onlineLCA Security - FAQ

Q: Does onlineLCA comply with recognised security standards?

A: At present, onlineLCA does not have formal ISO certification. However, an Information Security Management System (ISMS) is in place and compliance with the requirements of ISO 27001 can be demonstrated.

Q: Where is onlineLCA hosted and where are customer data stored?

A: All data processing and storage take place within the European Union. Hosting servers are located in the EU to ensure compliance with GDPR and to avoid transfers to third countries. onlineLCA can also be self-hosted by the client on request.

Q: What security certifications does the cloud hosting provider have?

A: The hosting provider for onlineLCA has ISO27017/27018, CSA STAR Level 1 and SOC 1, 2, 3 certifications.

Q: How is vulnerability managed? Are regular penetration tests performed on onlineLCA?

A: We carry out periodic penetration and vulnerability tests both during development of software as well as on existing versions of released software.

Q: How are data backed up and protected against loss?

A: Data are backed up daily. Company policy is to retain backups from at least the last 3 days, the last 2 weeks and the last month.

Q: Who owns the data stored in onlineLCA?

A: The client retains ownership of their data stored in onlineLCA.

Q: How is confidentiality of sensitive data managed?

A: NDAs can be put in place to ensure confidentiality of sensitive data. In the case of self-hosting by the client, all data remain entirely under the control of the client and are not shared with us.

Q: Is single sign on (SSO) available?

A: SSO is available on request.

onlineLCA Security - FAQ

Q: How long are data retained by onlineLCA?

A: Current onlineLCA policy is to hold data for 6 months after termination of the service before clearing, unless otherwise specified or requested by the client in advance.

Q: Is two-factor authentication available?

A: Yes.

Q: How secure is user and administrator access to the application?

A: Access to the application is secured with identity and access controls, including two factor authentication (2FA) for administrators and users, role-based access control (RBAC) with least-privilege permissions and secure session handling with token expiration.

Q: Can access be managed within onlineLCA by defined user roles?

A: Yes, administrators can define and assign user roles within onlineLCA to manage access.

Q: Is it ensured that sensitive data can only be viewed and used by authorised persons or systems? If so, how?

A: Sensitive data are protected by the user rights management system in onlineLCA.

Q: Are connections with external systems possible?

A: Yes, onlineLCA can connect with many external systems via an API. Examples include ERP systems, PLM systems and other tools that have an API.

Q: How are sensitive data encrypted within onlineLCA?

A: Yes, administrators can define and assign user roles within onlineLCA to manage access.

Q: Are administrative activities logged?

A: Yes. Administrative actions are logged and monitored to ensure traceability and accountability.