

Data Processing Addendum

Last updated October 25, 2026 · stationclipboard.com/data-processing-addendum

Key points

- It applies automatically to every Organization. No signature is needed, but you can sign a copy using our DPA for Signature form.
- We process your Organization's personal data only on its instructions, never sell it, and never use it to train AI models of our own.
- We notify you of a confirmed security incident within 72 hours.
- You can export your records at any time, and we delete them when your account ends.

This summary is for convenience. The full text below is what governs.

This Data Processing Addendum ("DPA") is part of the agreement between **Station Automation Solutions LLC** ("we," "us," or "our") and each Organization that uses Station Clipboard, made up of our Terms of Service and any signed agreement (together, the "Agreement"). It applies automatically, with no signature needed. An Organization that wants a signed copy can complete our DPA for Signature form and email it to hello@stationclipboard.com, and we will countersign it.

1. Definitions

- **"Customer Personal Data"** means personal information in Customer Data that we process on the Organization's behalf.
- **"Process"** means any operation on data, such as collecting, storing, using, sending, or deleting it.
- **"Subprocessor"** means a service provider we engage that processes Customer Personal Data.
- **"Security Incident"** means a confirmed breach of security that leads to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, Customer Personal Data.
- **"Privacy Laws"** means the U.S. federal and state privacy, biometric privacy, consumer health data, and data security laws that apply to the processing, such as the California Consumer Privacy Act and the Texas Data Privacy and Security Act.

Other capitalized words mean what they mean in the Terms of Service.

2. Roles

The Organization decides why and how Customer Personal Data is processed, and is its controller (or "business" or the equivalent under Privacy Laws). We process it only on the Organization's behalf, as its processor (or "service provider," "contractor," or the equivalent).

The Organization is responsible for having a lawful basis, and for giving every notice and obtaining every consent Privacy Laws require, for the Customer Personal Data it puts in the Service and the features it turns on, including face clock-in, clock-in areas, Community Alerts, Recruiting and its AI application reviews, Information Requests, public complaints, Fire Investigations, and Incident Reporting.

3. Details of the Processing

Subject matter	Providing Station Clipboard to the Organization under the Agreement
Duration	The term of the Agreement, and afterwards until the data is deleted as Section 11 describes
Nature and purpose	Hosting, storing, organizing, displaying, transmitting, analyzing, and deleting Customer Personal Data so that the Organization's users can use the modules, integrations, AI features, and public pages it enables; providing support; and keeping the Service secure
People whose data is processed	The Organization's members, employees, volunteers, and contractors; applicants and references; residents and alert subscribers; business owners, contacts, and permit applicants; people who make complaints; people involved in incidents and investigations; meeting guests; and others whose information the Organization puts in the Service
Kinds of personal data	Contact and identity details; account and sign-in records; employment, scheduling, time, and payroll records; training and certification records; messages and files; incident, inspection, and investigation records; locations; and the other data described in our Privacy Policy

Sensitive data	As the Organization chooses to use the features that hold them: Social Security numbers, government identification, health information, biometric information (face templates), precise location at clock-in, information about minors, and information about criminal investigations, each protected as our Privacy Policy describes
-----------------------	---

4. Processing on the Organization's Instructions

We process Customer Personal Data only to provide the Service, and only on the Organization's documented instructions. The Agreement, this DPA, and the Organization's configuration and use of the Service, including the modules, integrations, AI features, Workflows, and NERIS connection it enables, are its instructions. We will tell the Organization if we believe an instruction violates Privacy Laws.

We will not:

- Sell or share Customer Personal Data, or use it for targeted or cross-context behavioral advertising
- Retain, use, or disclose it for any purpose other than providing the Service, or outside our direct business relationship with the Organization, except as Privacy Laws permit
- Combine it with personal information we receive from others, except as Privacy Laws permit for providing the Service
- Use it to train AI models of our own

We will comply with the obligations Privacy Laws place on us as a processor and service provider, and give Customer Personal Data the level of privacy protection those laws require. We will tell the Organization if we determine that we can no longer meet those obligations. The Organization may take reasonable and appropriate steps to stop and fix any unauthorized processing of Customer Personal Data. We certify that we understand and will comply with the restrictions in this section.

We may create information that is de-identified so that it cannot reasonably be linked to a person or an Organization, such as performance measurements, and use it to maintain and improve the Service. We will keep it de-identified, will not try to re-identify it, and will require anyone we share it with to do the same.

5. Our Personnel

We limit access to Customer Personal Data to personnel who need it to provide, support, and secure the Service. They are bound by confidentiality obligations. Their entry into an Organization's account, any time they view the Service as a user, and the changes and queries they make with our database tools are recorded in our audit log, as the Terms of Service describe.

6. Security

We maintain technical and organizational measures designed to protect Customer Personal Data, appropriate to its nature and the risks, including those listed in Section 14. We may update these measures as long as the update does not materially lower the overall protection of Customer Personal Data.

7. Subprocessors

The Organization authorizes us to engage the Subprocessors described on our Subprocessors page. Some providers are described there by category; the Organization may ask us for their names, which we will give under confidentiality. We require each Subprocessor, by a written contract or its terms of service, to protect Customer Personal Data and to use it only to provide its service to us, and we are responsible for our Subprocessors' compliance with this DPA.

We will update the Subprocessors page before a new Subprocessor begins processing Customer Personal Data, and an Organization can ask us to email it when we do. If an Organization has a reasonable objection related to data protection, it may tell us within 15 days. We will work with it in good faith to address the objection, and if we cannot, it may end the affected part of the Service and receive a refund of any prepaid fees for the remaining term.

Services an Organization connects with its own account, such as Active911, PSTrax, WhenToWork, Google Sheets, a weather service, or a Twilio account, and NERIS, receive data at the Organization's direction. They are not our Subprocessors, and the Organization's own arrangements with them apply.

8. Security Incidents

If we confirm a Security Incident, we will notify the affected Organization without undue delay, and no later than 72 hours after we confirm it. We will tell the Organization what we know, including the nature of the incident, the kinds of data and people affected, the likely consequences, and what we are doing about it, and we will update it as we learn more.

We will take reasonable steps to contain, investigate, and fix the incident, and will help the Organization meet its own notification obligations. Unless the law requires us to, we will not notify the Organization's members or residents directly without consulting the Organization first. Our notice of a Security Incident is not an admission of fault.

9. Requests and Assistance

- **Individuals' requests.** If we receive a request from a person to access, correct, or delete their Customer Personal Data, we will pass it to the Organization and not answer it ourselves, unless the law requires. The Service lets Organizations find, correct, export, and delete most personal information themselves, and we will provide reasonable help where it does not.
- **Public records requests.** We will refer public records requests for Customer Data to the Organization and give reasonable help exporting records it needs to respond.
- **Legal demands.** If a government or court demands Customer Personal Data from us, we will refer it to the Organization where possible, and tell the Organization before we respond unless the law prohibits it.
- **Assessments.** We will provide information reasonably needed for the Organization to complete data protection assessments, privacy impact assessments, and security reviews that Privacy Laws or its procurement rules require of it.

10. Information and Audits

Once a year, or after a Security Incident, an Organization may ask us to answer a reasonable written security questionnaire or provide documentation that shows our compliance with this DPA. If Privacy Laws require more, such as an assessment by an independent auditor, we will agree in good faith on a reasonable scope, timing, and confidentiality, at the Organization's expense.

11. Return and Deletion

While its account is active, an Organization can export its records using the exports in each module, and we will provide reasonable help exporting records it needs.

When an Organization's account ends or is scheduled for deletion, it goes offline and can be restored for 7 days, including to complete a final export. After that, we delete Customer Personal Data from our production database, unless the Organization's agreement or the law requires us to keep it. Uploaded files are deleted from our file storage in a separate step. Copies in backups are deleted as backups are overwritten in their normal cycle, and remain protected under this DPA until then. Face templates are destroyed on the schedule in our Biometric Information Policy. On request, we will confirm in writing that the Organization's records and files have been deleted. Our Account Closure and Data Export Request form is the easiest way to ask.

12. Specific Kinds of Data

- **Biometric information.** Our Biometric Information Policy applies to face templates and is part of this DPA.
- **Health information.** We are not a business associate under HIPAA unless we sign a business associate agreement with the Organization. Without one, the Organization must not enter protected health information beyond what the Incident Reporting and medical record fields ask for.
- **Social Security numbers.** The Organization decides whether to turn on the Social Security number field. We store it encrypted and never send it to an AI provider.
- **Criminal justice information.** The Service is not designed for criminal justice information that requires CJIS compliance, and the Organization must not send it to the Service.
- **Children's information.** The Organization is responsible for any parent or guardian consent required for minors' information, including for face clock-in.

13. Where Data Is Processed

We store Customer Personal Data in the United States, and we will not move where it is stored outside the United States without telling the Organization first.

14. Security Measures

- **Encryption.** HTTPS with HTTP Strict Transport Security for all traffic; AES-256-GCM encryption at rest for face templates, Social Security numbers, authenticator secrets, election ballots, Google account tokens, text messaging credentials, and stored outside-service logins; one-way hashing for passwords and kiosk PINs.
- **Access control.** Logical separation of each Organization's data; role-based permissions the Organization controls; two-factor sign-in available to every Organization; sign-in throttling; sessions that expire after a week without use.
- **Our staff.** Access limited to personnel who need it; confidentiality obligations; two-factor sign-in required for database administration tools; staff access and database changes recorded in a permanent audit log.
- **Logging.** An activity log for each Organization, sign-in records kept for 180 days, and separate audit trails for payroll, HR, elections, onboarding, NERIS, and medical record views.

- **Public pages.** Rate limits, single-purpose links that expire, and tokens stored only as one-way hashes for emailed links.
- **AI features.** Off until turned on for an Organization; limited to the areas and roles it chooses; passwords, PINs, face templates, Social Security numbers, and medical records never sent.
- **Infrastructure.** Hosting in U.S. data centers operated by major cloud providers that maintain recognized security programs, with regular backups.
- **Response.** A process to investigate, contain, and notify Organizations of Security Incidents, and a public vulnerability disclosure policy.

15. General

This DPA lasts as long as we process Customer Personal Data for the Organization. If this DPA conflicts with the Terms of Service about personal information, this DPA controls; if a signed agreement or signed DPA between us and the Organization conflicts with this DPA, the signed document controls. Limits on liability in the Agreement apply to this DPA to the extent the law allows. We may update this DPA to reflect changes in law or in the Service, without reducing its protections for Customer Personal Data already collected.

Data Processing Addendum · Last updated October 25, 2026

Questions about this document: hello@stationclipboard.com or (979) 341-9333. Every legal document and fillable form is in the Legal Center.



Data Processing Addendum: Signature Page

This page goes with the Station Clipboard Data Processing Addendum dated October 25, 2026, printed on the pages before it. The DPA already applies to every Organization without a signature; sign this page if your Organization wants a signed copy for its records.

1 ORGANIZATION

ORGANIZATION'S LEGAL NAME

STATION CLIPBOARD ORGANIZATION ID

ADDRESS

- ☐ The Organization is a governmental entity
- ☐ The Organization is a HIPAA covered entity and wants to discuss a business associate agreement
- ☐ Email our privacy contact when the Subprocessors page changes

2 CONTACTS FOR NOTICES UNDER THE DPA

PRIVACY CONTACT NAME

EMAIL

PHONE

SECURITY INCIDENT CONTACT NAME

EMAIL

PHONE (24/7 IF POSSIBLE)

3 SIGNATURES

By signing, each party agrees to the Data Processing Addendum printed with this page, which forms part of the agreement between them made up of the Station Clipboard Terms of Service and any signed agreement. Each person signing confirms that they are authorized to sign for their party.

FOR THE ORGANIZATION

NAME

TITLE

SIGNATURE

DATE

FOR STATION AUTOMATION SOLUTIONS LLC

NAME

TITLE

SIGNATURE

DATE

Email the signed DPA to **hello@stationclipboard.com** with the subject line "Signed DPA." We countersign it and send a copy back.

FOR OFFICE USE ONLY

DATE RECEIVED

COUNTERSIGNED ON

COPY RETURNED ON