EYESmart Data Processing Agreement

Effective Date: 01/09/2025
Version 1.0

The Customer

(hereinafter **"Customer"**) and

Early Years Evaluation Smart Ltd., 20 Wenlock Road, London, England, N1 7GU
(hereinafter **"EYESmart"**)

(each a "Party" and collectively the "Parties")

have concluded this Data Processing Agreement (this "***DPA***") regarding the Processor's processing of personal data on behalf of the Customer.

This DPA is effective as of the date of the Agreement.

Definitions

"**Agreement**" means the main agreement (terms and conditions and EYESmart Offer) entered into between the Customer and EYESmart as amended from time to time in accordance with its terms;

"Application Log" means the log used for storing access to Customer Data;

"**Applicable Data Protection Laws**" means laws and regulations applicable to EYESmart's Processing of Personal Data under the Agreement, including but not limited to (a) EEA Data Protection Laws, (b) UK Data Protection Laws (c) CCPA, (d) Swiss new Federal Act on Data Protection (nFADP), and (e) Texas Data Privacy and Security Act (as applicable);

"**Authorised Sub-Processors**" means the Sub-Processors set out in Appendix B as may be amended from time to time;

"**CCPA**" means collectively the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (the "**CPRA**"), and any regulations promulgated thereunder;

"**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data;
"**Customer Data**" means the Personal Data regarding individuals made available to EYESmart by or on behalf of the Customer, pursuant to the Agreement for Processing to provide the Services;

"**Customer Point of Contact**" has the meaning given in Clause 18.3;

"**Data Breach** " has the meaning given in Clause 10.1;

"**Data Centres**" means the data centres used for hosting and storing of Customer Data on the EYESmart Platform;

"**Data Subject Request**" has the meaning given in Clause 9.1;

"**DPA**" means this Data Processing Agreement, including any schedules attached or referred to and including any future written amendments and additions (as applicable);

"**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EU;

"**EEA**" means the European Economic Area, and the countries which are party to the European Economic Area Treaty;

"**EEA Data Protection Laws**" means all applicable laws and regulations relating to privacy and/or processing of Personal Data, including but not limited to the GDPR (as amended from time to time);

"**Personal Data**" means "personal data", "personal information", "personally identifiable information" or similar term defined in Applicable Data Protection Laws;

"**Process**" and inflections thereof means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

"**Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller;

"**Services**" means the EYESmart Platform services described and provided under the Agreement and in accordance with this Data Processing Agreement; "**Sub-Processor**" has the meaning given in Clause 6.1;

"**Supervisory Authority**" shall have the same meaning as in the Applicable Data Protection Laws;

"**UK Data Protection Laws**" means all applicable privacy and data protection laws relating to the processing of Personal Data and the privacy of electronic communications including the UK GDPR, Data Protection Act 2018, the Privacy and Electronic Communications Directive (2002/58/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426) and any laws that replace, extend, re-enact, consolidate or amend any of the foregoing;

"**UK GDPR**" means the GDPR as amended and incorporated into UK law under the European Union (Withdrawal) Act 2018;

"**UK** " means the United Kingdom;

"**Transfer Mechanism**" means (i) the Standard Contractual Clauses approved by the European Commission Decision of 4 June 2021 (processor to processor) as amended from time to time, (ii) the International Data Transfer Agreement ("IDTA") issued by the Information Commissioner's
Office under Section 119A of the Data Protection Act 2018 (effective from 21 March 2022), (iii), the International Data Transfer Addendum ("Addendum") issued by the Information Commissioner's
Office under Section 119A of the Data Protection Act 2018 (effective from 21 March 2022), (iv) Data Protection Clauses approved by the Swiss Federal Data Protection and Information Commissioner ("FDPIC"), and (v) any other such legally approved mechanisms for ensuring the safety and security of data transfers from outside of the EEA/UK/Switzerland.

All capitalized terms not otherwise defined herein shall have the meaning set out in the Agreement.

Any reference to **writing** or **written** includes email.

1. Background

1.1. The Parties have entered into the Agreement, where the Customer has engaged EYESmart to provide the Services. This DPA, including all attached appendices, is incorporated into the Agreement by reference.

1.2. For the purposes of providing the Services under the Agreement, EYESmart will Process Customer Data throughout the Term of this DPA. This DPA applies to any and all activities associated with the Agreement, in whose scope EYESmart's employees or agents Process the Customer Data on behalf of the Customer.

2. Responsibilities and Instructions

2.1. The parties agree that under this DPA the Customer and the Customer's end-customer are the Controller of the Customer Data and EYESmart is the Processor of the Customer Data. The Customer agrees that this DPA, and not EYESmart's Privacy Policy, applies to EYESmart's processing of Customer Data as a Processor.

2.2. The Customer is responsible for compliance with the Applicable Data Protection Laws, including but not limited, to the lawfulness of disclosing Customer Data to EYESmart and the lawfulness of having the Customer Data Processed by EYESmart on behalf of the Customer. The Customer warrants that it is

lawfully authorised to Process and disclose the Customer Data to EYESmart. The Customer is responsible for maintaining and updating its respective privacy policy, notices and statements, including to mention EYESmart in it as its Processor.

2.3. EYESmart shall process Customer Data only on documented instructions from the Customer, unless required to do so by the Applicable Data Protection Laws or any other applicable law to which EYESmart is subject. Such instructions shall be specified in this DPA and Appendices A and C. Subsequent instructions can also be given by the Customer throughout the duration of Processing of Customer Data, but such instructions shall always be documented and kept in writing, including electronically, in connection with this DPA.

2.4. EYESmart shall immediately inform the Customer if instructions given by the Customer, in the opinion of EYESmart, contravene the Applicable Data Protection Laws. EYESmart is entitled to suspend performance on such instruction until the Customer confirms or modifies such instruction.

2.5. EYESmart may access Customer Data on a limited and need-to-know basis for the purposes of providing support, troubleshooting and maintaining the Platform, provided that such access is solely for the purpose of delivering the Services in accordance with the Agreement and DPA.

3. Details of Processing

3.1. The subject matter and nature of EYESmart's Processing of Customer Data are the performance of the Services pursuant to the Agreement and the purposes set forth in this DPA. The Customer and/or its Authorised Users upload/insert the Customer Data to the Platform, and the types of Customer Data Processed depend on the Customer use of the Services. The purpose of Processing, the types of Customer Data and categories of Data Subjects that may be Processed under this DPA is further specified in Appendix A.

3.2. The Processing of Customer Data shall continue for the duration of the Agreement and this DPA and for 60 days after termination, unless the Customer requests earlier deletion, performs a deletion themselves, or as otherwise specified in Appendix A.

3.3. Appendix D (Additional Data Protection Legislation) to this DPA applies only if and to the extent EYESmart's Processing of Customer Data under the Agreement is subject to (i) the

Swiss new Federal Act on Data Protection (nFADP), (ii) the CCPA with respect to which Customer is a "business" as defined in the CCPA, or (iii) the Texas Data Privacy and Security Act.

4. Security of Processing

4.1. EYESmart is responsible for implementing technical and organisational measures to ensure the adequate protection of the Customer Data, which measures must fulfil the requirements of the Applicable Data Protection Laws and ensure ongoing security, confidentiality, integrity, availability and resilience of processing systems and Services. Such measures are described in Appendix C of this DPA.

4.2. EYESmart shall regularly review, assess and update, as necessary, these measures to address evolving security risks, industry standards, technological advancements, and regulatory changes. EYESmart reserves the right to modify the measures and safeguards implemented, provided that the level of security is not less protective than initially agreed upon. In the event of considerable changes to the measures, EYESmart shall notify the Customer of the changes.

4.3. EYESmart warrants that the company fulfils its obligations under Applicable Data Protection Laws to implement a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

4.4. The Customer is familiar with the technical and organisational measures set out in Appendix C, and it shall be the Customer's responsibility that such measures ensure a level of security appropriate to the risk.

5. Confidentiality

5.1. EYESmart will keep the Customer Data confidential. This obligation persists without time limitation and will survive the termination or expiration of the Agreement and this DPA.

5.2. EYESmart shall only grant access to the Customer Data being processed on behalf of the Customer to persons under EYESmart's authority who have committed themselves to confidentiality or are under appropriate statutory obligation of confidentiality and only on a need-to-know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and Customer Data consequently not be accessible anymore to those persons.

5.3. EYESmart shall at the request of the Customer demonstrate that the concerned persons under EYESmart's authority are subject to the abovementioned confidentiality.

6. Sub-Processing

6.1. Customer generally authorises EYESmart to appoint and engage Sub-Processors in accordance with this Clause 6. The Customer acknowledges that EYESmart uses subcontractors that act as Sub-Processors on behalf of the Customer ("**Sub-Processor**").

6.2. The Customer agrees that the Sub-Processors listed in Appendix B are authorised for the purpose of the Processing of the Customer Data under this DPA, **giving affirmative consent thereto**.

6.3. EYESmart will, prior to the use of new Sub-Processor or a replacement of Sub-Processor, inform the Customer Point of Contact thereof with at least thirty (30) days' prior written notice. The Customer is entitled to object in writing within fourteen (14) days after

receipt of the notice from EYESmart, provided that such objection is based on reasonable grounds relating to data protection. EYESmart will evaluate the concerns and discuss possible solutions with the Customer. If these solutions are not reasonably possible in EYESmart's discretion and the Customer continues to not approve the change (such approval may not be unreasonably withheld), the Customer may terminate the

Agreement by giving fourteen (14) days' written notice after having received EYESmart's aforementioned decision. If the Customer does not terminate the Agreement within this timeframe, the Customer is deemed to have accepted the respective Sub-Processor. The Customer will receive a refund of any prepaid fees for the period following the effective date of termination in respect of such terminated services. No other claims of the Customer against EYESmart or of EYESmart against the Customer may be based on such termination.

6.4. The Customer accepts that an exchange of a Sub-Processor may be required in cases where the reason for the change is outside of EYESmart's reasonable control (so-called emergency replacement). EYESmart will notify the Customer of such change. If the Customer reasonably objects to the use of this Sub-Processor, the Customer may exercise its right to terminate the Agreement as described in the Clause above.

6.5. Where EYESmart engages Sub-Processors, EYESmart is responsible for ensuring that EYESmart's obligations on data protection resulting from the Agreement and this DPA are, to the extent applicable to the nature of the services provided by such Sub-Processor, valid and binding upon subcontracting. EYESmart will enter into written agreement and will restrict the Sub-Processor (and any new Sub-Processors) access to Customer Data only to what is necessary to provide or maintain the Services in accordance with the Agreement and this DPA.

6.6. If the Sub-Processor does not fulfil its data protection obligations, EYESmart will remain fully liable to the Customer as regards the fulfilment of the obligations of the Sub-Processors. EYESmart's liability will be to the same extent as if EYESmart were directly performing those services, but within limitations of liability set out in this DPA and Agreement.

7. Location of Customer Data and Third Country Transfer

7.1 The location(s) of the Customer Data is set out in Appendix B to this DPA.

7.2. Subject to Authorised Sub-Processors in Appendix B, EYESmart will not transfer the Customer Data outside the EEA, the UK and/or Switzerland without following the notification and objection process set out in Clause 6.3.

7.3. Customer Data may be transferred from the EEA, the UK and/or Switzerland to countries that have been recognised as providing an adequate level of data protection, either through an adequacy decision by the European Commission or by the relevant data protection authorities of the UK and Switzerland ("Adequacy Decisons"), as applicable, without any further safeguards being necessary.

7.4. If the processing of the Customer Data includes a transfer from the EEA, the UK and/or Switzerland to other countries which have not been subject to relevant Adequacy Decision ("Third Country Transfer"), the transfer shall be secured following the undertaking by EYESmart of a transfer risk assessment/transfer impact assessment (under EU, UK, and/or Swiss law as applicable to the Customer), through the implementation, and negotiation if applicable, of an agreement incorporating the appropriate Transfer Mechanism. If the Transfer Mechanism is insufficient to safeguard the transferred Customer Data, supplementary measures will be implemented to ensure the Customer Data is protected to the same standard as required under Applicable Data Protection Laws, including those set out in Appendix D. The Customer acknowledges and agrees that EYESmart has incorporated the appropriate Transfer Mechanism into all agreements with Sub-Processors in third countries, where Adequacy Decision is not in place, ensuring that such Third Country Transfer comply with the Applicable Data Protection Legislation.

8. Deletion, correction or return of Customer Data

8.1. Customer may delete Customer Data using the functionality provided by the Services. Where the Customer is unable to perform the deletion and/or correction of the Customer Data, EYESmart must perform the action if so, instructed by the Customer and permitted under Applicable Data Protection Laws. Where a deletion request relating to Customer Data, consistent with Applicable Data Protection Laws or a corresponding restriction of Processing is impossible, EYESmart will, based on the Customer's instructions, and unless agreed upon differently in the Agreement, destroy or otherwise put out of use if so instructed, in compliance with Applicable Data Protection Laws, all Customer Data or return the same to the Customer.

8.2. Within 60 days following the termination of the Agreement, EYESmart shall, upon the Customer's end-customer's (parents of childcare providers) or individual parent Customer's instructions, return all Customer Data to the Customer or delete the same (all children's data will be deleted upon receiving the request from parents directly, rather than the childcare provider, if the Customer is childcare provider), unless required otherwise by the Applicable Data Protection Laws. The Customer Data shall be irreversibly deleted and cannot be retrieved and provided to the Customer after such 60 days. In specific cases designated by the Customer, Customer Data will be stored. The associated remuneration and protective measures will be agreed upon separately, unless already agreed upon in the Agreement.

9. Data Subject Request

9.1. Where a Data Subject asserts claims for rectification, erasure, objection or access ("Data Subject Request") against EYESmart, and where EYESmart is able to correlate the Data Subject to the Customer, based on the information provided by the Data Subject, EYESmart will without undue delay refer such Data Subject to contact the Customer directly.

9.2. EYESmart will, based upon the Customer's instructions, support the Customer to the extent reasonably possible in fulfilling a Data Subject Request, where the Customer cannot do so without EYESmart's assistance. EYESmart will not be liable in cases where the Customer fails to respond to the Data Subject's request in total, correctly, or in a timely manner.

10. Data Breaches

10.1. EYESmart will notify the Customer as soon as possible upon becoming aware of any unauthorised or unlawful processing, alteration, loss, destruction or disclosure of, or damage or access to the Customer Data ("Data Breach") that occurs within EYESmart's scope of responsibility. This includes Data Breaches involving any Sub-Processors engaged by EYESmart, to the extent EYESmart becomes aware of such breach. EYESmart will implement the measures necessary for securing Customer Data and for mitigating potential negative

consequences for the Data Subject. EYESmart will coordinate such efforts with the Customer without undue delay.

10.2. EYESmart will support the Customer, to the extent reasonably possible and only where the Customer cannot do so without EYESmart's assistance, in communicating Data Breaches to the affected Data Subjects and notifying Data Breaches to the applicable authorities as required by Applicable Data Protection Laws (provided that this support does not result in any breach of EYESmart's confidentiality obligations towards third parties).

11. Data Protection Impact Assessment and Consultation with Supervisory Authorities

11.1. To the extent that the required information is available to EYESmart, and the Customer does not otherwise have access to the required information, EYESmart will, upon written request, provide reasonable assistance to the Customer with any data protection impact assessment, and prior consultations with applicable Supervisory Authorities or the extent required under Applicable Data Protection Laws.

12. Audits and Inspections

12.1. EYESmart will on an annual basis undergo an independent external audit of information security and measures pursuant to this DPA. EYESmart will document EYESmart's compliance with the technical and organisational measures agreed upon in this DPA by appropriate measures.

12.2. To the extent required under the Applicable Data Protection Laws and upon the Customer written request, EYESmart will provide the Customer with all information necessary to demonstrate compliance under this DPA and provide a copy of an independent external audit report, as may be applicable. The documentation is EYESmart's confidential information and must be treated as such.

12.3. The Customer agrees to exercise its audit and inspection rights by instructing EYESmart to share the audit report described in clause 12.2 of this DPA. If the Customer reasonably concludes that an onsite audit or inspection is necessary to monitor the compliance with the technical and organisational measures in an individual case or compliance with this DPA, the Customer has the right to carry out respective onsite audits or inspections in individual cases or to have them carried out by an auditor (that is no competitor of EYESmart) provided that such audits or inspections will be conducted (i) during regular business hours, and (ii) without disproportionately interfering with EYESmart' business operations, (iii) upon prior reasonable notice and further consultation with EYESmart, (iv) all subject to (if not covered already by the Agreement) the execution of a confidentiality undertaking, in particular to protect the confidentiality of the technical and organisational measures and safeguards implemented. Onsite audit or inspection may be unannounced where the Customer has a legally binding request by a Supervisory Authority or a documented suspicion of a material breach or non-compliance with Applicable Data Protection Laws. Justification of an unannounced audit or inspection must be provided at the time of arrival.

12.4. In case of an onsite audit or inspection the Customer will bear its own expenses and compensate EYESmart the cost for its internal resources required to conduct the onsite audit or inspection (based on time and material according to the then current price list). If the audit or inspection reveals that EYESmart has breached its obligations under the Agreement or this DPA, EYESmart will promptly remedy the breach at its own cost and refund any payments made by the Customer towards the cost of EYESmart's internal resources related to the Customer onsite audit or inspection.

13. Application Log and Linked Services

13.1. EYESmart stores Customer Data in the Application Log (the "***Application Log Data***") for 60 days.

13.2. The Application Log Data is used by EYESmart for demonstrating compliance with regulatory and legal requirements, and for the purposes of ensuring good functioning of the Platform, only.

13.3. Access to the Application Log Data is strictly limited to the above use cases.

a) Should Customer require access to the Application Log Data for the purposes of regulatory or legal compliance, safeguarding, audit, or other similar purpose, EYESmart can provide access to the Customer.

13.4. Should Customer engage a Linked Service Provider, as defined in the EYESmart Terms & Conditions, then EYESmart may provide an Open API for access to certain Customer Data to enable the functioning of the Linked Services. Customer is solely responsible for ensuring that the Linked Service Provider provides sufficient protection for Personal Data, as required by the Applicable Data Protection Laws. Under no circumstances will a Linked Service Provider be considered a Sub-Processor to EYESmart of the Customer Data.

14. Defence Support

14.1. Where a Data Subject asserts any claims against the Customer as permitted by Applicable Data Protection Laws, EYESmart will provide all reasonable assistance to the Customer in defending against such claims.

14.2. The clause above will apply, mutatis mutandis, to claims asserted by Data Subjects against EYESmart in accordance with Applicable Data Protection Laws.

15. Term of this DPA

15.1. This DPA and Processing will continue in force until 60 days after the termination of the Agreement, except where this DPA stipulates obligations beyond the term of the Agreement.

16. Limitations of Liability

16.1. EYESmart is only liable for data protection losses, costs and expenses incurred as a result of i) EYESmart not complying with its obligations under this DPA; ii) EYESmart not complying with its Processor obligations under the Applicable Data Protection Laws; or iii) EYESmart's Authorised Sub-Processor not complying with its data protection obligations (whether imposed under contract to EYESmart or by Applicable Data Protection Laws).

16.2. Each Party's total aggregate liability arising out of or related to this DPA shall be subject to the exclusions and limitations of liability set forth in Clause 15 of the Agreement, unless otherwise agreed.

16.3. Subject to Clause 16.1 and 16.2, each party (the "Indemnifying Party") will indemnify the other Party (the "Indemnified Party") against all claims and proceedings and all liability, loss, costs and expenses incurred by the Indemnified Party as a result of any claim made or brought by a Data Subject or other legal person in respect of any loss, damage or distress caused to them, or any fine imposed by a regulatory authority, as a result of any breach of the Applicable Data Protection Laws by the Indemnifying Party, its employees or agents, provided that the Indemnified Party gives to the Indemnifying Party prompt notice of such claim, full information about the circumstances giving rise to it, reasonable assistance in dealing with the claim and sole authority to manage, defend or settle it.

17. Obligations to Inform, Amendments & Data Protection Officer

17.1. Where the Customer Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while in EYESmart's control, EYESmart will notify the Customer of such action without undue delay and follow the Customer's reasonable instructions to preserve the confidentiality of the Customer Data. EYESmart will, without undue delay, notify to all pertinent parties in such action, that any Customer Data affected thereby is in the Customer's sole property and area of responsibility, that Customer Data is at the Customer's sole disposition, and that the Customer is the responsible body pursuant to the Applicable Data Protection Laws.

17.2. Clause 21 of the Agreement regarding EYESmart's right to amend the terms of the Agreement applies to changes to this DPA as this DPA forms part of the Agreement. For the avoidance of doubt, this does not apply to notifications of new Sub-Processors under Clause 6.3.

17.3. EYESmart has appointed a Data Protection Officer, who is responsible for matters relating to privacy and data protection. This Data Protection Officer can be reached at the following address:

Early Years Evaluation Smart Ltd.,
20 Wenlock Road, London, England,
N1 7GU
privacy@eyesmart.com

18. Point of Contact

18.1. The Parties must notify each other of a point of contact for any issues related to data protection arising out of or in connection with the Agreement and this DPA.

18.2. For any such matters, the Customer can reach out to the EYESmart Security & Privacy Team at privacy@eyesmart.com.

18.3. The childcare settings Customer will inform EYESmart of its point of contact ("Customer Point of Contact").

Such contact shall be the main point of contact when EYESmart is assisting with Data Subject Requests, informing of Data Breaches, and informing the Customer of new Sub-Processors or amendments to this DPA. The individual parents Customer will be contacted directly.

19. Entire Agreement

19.1. Except as amended by this DPA, the Agreement will remain in full force and effect. Where individual regulations of this DPA are invalid or unenforceable, the validity and enforceability of the other regulations of this DPA shall not be affected.

19.2. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (i) any Transfer Mechanism, (ii) Appendix D (Additional Data Protection Legislation), (iii) Appendix E (Supplemental Clauses to the Transfer Mechanisms), (iv) this DPA, and (v) Terms & Conditions.

20. Governing Law & Dispute Resolution

Clause 25 of the Terms & Conditions (*Governing Law and Dispute Resolution*) shall apply to this DPA.

Appendix A: Details of Processing

Nature, Purpose of Processing, Type of Personal Data and Categories of Data Subjects: The subject matter and nature of EYESmart's Processing of Customer Data is the performance of the Services pursuant to the Agreement and the purposes set forth below:

Type of Customer Data	Purpose (subject matter) of Processing on behalf of Customer	Categories of Data Subjects Affected
Basic data (such as name, date of birth, birthplace, social security number, gender, languages, dietary considerations etc.)	Ensure that the Customer has all relevant information about the child to run the business and to comply with regulatory requirements; to track the child's development in a age-appropriate manner.	Children
Sensitive data (such as religion, ethnicity, allergies, vaccines, medicines, injuries/accident reports)	Ensure that the Customer has all relevant information about the child to run the business and to comply with regulatory requirements.	Children
Attendance data (such as sick days, holidays, sign in/out data etc.)	To store attendance data and create attendance reports & track development.	Children
Activity data (such as details of learning or development activity etc.)	To be able to digitally track the child's activities, e. g. sleeping, trips, eating, learning.	Children
Photos and files	To share photos of children and other necessary files, that may contain Customer Data, with the parents/guardians. Employees may possibly be in photos.	Children, Employees
Contact Details (such as name, address, email address, phone number)	Ensure that the parents can be contacted.	Parents/guardians/other family member
Financial Information (such as bank account details, invoices etc.)	For the invoices.	Parents/guardians/other family member
National Insurance Number or equivalent	To validate child funding code, if applicable.	Parents/guardians
Employee Details (such as name, address, email address, phone number, date of birth, qualifications and certificates, next of kin information etc.)	To keep records of employees, to contact them and store emergency details	Customer Employees
Attendance data (sick days and holidays)	To store attendance data and create attendance reports.	Customer Employees

Any Customer Data or other personal data included in notes or shared in private or team messages via the Platform.	Necessary for the Customers to utilize the Platform features.	Customer Employees, Parents/guardians/other family members, children
Any Customer Data or other personal data shared with EYESmart Customer Experience Team.	Necessary to provide support services.	Customer Employees, Parents/guardians/other family members, children
Certain payer information (name, email, address, payment method, last 4 digits of card number, expiration date, one-time payment or future payment set up), card declines information, and any documentation containing personal data in relation to payment disputes.	Necessary to provide the in-app payment services, and to allow the payer to see and manage their payment methods and assist with payment disputes.	Parents/guardians who make payments via the in-app payments feature.
Any type of documents the Customer may upload to the Platform, which include Customer Data.	Necessary to manage records related to a child, employee or parent/guardian	Children, Customer Employees, Parents/Guardians

Duration of Processing:

The general retention period is set out in clause 3.2 of the DPA. The table below sets out specific retention periods related to specific potential Authorised Sub-Processors:

Sub-Processor	**Retention**
Rsync.net Inc.	Customer Data backups are retained for 30 days from the date of each backup.
Backblaze Inc.	Customer Data backups are retained for 30 days from the date of each backup

Intercom R&D Unlimited Company	Contact details of Customer employee is retained for 360 days as of the last interaction with EYESmart support team or if the Customer employee is not an active Customer employee for 30 days. Support ticket/message are retained for 360 days as of the date it was received by EYESmart.
JoinCube Inc. (“Beamer”)	Customer Data is retained for 60 days.
Microsoft Azure	Customer Data is retained for 60 days.
Twilio Ireland Limited	Customer Data chosen to be sent is retained by Twilio for 365 days.
CircleCo, Inc.	Customer Data is deleted within 30 days of expiry of EYESmart’s agreement with Circle, or upon request.
OpenAI Ireland Limited	Customer Data is retained by OpenAI for 30 days.
Zoom Video Communications Inc.	Customer Data shared in a video call is Processed for the duration of the video call. Such calls may be recorded if the Customer wishes and agrees and are retained for 90 days.
Dialpad Inc.	Customer Data communicated by the Customer during a phone call is Processed for the duration of the phone call, unless otherwise mentioned in the EYESmart Privacy Policy (in the event EYESmart acts as an independent controller).

Appendix B - Authorised Sub-Processors

As set out in Clause 6.2 the Customer agrees that the following Sub-Processors may be authorised for the purpose of the Processing of the Customer Data under this DPA, giving affirmative consent thereto:

Authorised Sub-Processors			
Sub-Processor	**Location of Processing**	**Description of subcontracted service**	**Customer Data Processed**
Microsoft Azure	UK	Data Centre for hosting of the Platform.	All types and categories of Customer Data set out in Appendix A.
Rsync.net Inc.	Zürich, Switzerland	For back up. All data is encrypted by EYESmart with a private key before being transferred to the provider for backup storage. The provider does not hold a key to decrypt the data.	All types and categories of Customer Data set out in Appendix A.
Backblaze Inc.	Amsterdam, the Netherlands	Used for backup of files, photos, videos, and logs. All data is encrypted and cryptographically salted by EYESmart with a private key before being transferred to the provider for backup storage. The provider does not hold a key to decrypt the data.	Photos, videos and any other Customer Data set out in Appendix A that is part of any logs.
Intercom R&D Unlimited Company	Northern Virginia, USA	Used for handling EYESmart's written customer support interactions. Intercom's AI tool, Fin, is enabled. Processing is subject to a data processing agreement that includes the appropriate Transfer Mechanism. In addition, Intercom Inc., the parent company, is a certified company under the EU-U.S. Data Privacy Framework	Contact details (name, email) of the person requesting for assistance, and any Customer Data (such as documentation) shared by such person in the support chat function (if any). Only, if strictly necessary to provide the requested assistance, Customer Data may be shared by the Customer Experience Team.

Hubspot Ireland Limited	Germany	For customer success and support services	Name and email addresses of Authorised Users, and any Customer Data provided via Intercom.
Planhat AB	Sweden & Ireland	For customer success and support services	Name and email addresses of Authorised Users.
Joincube, Inc. ("***Beamer***")	The United States	Used to communicate with users when updates are made to the platform, and to gather feedback on those updates. Very limited information is processed by Beamer. Processing is subject to a data processing agreement that includes the appropriate Transfer Mechanism	Full name, email and UID of users submitting feedback.
Google Cloud EMEA Limited (only an Authorised Sub-Processor if the Customer has the Translation Feature enabled)	UK	Translation services as per the Additional Product Terms.	Customer Data that may be included in Newsfeeds, including Observation posts, on the Platform which Family User translates.
Stripe Payments Europe Ltd., or Stripe Inc., only if the Customer is located in the US, (only an Authorised Sub-Processor if the Customer makes use of the in-app payments feature)	The United States	Payment processing as per the Additional Product Terms.	Data transmitted from EYESmart to Stripe includes payer details (name, email, address, other data as necessary for payment processing), documentation (which may contain personal data) provided by the Customer to EYESmart in relation to payment disputes, card declines information and potential documents relating to KYC and AML regulations. EYESmart does NOT process the full credit card number, such information is transmitted directly to Stripe and is subject to the terms

			between the Customer and Stripe.
Twilio Ireland Ltd. (only an Authorised Sub-Processor if the Customer uses the SMS feature)	The United States *	Used to notify parents/guardians of newsfeed posts and messages marked for notification by SMS by Customer representatives, as per the Additional Product Terms. Processing is subject to a data processing agreement that includes the appropriate Transfer Mechanism.	Phone number of parent/guardians. Any Personal Data included in a relevant newsfeed post or message.
CircleCo, Inc. (only an Authorised Sub-Processor if the Customer elects to participate in Village - currently only available in the UK)	The United States	Used to provide Village, as per the Additional Product Terms. Processing is subject to a data processing agreement that includes the appropriate Transfer Mechanism.	Full name, email and any data entered by users into Village.
OpenAI Inc. (only an Authorised Sub-Processor if the Customer has AI features made available on the Platform enabled)	The United States	Used to offer AI features on the Platform via OpenAI API, as per the Additional Product Terms. Processing is subject to a data processing agreement that includes the appropriate Transfer Mechanism.	Any Customer Data which is used by an AI feature to provide generative outputs, such as rephrasing of text, summaries of information in the Platform, recommendations, etc.
Zoom Video Communications Inc.	The United States but recordings are stored in Germany.	Used to communicate with customers via video call. Video calls may be recorded if the Customer wishes to share them internally for training purposes.	Name of Staff Users, and potentially other Customer Data shared by such person via video call.
Dialpad Inc.	The United States, but the recordings are stored in the EU region.	Used to provide customer support via phone. EYESmart may request to record and/or transcribe phone calls for quality and training purposes upon explicit consent. In such cases EYESmart is acting as the controller and processing is subject to the EYESmart Privacy	Name of Staff Users, and potentially other Customer Data shared by such person via phone call.

		Policy. Processing is subject to a data processing agreement that includes the appropriate Transfer Mechanism. Furthermore, Dialpad is a certified organisation under the EU-U.S. Data Privacy Framework.	
Cloudflare Inc.	UK	Used to ensure fast and reliable access to our website, to secure our applications from DNS-based attacks	All types and categories of Customer Data set out in Appendix A.

*Twilio has Binding Corporate Rules (BCRs) approved by a Supervisory Authority within the EU, meaning that it is bound by GDPR across all of its operations, globally. Its approved processor BCRs require it to handle the data of third-party Controllers located in the EU compliantly with the GDPR.

Appendix C - Technical and Organisational Security Measures

EYESmart has in place certain technical and organisational security measures to ensure compliance with the Applicable Data Protection Laws. Those measures are set in place to prevent improper destruction, alteration, disclosure, access, and other improper form of processing of Customer Data.

EYESmart reserves the right to modify the measures and safeguards implemented, provided that the level of security is not less protective than initially agreed upon. In the event of considerable changes to the measures, EYESmart shall notify the Customer of such changes.

1. Confidentiality (Article 32 Paragraph 1 Point b GDPR)

Physical Access Control

Unauthorized access (in the physical sense) must be prevented.

Technical and organizational measures to control access to premises and facilities, particularly to check authorisation:

- EYESmart's offices are protected with fire detection as well as electronic security and intrusion alarms. No customer data is stored at EYESmart's offices or on local employee computers. All data is accessed by EYESmart employees via secure encrypted connections with the Data Centres.
- The Data Centres used by EYESmart are state of the art. The Data Centre providers have many years of experience in designing, constructing, and operating largescale data centres. This experience has been applied to the platform and infrastructure. Data Centres are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorised staff must pass two-factor authentication a minimum of two times to access data centre floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. All physical access to Data Centres is logged and audited routinely.
- Physical Media: Physical media (e.g. transcripts) that contains personal data from the EYESmart Platform shall be stored in locked cabinets when they are not in use and up to the time of destruction, cf. the section on Physical Media below. Only employees with a specific requirement may access such physical media.

Electronic Access Control

Unauthorized access to IT systems must be prevented.

Technical and organisational measures for user identification and authentication:

- Firewalls: Updated firewalls are applied to protect the network at EYESmart's office against unauthorized access. The same standards are applied at the Data Centres, where firewalls and other technical methods are used to protect the Data Centres network against unauthorized access.
- Anti-virus/anti-malware: IT devices used by EYESmart to access Personal Data on the EYESmart Platform, including servers that are used in the operation are, to the extent possible and relevant, protected with updated anti-virus- and anti-malware software.
- Encryption: In relation to the transfer of data within the EYESmart Platform through public communication connections, including when the EYESmart Platform is accessed by users, secure encryption is applied, based on generally recognised algorithms that as a minimum will be equivalent to SSL 256 bit. All WIFI connections used at the EYESmart office and in the Data Centres are secured through use of encryption in the form of WPA or better.
- EYESmart's Remote Access: When EYESmart's employees access the EYESmart Platform through remote access, such connections are secured through encryption e.g. in the form of VPN. Any access to the EYESmart Platform requires that the EYESmart employees register a username, password and two-factor. EYESmart complies with the conditions in this Data Processing Agreement, irrespective of the use of remote access.
- EYESmart's Password Policy: EYESmart Employees with access to the EYESmart Platform are covered by a strict password policy. Passwords must be minimum 10 characters and contain: Upper case as well as lower case letters, numerals, and special characters. Passwords are required to be changed periodically. Passwords must not contain any names or usernames.
- Penetration Testing : EYESmart has penetration tests performed on the EYESmart Platform by an external agency according to industry standards on a regular basis.

Internal Access Control

Activities in IT systems not covered by the allocated access rights must be prevented.

Requirements-driven definition of the authorisation scheme and access rights, and monitoring and logging of accesses:

a) Authorisation

- All EYESmart employees with access to Personal Data are authorized by EYESmart. Such authorisations specify which access and for what purpose each employee can access the Personal Data. The EYESmart employees are solely authorized to access the Customer's Personal Data for operational or technical purposes. The EYESmart employees do not have access to Personal Data that is not included in their authorisation. All access to Personal Data by EYESmart employees is logged.
- EYESmart checks and updates all employee authorisations on a regular basis, as a minimum semi-annually. The authorisations are adapted or revoked in relation to employees changing job positions, responsibilities or termination of employment.
- The EYESmart Platform is configured so that the Customer can authorise its employees based on access roles. The Customer assigns its employee authorisations through the web or app module provided by EYESmart.
- All EYESmart employees with access to Personal Data are informed of this Data Processing Agreement and are obliged to comply with the employee targeted requirements of this Data Processing Agreement.
- Data security and privacy awareness training is conducted for all new EYESmart employees and a refresher training is conducted for all EYESmart employees at least annually.
- All EYESmart employees with access to Personal Data have their criminal record checked by EYESmart in connection with their employment and checked again at least annually during their employment.
- All product development and bug fixing activities are to the extent possible done on dummy test data and not on actual Customer Data.

b) Login, Username and Passwords

- All employees at EYESmart and at the Data Centres have unique usernames and passwords. Usernames and passwords are created and altered from generally recognised principles and no username is reused within a period of at least six months since the username was last in use. Provided that a EYESmart employee has not used their username within a period of three months, the username will automatically be suspended.
- After multiple successive failed login-attempts with the same username, the login with the respective username will be blocked. This applies to both employees of EYESmart and the Customer. The blocking of access in the previously mentioned scenarios can not cause any liability towards EYESmart. In case a block of a EYESmart employee account occurs, EYESmart will conduct a follow-up on the matter as soon as possible.
- It is not possible to log into the EYESmart Platform by using an anonymous user account or guest account.

c) Confidentiality

- All EYESmart employees with access to Personal Data are subject to strict confidentiality throughout their employment contracts and all employees within the Data Centre are subject to confidentiality.
- The confidentiality is maintained beyond the termination of the Agreement or if the Agreement with Data Sub-processors ceases. EYESmart employees are also subject to the confidentiality obligation upon cessation of their employment.

Isolation Control

Data collected for different purposes must also be processed separately.

Measures to provide for separate processing (storage, amendment, deletion, transmission) of data for different purposes:

- Storing of Data: Within the EYESmart Platform, all Data is stored in the Data Centres. The Customer's Data is stored logically separated from other Customers' Data for whom EYESmart is carrying out data processing for. All Data is tagged with unique ids which can identify which end-user or Customer the data belongs to.

2. Integrity (Article 32 Paragraph 1 Point b GDPR)

Data Transfer Control

Aspects of the disclosure of Personal Data must be controlled: electronic transfer, data transmission, etc.

Measures to transport, transmit and communicate or store data on data media (manual or electronic) and for subsequent checking:

- IT Storage Media: In case of recycling, discarding, repairs or service on storage media used for Personal Data, it is ensured that third parties cannot gain access to data on such media. Such security procedures are conducted either through encryption or by thorough deletion or overwriting to ensure that all previously stored Personal Data cannot be recovered by using a generally recognized specification (e.g. DOD 5220-22-M).
- Physical Media: All physical media that may contain Personal Data from the Customer's IT solution (e.g. prints), will be discarded in a safe manner when the physical media has fulfilled its purpose. This can be executed through shredding or through other means that ensures that access to Personal Data is not possible.
- Virtual Private Network: When EYESmart's employees access the EYESmart Platform, such connections are secured through encryption e.g. in the form of VPN. Any access to the EYESmart Platform requires that the EYESmart employees register a username, password and two-factor.
- Electronic Signature: EYESmart uses 256-bit SSL certificates to the authenticity of EYESmart towards the end-users.
- Transport Security: EYESmart utilises end-to-end SSL encryption from end-user devices all the way to the database in the Data Centres as well as between internal services on the servers in the Data Centres.

Data Entry Control

Full documentation of data management and maintenance must be maintained.

Measures for subsequent checking whether data have been entered, changed or removed (deleted), and by whom:

- Any access to Personal Data related to the use of the EYESmart Platform is automatically logged in the Application Log. By logging the time, username, type of application and the person that the data is concerning, or the used search criteria is registered. The log is kept for a minimum of six months and is deleted after a maximum of seven months.
- The Customer can gain access to specific information from the Application Log by special request to EYESmart.
- Provided that access to the EYESmart Platform is made in connection with technical issues e.g. support, error correction or other technical causes, such access will be logged in the Application Log.

3. Availability and Resilience (Article 32 Paragraph 1 Point b and c GDPR)

Availability Control

The data must be protected against accidental destruction or loss.

Measures to assure data security:

- Fire, Power Outages: EYESmart's office and Data Centres are secured in the usual manner to protect against fire. The Data Centres are furthermore secured so that the operations can continue even during power outages of a certain duration, protection against loss of communicative connections to the Data Centres has also been established.
- Backups: EYESmart secures Data stored in the EYESmart Platform through continuous backups of Data several times daily. The backup is conducted as a mix of full backup and incremental (whereby the changes are stored) backup. EYESmart regularly conducts restore-tests of previously completed backups to make sure that the backup routines function as intended. Backups are for extra safety reasons also duplicated and stored in another Data Centre from a different provider.
- Uninterruptable Power Supply (UPS): The Data Centre electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data Centres use generators to provide back-up power for the entire facility.
- Climate and Temperature: Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centres are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels. Electrical, mechanical, and life support systems and equipment are monitored so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

Rapid Recovery

- In case of a major incident EYESmart has the ability to quickly recover access to Personal Data by restoring recent backed up files to production environments on new booted servers. This can be done in a matter of hours and ensures that any potential downtime is minimised.

4. Procedures for regular testing, assessment, and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)

Incident Response Management Security Breach Procedure

- Provided that EYESmart detects a security breach or threat hereof in relation to the EYESmart Platform, EYESmart will seek to locate and identify such breach or threat as well as the scope of the issue as soon as possible, seek to limit the potential or occurred damage to the extent possible, seek to hinder such a security breach in the future and to the extent possible, restore any lost Data.
- In the case of a security breach where unauthorised people gain access to the Customer's Data or where loss of Data has occurred, EYESmart will, when possible, notify the Customer in a written notice about the security breach. Such notifications will contain information about which Data EYESmart deems to have been accessed unauthorised, whether EYESmart has initiated special precautions, and the notification will inform whether the Customer, according to EYESmart's evaluation, must take special precautions.

Order or Contract Control

- EYESmart has entered into market standard data processing agreements with Data Sub-processors in order to comply with the terms under this Data Processing Agreement.

Audit

- EYESmart will at least annually have an external auditor verify that the procedures specified in this Data Processing Agreement are followed.

Appendix D - Additional Data Protection Legislation

The sections below apply only to the extent the local laws apply to the Customer.

Part 1: Swiss new Federal Act on Data Protection (nFADP)

This Part 1 forms a part of the Data Processing Agreement (DPA) between EYESmart and Customer, for Customers located in Switzerland.

1. Definitions:

1.1 To the extent that differences exist between the definitions in the GDPR and nFADP, this DPA shall be interpreted to align with the nFADP where applicable. Any necessary adjustments to ensure compliance with the nFADP shall be deemed incorporated without requiring explicit amendments, provided that EYESmart's actual Processing activities remain compliant with both legislations.

Part 2: California Consumer Privacy Act

This Part 2 forms a part of the Data Processing Agreement (DPA) between EYESmart and Customer, for Customers located in California.

1. Definitions. CCPA and other capitalized terms not defined in this Schedule are defined in the DPA.

1.1. "Business purpose", "commercial purpose", "personal information", "sell", "service provider" and "share" have the meanings given in the CCPA.

1.2. The definition of "Data Subject" includes "consumer" and "household" as defined in the CCPA.

1.3. The definition of "Controller" includes "business" as defined in the CCPA.

1.4. The definition of "Processor" includes "service provider" as defined in the CCPA.

2. Obligations.

2.1. Customer is providing the Customer Data to EYESmart under this Agreement for the limited and specific business purposes described in Clause 3 (Scope and Specification of Processing) and otherwise defined in the Agreement.

2.2. EYESmart will comply with its applicable obligations under the CCPA and provide the same level of privacy protection to Customer Data as is required by the CCPA.

2.3. EYESmart acknowledges that Customer has the right to: (i) take reasonable and appropriate steps under Clause 13 (Audits) of this DPA to help to ensure that EYESmart's use of Customer Data is consistent with Customer's obligations under the CCPA, (ii) receive from EYESmart notice and assistance under Clause 10 (Data Subject Requests) of this DPA regarding consumers' requests to exercise rights under the CCPA and (iii) upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Personal Data.

2.4. EYESmart will notify Customer promptly after it makes a determination that it can no longer meet its obligations under the CCPA.

2.5. EYESmart will not retain, use, or disclose Customer Data: (i) for any purpose, including a commercial purpose, other than the business purposes described in Clause 2.1 of this Annex 2 (California Annex) or (ii) outside of the direct business relationship between EYESmart with Customer, except, in either case, where and to the extent permitted by the CCPA.

2.6. EYESmart will not sell or share Customer Data.

2.7. EYESmart will not combine Customer Data with other personal information except to the extent the CCPA expressly permits a service provider to do so.

Part 3: Texas Data Privacy and Security Act

This Part 3 forms a part of the Data Processing Agreement (DPA) between EYESmart and Customer, for Customers located in Texas.

1. Definitions

For the purposes of this Annex, the terms used herein shall have the same meanings as defined in the Texas Data Privacy and Security Act (TDPSA), unless otherwise specified**.**

2. Scope and Application

The obligations set out in this Annex shall apply to the processing of personal data as defined under the TDPSA. The data subjects are residents of the State of Texas, and the processing activities are subject to the TDPSA.

3. Data Processor Obligations

3.1. Data Security: The Data Processor shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal data from unauthorised access, destruction, use, modification, or disclosure.

3.2. Data Breach Notification: In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed, the Data Processor shall promptly notify the Data Controller without undue delay and, where feasible, not later than 72 hours after becoming aware of it.

3.3. Data Rights Compliance: The Data Processor shall assist the Data Controller in fulfilling data subject rights under the TDPSA including access, correction, deletion, and data portability requests.

3.4. **Audits and Inspections:** The Data Processor agrees to submit to audits and inspections by the Data Controller and provide the Data Controller with whatever information it needs to ensure that both parties are meeting their Article 28 obligations.

4. Sub processors

The Data Processor may not engage another processor (Sub processor) without prior specific or general written authorisation of the Data Controller. In the case of general written authorisation, the Data Processor shall inform the Data Controller of any intended changes concerning the addition or replacement of other processors, thereby giving the Data Controller the opportunity to object to such changes per Section 6 of the DPA.

5. Data Transfer

The transfer of personal data outside the geographic boundaries of the State of Texas shall be conducted in compliance with the TDPSA and applicable laws regarding data privacy and security.

6. Termination

Upon termination of the data processing services, the Data Processor shall, at the choice of the Data Controller, delete or return all the personal data to the Data Controller, and delete existing copies unless legislation requires storage of the personal data.

7. Modification

This Annex may be modified or updated periodically to remain in compliance with the Texas Data Privacy and Security Act and other relevant laws. Any such modifications will be communicated to the Data Controller in a timely manner.

Appendix E - Supplemental Clauses to the Transfer Mechanisms

1. Personal Data will be encrypted both in transit and at rest using industry standard encryption technology.

2. EYESmart will resist, to the extent permitted by Law, any request under Section 702 of the U.S. Foreign Intelligence Surveillance Act ("FISA").
3. EYESmart will use reasonably available legal mechanisms to challenge any demands for data access through the national security process that it may receive in relation to Customer's data.
4. No later than the date on which your acceptance of the DPA becomes effective, EYESmart will notify you of any binding legal demand for the Personal Data it has received, including national security orders and directives, which will encompass any process issued under Section 702 of FISA, unless prohibited under Law.
5. EYESmart will ensure that its data protection officer has oversight of EYESmart's and its affiliates' approach to international data transfers.