Data Processing Agreement

Last Updated: March 18, 2026. Turn Technologies, Inc.

This Data Processing Agreement (“DPA”) is incorporated into the services agreement (“Agreement”) between Turn Technologies, Inc., a Delaware corporation with offices at 311 West Monroe Street, 3rd Floor, Chicago, IL 60606 (“Turn,” “we,” “us,” or “Processor”) and the customer identified in the Agreement (“Customer,” “you,” or “Controller”).

This DPA governs Turn’s processing of Personal Data on Customer’s behalf in connection with background screening services. If this DPA conflicts with the Agreement, this DPA prevails for Personal Data matters.

1. Definitions

"Applicable Laws" means GDPR, UK GDPR, Swiss FADP, CCPA, FCRA, other applicable U.S. federal and state privacy and consumer reporting laws, and all data protection laws applicable to the processing under this DPA.

"Personal Data" means information relating to an identified or identifiable person provided to Turn by Customer for the Services.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed by Turn or its Sub-Processors in connection with the Services.

"Services" means Turn's AI-powered background screening services, including criminal checks, identity verification, employment/education verification, motor vehicle records checks, drug testing, continuous monitoring, and related services.

"Sub-Processor" means third parties (including Data Furnishers and infrastructure vendors) engaged by Turn to process Personal Data in connection with the Services.

"Data Furnisher" means a third-party entity that supplies background data to Turn, such as criminal records, motor vehicle records, identity records, and employment/education verification data.

"Standard Contractual Clauses" or "SCCs" means the EU Commission's standard contractual clauses for international transfers (Decision 2021/914).

Terms like "Controller," "Processor," "Data Subject," and "processing" have the meanings given in Applicable Laws.

2. Scope and Instructions

2.1 Turn processes Personal Data only: (a) as described in Annex 1; (b) per Customer's documented instructions via the Services; and (c) as required by law (with prior notice to Customer unless prohibited).

2.2 Turn shall notify Customer if it cannot comply with instructions due to legal requirements or if it determines it can no longer meet its obligations under this DPA or Applicable Laws.

2.3 **FCRA Compliance.** Turn is a Consumer Reporting Agency under the Fair Credit Reporting Act ("FCRA") and is accredited by the Professional Background Screening Association ("PBSA"). Customer acknowledges that it shall: (a) use background screening reports obtained through the Services only for permissible purposes under FCRA; (b) provide all required disclosures and obtain proper authorization from Data Subjects before initiating background checks; (c) comply with adverse action requirements under FCRA, including providing pre-adverse and adverse action notices; and (d) otherwise comply with all FCRA obligations applicable to end-users of consumer reports.

3. Security and Confidentiality

3.1 Turn maintains technical and organizational security measures as described in Annex 2, including encryption, access controls, monitoring, and regular security testing. Turn holds SOC 2 Type II certification and maintains policies aligned with ISO 27001 Annex A requirements. Turn uses Drata for continuous compliance monitoring and automated evidence collection.

3.2 All Turn personnel authorized to process Personal Data are bound by confidentiality obligations and receive regular security and privacy training.

3.3 Upon detecting a Personal Data Breach, Turn shall notify Customer within 72 hours with: (a) a description of the nature of the breach, including categories and approximate number of Data Subjects and records affected; (b) the likely consequences; (c) measures taken or proposed to address the breach and mitigate adverse effects; and (d) a contact point for further information. Where full information is not immediately available, Turn shall provide updates without undue delay.

4. Sub-Processors

4.1 Customer authorizes Turn to engage Sub-Processors, including Data Furnishers, to process Personal Data on Customer's behalf. The current list of Sub-Processor categories is in Annex 3.

4.2 Turn shall provide 30 days' advance notice before engaging new Sub-Processors via email to the address on file or by contacting privacy@turn.ai for subscription to notifications.

4.3 Customer may object to new Sub-Processors on reasonable data protection grounds within 30 days. If objections cannot be resolved, Customer may suspend or terminate affected Services without penalty.

4.4 Turn imposes equivalent data protection obligations on all Sub-Processors and remains liable for their acts.

5. Data Subject Rights and Assistance

5.1 Turn provides tools within the Services enabling Customer to fulfill Data Subject requests (access, correction, deletion, restriction).

5.2 Turn shall, upon Customer's written request, provide reasonable assistance with Data Subject requests that Customer cannot fulfill independently. Customer reimburses Turn's reasonable costs for such assistance.

5.3 If a Data Subject contacts Turn directly, Turn shall promptly refer them to Customer.

6. International Transfers

6.1 Customer acknowledges Personal Data may be processed in the United States and other jurisdictions where Turn and its Sub-Processors operate.

6.2 Turn participates in the EU-U.S., Swiss-U.S., and UK Extension Data Privacy Framework. Transfers covered by the DPF rely on Turn's DPF certification.

6.3 For European Data transfers not covered by an adequacy decision or DPF, the SCCs (incorporated by reference) apply:

- Module Two (Controller-to-Processor) applies where Customer is a Controller
- Module Three (Processor-to-Processor) applies where Customer is a Processor
- For UK transfers: UK Addendum applies
- For Swiss transfers: SCCs apply with Swiss law modifications
- Governing law: Republic of Ireland

7. U.S. State Privacy Laws

7.1 Where CCPA applies, Customer is a "Business" and Turn is a "Service Provider."

7.2 Turn certifies it: (a) processes Personal Data solely to perform Services; (b) does not sell or share Personal Data; (c) does not retain, use, or disclose Personal Data outside the direct business relationship; and (d) complies with CCPA Service Provider obligations.

7.3 Turn shall notify Customer if it determines it can no longer meet its obligations as a Service Provider under the CCPA or any other applicable U.S. state privacy law.

8. Audit and Compliance

8.1 Turn maintains SOC 2 Type II certification, policies aligned with ISO 27001 Annex A requirements, and PBSA accreditation. Turn shall provide audit reports, certifications, and penetration testing summaries upon reasonable request (subject to confidentiality).

8.2 Customer may audit Turn's compliance once per year (or more frequently following a Personal Data Breach or as required by law) upon 30 days' notice, during business hours, at Customer's expense. Any third-party auditor must be subject to confidentiality obligations.

9. Data Return and Deletion

9.1 Upon termination or Customer's request, Turn shall delete or return all Personal Data within 30 days and certify deletion, except where retention is required by law (including FCRA record retention requirements), in which case Turn isolates such data from further processing.

9.2 For expired or terminated accounts, Turn deletes associated Personal Data within 30 days. Individual Data Subjects (workers/applicants) may request deletion of their data at any time, and Turn shall process such requests promptly.

10. General

10.1 This DPA is governed by the law governing the Agreement unless Applicable Laws require otherwise.

10.2 This DPA survives termination for as long as Turn processes Personal Data on Customer's behalf.

10.3 Liability is subject to limitations in the Agreement.

10.4 This DPA may be modified only by written agreement signed by both parties.

10.5 If any part of this DPA is held unenforceable, the validity of all remaining parts shall not be affected.

Annex 1 — Details of Processing

Data Exporter
Customer (name, address, contact per Agreement)

Data Importer
Turn Technologies, Inc., 311 West Monroe Street, 3rd Floor, Chicago, IL 60606
Contact: Turn Compliance Team, privacy@turn.ai | +1-888-499-8876

Data Subjects
Job applicants, candidates, employees, contractors, and individuals submitted by Customer for screening.

Categories of Data
Name, date of birth, SSN/national ID, address, email, phone, employment history, education history, driver's license, criminal records, court records, drug test results, motor vehicle records, and background check results.

Sensitive Data
Criminal conviction/offense data; biometric data (identity verification); drug test results. Safeguards: purpose limitation, access restrictions, encryption (AES-256 at rest, TLS 1.2+ in transit), audit logging, staff training, and tokenization of PII.

Processing Activities
Collection, storage, organization, retrieval, use, disclosure by transmission, and deletion of Personal Data to perform background screening services, including criminal checks, identity verification, employment/education verification, MVR checks, drug testing, adjudication, and continuous monitoring.

Purpose
To perform AI-powered background screening and workforce compliance services as described in the Agreement.

Duration
For the term of the Agreement plus any legally required retention period (including FCRA requirements). Expired account data deleted within 30 days of termination. Individual deletion requests processed promptly upon receipt.

Transfer Locations
United States (primary — Heroku, AWS, Google Cloud Platform); additional locations where Sub-Processors and Data Furnishers operate (see Annex 3).

Annex 2 — Security Measures

Turn implements SOC 2 Type II certified security controls with policies aligned to ISO 27001 Annex A requirements:

Encryption. TLS 1.2+ for data in transit (HTTPS enforced); AES-256 encryption for data at rest. Key rotation performed at least annually via managed key management services.

Access Control. Role-based access with least privilege enforcement, MFA on all critical systems, automatic session timeout, password complexity requirements, annual access reviews, and offboarding within 1 business day of termination.

PII Management. Sensitive fields (SSN, DOB) protected through tokenization and encryption. Data classification policies identify and protect PII across all systems.

Physical Security. Cloud infrastructure hosted on Heroku, AWS, and Google Cloud Platform with restricted data center access, logging, monitoring, and alarm systems.

Monitoring & Logging. All data access logged and monitored via Datadog, New Relic, Papertrail, and Bugsnag. Real-time alerting with dedicated incident response channels.

Availability. 99.99% uptime SLA. Infrastructure redundancy across multiple availability zones. Continuous backups every minute (Point-in-Time Recovery) with 11 nines data durability. Documented disaster recovery and business continuity plans with regular tabletop and technical testing.

Penetration Testing. Annual independent penetration tests with 30-day remediation SLA. Most recent assessment rated overall security risk as "low."

Vulnerability Management. Automated scanning via GitHub Dependabot, Drata agents, and Datadog with Jira-tracked remediation SLAs.

Compliance Automation. Continuous monitoring of security controls via Drata, with automated evidence collection supporting SOC 2 Type II, GDPR, and CCPA compliance.

Training. Mandatory security and privacy training for all personnel with access to Personal Data.

Separation. Logical separation of customer data via application security and database-level controls with normalized schemas.

Turn regularly tests, assesses, and evaluates the effectiveness of these measures and updates them as appropriate.

Annex 3 — Sub-Processors and Data Furnishers

Turn engages the following categories of Sub-Processors and Data Furnishers:

Infrastructure Providers

- **Heroku (Salesforce)** — United States — Primary application hosting, database (PostgreSQL), Redis cache, task queues, logging (Papertrail)
- **Amazon Web Services (AWS)** — United States — Secure document storage (S3)
- **Google Cloud Platform** — United States — Firebase (real-time updates), Google Maps, reCAPTCHA

Data Furnishers

- **Criminal Records Database Providers** — United States — Federal, state, and county court records

- **Identity Verification Services** — United States — Document authentication, biometric verification
- **Employment & Education Verification Services** — United States — Employer and institution verification
- **Motor Vehicle Records Providers** — United States — State DMV database access
- **Drug Testing Laboratory Partners** — United States — Specimen collection and lab analysis

Operational Tools

- **Drata** — United States — Compliance automation and continuous monitoring
- **Datadog / New Relic** — United States — Application and infrastructure monitoring
- **Twilio** — United States — SMS and communication services
- **Mandrill (Mailchimp)** — United States — Transactional email delivery
- **Stripe** — United States — Payment processing
- **Bugsnag** — United States — Error monitoring

For the current detailed list including specific entity names, contact privacy@turn.ai.