Data Processing Agreement

June 2019

Between	**The Customer** (hereafter "The Customer")
And	**Famly ApS** Købmagergade 19, 2tv 1150 Copenhagen K Denmark VAT no.: 35 41 37 58 (hereafter 'Famly')

on the processing of personal data on behalf of a controller in accordance with Article 28 (3) of the EU General Data Protection Regulation (GDPR) (hereinafter "Data Processing Agreement").

Preamble

This annex details the parties' obligations on the protection of personal data, associated with the processing of personal data on behalf of the Customer as a data controller, and described in detail in the main agreement (hereinafter, the "Agreement"). Its regulations shall apply to any and all activities associated with the Agreement, in whose scope Famly's employees or agents process the Customer's personal data (hereinafter, "Data") on behalf of the Customer as a controller (hereinafter, "Contract Processing").

1. Scope, duration and specification of contract processing of data

The scope and duration and the detailed stipulations on the type and purpose of Contract Processing shall be governed by the Agreement. Specifically, Contract Processing shall include, but not be limited to, the following Data:

Type of Data	Type and purpose (subject matter) of Contract Processing	Categories of data subjects affected
Basic data	Ensure that the Customer has all relevant information about the child to run the business.	Children

Contact Details	Ensure that the parents can be contacted.	Parents
Financial Information	Invoices issued to parents and potentially bank account information in order to make the Customer able to service their clients.	Parents
Attendance data	To store attendance data and create attendance reports.	Children
Activity data	In order to be able to digitally track the child's activities, e. g. sleeping, tours, eating.	Children
Contact Details	To keep records of employees and contact them.	Employees
Attendance data	To store attendance data and create attendance reports.	Employees

Except where this annex stipulates obligations beyond the term of the Agreement, the term of this annex shall be the term of the Agreement.

2. Scope of application and responsibilities

1. Famly shall process Data on behalf of the Customer. Such Contract Processing shall include all activities detailed in the Agreement. Within the scope of this annex, the Customer shall be solely responsible for compliance with the applicable statutory requirements on data protection, including, but not limited to, the lawfulness of disclosing Data to Famly and the lawfulness of having Data processed on behalf of the Customer. the Customer shall be the »controller« in accordance with Article 4 no. 7 of the GDPR.
2. The Customer's individual instructions on Contract Processing shall, initially, be as detailed in the Agreement. The Customer shall, subsequently, be entitled to, in writing or in a machine-readable format (in text form), modifying, amending or replacing such individual instructions by issuing such instructions to the point of contact designated by Famly. Instructions not foreseen in or covered by the Agreement shall be treated as requests for changes to the Agreement. The Customer shall, without undue delay, confirm in writing or in text form any instruction issued orally.

3. Famly's obligations

1. Except where expressly permitted by Article 28 (3)(a) of the GDPR, Famly shall process data subjects' data only within the scope of the Agreement and the instructions issued by the Customer. Where Famly believes that an instruction would be in breach of applicable law, Famly shall notify the Customer of such belief without undue delay. Famly shall be entitled to suspending performance on such instruction until the Customer confirms or modifies such instruction.
2. Famly shall, within Famly's scope of responsibility, organise Famly's internal organization so it satisfies the specific requirements of data protection. Famly shall implement technical and organisational measures to ensure the adequate protection of the Customer's Data, which measures shall fulfil the requirements of the GDPR and specifically its Article 32. Famly shall implement technical and organisational measures and safeguards that ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services. the Customer is familiar with these technical and organisational measures, and it shall be the Customer's responsibility that such measures ensure a level of security appropriate to the risk. Famly reserves the right to modify the measures and safeguards implemented, provided, however, that the level of security shall not be less protective than initially agreed upon.
3. Famly shall support the Customer, to the extent reasonably possible for Famly and only where the Customer cannot do so without Famly's assistance, in fulfilling data subjects' requests and claims, as detailed in chapter III of the GDPR and in fulfilling the obligations enumerated in Articles 33 to 36 of the GDPR (provided that this support does not result in any breach of Famly's confidentiality obligations towards third parties).
4. Famly warrants that all employees involved in Contract Processing of the Customer's Data and other such persons as may be involved in Contract Processing within Famly's scope of responsibility shall be prohibited from processing Data outside the scope of the instructions. Furthermore, Famly warrants that any person entitled to process Data on behalf of Controller has undertaken a commitment to secrecy or is subject to an appropriate statutory obligation to secrecy. All such secrecy obligations shall survive the termination or expiration of such Contract Processing.
5. Famly shall notify the Customer, without undue delay, if Famly becomes aware of breaches of the protection of personal data within Famly's scope of responsibility. Famly shall implement the measures necessary for securing Data and for mitigating potential negative consequences for the data subject; the Famly shall coordinate such efforts with the Customer without undue delay.
6. Famly shall notify to the Customer the point of contact for any issues related to data protection arising out of or in connection with the Agreement.
7. Famly warrants that Famly fulfills its obligations under Article 32 (1)(d) of 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.
8. Famly shall correct or erase Data if so instructed by the Customer and where covered by the scope of the instructions permissible. Where an erasure, consistent with data protection requirements, or a corresponding restriction of processing is impossible, Famly shall, based on the Customer's instructions, and unless agreed upon differently in the Agreement, destroy, in compliance with data protection requirements, all carrier media and other material or return the same to the Customer.In specific cases designated by the Customer, such Data shall be stored or handed over. The associated remuneration and protective measures shall be agreed upon separately, unless already agreed upon in the Agreement.

9. Famly shall, upon termination of Contract Processing and upon the Customer's instruction, return all Data, carrier media and other materials to the Customer or delete the same. In case of testing and discarded material no instruction shall be required. The Customer shall bear any extra cost caused by deviating requirements in returning or deleting data.
10. Where a data subject asserts any claims against the Customer in accordance with Article 82 of the GDPR, Famly shall support the Customer in defending against such claims, where possible.

4. The customer's obligations

1. The Customer shall notify Famly, without undue delay, and comprehensively, of any defect or irregularity with regards to provisions on data protection detected by the Customer in the results of Famly's work.
2. Section 3 para. 10 above shall apply, mutatis mutandis, to claims asserted by data subjects against Famly in accordance with Article 82 of the GDPR.
3. The Customer shall notify to Famly the point of contact for any issues related to data protection arising out of or in connection with the Agreement.

5. Enquiries by data subjects

Where a data subject asserts claims for rectification, erasure or access 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 shall refer such data subject to the Customer. Famly shall forward the data subject's claim to the Customer without undue delay. Famly shall support the Customer, where possible, and based upon The Customer's instruction insofar as agreed upon. Famly shall 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.

6. Audit and options for documentation

1. Famly will on a regular basis audit the security of the computers and computing environment that it uses in processing the Customer's personal data when performing the services under the Agreement. Famly shall document Famly's compliance with the technical and organizational measures agreed upon in this Data Processing Agreement by appropriate measures.
2. If the Customer requests in writing, Famly will provide the Customer with a confidential summary of the results of this audit ("Summary Report") so that the Customer can reasonably verify Famly's compliance with the security obligations under this Data Processing Agreement. The Summary Report is Famly's confidential information.
3. The Customer agrees to exercise its audit right by instructing Famly to execute the audit as described in sections 6.2 of this Data Processing Agreement. 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, the Customer shall also have 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 and inspections will be conducted (i) during regular business hours, and (ii) without interfering with Famly' business operations,

(iii) upon prior notice (observing an appropriate notice period) 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.

4. In case of an onsite audit the Customer will bear its own expenses and compensate Famly the cost for its internal resources required to conduct the onsite audit (based on time and material according to the then current price list), the latter only if the audit does not reveal that Famly has in fact breached its obligations under the Agreement (in that case Famly will promptly remedy the breach at its own cost).

7. Subcontractors (Further processors on behalf of the customer)

1. Famly shall use subcontractors as further processors on behalf of the Customer only where approved in advance by the Customer.
2. A subcontractor relationship shall be subject to such consent of Famly commissioning further Famly or subcontractors with the performance agreed upon in the Agreement, in whole or in part. Famly shall conclude, with such subcontractors, the contractual instruments necessary to ensure an appropriate level of data protection and information security.
3. Famly will conduct the performance agreed upon, or the parts of the performance identified below, using the subcontractors enumerated below:

Agreed Sub-processors

Name of sub-processor: Amazon Web Services Inc.

Location of data processing/servers: Frankfurt am Main

Short description of subcontracted service: Hosting of the Solution

Famly shall, prior to the use of new subcontractors or replacement of subcontractors, inform the Customer thereof with at least thirty (30) days prior notice. The Customer shall be entitled to reasonably contradict any change notified by Famly promptly in writing within ten (10) days after receipt of the Customer's notice. Famly will evaluate the concerns and discuss with the Customer possible resolutions. If these resolutions are reasonably not 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 upon 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 accept the respective subprocessor. The Customer shall 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 the Customer against Famly and of the Famly against the Customer may be based on reason of such termination.

The Customer accepts that an exchange of a subprocessor 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 the Customer respectively. If the Customer reasonably objects to the use of this

subprocessor, the Customer may exercise its right to terminate the Agreement as described in the section above.

1. Where Famly commissions subcontractors, Famly shall be responsible for ensuring that Famly's obligations on data protection resulting from the Agreement and this exhibit are valid and binding upon subcontracting.
2. For the avoidance of doubt, the approval requirements under this Data Processing Agreement shall not apply in cases where Famly or subprocessors subcontracts ancillary services/deliverables from third parties which are not specific to the provision of the services under the Agreement. Such ancillary services/deliverables shall, for example, include (but not be limited to) general infrastructure services like telecommunications services or facility management services. Famly and subprocessors shall nevertheless conclude, with such third parties, agreements necessary to ensure applicable data protection standards.

8. Obligations to inform, mandatory written form, choice of law

1. Where the 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 shall notify the Customer of such action without undue delay. Famly shall, without undue delay, notify to all pertinent parties in such action, that any data affected thereby is in the Customer's sole property and area of responsibility, that data is at the Customer's sole disposition, and that the Customer is the responsible body in the sense of the GDPR.
2. No modification of this annex and/or any of its components – including, but not limited to, Famly's representations and warranties, if any – shall be valid and binding unless made in writing or in a machine-readable format (in text form), and furthermore only if such modification expressly states that such modification applies to the regulations of this annex. The foregoing shall also apply to any waiver or modification of this mandatory written form.
3. In case of any conflict, the data protection regulations of this annex shall take precedence over the regulations of the Agreement. Where individual regulations of this annex are invalid or unenforceable, the validity and enforceability of the other regulations of this annex shall not be affected.
4. This annex is subject to the laws of Denmark.
5. Famly has appointed the following Data Protection Officer (DPO):

Name: Christian Harrington

Email: **security@famly.co**

Phone: +49 (0) 30 8878 9707 or +44 (0) 20 3514 4069

9. Liability and damages

1. The regulations on the parties' liability contained in the Agreement shall be valid also for the purposes of Contract Processing, unless expressly agreed upon otherwise.

Exhibit on technical and organizational security measures in accordance with Article 32 of the GDPR

The technical and organisational security measures that Famly has in place with regards to prevent improper destruction, alteration, disclosure, access, and other improper forms of processing of information exported by the The Customer to Famly including the following:

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 from Famly's offices via secure encrypted connections with the data center.
- The data centers used by Famly are state of the art, utilizing innovative architectural and engineering approaches. Our provider has many years of experience in designing, constructing, and operating largescale data centers. This experience has been applied to the platform and infrastructure. Data centers 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 by is logged and audited routinely.
- Physical Media: Physical media (e.g. transcripts) that contains personal data from the Famly IT 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 (ID/password security) and organizational (user master data) 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 Operations Center, where firewalls and other technical methods are used to protect the Operations Center network against unauthorized access.

- Anti-virus/anti-malware: IT devices used by Famly to access the Famly IT solution, 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 IT solution through public communication connections, including when the IT solution 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 Operations Center are secured through use of encryption in the form of WPA or better.
- Famly's Remote Access: When Famly's employees access the Famly IT solution through remote access, such connections are secured through encryption e.g. in the form of VPN. Any access to the Famly IT systems requires that the Famly employees register a username and a password. 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 Famly's IT Solution 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 changed at least every 3 months. Passwords can not contain any names or usernames.

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 are logged.
- Famly checks and updates all employee authorizations on a regular basis, as a minimum semiannually. The authorizations are adapted or withdrawn in relation to employees changing job positions, responsibilities or resigning.
- Employees within the Operations Center are solely authorized to access personal data with an operational purpose. Such accesses are logged, cf. section "Logging" and the authorization is withdrawn when it has outdated its operational purpose.
- Famly's IT system is configured so that the Customer can authorize its employees on the basis of roles. The Customer assigns its employee authorizations through the web module provided by Famly. Other users of the Solution shall in addition be subjected to authorization that provides relevant access.
- 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. The Famly employees do not have access to personal data that is not included in their authorization.
- All Famly employees with access to personal data have their criminal record checked by Famly in connection with their employment.

b) Login, Username and Passwords

- All employees at Famly and at the Operations Center 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. Provided that the successive failed login attempts occurred from the same IP-address, the access from the respective IP-address will be blocked. 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 IT systems by using an anonymous user account or guest account.

c) Confidentiality

- All Famly employees with access to personal data are subject to confidentiality throughout their employment contracts and all employees within the Operations Center are subject to confidentiality.
- The confidentiality is maintained beyond the termination of the Famly Agreement or if the Famly Agreement with sub-data processors ceases. 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 IT solution, all data is stored in the Operations Center. 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 transport, transmission control, 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 IT solution, such connections are secured through encryption e.g. in the form of VPN. Any access to the Famly IT systems requires that the Famly employees register a username and a password.
- Electronic signature: Famly uses 256-bit SSL certificates to the authenticity of Famly towards the endusers.
- Transport Security: Famly utilizes end-to-end SSL encryption from enduser device all the way to the database as well as between internal services on the servers.

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 IT solution is automatically logged ("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 the Application Log by special request.
- Provided that access to the Famly IT solution is made in connection with technical issues e.g. support, error correction or other technical causes, such access will be logged in dedicated logs. In cases where the use of the Famly's IT solution is similar to the way other users are using the Famly IT solution, the access will be logged in the Application Log.

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 IT solution is automatically logged ("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 the Application Log by special request.
- Provided that access to the Famly IT solution is made in connection with technical issues e.g. support, error correction or other technical causes, such access will be logged in dedicated logs. In cases where the use of the Famly's IT solution is similar to the way other users are using the Famly IT solution, the 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 (physical/logical):

- Fire, Power Outages: Famly's office and Operations Center is secured in the usual manner to protect against fire. The Operations Center is furthermore secured so that the operations can continue even during power outages of a certain duration, protection against loss of communicative connections to the Operations Center has also been established.
- Backup: Famly secures data stored in the Famly IT solution through continuous backup of stored 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 in order to make sure that the backup routines function as intended. Backups are for safety reasons also duplicated and stored in another data center from the same provider in the same country and region.
- Uninterruptable Power Supply (UPS): The data center 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 centers 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 centers 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 an 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 minutes 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 IT solution, 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, cf. e.g. the section "Procedure", 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 GDPR data processing agreements with suppliers in order to comply with the terms under this agreement.

Audit

Famly will at least once a year have an external auditor verify that the procedures specified in this agreement are followed.