

Data Processing Addendum

Effective Date: March 3, 2026

Last Updated: October 14, 2026

This Data Processing Addendum ("DPA") supplements the Master Subscription Agreement ("Agreement") between Social News Desk, Inc. dba CivAll ("CivAll") and the entity identified in the applicable order form ("Customer"). This DPA governs the processing of Personal Data in connection with CivAll's provision of the Platform.

This DPA is incorporated into the Agreement by reference. In the event of a conflict between this DPA and the Agreement regarding the processing of Personal Data, this DPA controls.

1. Definitions

Capitalized terms not defined herein have the meanings given in the Agreement.

1.1. **"Controller"** means the party that determines the purposes and means of Processing Personal Data. Under this DPA, Customer is the Controller.

1.2. **"Data Privacy Laws"** means the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("CCPA/CPRA"); the Virginia Consumer Data Protection Act ("VCDPA"); the Colorado Privacy Act ("CPA"); the Connecticut Data Privacy Act ("CTDPA"); the Texas Data Privacy and Security Act ("TDPSA"); and all other applicable US state consumer privacy laws, including any amendments or successor statutes.

1.3. **"Data Subject"** means an identified or identifiable natural person whose Personal Data is Processed under this DPA.

1.4. **"Personal Data"** means Customer Data and Citizen Data that relates to an identified or identifiable natural person. Personal Data includes information defined as "personal information," "personal data," or equivalent terms under applicable Data Privacy Laws.

1.5. **"Personal Data Breach"** means a confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

1.6. **"Process" or "Processing"** means any operation or set of operations performed on Personal Data, including collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment, combination, restriction, erasure, or destruction.

1.7. **"Processor"** means the party that Processes Personal Data on behalf of the Controller. Under this DPA, CivAll is the Processor.

1.8. **"Service Provider"** has the meaning given under the CCPA/CPRA and, for purposes of this DPA, refers to CivAll's role in Processing Personal Data on behalf of Customer.

1.9. **"Sub-processor"** has the meaning given in the Agreement.

2. Scope and Applicability

2.1. This DPA applies when CivAll Processes Personal Data on behalf of Customer in connection with the Platform.

2.2. The details of Processing — including the subject matter, duration, nature, purpose, categories of Data Subjects, and types of Personal Data — are described in Annex A.

2.3. This DPA does not apply to data that CivAll Processes as an independent Controller (such as marketing website visitor data and prospective customer information), which is governed by CivAll's Privacy Policy.

3. Roles and Responsibilities

3.1. Customer as Controller

Customer determines the purposes and means of Processing Personal Data through the Platform. Customer is responsible for:

- (a) The lawfulness of its collection and use of Personal Data, including providing any required notices to Data Subjects and obtaining any required consents.
- (b) The accuracy and quality of Personal Data submitted to the Platform.
- (c) Ensuring that its Processing instructions to CivAll comply with applicable Data Privacy Laws.
- (d) Responding to Data Subject requests, with CivAll's assistance as described in Section 8.

3.2. CivAll as Processor / Service Provider

CivAll Processes Personal Data only on behalf of Customer and in accordance with Customer's documented instructions, which include the Agreement, this DPA, and Customer's configuration and use of the Platform. CivAll will not:

- (a) Process Personal Data for any purpose other than providing the Platform and performing its obligations under the Agreement.
- (b) Sell, rent, lease, or trade Personal Data to any third party, or "sell" or "share" Personal Data as those terms are defined under the CCPA/CPRA.

(c) Retain, use, or disclose Personal Data outside of the direct business relationship between CivAll and Customer.

(d) Combine Personal Data received from or on behalf of Customer with Personal Data received from other sources, except as necessary to provide the Platform in accordance with the Agreement.

3.3. CCPA/CPRA Certification

CivAll certifies that it understands and will comply with the restrictions in Section 3.2 and applicable requirements of the CCPA/CPRA. CivAll will notify Customer if it can no longer meet its obligations under this DPA.

4. Processing Instructions

4.1. CivAll will Process Personal Data in accordance with Customer's documented instructions. The Agreement, this DPA, and Customer's use and configuration of the Platform constitute Customer's complete Processing instructions.

4.2. If CivAll believes an instruction from Customer infringes applicable Data Privacy Laws, CivAll will promptly inform Customer. CivAll is not required to independently assess whether Customer's instructions comply with applicable law, but will not knowingly assist with Processing that violates applicable law.

4.3. If CivAll is required by law to Process Personal Data for a purpose other than providing the Platform, CivAll will inform Customer of that requirement before Processing, unless prohibited by law from doing so.

5. Prohibited Data Types

5.1. As described in Section 8.9 of the Agreement, the Platform is not designed to serve as a system of record for: (a) protected health information (PHI) as defined by HIPAA; (b) payment card data governed by PCI DSS; (c) criminal justice information governed by the CJIS Security Policy; or (d) biometric identifiers (collectively, "Prohibited Data Types").

5.2. Customer shall not use the Platform to intentionally collect, Process, or store Prohibited Data Types, and shall not solicit or require End Users to submit them through the Platform. CivAll has no obligation or liability arising from Customer's intentional use of the Platform to collect, Process, or store Prohibited Data Types in violation of this Section.

5.3. Personal Data submitted by End Users or other third parties without Customer's solicitation and captured by the Platform in the ordinary course, as described in Section 8.9(b) of the Agreement, does not violate this Section, and CivAll Processes it as Personal Data under this DPA.

6. Confidentiality

6.1. CivAll ensures that all personnel authorized to Process Personal Data are subject to appropriate confidentiality obligations, whether by contract or statutory duty.

6.2. CivAll restricts access to Personal Data to personnel who require access to perform their job functions in connection with the Platform.

7. Security Measures

7.1. CivAll maintains appropriate technical and organizational security measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or unauthorized access. These measures are described in Annex B, currently include the following, and apply to CivAll's production systems; CivAll may satisfy them through equivalent or stronger measures that achieve a comparable or better level of protection:

- (a) Encryption of data in transit (TLS 1.2 or higher) and at rest (AES-256).
- (b) Role-based access controls for internal personnel and Customer users.
- (c) Logical tenant isolation within the Platform.
- (d) Automated daily backups stored in a geographically separate availability zone.
- (e) Employee security training, vulnerability scanning, and incident response procedures.

7.2. CivAll will periodically review and update its security measures to address evolving threats and industry practices. Updates will not materially reduce the overall level of protection.

8. Data Subject Requests

8.1. Because CivAll acts as a Processor, Customer is responsible for responding to requests from Data Subjects exercising rights under applicable Data Privacy Laws (including rights of access, correction, deletion, portability, and opt-out).

8.2. If CivAll receives a Data Subject request directly, CivAll will promptly redirect the request to Customer and will not respond to the Data Subject without Customer's prior authorization, unless required by law.

8.3. CivAll will provide Customer with reasonable technical assistance to help Customer respond to Data Subject requests, including by making available self-service export and deletion tools within the Platform.

9. Sub-processors

9.1. Customer authorizes CivAll to engage Sub-processors to assist in providing the Platform. CivAll's current Sub-processors are listed in Annex C and in CivAll's Privacy Policy.

9.2. CivAll will enter into written agreements with each Sub-processor that impose data protection obligations no less protective than those set forth in this DPA.

9.3. CivAll will provide Customer at least thirty (30) days' advance written notice before engaging a new Sub-processor, as described in the Agreement. The notice will identify the Sub-processor, the Processing activities, and the categories of Personal Data involved.

9.4. If Customer objects to a new Sub-processor on reasonable data protection grounds, the parties will work in good faith to find an alternative solution. If no alternative is available, Customer may terminate the affected Subscription as described in the Agreement.

9.5. CivAll remains responsible for the acts and omissions of its Sub-processors to the same extent as if CivAll were performing the Processing directly.

9.6. **Third-Party Platforms Are Not Sub-processors.** Where Customer directs Personal Data to a Third-Party Platform (as defined in the Agreement) through an Integration that Customer has chosen to use — for example, by publishing content to, or exchanging data with, a social network or messaging service — that Third-Party Platform receives the Personal Data at Customer's direction and acts as a separate, independent controller or recipient, not as a Sub-processor of CivAll. The Sub-processor notice and objection process in Sections 9.3 and 9.4 does not apply to such Third-Party Platforms. Customer is responsible for its own relationship with, and the terms governing its use of, any Third-Party Platform, including the lawfulness of directing Personal Data to it.

10. Personal Data Breach

10.1. CivAll will notify Customer of a Personal Data Breach within seventy-two (72) hours of confirmation, as described in the Agreement.

10.2. The notification will include the following, to the extent known to CivAll at the time, and will be supplemented as further information becomes reasonably available: (a) the nature and scope of the breach; (b) the categories and approximate number of Data Subjects and records affected; (c) the measures taken or proposed to address the breach and mitigate its effects; (d) recommendations for steps Customer can take to protect affected individuals; and (e) a designated point of contact for further information. CivAll's notice and any related disclosure are made in good faith and are not an admission of fault or liability.

10.3. CivAll will cooperate with Customer in investigating the breach, providing ongoing updates, and implementing remediation measures.

10.4. CivAll will not notify Data Subjects or regulatory authorities directly without Customer's prior written authorization. Customer, as Controller, determines whether and how to provide notifications to Data Subjects and regulatory authorities in accordance with applicable breach notification laws.

11. Audit Rights

11.1. Customer may audit CivAll's compliance with this DPA no more than once per twelve (12) month period, with at least thirty (30) days' advance written notice, during normal business hours, and in a manner that does not unreasonably interfere with CivAll's operations. Customer bears the cost of any audit it initiates.

11.2. CivAll may satisfy Customer's audit request by providing a current independent third-party audit report (such as a SOC 2 Type II report) under a mutually executed non-disclosure agreement.

11.3. Upon Customer's written request, CivAll will make available information reasonably necessary to demonstrate compliance with this DPA.

12. Data Residency

12.1. All Personal Data is stored in data centers located in the United States, as described in the Agreement.

12.2. CivAll does not transfer or store Personal Data outside the United States, except for temporary CDN edge caching of static assets that do not contain Personal Data.

13. Data Return and Deletion

13.1. During the Subscription Term, CivAll retains Personal Data as necessary to provide the Platform.

13.2. After expiration or termination of the Subscription, CivAll provides a ninety (90) day data export window during which Customer may export all Personal Data, as described in the Agreement.

13.3. After the data export window closes, CivAll permanently deletes all Personal Data from production systems within thirty (30) days. Backup copies are purged on the next backup rotation cycle, not to exceed thirty (30) additional days.

13.4. Upon Customer's request, CivAll will provide written confirmation that deletion has been completed in accordance with this Section 13 and CivAll's standard deletion procedures, excluding backup copies pending purge under Section 13.3 and any Personal Data CivAll is permitted or required to retain under Sections 13.5 and 13.6.

13.5. CivAll may retain anonymized, aggregated data that cannot be used to identify any individual or Customer, as described in the Agreement. CivAll may also retain Personal Data to the extent required by applicable law, in which case CivAll will continue to protect such data in accordance with this DPA.

13.6. Personal Data within records in CivAll Archive that is subject to an active retention schedule or legal hold is retained and handled in accordance with the CivAll Archive Product Schedule, notwithstanding Sections 13.2 and 13.3. CivAll continues to protect such Personal Data in accordance with this DPA for so long as it is retained.

14. Government-Specific Provisions

14.1. CivAll acknowledges that Customer may be a government entity that is exempt from certain Data Privacy Laws in its capacity as a Controller. Regardless of Customer's exempt status, CivAll will comply with its obligations under this DPA and applicable Data Privacy Laws in its capacity as a Processor and Service Provider.

14.2. Customer may be subject to government data practices laws, public records laws, or similar statutes specific to its jurisdiction. CivAll will cooperate with Customer's reasonable requests related to compliance with such laws, as described in the Agreement.

14.3. CivAll will not use Personal Data for political campaign purposes, voter profiling unrelated to Customer's authorized use, or any purpose that would violate applicable government ethics or data practices laws.

14.4. Where Customer uses the Platform for time-sensitive public communications, CivAll's security measures and availability commitments are set out in this DPA and the SLA, and the remedies stated in the SLA are Customer's exclusive remedies for any failure to meet the availability commitment.

15. Term and Survival

15.1. This DPA is effective as of the Effective Date of the Agreement and continues for the term of the Agreement.

15.2. CivAll's obligations under this DPA survive as long as CivAll retains any Personal Data on behalf of Customer.

Annex A: Processing Details

Item	Description
Subject Matter	Processing Personal Data in connection with the CivAll civic engagement platform
Duration	Term of the Agreement plus the data export and deletion period
Nature and Purpose	Hosting, processing, storing, and transmitting Personal Data to enable civic engagement functionality, including notifications, citizen interactions, content management, analytics, and AI-assisted features
Categories of Data Subjects	(1) Authorized Users: government employees, contractors, and agents who administer the Platform; (2) End Users / Citizens: members of the public who interact with government services through the Platform
Types of Personal Data — Authorized Users	Name, email address, phone number, job title, department, agency affiliation, login credentials, usage activity
Types of Personal Data — Citizens	Contact information (name, email, phone, address), form and survey submissions, public comments and feedback, communication preferences, service requests, device and access information (IP address, browser type, general location)

Annex B: Security Measures

The following describes CivAll's current technical and organizational security measures, as applicable to its production systems. CivAll may implement equivalent or stronger measures, and may update these measures to address evolving threats and industry practices, provided that any update does not materially reduce the overall level of protection. Specific tools, vendors, and parameters (such as backup cadence and retention) may change accordingly.

Technical Measures

- Encryption in transit: TLS 1.2 or higher for all data in transit
- Encryption at rest: AES-256 for all data at rest
- Role-based access controls (RBAC) for internal personnel and Customer users
- Logical tenant isolation between customers
- Multi-factor authentication for internal systems
- Automated daily backups stored in a separate AWS availability zone within the United States
- Backup retention: not to exceed thirty (30) days
- Vulnerability scanning and dependency monitoring
- Application-level logging and monitoring

Organizational Measures

- Employee security awareness training
 - Confidentiality agreements for all personnel with access to Personal Data
 - Access limited to personnel with a business need
 - Incident response procedures and designated response team
 - Periodic review and updating of security measures
-

Annex C: Sub-processors

The following Sub-processors are authorized to Process Personal Data on CivAll's behalf as of the Last Updated date of this DPA. An up-to-date list is also maintained in CivAll's Privacy Policy.

Sub-processor	Purpose	Data Categories Processed	Location
Amazon Web Services (AWS)	Cloud hosting, infrastructure, email delivery (Amazon SES), and AI model inference (Amazon Bedrock)	All Customer Data and Citizen Data	United States