ACCOUNTOR PORTAL SECURITY AND DATA STATEMENT

As a professional service provider, we take responsibility for complying with applicable laws as well as the authorities' decisions. We are also committed to following the best industry practices in our processing operations. We handle all personal data responsibly and confidentially. This is essential to fulfill our mission, which is to be the leading partner for companies of all sizes and to enhance employee experience. We have a strong and strict stance on security. Accountor is trustworthy, responsible, and ethical towards our clients, partners, employees, directors, and other stakeholders in all our operations.

Governance: Data protection

Accountor has a governance framework to ensure compliance with privacy laws, internal policies, and industry best practices. We have established dedicated privacy roles across our organization. In our governance model, the Risk and Compliance Committee, consisting of selected Leaderment team members, governs and monitors privacy compliance and related risks at the group level with the help of the Data Protection Officer (DPO). The DPO reports to Chief Information Officer (CIO), who is a member of Accountor Leaderment Team.

Each business unit is responsible for the implementation of data protection requirements in their operations. The data protection managers provide operational privacy support for the units. The data protection managers are part of group privacy team led by the DPO. We have a data protection policy approved by the Risk and Compliance Committee. The policy is a basis of more detailed instructions on specific areas of data protection. Such instructions often include methods for implementation in practice e.g., risk assessment or supplier compliance verification templates and processes.

Governance: Information Security

Accountor has an information security framework that is aligned with industry best practices and applicable laws. Our Information Security policy is approved by the Risk and Compliance Committee and is reviewed yearly. The policy is implemented through more detailed instructions derived therefrom as well as with daily practices. ISO 27001 has been the guiding framework for the policy, instructions, and practices.

Information security is managed by the group Information Security ('InfoSec') Team. The team is led by the Group Information Security Officer ('CISO') who is reporting to the CIO, who in turn reports to Accountor's CEO. Information Security operations includes performing risk assessments and audits, creating work plans to reduce risks, and implementing those work plans. Implementation of security activities are documented and regularly reviewed. Accountor carries out yearly trainings for its employees on information security. The training reflects the policy and instructions to ensure compliance with applicable requirements.

Portal Information Security and Data protection

Accountor's portal has been developed specifically to tend to the needs of the clients of Accountor. Many improvements and new features will be part of the continuous development thereof. The Chief Information Security Officer and the Data Protection Officer are active stakeholders of the Accountor portal. This ensures that the portal is developed and used in full compliance with rules and regulations. Contractors and partners are required to adhere to these high standards as well. The portal is hosted by Accountor's ISO 27001 certified IT-partner. The Information Security department led by the CISO, is performing real-time security monitoring through various tools, including vulnerability scans, a 24/7-operating Security Operations Center (SOC) and regular external IT audits. InfoSec has a far-reaching mandate to act in case of (ad-hoc) risks.

Industry best-practice algorithms are used to protect authentication information and data. The portal is using the 'principle of least privilege' for Identity and Access Management. Access to Accountor employees is granted on a Need to know or Need to Use basis. The same principle and setup is provided to the Client Administrators, who are themselves responsible for granting or revoking access and user rights of their own users. Audit and event logs are collected, stored, protected, and reviewed. Accountor takes and tests backups and has built multiple layers of redundancy into the company's platform.

For further information, please feel free to check the information in the links below or to contact your Accountor Business contact person or team.

https://www.accountor.com/en/global/privacy-statement
https://www.accountor.com/en/global/privacy-compliance
https://www.accountor.com/en/global/contact