

## KLA Data Protection Standards

*Effective as of November 16, 2021. Updated September 22, 2022.*

KLA Corporation and its affiliates and subsidiaries (collectively “KLA”) requires that service providers, contractors, suppliers, distributors and other business partners and their employees (collectively “You”) comply with the requirements set forth in these Data Protection Standards (“Standards”) with respect to any information (“KLA Data”) that KLA or its employees, representatives, customers, distributors, or other business partners make available to You in the context of Your business relationship with KLA or an KLA customer.

1. **Use and Transfer Limitations.** You must not access, collect, store, retain, transfer, use or otherwise process in any manner any KLA Data, except: (a) in the interest and on behalf of KLA; (b) as directed by authorized personnel of KLA in writing; and (c) in accordance with applicable law. Without limiting the generality of the foregoing, You may not make KLA Data accessible to any subcontractors or relocate KLA Data to new locations, except as set forth in written agreements with, or written instructions from KLA. You must return or delete any KLA Data at the end of Your relationship with KLA and, at any time, at KLA’s request. You must impose contractual obligations on all employees, contractors and onward recipients that are at least as protective of KLA Data as these Standards.
2. **Comply with Approved Policies.** You must keep KLA Data secure from unauthorized access and other data processing by using Your best efforts and state-of-the art organizational and technical safeguards. If You conduct SSAE 16, SOC or similar or successor audits, You must comply with Your SSAE 16, SOC or similar or successor standards and provide KLA with thirty (30) prior days’ notice of any changes.
3. **Cooperate with Compliance Obligations.** At KLA’s reasonable request, You must: (a) execute a business associate agreement under the U.S. Health Insurance Portability and Accountability Act of 1996 and related regulations, as amended (“HIPAA”) as well as similar agreements as required under other jurisdictions’ laws, (b) contractually agree to comply with laws and industry standards designed to protect KLA Data, including, without limitation, the Standard Contractual Clauses approved by the European Commission for data transfers to processors and/or (see clause 7 below), PCI Standards, as well as similar and other frameworks, if and to the extent such frameworks apply to any KLA Data that You come into contact with; or (c) allow KLA to terminate certain or all contracts with You, subject to (i) a proportionate refund of any prepaid fees, (ii) transition or migration assistance as reasonably required, and (iii) without applying any early termination charges or other extra charges.
4. **Submit to Audits.** You must provide information on Your compliance program and submit to reasonable data security and privacy compliance audits by KLA or, at KLA’s request, by an independent third party, or customers of KLA, to verify compliance with these Standards, applicable law, and any other applicable contractual undertakings.
5. **Notify Breaches.** If You become aware of unauthorized access to KLA Data, or of any security breach that is reportable under the EU General Data Protection Regulation (GDPR) or laws applicable to You or KLA, You must immediately notify KLA, consult and cooperate with investigations and potentially required notices, and provide any information reasonably requested by KLA. You must also indemnify KLA from any resulting damages and costs, including, without limitation, identity protection assistance and services procured for data subjects and reasonable attorneys and technical consultant fees for KLA’s handling of the incident.
6. **No Information Selling or Sharing for Advertising.** You acknowledge and confirm that You do not receive any KLA Data as consideration for any services or other items that You provide to KLA. You shall not have, derive or exercise any rights or benefits regarding KLA Data. You must not sell or share any KLA Data, as the terms “sell” and “share” are defined in the California Consumer Privacy Act of 2018, as amended, including by the California Privacy Rights Act of 2020 (“CCPA”) or under any other laws. You must not collect, retain, use, or disclose any KLA Data (a) for targeted or cross-context behavioral advertising, (b) but for the business purposes specified in a written contract with KLA, or (c) outside the direct business relationship with KLA. You must not combine KLA Data with other data if and to the extent this would be inconsistent with limitations on service providers under the CCPA or other laws. You certify that You understand the rules, requirements and definitions of the CCPA, and all restrictions in the Data Protection Standards. You agree to refrain from taking any action that would cause any transfers of KLA Data to or from You to qualify under the CCPA or other laws as “sharing” for advertising purposes or as “selling” personal information.

7. EEA and UK Personal Data: With respect to any KLA Data that is subject to the GDPR or similar laws of other EEA countries and the UK as "personal data," You accept the attached Standard Contractual Clauses 2021 promulgated by Commission implementing decision (EU) 2021/914 of 4 June 2021, Modules 1 to 3, and you will provide completed Annexes, a list of sub processors, draft instructions and a transfer impact assessment (as required by Clause 14) without undue delay. The UK Addendum to the EU Commission Standard Contractual Clauses also applies in respect of personal data, which originates from the UK.

8. Integration. These Standards apply in addition to, not in lieu of, any other terms and conditions agreed with KLA, except as specifically and expressly agreed in writing with explicit reference to these Standards. For the avoidance of doubt, in the event of conflict with other terms, these Standards shall apply. These Standards shall not create any rights for anyone other than KLA.