Turn Data Processing Agreement

Turn Technologies, Inc. Last Updated: October 14, 2026. Effective date: October 14, 2026. This is version 2026-10-14. The version in effect before this date is available on request to privacy@turn.ai.

This Data Processing Agreement ("DPA") is incorporated into and forms part of the agreement under which Customer procures the Services (the "Agreement"). The Agreement is the signed written services agreement between the parties or, where the parties have not signed a written services agreement, the Turn Business Customer Terms in effect when Customer procures or uses the Services, in each case together with any order form, statement of work, or online order under it. This DPA is 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. Where Customer and Turn have executed a separate data processing agreement or data protection addendum that is signed by both parties, that agreement governs the processing it covers and this DPA does not apply to, amend, or supplement it, except that Section 2.3 and Sections 2.5 through 2.8, which allocate obligations under the Fair Credit Reporting Act between Turn as a consumer reporting agency and Customer as the user of consumer reports, continue to apply to Customer in addition to that signed agreement unless that signed agreement expressly addresses the same subject matter.

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.

"Data Subject Request" means a request from a Data Subject to exercise a right under Applicable Laws with respect to that Data Subject's Personal Data, including a right of access, correction, deletion, restriction, portability, or objection.

"De-Identified Data" means data derived from Personal Data that has been processed so that it cannot reasonably be used to identify, relate to, describe, or be linked to a particular Data Subject or to Customer, and that is maintained and used in that form.

"European Data" means Personal Data that is subject to the GDPR, the UK GDPR, or the Swiss FADP.

"Personal Data" means information relating to an identified or identifiable person that Turn processes on Customer's behalf in connection with the Services, whether that information is provided to Turn by Customer or by the Data Subject, or is obtained, received, generated, or derived by Turn from another source in the course of providing the Services to Customer, including the contents of a consumer report and the records supporting it.

"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 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"). Turn is a member of the Professional Background Screening Association ("PBSA"). That statement is a statement of present fact for informational purposes. It is not a warranty, representation, condition, or continuing covenant of Turn, and a change in Turn's membership status is not a breach of this DPA or of the Agreement. Customer certifies to Turn, and Turn relies on that certification as required by 15 U.S.C. § 1681e(a) and permitted by 15 U.S.C. § 1681b(b)(1), that it has a permissible purpose for each consumer report it procures and 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; (d) where a Data Subject is under eighteen (18) years of age, obtain the disclosure and authorization required by Section 604(b)(2) of the FCRA signed by that Data Subject's parent or legal guardian, together with any further parental consent required by applicable state law, before initiating a background check, and retain a record of that authorization; and (e) otherwise comply with all FCRA obligations applicable to end-users of consumer reports.

2.4 De-Identified and Aggregated Data. Turn may create De-Identified Data from Personal Data and may use and retain it to operate, secure, develop, test, benchmark, and improve the Services and to produce aggregated statistical and industry analyses. Turn shall not attempt to re-identify De-Identified Data and shall not disclose it in a form that identifies Customer or any Data Subject. Where Turn discloses De-Identified Data to a third party, Turn shall contractually obligate that party not to attempt to re-identify it and not to disclose it to any further recipient except on the same obligation. Turn maintains technical and organizational measures designed to prevent re-identification and does not attempt to re-identify De-Identified Data. This Section 2.4 does not apply to European Data.

2.5 Ongoing Screening and Monitoring. Where Customer procures continuous or periodic monitoring, Customer certifies that the disclosure it provided to the Data Subject and the authorization it obtained cover reports obtained on an ongoing basis for the duration of the engagement, and that Customer will cease requesting reports about a Data Subject when that authorization is withdrawn or the engagement ends. Customer shall notify Turn without undue delay when either occurs.

2.6 No Re-disclosure or Re-furnishing. Customer shall not resell, redistribute, or otherwise furnish a consumer report or the information in it to any third party, and shall not use it to assemble or maintain a database or file for the purpose of furnishing consumer reports to others. Customer may disclose a report to the Data Subject, to its own personnel and professional advisers who need it for the permissible purpose for which it was obtained, and to a service provider or software tool that acts solely for Customer in connection with that permissible purpose and is bound by written confidentiality, security, retention, and use restrictions no less protective than this DPA, and may make any disclosure required by law. A service provider or software tool that receives a report under this Section acts for Customer. Customer remains responsible for its handling of the report and shall not permit it to use the report or the information in it for its own purposes or for any person other than Customer.

2.7 Disputes and Reinvestigation. Where a Data Subject disputes the accuracy or completeness of information in a report, Customer shall cooperate with Turn as reasonably necessary for Turn to meet its reinvestigation obligations under 15 U.S.C. § 1681i, including by providing, on Turn's reasonable request, the disclosure and authorization records for that Data Subject and any information Customer holds that is relevant to the disputed item.

2.8 Investigative Consumer Reports. Where Customer procures a report that includes information obtained through personal interviews, Customer is responsible for the disclosure and disclosure-on-request obligations that 15 U.S.C. § 1681d imposes on the person who procures such a report.

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 a SOC 2 Type II report issued by an independent auditor and maintains policies aligned with ISO 27001 Annex A requirements. Turn uses a continuous compliance monitoring platform for automated evidence collection. Turn may update the measures described in Annex 2 in accordance with the final paragraph of that Annex.

3.2 All Turn personnel authorized to process Personal Data are bound by confidentiality obligations and receive regular security and privacy training. Each party shall keep confidential the non-public information of the other party that it receives in connection with this DPA, including Personal Data, audit reports, penetration testing summaries, security documentation, and the results of any assessment or inspection, shall use that information only as necessary to perform or to verify performance under this DPA and the Agreement, and shall disclose it only to those of its personnel, professional advisers, and contractors who need it for that purpose and who are bound by obligations of confidentiality no less protective than these. This obligation does not apply to information that is or becomes public through no breach of this Section, and does not prevent a disclosure required by law, provided that the disclosing party gives the other party such notice as the law permits.

3.3 Turn shall notify Customer without undue delay and, where feasible, within 72 hours after becoming aware of a Personal Data Breach affecting Personal Data processed under this DPA. The notification shall include, to the extent then known to Turn: (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 available at the time of the initial notification, Turn shall provide it in phases without undue delay as it becomes available.

3.4 Unsuccessful attempts to gain access to Personal Data or to the systems on which Personal Data is stored, and events that do not compromise the security, confidentiality, or integrity of Personal Data, including pings, port scans, unsuccessful log-on attempts, denial of service attacks, and similar activity, are not Personal Data Breaches and do not require notification under Section 3.3. Turn's notification of, or response to, a Personal Data Breach is not an acknowledgment by Turn of fault or liability.

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 Sub-Processors and Data Furnishers are identified in Annex 3, which Turn may update in accordance with Section 4.2.

4.2 Where Turn engages a Sub-Processor to perform a function not already described in Annex 3, Turn shall publish an updated Annex 3 describing that function at least 30 days before that Sub-Processor begins processing Personal Data. Where Turn engages a Sub-Processor to perform a function already described in Annex 3, including in substitution for or in addition to an existing Sub-Processor performing that function, Turn shall update Annex 3 within a reasonable period and no advance notice period applies. Publication of the updated Annex 3 constitutes notice to Customer for purposes of this Section 4, and Turn is not required to give separate notice. Customer is responsible for reviewing Annex 3 and may request email notification of changes by contacting privacy@turn.ai.

4.3 Customer may object to a new Sub-Processor on reasonable data protection grounds by written notice to privacy@turn.ai within 30 days after the updated Annex 3 is published. The parties shall work in good faith to resolve the objection. If it cannot be resolved within a reasonable period, Customer's sole and exclusive remedy is to terminate the affected Services on written notice, without penalty and without refund of amounts already incurred. Customer's failure to object within the 30-day period constitutes approval of the Sub-Processor.

4.4 Turn shall impose on each Sub-Processor written data protection obligations that are no less protective in all material respects than those in this DPA, to the extent relevant to the services that Sub-Processor performs. Turn remains responsible for the performance of each Sub-Processor's obligations, and any resulting liability of Turn is subject to the limitations and exclusions of liability in the Agreement. This Section 4.4 does not apply to a Data Furnisher to the extent that Data Furnisher determines the purposes and means of its own processing and acts as an independent controller, including a consumer reporting agency, court, government agency, or other public record source; with respect to such a Data Furnisher, Turn remains responsible for its own selection of, and instructions to, that Data Furnisher.

5. Data Subject Rights and Assistance

5.1 Where the Services include functionality that allows Customer to access, correct, delete, or restrict Personal Data, Customer may use that functionality to respond to Data Subject Requests. Turn does not warrant that the Services include functionality sufficient to satisfy every Data Subject Request.

5.2 Turn shall, upon Customer's written request, provide reasonable assistance with Data Subject Requests that Customer cannot fulfill independently, taking into account the nature of the processing and the information available to Turn. Customer shall reimburse Turn's reasonable costs, including personnel time, for such assistance.

5.3 If a Data Subject contacts Turn directly with a Data Subject Request, Turn shall promptly refer the Data Subject to Customer and shall not otherwise respond to the request, except where Turn is required or permitted to respond directly under Applicable Laws, including its obligations as a Consumer Reporting Agency to provide file disclosures and to conduct reinvestigations under the FCRA, or as described in Section 9.3. Turn shall inform Customer of any such direct response where permitted to do so.

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 For European Data transfers not covered by an adequacy decision, 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 the CCPA applies, Customer is a "Business" and Turn is a "Service Provider." Where another U.S. state privacy law applies, Customer is the controller or business and Turn is the processor or service provider, as those or equivalent terms are defined in that law.

7.2 Turn certifies it: (a) processes Personal Data solely to perform the Services; (b) does not sell or share Personal Data; (c) does not retain, use, or disclose Personal Data outside the direct business relationship, except as permitted by Applicable Laws, including for the retention purposes described in Section 9.1 and the De-Identified Data uses described in Section 2.4; 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.

7.4 Certain Personal Data processed under this DPA is regulated by the FCRA and is exempt from the CCPA and from comparable state privacy laws to the extent provided in those laws. Nothing in this Section 7 requires Turn to act in a manner inconsistent with the FCRA.

8. Audit and Compliance

8.1 Turn maintains a SOC 2 Type II report issued by an independent auditor and policies aligned with ISO 27001 Annex A requirements. Turn shall provide its most recent SOC 2 Type II report, any third-party assessments it holds, and penetration testing summaries upon reasonable written request, no more than once in any twelve (12) month period and subject to confidentiality obligations. The parties agree that these materials satisfy Customer's audit and information rights under Applicable Laws in the first instance.

8.2 Where the materials in Section 8.1 are not sufficient to demonstrate compliance, Customer may audit Turn's compliance once per year, or more frequently following a Personal Data Breach affecting Customer's Personal Data or where required by law, upon 30 days' prior written notice, during business hours, and at Customer's expense, including reimbursement of Turn's reasonable costs and personnel time incurred in supporting the audit. Any audit shall be limited to Turn's processing of Customer's Personal Data, shall not extend to data of Turn's other customers or to Turn's confidential commercial information, shall not include intrusive or automated testing of Turn's systems without Turn's prior written consent, and shall not unreasonably disrupt Turn's business. Any third-party auditor must not be a competitor of Turn and must be subject to confidentiality obligations.

9. Data Return and Deletion

9.1 Upon termination of the Agreement, or upon Customer's earlier written request, Turn shall delete or return Personal Data processed on Customer's behalf within 30 days, except to the extent that retention is required or permitted by Applicable Laws or is reasonably necessary for Turn to: (a) meet its recordkeeping, file disclosure, reinvestigation, and dispute obligations as a Consumer Reporting Agency under the FCRA and comparable laws; (b) establish, exercise, or defend legal claims, including throughout any applicable limitations period; (c) comply with a litigation hold, subpoena, court order, or request from a regulator or supervisory authority; (d) retain records of disclosures, authorizations, and consents; or (e) detect, prevent, and investigate fraud, misuse, and security incidents. Customer acknowledges that these exceptions apply to most Personal Data that Turn processes in connection with background screening, including consumer reports and the records supporting them, and that Turn ordinarily retains such Personal Data after termination. Personal Data retained under an exception remains subject to this DPA and to the security measures described in Annex 2, and Turn does not use it for any purpose other than the purpose for which it is retained. Personal Data residing in backup, archival, or disaster recovery media is retained in accordance with Turn's ordinary backup practices and remains subject to this DPA. Upon Customer's written request, Turn shall confirm in writing what Personal Data has been deleted or returned and what has been retained under an exception. With respect to European Data, at the end of the provision of the Services Turn shall delete or return the data at Customer's election, except to the extent Applicable Laws require or permit continued storage on a ground described in this Section 9.1. Customer may make that election at any time by written notice to privacy@turn.ai.

9.2 Turn does not automatically delete Personal Data when an account expires or is terminated. Deletion or return is carried out on Customer's written request under Section 9.1, or where Applicable Laws require it.

9.3 Deletion Requests from Data Subjects. Where a Data Subject asks Turn directly to delete Personal Data, Turn shall verify the identity of the requester before taking any action and shall handle the request in accordance with Section 5.3 and Applicable Laws. Turn is not required to delete Personal Data where an exception applies under Applicable Laws, including where the Personal Data is regulated by the FCRA or a comparable consumer reporting law, where retention is necessary for any purpose described in Section 9.1, or where deletion would prevent Turn from meeting an obligation owed to the Data Subject, to Customer, or to a regulator. Turn shall respond within the period required by Applicable Laws or, where no period is specified, within 45 days of verifying the request.

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 Each party's liability arising out of or related to this DPA is subject to the limitations and exclusions of liability in the Agreement, and any reference in this DPA to liability is to be read accordingly. Liability under the Standard Contractual Clauses is governed by those clauses.

10.4 Turn may update this DPA from time to time by publishing a revised version and updating the "Last Updated" date. The revised version takes effect immediately upon publication and governs all processing from that time. Publication is the only notice required, and Turn is not obligated to give separate or advance notice of an update. No update may materially reduce Turn's obligations regarding the security or confidentiality of Personal Data, and no update alters the Standard Contractual Clauses, which may be modified only as those clauses permit. If an update materially and adversely affects Customer, Customer may terminate the affected Services by written notice to privacy@turn.ai given within 30 days after publication, and the version of this DPA in effect immediately before that update continues to govern processing for that Customer until the termination takes effect. Absent such notice within that period, Customer is deemed to have accepted the update. Where a change is required by Applicable Laws or by a supervisory authority, it takes effect on the date required. This Section 10.4 does not apply where the parties have executed a separate signed data processing agreement, which may be modified only in accordance with its own terms.

This Section 10.4 governs updates published on or after the date this Section 10.4 takes effect. For a Customer whose processing was governed by a version of this DPA published before that date, the publication of this Section 10.4 is itself an update, and that Customer may terminate the affected Services on the terms set out above by written notice given within 30 days after publication. The version of this DPA in effect immediately before that publication continues to govern that Customer until the termination takes effect or the notice period expires without notice.

10.5 Except as provided in Section 10.4, this DPA may be modified only by written agreement signed by both parties.

10.6 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. This may include individuals aged thirteen (13) to seventeen (17) where Customer has obtained the parental or guardian authorization required by Section 2.3. Turn does not knowingly process Personal Data of an individual under thirteen (13) years of age for screening purposes.

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 and offense data; identity verification data, including images of identification documents and self-taken photographs submitted for 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 background screening and workforce compliance services as described in the Agreement.

Duration. For the term of the Agreement plus any retention period described in Section 9.1, including retention required or permitted under the FCRA and other Applicable Laws. Turn does not automatically delete Personal Data associated with expired or terminated accounts. Deletion or return is carried out in accordance with Section 9, which describes the request-based process and the grounds on which

Turn retains Personal Data as a Consumer Reporting Agency. Requests from Data Subjects are handled in accordance with Sections 5.3 and 9.3.

Transfer Locations. United States (primary); Canada; additional locations where Sub-Processors and Data Furnishers operate. Current providers and locations are identified in Annex 3.

Annex 2 — Security Measures

Turn implements the security controls described below. Those controls are within the scope of Turn's SOC 2 Type II report, and Turn's policies are 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 is hosted with major commercial cloud providers whose data centers maintain restricted access, logging, monitoring, and alarm systems. Current providers are identified in Annex 3.

Monitoring & Logging. Access to Personal Data is logged and monitored using application performance monitoring, log aggregation, and error tracking tools, with real-time alerting and dedicated incident response channels.

Availability. Infrastructure redundancy across multiple availability zones. Continuous backup with point-in-time recovery. Documented disaster recovery and business continuity plans, tested at least annually through tabletop and technical exercises. Any service level commitment and its associated remedies are set out in the Agreement and not in this DPA.

Penetration Testing. Annual independent penetration testing. Findings are triaged by severity and remediated on a risk-based schedule, with critical and high severity findings prioritized for prompt remediation. Summary results are available under Section 8.1.

Vulnerability Management. Automated dependency, code, and infrastructure scanning, with findings tracked to remediation and prioritized by severity.

Compliance Automation. Continuous automated monitoring of security controls, with 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. Turn may modify the measures described in this Annex 2 from time to time, including by changing the specific technologies or vendors used, provided that no modification materially reduces the overall level of security applied to Personal Data. The named categories of tooling in this Annex are descriptive of function and are not a commitment to any particular product or vendor.

Annex 3 — Sub-Processors and Data Furnishers

This Annex 3 is Turn's sub-processor list for purposes of Applicable Laws. Turn engages the following Sub-Processors and Data Furnishers, and may update this Annex 3 in accordance with Sections 4.2 and 10.4:

Infrastructure Providers

- **Cloud Application Hosting and Managed Database Providers** — United States — Primary application hosting, managed relational database, in-memory cache, task queues, and application logging
- **Cloud Object Storage Providers** — United States — Encrypted storage of documents and report artifacts
- **Cloud Platform Service Providers** — United States — Real-time application updates, address and mapping lookup, and automated abuse prevention

Data Furnishers

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

- **Compliance Automation and Continuous Control Monitoring** — United States — Security and compliance program monitoring
- **Application and Infrastructure Monitoring Providers** — United States — Performance, availability, and error monitoring
- **Messaging and Communication Providers** — United States — SMS and related transactional messaging
- **Transactional Email Providers** — United States — Delivery of service and notice emails
- **Payment Processing Providers** — United States — Billing and payment processing for business customers
- **Error and Crash Reporting Providers** — United States — Application error diagnostics

Where a category above lists a function rather than a named entity, Turn will identify the specific entities on written request to privacy@turn.ai. Turn may substitute a Sub-Processor performing the same function, subject to Sections 4.2 through 4.4.