender, sex, nationality, country of residence, signature, passport number, social security number, driver's license number, state or national ID card number, other ID card number, personal identification number, face image, eye color, weight, height, organ donor status, other categories of data found on transferred identity documents, and biometric data (not used to undeniably identify an individual).

***Sensitive data processed***

No sensitive data is intended for processing. If any sensitive data is transferred, Controller will notify the Processor and Processor will apply needed restrictions and safeguards.

***Nature of the processing***

**Applicable if Controller uses Processor's verification service:** Using Controller's Solution, the data subject scans the identity document's front and/or back. The scans are sent to Processor's cloud infrastructure on Google Cloud Platform, where, using Processor's technology, personal data is extracted from the scan, and the presence of security features is checked and/or the analysis of physical attributes of the scanned document is performed. Once the verification process is completed, Processor returns the verification response to the Controller and, after the verification session has ended, personal data is deleted from Processor's cloud infrastructure.

**Applicable if Controller uses Processor's extraction service:** Using Controller's Solution, the data subject scans the identity document's front and/or back. The scans are sent to Processor's cloud infrastructure on Google Cloud Platform, where, using Processor's technology, personal data is extracted from the scan. Processor sends the extraction results and/or scanned images to the Controller when the extraction process is completed, and personal data is deleted from Processor's cloud infrastructure.

**Applicable if Controller uses Processor's support services:** To securely transfer images of documents Controller has issues with to Processor, Controller uses Processor's Secure Image Upload. Processor analyzes the issue in accordance with

Controllers's request for support to provide support services. Depending on the Controller's support request, providing support services can include debugging issues on an already supported document type, supporting a new version of a supported document, and improving accuracy for an already supported document type, if the product does not work. Providing support services may, depending on the Controller's support request, include retraining of models.

***Purpose(s) for which the personal data is processed on behalf of the controller***

**Applicable if Controller uses Processor's verification service:** Purpose of the processing is to check the presence of security features on the identity document and to return the verification response to the Controller, in accordance with the Agreement.

**Applicable if Controller uses Processor's extraction service:** Purpose of the processing is to extract the data from the identity document and send the extraction results to the Controller, in accordance with the Agreement.

**Applicable if Controller uses Processor's support services:** Purpose of the processing is to provide support services to the Controller, in accordance with the Agreement.

***Duration of the processing***

**Applicable if Controller uses Processor's verification and/or extraction service:** Processing is ongoing (for as long as Controller uses the technology or services). Processor retains input data during verification or extraction sessions, as applicable, but does not store processed data, unless a different retention period is agreed upon in writing with the Controller.

**Applicable if Controller uses Processor's support services:** Processor retains the images until the issue is resolved.

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

**Google Cloud Platform** – Microblink LLC's cloud infrastructure on Google Cloud Platform will be used for running Processor's technology. Processing of personal data shall be performed continuously, as long as the Controller uses the technology.

**Microblink LLC** is a support-providing Microblink entity and acts as a sub-processor when it is not a contract-signing entity. The data shall be processed as described above, and security measures shall be applied as described in Annex III.

**ANNEX III TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

***Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services***

Processor has defined policy on classified data handling, which defines data classification, disclosure and protection. All Processor's employees are required to sign confidentiality clauses that state trade secrets and confidential information have to remain confidential in perpetuity and turned in after contract termination, while each breach is considered a severe violation. Furthermore, the Processor will ensure that Application Programming Interface is adequately protected and monitored with Web Application Firewall and DDoS protection.

The Processor will apply the 'least-privileged' and 'need-to-know' concepts and ensure segregation of duties. The Processor will ensure that proper procedures are in place to register new users/ additional access rights and to de-register users. The Processor will ensure that privileged access management is monitored closely and based on a regular review of the access rights, with access rights being withdrawn if not required anymore.

***Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident***

In relation to the subject of this Agreement, the Processor will report any security related (near) incident as soon as possible and according to the Agreement to the Controller's contact including the protective measures taken to mitigate the impact of the incident, the preventive measures proposed to prevent the (near) incident in the future and an estimation of the impact incurred because of the incident. Processor has defined a policy on information security incident management which defines roles and responsibilities in the incident management process. The policy also describes incident classification and steps the incident response team has to take, such as incident assessment, containment, threat eradication, recovery, reporting and learning from the incidents. The Processor shall ensure the spread of knowledge and expertise to ensure the availability of skilled people even in case of a disaster.

***Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing, and measures to ensure accountability***

At Processor's complete discretion, a periodic self-certification process will be completed by the Processor to ensure that all security-related policies and procedures are still applied. Furthermore, Processor will regularly conduct vulnerability assessments of related services through penetration and vulnerability testing. Processor has internal policies, rulebooks and procedures in place to ensure the accountability of employees to process personal data responsibly. Processor ensures that its employees are informed about the Processor's security requirements and policies and developments in the area of information security. Processor is entirely responsible for the conduct of its employees.

***Measures for ensuring physical security of locations at which personal data are processed***

Sub-processor's (Google Cloud Platform) measures for security of physical premises, which provides private cloud infrastructure service, include multiple physical security layers to protect the data centers, such as biometric identification, metal detection, cameras, vehicle barriers, and laser-based intrusion detection systems. (https://www.google.com/about/datacenters/data-security/)

In case processing of personal data occurs on the Processor's or Processor's Affiliated company's infrastructure, Processor will also ensure adequate physical security through use of cameras, entry cards and security guards.

***Measures for ensuring events logging***

All system and application logging functions related to provided services by the Processor are enabled and information security events are regularly reviewed.

***Measures for ensuring system configuration, including default configuration***

Processor will apply system hardening for all Internet-facing services through centralised configuration management, regular vulnerability scanning and configuration review.

***Measures for internal IT and IT security governance and management***

Processor maintains an efficient information security management system in place to ensure proper organisation of information security responsibilities and a security risk assessment is performed on a periodic basis to ensure the identification of new or changed risks.

Processor shall allocate resources and employees that have the required expertise for carrying out any specific task in relation to its security responsibilities under this Agreement.

Processor will ensure that there is proper protection of all assets containing personal data provided by the Controller in the context of this Agreement.

***Measures for certification/assurance of processes and products***

At Processor's complete discretion, a periodic self-certification process will be completed by the Processor to ensure that all security-related policies and procedures are still applied.

***Measures for user identification and authorisation***

**Applicable if Controller uses Processor's verification and/or extraction service:** Access to the service is granted to only authorized users through unique client credentials which can be revoked and renewed at any time by the Controller.

***Measures of pseudonymisation and encryption of personal data and for the protection of data during transmission***

**Applicable if Controller uses Processor's verification and/or extraction service:** The Processor will use strong encryption methods such as TLS (latest supported versions) for data in transit.

**Applicable if Controller uses Processor's support services:** To securely transfer personal data to Processor, Controller shall use Processor's Secure Image Upload.

***Measures for ensuring data minimisation, limited data retention and erasure***

**Applicable if Controller uses Processor's verification and/or extraction service:** The Processor does not store personal data after the verification process has been carried out.

**Applicable if Controller uses Processor's support service:** Processor shall implement data retention schedules and irreversibly delete the data according to the schedule.

***Measures for ensuring data quality***

**Applicable if Controller uses Processor's verification and/or extraction service:** Controller is responsible for data that is sent to the Processor, including its quality. The Processor will send to the Controller personal data extracted from the documents sent by the Controller together with personally identifiable information (PII) data and metadata scraped from the documents.

**Applicable if Controller uses support services:** Controller and Processor will determine what quality of data needs to be shared to resolve the issue raised by the Controller.

***Measures for the protection of data during storage***

**Applicable if Controller uses Processor's support service:** Microblink uses Key Management Service for encryption of data at rest.

***Measures of pseudonymisation and encryption of personal data and for the protection of data during transmission***

**Applicable if Controller uses Processor's verification and/or extraction service:** The Processor will use strong encryption methods such as TLS (latest supported versions) for data in transit.

**Applicable if Controller uses Processor's support services:** To securely transfer Personal Data to Microblink, Licensee shall use Microblink' Secure Image Upload.

***For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the***

***(sub-) processor to be able to provide assistance to the controller***

The Processor shall have data processing agreements with sub-processors in place to ensure assistance to the Controller.

***Description of the specific technical and organisational measures to be taken by the processor to be able to provide assistance to the controller.***

**Applicable if Controller uses Processor's support services:** Controller shall make sure that they can identify their end-users and, in case of a data subject's request, deliver their identifiers to the Processor. Processor shall provide assistance to the Controller in carrying out the data subject's request in accordance with the procedure for data deletion.

**ANNEX IV: LIST OF SUB-PROCESSORS**

The controller has authorised the use of the following sub-processors:

1. Name: Microblink LLC (if the signatory is Microblink Ltd. or Microblink USA LLC)

Address: Trg Drage Iblera 10, 10000 Zagreb, Croatia

Contact person's name, position and contact details: Ena Oršić, Legal Associate and Data Protection Officer

Description of the processing: Providing support services.

2. Name: Google Cloud Platform

Address: As specified on the following link (https://cloud.google.com/terms/google-entity).

Contact person's name, position and contact details: As specified on the following link (https://cloud.google.com/privacy/gdpr).

Description of the processing: Sub-processor's platform will be used for running Processor's technology for processing the personal data during the extraction and/or verification session. After the finished session, the data will not be stored.

**Microblink**


Signatory: Hartley Thompson

Title: Director

Email of signatory: hartley.thompson@microblink.com

Timestamp: Monday, 11 March 2024 12:54 UTC

# Data processing addendum for the use of Microblink technology and support services

Contract ID
65e5982672e3811feddacce6

Filename

## Microblink


Signatory: Hartley Thompson

Email of signatory: hartley.thompson@microblink.com

Timestamp: Monday, 11 March 2024 12:54 UTC

| | What | When | Where |
|---|---|---|---|
| | Signed by Hartley Thompson<br>hartley.thompson@microblink.com | 11 Mar 2024<br>12:54 UTC | IP 166.198.21.41<br>Mozilla/5.0 (iPhone; CPU iPhone OS 17_4 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.4 Mobile/15E148 Safari/604.1 |
| | Viewed by Hartley Thompson<br>hartley.thompson@microblink.com | 11 Mar 2024<br>12:54 UTC | IP 166.198.21.41<br>Mozilla/5.0 (iPhone; CPU iPhone OS 17_4 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.4 Mobile/15E148 Safari/604.1 |
| + | Created by Ena Oršić<br>ena.orsic@microblink.com | 4 Mar 2024<br>09:45 UTC | IP 141.138.10.94<br>Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:121.0) Gecko/20100101 Firefox/121.0 |