Data Processing Addendum

Version: v1
Effective Date: October 3, 2025

This Data Processing Addendum (“DPA”) forms part of any agreement under which Landa Solutions Ltd. DBA Kleerr (“Processor”) provides services to a customer (“Customer”). Regional applicability. This DPA applies globally; EEA/UK/CH-specific terms apply only where those laws govern the processing. By using the Services, Customer agrees this DPA applies whenever Kleerr processes Customer Data on Customer’s behalf.

1. Scope & Roles

Controller/Processor. Customer is the Controller of Customer Data; Kleerr is the Processor processing Customer Data on Customer’s behalf. Where Customer is a Processor of a third party, Kleerr is a Subprocessor and Customer warrants it has authority to appoint Kleerr.

2. Processing Instructions

Kleerr will process Customer Data only per Customer’s documented instructions (the Agreement, this DPA, and configuration via the Services). Kleerr will promptly inform Customer if an instruction appears unlawful.

3. Confidentiality & Personnel

Kleerr ensures personnel accessing Customer Data are bound by confidentiality and receive appropriate privacy/security training.

4. Security Measures

Kleerr implements technical and organizational measures appropriate to risk, including encryption in transit/at rest; access controls; network and perimeter protections; secure software development; logging/monitoring; and business continuity. Details are set out in Annex II.

5. Subprocessors

Customer provides general authorization for Kleerr to engage Subprocessors to process Customer Data. Kleerr will maintain a current list of Subprocessors at

kleerr.com/legal/subprocessors, which Kleerr may update from time to time, and will indicate the last-updated date on that page. Customers may subscribe to email notifications of changes as described on that page. Where feasible, Kleerr will provide at least 30 days' advance email notice to subscribed Customer admins for material changes (emergency replacements excluded). Customer may object in writing to a new or replacement Subprocessor on reasonable, documented data-protection grounds within 10 business days after the update is posted. Upon a valid objection, the parties will work in good faith for up to 30 days to implement a reasonable alternative (for example, use an alternative Subprocessor for Customer or apply materially equivalent controls). If no reasonable alternative is available, Customer may terminate only the impacted Services; termination is effective at the end of the current billing period, and Kleerr will provide a prorated refund of prepaid, unused fees for the impacted Services, except where otherwise required by law. For emergency replacements needed to preserve security/availability, Kleerr may replace first and notify promptly; the objection/cure flow then applies. Changes among Kleerr's Affiliates or between data centers/products of the same cloud provider are not material changes.

6. International Transfers

Kleerr will only transfer Customer Data across borders in compliance with applicable data protection laws.

Conditional SCCs. Where a transfer of Customer Data is subject to EEA/UK/Swiss data protection law, the Parties incorporate by reference the European Commission's Standard Contractual Clauses (SCCs) (Modules 2 and/or 3, as applicable) and, for UK transfers, the UK International Data Transfer Addendum. Annexes I–III of this DPA serve as the SCC Annexes. The Parties select Ireland as the governing law and courts for Clauses 17–18. These instruments apply only to restricted transfers that fall within their scope under applicable law.

7. Data Subject Requests

Taking into account the nature of processing, Kleerr will provide reasonable assistance through the Services or available documentation to help Customer respond to requests to exercise data subject rights (access, correction, deletion, restriction, portability, objection), where legally required. Additional assistance beyond this may be subject to a separate fee.

7A. Regulatory & Security Assistance

Taking into account the nature of processing and the information available to Kleerr, Kleerr will provide reasonable assistance to Customer with (a) data protection impact assessments and prior consultations with supervisory authorities, and (b) Customer's security, breach notification, and record-keeping obligations under applicable Data Protection Laws. Kleerr may charge

reasonable, documented fees for assistance beyond standard product features and documentation.

8. Incident Notification

Kleerr will notify Customer without undue delay and, where required by law, within 72 hours after confirming a Personal Data Breach (a “Security Incident”) involving Customer Data and will provide information reasonably necessary for Customer to meet its obligations, consistent with applicable law, with updates as the investigation progresses.

9. Audits & Assurance

Upon reasonable written request and not more than once every 12 months, or following a confirmed Security Incident or material breach of this DPA, Kleerr will make available information needed to demonstrate compliance with this DPA (e.g., security overview, policies) and allow audits by Customer or its auditor, subject to confidentiality, scheduling, and burden limits. Customer bears its own audit costs and Kleerr’s reasonable support costs. Kleerr may satisfy audit requests by providing written responses to reasonable security questionnaires and relevant policy excerpts. If a third-party audit report (e.g., SOC 2) becomes available, it will be deemed sufficient absent a specific legal requirement for additional procedures. Remote/document reviews are preferred. Audits must be conducted during normal business hours, on reasonable notice, and may not unreasonably disrupt Kleerr’s business operations.

10. Return/Deletion

At termination or expiry, on Customer’s written instruction, Kleerr will delete or return Customer Data and delete existing copies, subject to legal retention.

Kleerr will complete deletion or return within 30 days of such instruction and will certify deletion upon request. Backup deletion follows standard rotation schedules.

11. CCPA/CPRA; Other Laws

For personal information subject to the CCPA/CPRA that Kleerr processes on Customer’s behalf, Kleerr acts as Customer’s service provider/contractor and certifies that it will not sell or share such information; will not retain, use, or disclose it for any purpose other than providing the Services to Customer (including no use for cross-context behavioral advertising or profiling) or as otherwise permitted by the CCPA/CPRA; will not retain, use, or disclose it outside the direct business relationship; and will not combine it with personal information it receives from

another source except as permitted by the CCPA/CPRA. Kleerr will enable Customer to comply with applicable consumer requests to the extent required by law.

12. Liability & Order of Precedence

Each Party's liability under this DPA is subject to the limitations and exclusions in the Agreement. In the event of conflict, this DPA controls with respect to data protection, subject always to those limitations.

ANNEX I – Details of Processing

- Subject matter: Provision of the Kleerr analytics Services.
- Duration: Term of the Agreement + limited post-term retention per Section 10.
- Nature & purpose: Collecting, unifying, and analyzing web/app interaction data to provide attribution and insights.
- Types of personal data: Online identifiers (cookie/ID), IP address, device/browser metadata, page views, clickstream, referral URLs, event data, limited contact fields provided by Customer (e.g., email) where configured.
- Special categories: Not intended. No PHI without a separate BAA.
- Data subjects: End users/visitors of Customer's digital properties; Customer personnel with accounts.
- Authorized recipients: Kleerr and approved Subprocessors.

ANNEX II – Security Measures (Summary)

Kleerr implements technical and organizational measures appropriate to the risk of processing Customer Data, designed to protect against unauthorized access, loss, or disclosure. These include, at a minimum:

- Encryption: Encryption of Customer Data in transit (TLS) and at rest, with key management provided by trusted cloud services.
- Access Controls: Role-based access and least-privilege principles; MFA is required for internal administrative access.
- Network & Infrastructure Security: Isolation of customer environments, firewalls, and hardening of servers and endpoints.
- Secure Development Practices: Code review, dependency management, and vulnerability monitoring as part of the software development lifecycle.
- Vulnerability Management: Kleerr maintains an ongoing vulnerability management program covering code, dependencies, and infrastructure. Vulnerabilities are prioritized by severity and risk; Kleerr will use commercially reasonable efforts to remediate or

implement compensating mitigations within the following targets: Critical: 14 days; High: 30 days; Medium: 90 days; subject to technical feasibility and vendor patch availability.

- Monitoring & Logging: System logging and monitoring of infrastructure for anomalies or security events.
- Backup & Recovery: Regular backups of critical data with retention policies and tested restoration procedures.
- Change Management: Processes for reviewing and documenting significant changes to production systems.
- Personnel Practices: Confidentiality agreements for employees and contractors; security awareness training; background checks where legally permitted and appropriate for sensitive roles, at Kleerr's discretion.
- Vendor Management: Due diligence and contractual safeguards for Subprocessors handling Customer Data.

This DPA is deemed accepted and effective as of the date Customer first uses the Services or enters into an Agreement with Kleerr.