DATA PROCESSING AGREEMENT

BETWEEN

SHARINPIX, a French registered "***Société à Responsabilité Limitée"*** **(SARL)** governed by the laws of France, having its registered offices located at 23, rue d'Anjou, 75008 Paris, France, registered in the Trade and Companies Register of Paris under the number 811 371 145, represented by Mr. Jean-Michel Mougeolle, duly empowered for the purposes hereof (hereafter "**SHARINPIX**").

Hereinafter the "**Provider**" or the "**Processor**"

AND

[Customer], corporate form, with a capital of XXX €, whose registered office is located XXX, registered in the trade and companies register of XXX under the number XXX, represented by XXX, [function],

Hereinafter the "**Customer**" or the "**Controller**"

Together the "Parties", individually a "Party".

HAVE JOINTLY AGREED AS FOLLOWS:

The Parties have entered into an agreement (specify Agreement reference) dated XXX, hereinafter the "Agreement".

The performance of the Agreement, by the provider, does not involve a processing of personal data on behalf of the Customer. However, if evidence is provided by one of the Parties that, in the context of the performance of the Agreement, the Provider processes personal data on behalf of the Customer, as data processor, then the provisions of this Data Protection Agreement ("DPA") apply.

In such hypothesis, the term "Controller" shall refer to the Customer, and the term "Processor" shall refer to the Provider, for the purposes hereof.

ARTICLE I: PURPOSE AND SCOPE

The purpose of this DPA is to ensure compliance of the Processing the with all laws and regulations applicable to the processing of Personal Data, the EU GDPR, the UK GDPR, the UK Data Protection Act 2018, the Swiss Federal Act on Data Protection of 19 June 1992 (SR 235.1; FDPA), the California Consumer Privacy Act of 2018 and any applicable national implementing laws, regulations and secondary legislation relating to the processing of Personal Data (hereafter referred to as the "Regulation"),

If there is no clear evidence that Personal Data is being processed while performing the Agreement or that the Provider acts as data processor, the provisions of the present DPA shall not apply and shall not be enforceable by any Party.

ARTICLE II: INTERPRETATION

Where this DPA uses the terms defined in the Regulation, those terms shall have the same meaning as in the Regulation.

ARTICLE III: HIERARCHY

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, this DPA shall prevail.

ARTICLE IV: DESCRIPTION OF THE PROCESSING

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 I.

ARTICLE V: OBLIGATIONS OF THE PROCESSOR

5.1 Instructions

The Processor shall process personal data only on documented instructions from the Controller, unless required to do so by Union or Member State law 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.

The Processor shall immediately inform the Controller if, in the Processor's opinion, instructions given by the Controller infringe the Regulation.

5.2 Duration

The Processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex I and only for the duration of the Agreement, unless it receives further instructions from the Controller.

5.3 Security

The Processor shall at least implement the technical and organizational measures specified in Annex II 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, unauthorized disclosure or access to the data (personal data breach).

The Processor shall ensure that persons authorized to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

The Processor is not responsible for the management of the rights of access of the end user of its application and shall not be held liable on that regard.

5.4 Documentation and audits

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 the Regulation. At the Controller's request, the Processor shall also permit and contribute to audits of the processing activities covered by this DPA subject to a 30 days' notice. In deciding on a

review or an audit, the Controller may take into account relevant certifications held by the Processor.

Any audit conducted under this DPA shall only consist of examination of the most recent reports, certificates and/or extracts prepared by an independent third-party auditor appointed by both Parties and that has no competitive relationship whatsoever with the Provider.

The third-party auditor will be bound by the same confidentiality provisions as to those set out in the Agreement agreed upon between both parties.

The audit operations will be (i) at the Controller's expense; (ii) limited in scope to matters specific to the Controller and agreed in advance by the Processor; (iii) carried out during the Processor's usual business hours and upon reasonable notice which shall be not less than 4 weeks and (iv) conducted in a way which does not interfere with the Processor's day-to-day business (v) limited to one (1) audit per calendar year, except for the audits carried out on the instructions of a Supervisory Authority.

The Parties hereby acknowledge that, under no circumstances will the audit operations lead to the disclosure of the Provider's source codes without his prior written consent.

All audit costs incurred by the Processor, including costs arising from the mobilization of personnel by the Processor, will be borne by the Controller integrally and invoiced at the Provider's public price for assistance on the day of the audit.

5.5 Use of sub-processors

The Processor has the Controller's general authorization for the engagement of sub-processors. The Processor shall specifically inform in writing the Controller of any intended changes of 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).

If the opposition persists, the Processor will, at its choice:

- select another sub-processor.
- refrain from modifying, changing, adding or replacing the sub-processor; or
- maintain the modification, change, addition, or replacement, in which case the Controller may terminate the Agreement with 30 days' notice, without further liability to either party.

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 this DPA.

The sub-processors listed in Annex III are deemed accepted by the Controller. This authorization extends to AI Providers appointed pursuant to Annex IV of this DPA.

5.6 International transfers

The Controller authorizes the Processor to transfer personal data to a third country or an international organization, provided the Processor ensures compliance of this transfer to the

Regulation, for instance by signing Standard Contractual Clauses of the EU Commission with the recipient of the personal data.

5.7 Assistance to the Controller

The Processor shall promptly notify the Controller of any request it has received from the data subject. It shall not respond to the request itself.

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.

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:

- the obligation to carry out a data protection impact analysis 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 obligation to consult the competent supervisory authority 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;
- the obligation to implement the organizational and technical security measures adapted to the risk.

5.8 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 to notify and communicate the personal data breaches, taking into account the nature of processing and the information available to the Processor.

In particular, 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:

- a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
- the details of a contact point where more information concerning the personal data breach can be obtained.
- 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.

ARTICLE VI: OBLIGATIONS OF THE CONTROLLER

The Controller shall comply with the Regulation.

The Controller is responsible for the categorization of the personal data and shall ensure, in that regard, that the personal data entrusted to the Processor complies with the requirements of the

Regulation, its obligations under the Agreement (including if the Agreement specifies that the data processed by the Provider shall not include personal data) and the description of the processing specified in Annex I.

More generally, the Customer shall comply with applicable law and/or regulation. On that regard, the content processed by the Provider on behalf of the Customer shall not infringe applicable law and/or regulation (including legal confidentiality obligation, intellectual property, right to privacy, criminal law, etc.).

The Customer is solely responsible for ensuring that the content of all data processed by the Processor complies with current Regulations and does not infringe the rights of any third parties in any way whatsoever.

The Provider declines all responsibility if the Customer's data infringes any Regulation and/or violates the rights of any third parties. The Customer fully guarantees and hold the Provider harmless against any third-party action or claim, of any nature whatsoever, directly, or indirectly related to the content uploaded by the Customer into the Provider's Solution.

ARTICLE VII: TERMINATION

Following termination of the contract, 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 Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the Processor shall continue to ensure compliance with this DPA.

Date and signature of the Customer	Date and signature of the Provider

ANNEX I

Description of the processing

Categories of data subjects whose personal data is processed	Persons whose personal data are embedded within pictures submitted by the Customer
Categories of personal data processed	Picture, any personal data embedded within a picture submitted by the Customer
Nature of the processing	Collection, storage, alteration, consultation, disclosure by transmission, erasure
Purpose(s) for which the personal data is processed on behalf of the Controller	Provision of the service by the Provider
Duration of the processing	The duration of the agreement between the Customer and the Provider

ANNEX II

Security measures

Item	Description of the security measures
Confidentiality/Encryption	Both AWS S3 storage and Heroku Databases are encrypted at rest (disk level). In addition, all data in transit are encrypted with SSL/TLS 1.2 protocol minimum, following Salesforce Policy
Authentication	Authentication between Salesforce and SharinPix is based on OAuth 2.0 protocol. SharinPix is a Salesforce add-on and access rights to the SharinPix solution are managed by the Customer's administrator for the Customer's Salesforce environment. SharinPix is not responsible for management of end-user access rights to its solution.
Traceability (logging)	All admin action are logged and any access to customers' data raises an alert and must be justified .
Fighting malware and vulnerability remediation	Processor's services are delivered through a web app hosted at Heroku (Salesforce). Processor uses the network protection (firewalls etc) provided by Heroku. In addition, the app is protected by cloudflare (DDOS attacks). Vulnerabilities on servers and cloud infrastructure are patched by AWS/Heroku following their best practices policies. Source code is continuously monitored against vulnerabilities by using a security code scanning service (Github advanced Securty) As for public libraries used, in case of vulnerabilities in the code/application of the Processor, workaround is provided following patch availabilities in the Common Vulnerabilities and Exposures (CVE). Critical vulnerabilities are patched within 48 hours. Controller is responsible for software upgrades on mobile devices if they use the SharinPix mobile App. Processor uses heroku and can deploy new version of its application in less than an hour. For Salesforce components, ISV upgrade process allows to push upgrade automatically to all or part of all tenants.

Backups	Backups and disaster recovery plan are implemented. In case of a disaster (natural disaster, fire … i.e. unavailability of premises), service continuity is assured remotely by team members through secured connection. On-site intervention of the team can also be considered within a time frame of 72 hours. Images are duplicated and stored "on the fly" on 2 separate Amazon S3 storage sites. The database for image metadata (PostgreSQL) is hosted by Heroku (Salesforce) with a continuous backup plan: data is replicated within seconds between 2 different data center (redo log mechanism). Recovery Time Objectif (RTO) in case of total disaster is at a maximum of 12 hours, following Heroku/Salesforce engagement. Recovery Point Objectif (RPO) in case of total disaster is at a maximum of 4 hours, following Heroku/Salesforce engagement. This is the engagement for the image metadata database. Image files stored on Amazon Web services are duplicated in real time and cannot be lost
Removal of sources of risk	A development process including the analysis and the processing of security risk is implemented. An automated scan for security breaches is performed. Penetration tests are performed by an independent third-party provider. Processor conducts systematically 3 types of tests before any deployment: • Automated test These tests are defined during design phase and coded. For any new or changed code deployment, all automated tests (old and newly added tests) are run in order to ensure new features is compliant and does not generate regression on other features. • Predefined test scenario execution A dedicated SharinPix team member is executing functional testing on any new features, correction or existing feature (non-regression) • Exploratory testing "Exploratory testing seeks to find out how the software actually works, and to ask questions

	about how it will handle difficult and easy cases. The quality of the testing is dependent on the tester's skill of inventing test cases and finding defects. The more the tester knows about the product and different test methods, the better the testing will be." Exploratory testing is performed by advanced SharinPix users or developers continuously.
Security review process by Salesforce	A yearly program is implemented by Salesforce to review security measures and certify the procedures of ISV Partners apps. All applications enrolled in the ISVForce or Force.com Embedded Partner Programs must go through a mandatory periodic security review. The Security Review has been developed to assess the security posture of partner offerings, to ensure that applications published on the AppExchange follow industry best practices for security, and to promote trust. The scope of the security review depends on the composition of the offering. Most offerings contain one or more parts that are classified as Native, Composite (Web Applications), or Client/Mobile. Salesforce approach is to test all parts of the offering to ensure that our mutual customers and their data are not put at risk. The table below describes at a high level what testing is performed for each part.
Incident and data breach management	A security response plan and a cyber-attack response plan are implemented.
Personnel management	A background check is performed when personnel is recruited. Yearly training related to good practices and risks is performed.

ANNEX III

List of sub-processors

The Controller has authorized the use of the following sub-processors:

Name of the sub-processor	Location	Description of the processing
Amazon Web Services (unless the Customer wishes to use its own AWS hosting solution)	USA or EU depending on the specific situation of the Customer	Hosting of data
Cloudinary	USA, Israel, potentially worldwide	Images transformations & Content delivery network . %Use of cloudinary is not implemented in all customers configurations. (depends on use cases)
Heroku (Saleforce)	USA	Processing of data. (Platform as a Service hosting the SharinPix web app)
OpenAI, Inc.	USA	AI inference via API (image data extraction for AI Features) — see Annex IV.

ANNEX IV: AI Sub-Processor

This Annex IV supplements the DPA and governs the processing of Personal Data through AI Features (as defined in Article 9 of the License Agreement) and the appointment of any AI Provider as sub-processor.

Its provisions apply automatically upon the Controller's activation of AI Features under a Company AI Subscription. The list of AI Providers in force at any time is set out in Annex III. In the event of conflict, this Annex IV prevails over the general DPA provisions with respect to AI sub-processing.

I. Processing Roles

The Controller is the Data Controller. SharinPix (Processor) acts as Data Processor and appoints one or more AI Providers as sub-processors pursuant to Article 28(2) GDPR. The Processor remains liable to the Controller for each AI Provider's acts and omissions to the same extent as for its own, subject to the liability cap in the License Agreement.

II. Description of Processing

Subject matter: automated extraction and recognition of data from images, including serial numbers, VINs, and alphanumeric identifiers.

Nature: transmission of Customer Data to the AI Provider's API; receipt of output; delivery to Controller. Purpose: delivery of AI Features under Article 8bis of the License Agreement.

Duration: term of the License Agreement or until Controller deactivates AI Features. Data subjects: any individual whose Personal Data is incidentally present in images submitted by Controller; Controller is responsible for minimizing such presence.

Personal Data categories: any Personal Data incidentally present in submitted images; biometric data and special category data (Article 9 GDPR) are prohibited unless Controller has a valid legal basis and has notified the Processor in writing in advance.

III. International Transfers

Where an AI Provider is established in a third country, the transfer of Personal Data is governed by an appropriate transfer mechanism within the meaning of Chapter V GDPR — including Standard Contractual Clauses adopted pursuant to Commission Decision (EU) 2021/914, Module 3 (Processor to Sub-Processor), as incorporated in the relevant AI Provider's data processing addendum listed in Annex III. The Controller authorizes such transfers by activating AI Features under a Company AI Subscription.

IV. Specific Obligations of the Processor

In addition to Article V of this DPA, the Processor shall: (i) enter into a data processing agreement with each AI Provider imposing, in substance, the same data protection obligations as those set out in this DPA; (ii) contractually prohibit each AI Provider from using Customer Data to train, fine-tune, or improve any AI model; (iii) ensure that Customer Data transmitted via AI Features is not retained by any AI Provider beyond the time required to process the request and return the output; (iv) notify the Controller without undue delay of any Personal Data breach affecting data

processed by an AI Provider, to enable the Controller to meet its obligations under Article 33 GDPR; and (v) maintain encrypted transit for all transmissions to any AI Provider API.

V. Specific Obligations of the Controller

In addition to Article VI of this DPA, the Controller warrants that: (i) it has a lawful basis for any Personal Data transmitted via AI Features; (ii) it has provided all required information notices to data subjects; and (iii) it shall not submit special category data (Article 9 GDPR) through AI Features without the Processor's prior written consent. The Controller shall indemnify the Processor against any claim arising from the Controller's failure to comply with this section V.

VI. Retention and Deletion

AI Providers shall not retain API inputs beyond the time required to process the request and return the output, in accordance with their respective data processing addenda. The Processor does not independently retain AI inputs following delivery of the output to the Controller, except for security logging purposes for a maximum of 30 days. Upon termination or the Controller's deactivation of AI Features, the Processor shall cease all transmissions to AI Providers within 10 Business Days.