Famly Data Processing Agreement

Effective Date: 15/08/2025

Version 2.8

The Customer

(hereinafter **"Customer"**)

and

Famly ApS, Købmagergade 19, 2tv., 1150 Copenhagen, Denmark
(hereinafter **"Famly"**)

(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 Famly Offer) entered into between the Customer and Famly as amended from time to time in accordance with its terms;

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

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

"**Customer Data**" means the Personal Data (as defined in the GDPR) regarding individuals made available to Famly 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 Famly 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;

"**Services**" means the Famly 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;

"**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) Data Protection Clauses approved by the Swiss Federal Data Protection and Information Commissioner ("***FDPIC***"), (iii) and other such legally approved mechanisms for ensuring the safety and security of data transfers from outside of the EEA/Switzerland.

The terms "Controller", "Processor", "Processing", "Data Subject", "Personal Data", "Personal Data Breach" and "Supervisory Authority" shall have the same meaning as in the GDPR. 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 Famly 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, Famly 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 Famly's employees or agents process the Customer Data on behalf of the Customer as set out in Appendix A .

2. Responsibilities and Instructions

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

2.2. The Customer is solely responsible for compliance with the GDPR, including but not limited, to the lawfulness of disclosing Customer Data to Famly and the lawfulness of having the Customer Data processed by Famly on behalf of the Customer. The Customer warrants that it is lawfully authorised to process and disclose the Customer Data to Famly. The Customer is responsible for maintaining and updating its respective privacy policy, notices and statements, including to mention Famly in it as its' Processor.

2.3. Famly shall process Customer Data only on documented instructions from the Customer, unless required to do so by the GDPR or any other applicable law to which Famly 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. Famly shall immediately inform the Customer if instructions given by the Customer, in the opinion of Famly, contravene the GDPR. Famly is entitled to suspend performance on such instruction until the Customer confirms or modifies such instruction.

2.5. Famly 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 Processing of Customer Data by Famly is 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 nature, 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.

4. Security of Processing

4.1. Famly 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 GDPR 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. Famly shall regularly review, assess and update, as necessary, these measures to address evolving security risks, industry standards, technological advancements, and regulatory changes. Famly 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, Famly shall notify the Customer of the changes.

4.3. Famly warrants that the company fulfils its obligations under the GDPR 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. Famly 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. Famly shall only grant access to the Customer Data being processed on behalf of the Customer to persons under Famly'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. Famly shall at the request of the Customer demonstrate that the concerned persons under Famly's authority are subject to the abovementioned confidentiality.

6. Sub-Processing

6.1. Customer generally authorises Famly to appoint Sub-Processors in accordance with this Clause 6. The Customer acknowledges that Famly 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. Famly 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 Famly, provided that such objection is based on reasonable grounds relating to data protection. Famly will evaluate the concerns and discuss possible solutions with the Customer. If these solutions are not reasonably possible in Famly'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 Famly'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 Famly or of Famly 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 Famly's reasonable control (so-called emergency replacement). Famly 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 Famly engages Sub-Processors, Famly is responsible for ensuring that Famly'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. Famly 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, Famly will remain fully liable to the Customer as regards the fulfilment of the obligations of the Sub-Processors. Famly's liability will be to the same extent as if Famly were directly performing those services, but within limitations of liability set out in this DPA and Agreement.

7. Location of Customer Data and Transfer to Third Countries

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, Famly will not transfer the Customer Data outside the EEA 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 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 Switzerland ("Adequacy Decisions"), as applicable, without any further safeguards being necessary.

7.4. If the processing of the Customer Data includes a transfer from the EEA 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 Famly of a transfer risk assessment/transfer impact assessment (under EU 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 the GDPR, including those set out in Appendix D. The Customer acknowledges and agrees that Famly 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 GDPR.

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, Famly must perform the action if so instructed by the Customer and permitted under the GDPR. Where a deletion request relating to Customer Data, consistent with the GDPR or a corresponding restriction of Processing is impossible, Famly 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 the GDPR, all Customer Data or return the same to the Customer.

8.2. Within 60 days following the termination of the Agreement, Famly shall, upon the Customer's instructions, return all Customer Data to the Customer or delete the same, unless required otherwise by the GDPR. 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 Famly, and where Famly is able to correlate the Data Subject to the Customer, based on the information provided by the Data Subject, Famly will without undue delay refer such Data Subject to contact the Customer directly.

9.2. Famly 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 Famly's assistance. Famly 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. Famly will notify the Customer without undue delay, and in any event within 48 hours of 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 Famly's scope of responsibility. This includes Data Breaches involving any Sub-Processors engaged by Famly, to the extent Famly becomes aware of such breach. Famly will implement the measures necessary for securing Customer Data and for mitigating potential negative consequences for the Data Subject. Famly will coordinate such efforts with the Customer without undue delay.

10.2. Famly will support the Customer, to the extent reasonably possible and only where the Customer cannot do so without Famly's assistance, in communicating Data Breaches to the affected Data Subjects and notifying Data Breaches to the applicable Supervisory Authority (provided that this support does not result in any breach of Famly'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 Famly, and the Customer does not otherwise have access to the required information, Famly 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 the GDPR.

12. Audits and Inspections

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

12.2. To the extent required under the GDPR and upon the Customer written request, Famly 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 Famly's confidential information and must be treated as such. ¨

12.3. The Customer agrees to exercise its audit and inspection rights by instructing Famly to share the audit report summary as described in clause 12.2 of this DPA. If the Customer reasonably concludes that an onsite audit 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 inspections in individual cases or to have them carried out by an auditor (that is no competitor of Famly) provided that such audits or inspections will be conducted (i) during regular business hours, and (ii) without disproportionately interfering with Famly's business operations, (iii) upon prior reasonable notice and further consultation with Famly, (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 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 Famly 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 Famly has breached its obligations under the Agreement or this DPA, Famly will promptly remedy the breach at its own cost and refund any payments made by the Customer towards the cost of Famly's internal resources related to the Customer onsite audit or inspection.

13. Application Log and Linked Services

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

13.2. The Application Log Data is used by Famly 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, Famly can provide access to the Customer.

13.4. Should Customer engage a Linked Service Provider, as defined in the Famly Terms & Conditions, then Famly 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 GDPR. Under no circumstances will a Linked Service Provider be considered a sub-processor to Famly of the Customer Data.

14. Defence Support

14.1. Where a Data Subject asserts any claims against the Customer as permitted by Article 82 of the GDPR, Famly 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 Famly in accordance with the GDPR.

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

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 GDPR 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 Famly's control, Famly 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. Famly 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 in the sense of the GDPR.

17.2. Clause 21 of the Agreement regarding Famly'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. Famly 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:

Attn. Data Protection Officer
Købmagergade 19, 2. tv.
1150 Copenhagen K
Denmark
privacy@famly.co

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 Famly Security & Privacy Team at privacy@famly.co.

18.3. The Customer will inform Famly of its point of contact ("Customer Point of Contact"). Such contact shall be the main point of contact when Famly is assisting with Data Subject Requests, informing of Data Breaches, and informing the Customer of new Sub-Processors or amendments to this DPA.

19. Entire Agreement

19.1. Except as amended by this DPA, the Agreement will remain in full force and effect. In case of any conflict, the GDPR shall take precedence over the regulations of this DPA. 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 (Swiss Federal Data Privacy Act), Appendix E (Supplemental Clauses to the Transfer Mechanisms), (iii) this DPA, and (iv) the Agreement.

20. Governing Law & Dispute Resolution

Clause 25 of the Agreement (*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 Famly'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	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.	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.	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 Customer to be able to store relevant financial information in one place, to then be able to issue invoices etc.	Parents/guardians/other family member
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	Necessary for the Customers to utilize the Platform features.	Customer Employees, Parents/guardians/other

or shared in private or team messages via the Platform.		family members, children
Any Customer Data or other personal data shared with Famly 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) 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 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 Famly 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 Famly.
JoinCube Inc. (“Beamer”)	Customer Data is retained for 60 days.
Google Cloud EMEA Limited	Texts, which may contain Customer Data, sent to translation are held briefly in-memory in order to perform the translation and deliver the results. The translation is then retained for maximum 30 days on Famly server at AWS.

Twilio Ireland Limited	Customer Data chosen to be sent is retained by Twilio for 365 days.
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.
CircleCo, Inc.	Customer Data is deleted within 30 days of expiry of Famly's agreement with Circle, or upon request.
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 Famly Privacy Policy (in the event Famly acts as an independent controller).
DeepL SE	Customer Data forming part of posts translated by Family Users are retained by DeepL SE for the duration of the translation and is irreversibly deleted after the translation has been submitted. The translation is then retained for maximum 30 days on Famly server at SysEleven.

Appendix B - Authorised Sub-Processors

As set out in clause 6.2 the Customer agrees that the following Sub-Processors are 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**
Amazon Web Services EMEA SARL	Germany and very limited Processing in Ireland	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 backup. All data is encrypted by Famly with a private key before being transferred to the provider for backup storage. The	All types and categories of Customer Data set out in Appendix A.

		provider does not hold a key to decrypt the data.	
Backblaze Inc.	Amsterdam, the Netherlands	Used for backup of files, photos, videos, and logs. All data is encrypted and cryptographically salted by Famly 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 Famly'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.
Google Cloud EMEA Limited (This Sub-Processor is an Authorised Sub-Processor if the Customer has the Translation Feature enabled)	EU region	Translation services as per the Additional Product Terms.	Customer Data that may be included in Newsfeeds and Observation posts on the Platform which Family User translates.
DeepL SE (This Sub-Processor is an Authorised Sub-Processor if the Customer has the Translation Feature enabled)	Finland	Translation services as per the Additional Product Terms.	Customer Data that may be included in Newsfeeds and Observation posts on the Platform which Family User translates

Stripe Payments Europe Ltd., (this Sub-processor is 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. The Processing is subject to a data processing agreement that includes the appropriate Transfer Mechanism.	Data transmitted from Famly 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 Famly in relation to payment disputes, and potential documents relating to KYC and AML regulations. Famly 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.
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, such as if the Customer wishes to share it 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 recordings are stored in the EU region.	Used to provide customer support via phone. Famly may request to record and/or transcribe phone calls for quality and training purposes upon explicit consent. In such cases Famly is acting as the controller. Processing is subject to a data processing agreement that includes the appropriate Transfer Mechanism. Furthermore, Dialpad is a certified organisation under the EU-US Data Privacy Framework.	Name of Staff Users, and potentially other Customer Data shared by such person via phone call.
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.
Twilio Ireland Ltd. (only an Authorised Sub-Processor if the Customer	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.	Phone number of parent/guardians. Any Personal Data included in a relevant newsfeed post or message.

uses the SMS feature)		Processing is subject to a data processing agreement that includes the appropriate Transfer Mechanism.	
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 Ireland Ltd. for customers located in EEA/Switzerland (this Sub-processor is an Authorised Sub-Processor only if the Customer has enabled the AI features made available on the Platform)	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.
Famly Inc.	Virginia, USA	Subsidiary of Famly ApS. Customer Data may be accessible to a limited number of employees in order for them to provide EU/UK customers with support services. The Customer Data is only accessible to them and it is NOT being transferred to a server in the USA.	All types and categories of Customer Data set out in Appendix A.
Famly GmbH.	Berlin, Germany	Subsidiary of Famly ApS. Customer Data may be accessible to a limited number of employees in order for them to provide customer support services. The Customer Data is only accessible and it is NOT being transferred to a separate server in Germany.	All types and categories of Customer Data set out in Appendix A.
Famly Ltd.	United Kingdom	Subsidiary of Famly ApS. Customer Data may be accessible to a limited number of employees in order for them to provide EU/UK customers with support services. The Customer	All types and categories of Customer Data set out in Appendix A.

		Data is only accessible to them and it is NOT being transferred to a server in the United Kingdom.	

†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

Famly 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.

Famly 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, Famly 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 authorization:

- Famly's offices are protected with fire detection as well as electronic security and intrusion alarms. No customer data is stored at Famly's offices or on local employee computers. All data is accessed by Famly employees via secure encrypted connections with the Data Centres.
- The Data Centres used by Famly 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. Authorized staff must pass two-factor authentication a minimum of two times to access data center 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 Centers is logged and audited routinely.
- Physical Media: Physical media (e.g. transcripts) that contains personal data from the Famly Platform solution 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 Famly'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 Famly to access Personal Data on the Famly 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 Famly Platformthrough public communication connections, including when the Famly Platform is accessed by users, secure encryption is applied, based on generally recognized algorithms that as a minimum will be equivalent to SSL 256bit. All WIFI connections used at the Famly office and in the Data Centres are secured through use of encryption in the form of WPA or better.
- Famly's Remote Access: When Famly's employees access the Famly Platform Solution through remote access, such connections are secured through encryption e.g. in the form of VPN. Any access to the Famly Platformrequires that the Famly employees register a username, password and two-factor. Famly complies with the conditions in this Data Processing Agreement, irrespective of the use of remote access.
- Famly's Password Policy: Famly Employees with access to the Famly Platformare 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: Famly has penetration tests performed on the Famly PlatformSolution 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 authorization scheme and access rights, and monitoring and logging of accesses:

a) Authorization

- All Famly employees with access to Personal Data are authorized by Famly. Such authorizations specify which access and for what purpose each employee can access the Personal Data. The Famly employees are solely authorized to access the Customer's Personal Data for operational or technical purposes. The Famly employees do not have access to Personal Data that is not included in their authorization. All access to Personal Data by Famly employees is logged.
- Famly checks and updates all employee authorizations on a regular basis, as a minimum semi-annually. The authorizations are adapted or revoked in relation to employees changing job positions, responsibilities or termination of employment.

- The Famly Platform is configured so that the Customer can authorize its employees based on access roles. The Customer assigns its employee authorizations through the web or app module provided by Famly.
- All Famly 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 Famly employees and a refresher training is conducted for all Famly employees at least annually.
- All Famly employees with access to Personal Data have their criminal record checked by Famly 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 Famly and at the Data Centres have unique usernames and passwords. Usernames and passwords are created and altered from generally recognized principles and no username is reused within a period of at least six months since the username was last in use. Provided that a Famly 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 Famly and the Customer. The blocking of access in the previously mentioned scenarios can not cause any liability towards Famly. In case a block of a Famly employee account occurs, Famly will conduct a follow-up on the matter as soon as possible.
- It is not possible to log into the Famly Platform by using an anonymous user account or guest account.

c) Confidentiality

- All Famly 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. Famly 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 Famly Platform, all Data is stored in the Data Centres. The Customer's Data is stored logically separated from other Customers' Data for whom Famly 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 Famly's employees access the Famly Platform, such connections are secured through encryption e.g. in the form of VPN. Any access to the Famly Platform requires that the Famly employees register a username, password and two-factor.
- Electronic Signature: Famly uses 256-bit SSL certificates to the authenticity of Famly towards the end-users.
- Transport Security: Famly utilizes 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 Famly's 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 Famly.
- Provided that access to the Famly 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: Famly'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: Famly secures Data stored in the Famly 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. Famly 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 Famly 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 Famly detects a security breach or threat hereof in relation to the Famly Platform, Famly 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 unauthorized people gain access to the Customer's Data or where loss of Data has occurred, Famly will, when possible, notify the Customer in a written notice about the security breach. Such notifications will contain information about which Data Famly deems to have

been accessed unauthorized, whether Famly has initiated special precautions, and the notification will inform whether the Customer, according to Famly's evaluation, must take special precautions.

Order or Contract Control

- Famly 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

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

Appendix D – Swiss new Federal Act on Data Protection (nFADP)

For Customers resident or using the Services in Switzerland, the following Appendix shall apply and is accepted in its entirety.

1. **Applicability:**
    a. This Appendix shall modify the DPA, inclusive of Appendix C thereto, to which it is attached solely in the case that the Customer accepting the DPA is a resident of, or is using the Services in, the territory of the Swiss Confederation.

2. **Integral Part of the Data Protection Agreement:**
    a. Subject to Clause 1 of this Appendix D, above, this Appendix D, and all changes made by it to the text of the DPA, shall be read, construed, and understood as though they were written in that DPA originally, and form an inseparable and integral part of that DPA. Any clauses, sections, charges, stipulations, requirements or other provisions in that DPA not amended by this Annex 2 shall apply, *mutatis mutandis*.

3. **Definitions:**
    a. All references to GDPR in the DPA shall be replaced with references to the nFADP. The reference to Article 82 in Clause 14.1 of the DPA shall be read as reference to Article 32 of the nFADP.
    b. All references to a supervisory authority shall be understood to refer to the Federal Data Protection and Information Commissioner of the Swiss Confederation.
    c. All other such similar definitional changes, wherein changing the text of the DPA to ensure compliance, and the action actually taken by Famly would factually render Famly compliant with the nFADP, shall be considered to have been made.

4. **Notification of Breach**:
    a. Clause 10.1 of the DPA shall be replaced in its entirety with the following text:
        i. Famly 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 within Famly's scope of responsibility, on any Sub-Processor that may be Processing Customer Data on its behalf ("Data Breach"). Famly will implement the measures necessary for securing Customer Data and for mitigating potential negative consequences for the Data Subject. Famly will coordinate such efforts with the Customer without undue delay.

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. Famly will resist, to the extent permitted by applicable law, any request under Section 702 of Foreign Intelligence Surveillance Act (“FISA”).
3. Famly 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, Famly 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 applicable law.
5. Famly will ensure that its data protection officer has oversight of Famly's and its Affiliates’ approach to international data transfers.