Exasol
The analytics database

Data Security & Privacy Report 2021

Exasol's vision is to be the database company trusted by the world's most ambitious organizations. In order to live up to this trust, Exasol has made huge efforts in the first half of 2021 to further expand its internal organization and associated processes with respect to information and data security as well as data privacy. The company also created the necessary structural and organizational conditions to have these areas certified and audited.

Information Security Management System (ISMS) and Quality Management System (QMS) combined in the Integrated Management System (IMS)

Exasol has decided to address information security and quality management together by implementing an Integrated Management System to ensure that all internal processes are coordinated and all synergies can be exploited. To identify, analyze, assess and mitigate business risks which are impacted by security and quality in an appropriate and standardized manner, both the Information Security Management System (ISMS) and the Quality Management System (QMS) have been and are being defined, implemented, monitored and reviewed with a view to continuous improvement. An internal Integrated Management System organization has been established, which includes a Board-level committee, an Information Security Officer and a Quality Manager. This organization is accompanied by a defined framework of policies, guidelines, processes and the like (e.g. access control policy, physical security policy, encryption policy and incident response plan). The above framework defines reciprocal reporting obligations so that it is organizationally ensured that all relevant stakeholders are informed in a timely and comprehensive manner and are able to act in accordance with the specified processes.

Security Incident Response Team

Any security incidents are addressed by the Security Incident Response Team in a focused and effective manner in accordance with the specified processes. In addition, Exasol's systems are subject to regular safety checks. Software development is based on a secure software development lifecycle.

ISO/IEC 27001 and ISO 9001 certification

Both ISO/IEC 27001 certification and ISO 9001 certification were successfully completed in the first half of 2021.

In addition, regular internal and external audits are carried out as part of the Group-wide audit program. The external monitoring audits (ISO 27001 and 9001) for the financial year 2022 have already been scheduled. ISO/IEC 27001 stipulates regular – at least annual – external audits.

All employees are regularly trained in IT security in line with their respective position in the company. Awareness of IT security is raised through regular measures.
By achieving ISO/IEC 27001 certification, Exasol, as a software company, can in particular demonstrate that it meets high best practice requirements in the area of data and information security that have been established by an internationally recognized and independent organization.

Third party risk assessments

Exasol engages third parties in both the delivery of our services (e.g. ExaCloud) and in the day to day operational running of our organization. Any supplier that we deem to be critical to our business are subject to a due diligence review by our security team. This includes but is not limited to the check of Information Security requirements like ISO 27001 certifications, checks on their organization structure and management of Information Security, review of specific security controls relevant to the services we render. We additionally review these suppliers at least once a year as part of our pre-defined monitoring procedures, or when the services the supplier delivers changes (e.g. at contract renewal).

We require our suppliers to implement security controls depending on the level of service they are providing us, and the risk they represent to us as an organization. These requirements vary from Single Sign On, to encryption of data, to Secure coding practices.

Data privacy – policy

As an analytics database provider, data privacy is one of Exasol's top priorities. The company therefore attaches great importance to an appropriate data protection organization and an effective data protection management system to ensure that data privacy requirements are taken into account in all business processes.
The high data privacy standards of the GDPR are the benchmark for the implementation of data privacy, although stricter national regulations are also taken into account.
Data privacy is taken very seriously as a top priority at Exasol (top-down issue): there is a comprehensive set of rules on data privacy which has been defined by the highest management level. In addition, the data protection team regularly discusses data privacy issues with the top management. The company's management of course also attaches great importance to providing all the necessary human and financial resources to implement the data privacy requirements.

Data protection organization – auditing

In a data protection audit conducted in the first half of 2021, Projekt 29 GmbH und Co. KG (which also provides the external Data Protection Officer for the German Exasol companies) certified Exasol’s data protection organization as having a very high level of maturity. Data protection audits will be carried out annually in the future. The audit confirmed that awareness and knowledge of data privacy requirements are very well developed throughout the company. The controller’s obligation to demonstrate compliance stipulated in Articles 5 and 24 GDPR was used as the basis for the audit of the data protection organization.

The organization is based on a uniform, Group-wide set of rules, defined processes, regulations, policies and procedures, which together form the Data Protection Management System (DPMS).

As an internationally operating company, Exasol attaches great importance to the uniform application of the high data privacy standards set by the GDPR.

The most important element of the DPMS is the Data Protection Manual, which is communicated to all employees. It serves as the basis for handling data privacy-related issues at Exasol (e.g. directory of processing activities, review of order processing contracts, international data transfers and technical and organizational measures).

Minimal processing of data, dealing with service providers

Exasol has ensured that the processing of customer data complies with the applicable data privacy requirements at all times. Its business model does not include any sale of data. The rights of the persons affected in the context of data processing are taken into account comprehensively and there are elaborate processes for complying with any reporting obligations. No personal data or real data are, of course, used under any circumstances during product development; test data and customer data are strictly separated at all times. Service providers who process personal data are checked for data privacy compliance. They are only commissioned if the legally required contractual agreements have been concluded (especially data processing agreements) and Exasol is convinced that the respective service provider meets Exasol’s high data privacy standards. As part of these agreements, we also commit our service providers to extend the requirements to their own service providers.

Training, Data Protection Coordinators

All employees are responsible for compliance with data protection regulations. Data privacy is therefore a mandatory component of the compliance training concept, both for employees and freelancers. Data privacy training is also part of the onboarding process: Access to personal data or the corresponding systems will only be granted after participation in the data privacy training. The Data Protection Manual and all further information are available to all employees in the company’s internal network. In addition to the external Data Protection Officer, there are highly experienced internal Data Protection Coordinators who represent important interfaces between the company and the Data Protection Officer. Besides the relevant expertise, the coordinators have the necessary contacts to the various departments and a comprehensive overview of the relevant processes and workflows.