Background
SiO's vision is to make a better everyday life for students in Oslo and Akershus. In order for SiO to deliver the best possible service offering for students, we need to collect, store and process personal data about the students. Additionally, some of SiO's services are open to non-students, who are also required to register personal data to receive and use these services. SiO's employees are a third group whose personal data is registered with SiO.

Overall guidelines for how SiO collects, stores, processes and secures personal data is provided in SiO's privacy policy.

POLICY
SiO shall:

- Always act in accordance with laws and regulations. SiO's business must comply with GDPR regulation and Norwegian data privacy legislation.
- Only store and process personal data necessary to deliver quality service offerings, efficient operations and legally compliant management of customer and employee data. The purpose of storing personal data must be documented.
- Establish built-in privacy in all processes and systems. This implies that SiO should be able to handle events / discrepancies in an adequate and lawfully correct manner, and that person's rights in terms of deletion, access, change and portability shall be safeguarded. This also includes personal data about SiO's customers and employees registered with SiO's partners and suppliers.
- Have available and clear contact points for registered users who have questions or seek access / change / deletion / disclosure of personal data. This is also applicable for discrepancy notifications.
- Have a data protection officer who is always up to date with laws and regulations, completed required courses and has a direct reporting line for SiO's CEO.
- Have contracts and / or consent statements with terms and conditions where it is clearly stated why and how personal data is recorded and stored, in cases where registry, processing and retention of personal data is not stipulated by law.
- Leverage software solutions that have sufficient security for stored personal data and enable transfer and deletion of data. If current systems do not meet these requirements, SiO shall have a timely plan for necessary solution changes, and in the meantime have manual procedures ensuring a person's rights in the best possible way.
- Have access control routines that ensure that only authorized users can access personal data.
- Have clear roles and responsibilities internally within the organization. This is especially true for data controllers, security officers and the data protection officer. Additionally, general leadership responsibilities and buy-in must be clearly stated.
- Have a conscious relationship to the risk of errors and discrepancies. Systematically conduct risk assessments and assessing privacy implications, as well as implement adequate practices for troubleshooting and discrepancy processing.
- Provide necessary training of employees who process personal data.