DATA PROCESSING AGREEMENT (DPA)

1. Introduction

This Data Processing Agreement ("DPA") is entered into between:

1.1 Data Controller: The entity that determines the purposes and means of the processing of personal data and is using the services provided by Served.ch LLC.

1.2 Data Processor: Served.ch LLC

- Address: Chemin du Pélard 13, 1197 Prangins, Switzerland
- Contact Information: info@appdate.io
- Data Protection Contact: Olivier Krull (CEO)

This DPA is incorporated by reference into the Terms of Service and Privacy Policy of Served.ch LLC. By using the services provided by Served.ch LLC, the Data Controller agrees to the terms of this DPA.

1.3 Definitions

For the purposes of this DPA, the following terms shall have the meanings set out below:

- **Data Controller**: The entity that determines the purposes and means of the processing of personal data. In this context, the Data Controller is the customer using the services provided by Served.ch LLC.
- **Data Processor**: The entity that processes personal data on behalf of the Data Controller. In this context, Served.ch LLC is the Data Processor.
- **Personal Data**: Any information relating to an identified or identifiable natural person (a "Data Subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
- **Data Subject**: The individual to whom the personal data relates (e.g., end-users of the Data Controller's website).

- **Processing**: Any operation or set of operations performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, erasure, or destruction.
- **Sub-processor**: A third-party service provider engaged by the Data Processor to assist in processing personal data on behalf of the Data Controller.
- **GDPR**: The General Data Protection Regulation (EU) 2016/679, as applicable.

2. Scope of Data Processing

2.1 Data Processed on app.appdate.io (Data Controller's Account)

Types of Personal Data Collected:

- Full name, email address, password, and company name (collected during registration).
- Payment information (collected via Stripe Checkout during billing).

Purpose of Processing:

- To create and manage user accounts.
- To process payments for subscriptions.
- To send transactional emails via Brevo (email service provider).

Data Subjects:

- The Data Controller and its authorized users.

2.2 Data Processed on Behalf of the Data Controller (End Users)

Types of Personal Data Collected:

- End-user interaction data:
    - Clicks on push notifications and posts.
    - Pages visited on the Data Controller's website.
    - Time spent on pages.
- Technical data:

    - Operating system (OS), browser, device type, and language.
- Geolocation data:
    - Country and city (for analytics purposes).
- Unique identifier:
    - Anonymized user ID (used to track which posts have been read).

Purpose of Processing:

- To display analytics to the Data Controller about their end-users' behavior.
- To determine when to display badges indicating new content.
- To show which posts in the feed have been read or not.
- To personalize content (e.g., displaying posts in the correct language).

Data Subjects:

- End-users of the Data Controller (visitors to the Data Controller's website).

2.3 Third-Party Sub-processors:

- **Stripe**: Processes payment information for subscriptions.
- **Brevo**: Sends transactional emails on behalf of Served.ch LLC.
- **Amazon Web Services (AWS)**: Provides cloud infrastructure for data storage and processing (Frankfurt data centers).
- **MongoDB Atlas**: Used as the primary database service for storing customer and end-user data.
- **Redis**: Used for in-memory caching of transient data (e.g., session data).
- **Approximated**: Used to automate custom domains and their SSL certificates for customers. Approximated does not process personal data other than custom domain names.

3. Data Processing Activities

3.1 Data Collection:

- Data is collected through the following methods:
    - **Data Controller's Account**: Data is collected via the app.appdate.io platform during registration, billing, and usage of the service.
    - **End Users**: Data is collected via an embeddable news feed widget and push notifications integrated into the Data Controller's website.

3.2 Data Storage:

- Data is stored in the following systems:
    - **MongoDB Atlas**: Used as the primary database for storing customer and end-user data.
    - **Redis**: Used for in-memory caching of transient data (e.g., session data).
    - **AWS (Frankfurt Data Centers)**: All data is stored in secure AWS data centers located in Frankfurt, Germany.

3.3 Data Processing:

- Data is processed for the following purposes:
    - **Data Controller's Account**:
        - Account management, billing, and communication (via Brevo for emails).
    - **End Users**:
        - Analytics (e.g., page visits, clicks, time spent).
        - Personalization (e.g., displaying posts in the correct language).
        - Functionality (e.g., tracking read/unread posts, displaying badges for new content).

3.4 Technical and Organizational Measures:

- To ensure the security and confidentiality of personal data, the following measures are implemented:

- **Encryption**: Data is encrypted in transit (using HTTPS/TLS) and at rest (using AES-256 encryption).
- **Access Controls**: Access to personal data is restricted to authorized personnel, with strong password policies and multi-factor authentication (MFA) in place for all systems.
- **Monitoring**: System monitoring is conducted using default AWS monitoring tools to detect and respond to potential security incidents.
- **Backups**: Regular backups of data stored in MongoDB Atlas are performed to ensure data recovery in case of loss or corruption.
- **Incident Response Plan**: A data breach response plan is in place to promptly address and mitigate any security incidents.
- **Data Minimization**: Only data necessary for the specified purposes is collected and processed.

4. Data Subject Rights

4.1 Assistance to the Data Controller:

- Served.ch LLC will assist the Data Controller in fulfilling data subject requests in accordance with applicable data protection laws, including the GDPR.

4.2 Types of Requests:

- **Access**: Upon request from the Data Controller, Served.ch LLC will provide information about the personal data processed on their behalf.
- **Rectification**: Served.ch LLC will correct or update personal data as instructed by the Data Controller.
- **Deletion**:
  - The Data Controller can delete individual end-user data directly within the app.appdate.io application.
  - If the Data Controller closes their account, all data related to them and their end-users is immediately and permanently deleted.
- **Restriction of Processing**: The Data Controller can manually enable or disable certain analytics data collection within the app.appdate.io application.

- **Data Portability**: Served.ch LLC will provide personal data in a structured, commonly used, and machine-readable format as instructed by the Data Controller.

4.3 Response Time:

- Served.ch LLC will respond to the Data Controller's requests for assistance without undue delay and, in any event, within 30 days of receiving the request. If additional time is required due to the complexity of the request, Served.ch LLC will inform the Data Controller and provide an estimated timeline for resolution.

5. Data Breach Notification

5.1 Detection and Response:

- Served.ch LLC relies on its sub-processors, including Amazon Web Services (AWS), to monitor and detect potential data breaches. AWS has implemented advanced security measures and breach detection systems to identify and respond to security incidents.
- In the event that Served.ch LLC becomes aware of a data breach (either through AWS notifications or other means), Served.ch LLC will:
    - Investigate the breach to determine its scope and impact.
    - Take immediate steps to contain and mitigate the breach.
    - Document the breach and the actions taken to address it.

5.2 Notification to the Data Controller:

- If a data breach occurs that affects the Data Controller's data, Served.ch LLC will notify the Data Controller without undue delay and, in any event, within 72 hours of becoming aware of the breach.
- The notification will include:
    - A description of the nature of the breach.
    - The categories and approximate number of data subjects and records affected.
    - The likely consequences of the breach.
    - The measures taken or proposed to address the breach and mitigate its effects.

5.3 Assistance to the Data Controller:

- Served.ch LLC will provide reasonable assistance to the Data Controller in fulfilling their obligations under applicable data protection laws, including:
    - Assisting with notifications to data protection authorities, if required.
    - Supporting communication with affected data subjects, if necessary.
- Served.ch LLC will also cooperate with the Data Controller to investigate and resolve the breach.

6. International Data Transfers

6.1 Data Storage Location:

- All customer and end-user data processed by Served.ch LLC is stored in Amazon Web Services (AWS) data centers located in Frankfurt, Germany. This ensures that data remains within the European Economic Area (EEA) and complies with GDPR requirements.

6.2 Safeguards for International Transfers:

- In the event that data is transferred outside the EEA or Switzerland, Served.ch LLC will ensure that appropriate safeguards are in place to protect the data. These safeguards may include:
    - **Standard Contractual Clauses (SCCs)**: Approved by the European Commission for international data transfers.
    - **Adequacy Decisions**: Ensuring that the recipient country provides an adequate level of data protection (e.g., Switzerland).

6.3 Sub-processors and International Transfers:

- Served.ch LLC uses the following sub-processors, which may involve international data transfers:
    - **Stripe**: Processes payment information and may transfer data outside the EEA. Stripe complies with GDPR and uses SCCs for international transfers.
    - **Brevo**: Sends transactional emails and may transfer data outside the EEA. Brevo complies with GDPR and uses SCCs for international transfers.

    - **AWS**: Data is stored in Frankfurt, Germany, but AWS may transfer data outside the EEA for support or maintenance purposes. AWS complies with GDPR and uses SCCs for international transfers.

- Served.ch LLC ensures that all sub-processors comply with applicable data protection laws and have appropriate safeguards in place for international data transfers.

7. Data Retention and Deletion

7.1 Data Retention Periods:

- **Customer Account Data**: Retained for the duration of the Data Controller's active subscription. If the Data Controller closes their account, all data is deleted immediately.
- **End-User Interaction Data**:
    - **Analytics Data**: Most analytics data (e.g., pages visited, clicks, time spent) is retained for 6 months.
    - **Read/Unread Posts**: Data related to read/unread posts is retained indefinitely for as long as the Data Controller's account is active. This data is anonymized and cannot be linked to individual end-users.
    - If the Data Controller closes their account, all end-user interaction data (including analytics and read/unread posts) is immediately and permanently deleted.
- **Payment Data**: Processed by Stripe and retained in accordance with Stripe's data retention policies.

7.2 Deletion Upon Request:

- The Data Controller can delete individual end-user data directly within the app.appdate.io application.
- If the Data Controller requests the deletion of their account or specific data, Served.ch LLC will process the request without undue delay and confirm once the data has been deleted.

7.3 Deletion Upon Account Closure:

- If the Data Controller closes their account, all data related to them and their end-users is immediately and permanently deleted from Served.ch LLC's systems. This includes:
    - Customer account data (e.g., name, email, company name).
    - End-user interaction data (e.g., analytics, read/unread posts).
    - Data stored in MongoDB Atlas and Redis.
- Backups containing the deleted data will be updated within the next scheduled backup cycle to ensure complete removal.

8. Audit and Compliance

8.1 Compliance Measures:

- Served.ch LLC implements appropriate technical and organizational measures to ensure compliance with the GDPR and other applicable data protection laws. These measures include:
    - Encryption of data in transit and at rest.
    - Access controls to restrict access to personal data.
    - Regular reviews of data processing activities to ensure alignment with legal requirements.

8.2 Data Controller's Audit Rights:

- In accordance with applicable law, the Data Controller has the right to audit Served.ch LLC's compliance with this DPA and applicable data protection laws.
- To request an audit, the Data Controller must submit a written request to Served.ch LLC, specifying the scope and purpose of the audit.
- Audits will be conducted in a manner that minimizes disruption to Served.ch LLC's operations and protects the confidentiality of other customers' data.
- Served.ch LLC may require the Data Controller to use an independent third-party auditor approved by Served.ch LLC.

8.3 Cooperation with Authorities:

- In accordance with applicable law, Served.ch LLC will cooperate with data protection authorities and comply with their requests for information or audits as required by law.

9. Liability and Indemnification

9.1 Liability of the Processor (Served.ch LLC):

- Served.ch LLC shall be liable for any damages caused by its processing activities only to the extent that such damages result from a breach of this DPA or applicable data protection laws.
- Served.ch LLC's total liability under this DPA shall be limited to the total amount paid by the Data Controller to Served.ch LLC in the 12 months preceding the event giving rise to the liability.

9.2 Liability of the Controller (Data Controller):

- The Data Controller shall be liable for any damages caused by its instructions or use of the services in violation of this DPA or applicable data protection laws.
- The Data Controller agrees to indemnify and hold harmless Served.ch LLC from any claims, damages, or losses arising from the Data Controller's failure to comply with its obligations as a data controller.

9.3 Indemnification:

- Each party (the "Indemnifying Party") agrees to indemnify, defend, and hold harmless the other party (the "Indemnified Party") from and against any claims, liabilities, damages, losses, or expenses (including reasonable legal fees) arising out of or related to:
    - The Indemnifying Party's breach of this DPA or applicable data protection laws.
    - The Indemnifying Party's negligence or willful misconduct.
- This indemnification obligation does not apply to the extent that the claim, liability, damage, loss, or expense is caused by the Indemnified Party's breach of this DPA or applicable data protection laws.

10. Liability and Indemnification

10.1 Liability of the Processor (Served.ch LLC):

- Served.ch LLC shall be liable for any damages caused by its processing activities only to the extent that such damages result from a breach of this DPA or applicable data protection laws.
- Served.ch LLC's total liability under this DPA shall be limited to the total amount paid by the Data Controller to Served.ch LLC in the 12 months preceding the event giving rise to the liability.

10.2 Liability of the Controller (Data Controller):

- The Data Controller shall be liable for any damages caused by its instructions or use of the services in violation of this DPA or applicable data protection laws.
- The Data Controller agrees to indemnify and hold harmless Served.ch LLC from any claims, damages, or losses arising from the Data Controller's failure to comply with its obligations as a data controller.

10.3 Indemnification:

- Each party (the "Indemnifying Party") agrees to indemnify, defend, and hold harmless the other party (the "Indemnified Party") from and against any claims, liabilities, damages, losses, or expenses (including reasonable legal fees) arising out of or related to:
    - The Indemnifying Party's breach of this DPA or applicable data protection laws.
    - The Indemnifying Party's negligence or willful misconduct.
- This indemnification obligation does not apply to the extent that the claim, liability, damage, loss, or expense is caused by the Indemnified Party's breach of this DPA or applicable data protection laws.

11. Miscellaneous

11.1 Governing Law:

- This DPA shall be governed by and construed in accordance with the laws of the jurisdiction in which the Data Controller is established, without regard to its conflict of law principles.

11.2 Amendments:

- Any amendments to this DPA must be made in writing and signed by both parties.

11.3 Severability:

- If any provision of this DPA is found to be invalid or unenforceable, the remaining provisions shall remain in full force and effect.

11.4 Entire Agreement:

- This DPA constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior agreements and understandings, whether written or oral, relating to such subject matter.