Personal Data Privacy

Affected Parties: This policy applies to all employees, officers and directors of KLA Corporation and its subsidiaries worldwide.

Policy Statement: KLA respects privacy rights of individuals and will use, maintain and transfer personal data that we collect in accordance with applicable global data privacy laws and company policies. Employees who have access to personal data of individuals are required to prevent unauthorized use or transfer of this information and access it only as necessary to perform their job responsibilities.

Personal data refers to any information that can be used to identify a particular person such as name, identification number, email address, social security number or government identification number, and many others.

KLA will adhere to the following principles relating to the processing of personal data:

- Lawfulness, fairness and transparency (*using data legally, fairly and openly telling people how their data will be used*)
- Purpose limitation (*only using data for the original purpose it was collected*)
- Data minimization (*collecting and using only what is needed*)
- Accuracy (*aiming to keep data accurate and up to date*)
- Storage limitation (*deleting data that is no longer needed*)
- Integrity (*being true to KLA Values in particularly being Honest, Forthright, Consistent "HFC"*); and
- Confidentiality (*protecting individuals' privacy*)

Administration and Enforcement: The Chief Compliance Officer is responsible for the administration and enforcement of this policy.

Collecting and processing sensitive personal data: Seek prior approval from privacy@kla.com if you intend to collect and process personal data relating to health, race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, genetics or biometrics (such as fingerprints or facial recognition) or criminal allegations, proceedings or convictions. You also need to seek pre-approval if you intend to process personal data using new technology such as to automate decisions about someone where there is no human intervention, e.g., to award benefits or allow access to premises.

Onward Transfers to Agents and Third Parties: Where KLA plans to disclose KLA personal data to a supplier to process it (i.e., a third party to perform one or more functions on KLA's behalf), the

KLA employee responsible for the business relationship shall ensure compliance with the KLA Supplier Onboarding Protocol. The KLA Supplier Onboarding Protocol requires agreement with the supplier on contract terms such as the KLA Data Protection Standards, with the EU Standard Contractual Clauses (SCC) if EU data is shared, as well as required due diligence reviews by KLA's Cybersecurity and Privacy teams, before executing the contract with the supplier.

Breach notifications: Employees must submit an Incident Form (Incident Form - SAP NetWeaver Portal (kla-tencor.com) or report to Ethics Point if they believe an unauthorized disclosure of personal data has occurred. Employees should not attempt to investigate a potential unauthorized disclosure to determine severity but rather, **report it as soon as possible.**

Below are examples of unauthorized disclosures:

- KLA IT systems are hacked or suffer a cyberattack, which potentially comprises the security of personal data
- Personal data is accidentally published or released
- Hard copy files with personal data are inadvertently distributed to unauthorized recipients
- A device (laptop, phone, tablet) or media (thumb drive, portable drive, etc.) containing personal data is lost or stolen
- An insider (employee, contractor, temp, vendor, former employee, etc.), without appropriate authorization, accesses, downloads or views personal data of another

Employees who are responsible for relationships with these suppliers who process personal data on behalf of KLA must also complete an Incident Form or report the matter through EthicsPoint if the third party reports a breach incident in their environment. KLA is responsible for notifying the relevant supervisory authority, as required, even if the breach was not committed by KLA personnel or due to vulnerabilities to our systems.

Requests in relation to personal data: Worldwide regulations vary regarding an individual's rights over their personal data. Any request from external parties to access personal data or exercise rights in relation to it must be directed to privacy@kla.com **within 3 days** of receipt. Do not acknowledge or reply to the request, as there are strict rules in some jurisdictions as to how this must be done.

Additional Information: Employees who have access to personal data are required to complete the Personal Data Privacy WBT available in the KLA Learning Portal.

Additional references:

- KLA Supplier Onboarding Privacy Protocol
- KLA Data Protection Standards
- EU Standard Contractual Clauses

- KLA Supplier Information Security Requirements
- KLA Initial Privacy Assessment (IPA) Request Form

Exceptions: Any exceptions to this Personal Data Privacy Policy must be approved by the Chief Compliance Officer.

Date last updated: 1/25/2022

This document was current as of the date it was printed.
Please verify that no updated version has been posted in the PolicyTech before relying on this document.
The current version is in the KLA PolicyTech
KLA Corporation Confidential