SOCIAL ACCOUNTABILITY ACCREDITATION SERVICES

SAAS Notification

Issue: 1
Date: November 2, 2018
RE: Social Accountability International: Notification on SA8000 Certification System and GDPR

Purpose

In order to manage the risks involved in the execution of certification and accreditation activities in the SA8000 system, SAI has drafted this memo to convey our current approach to the handling of personal data and expectations for CBs and certified organizations in meeting the requirements and intent of the European Union's General Data Protection Regulation (GDPR), which came into force on 25 May, 2018.

SAI Approach

We have committed to comply with the GDPR principles in the way we handle data which could be deemed as "personal data" under the regulation. We follow the principles with regards to all personal data, including that of non-EU citizens, we collect, control and/or process within the certification and accreditation programs.

We have defined our lawful basis for processing personal data as meeting a legitimate interest. That interest is effectively operating the SA8000 certification and accreditation programs in a manner that meets the requirements of ISO 17011 and ISO 17021 as well as achieving meaningful impacts. The processing of personal data is necessary, at different times, in order to meet this interest. When this occurs in the system, it is conducted in a manner that minimizes any privacy impacts.

Certification Body and Certified Organization Expectations

In order to effectively mitigate privacy risks in the certification and accreditation systems, and to ensure adequate fairness and transparency, SAI expects accredited and applicant certification bodies to take appropriate steps within their internal processes as well as in their auditing practices.

Employee Privacy Notice

CBs with personnel who are citizens of the EU should immediately draft and distribute a Privacy Notice to all individuals whose activities may impact the accredited SA8000 system. This notice should:

a) Clearly define the purpose and lawful grounds for the processing of personal data in SA8000 accredited activities.
b) Provide sufficient detail so that personnel have a clear understanding of the types of data collected, the nature of the processing activities, and their rights under the GDPR.
c) This privacy notice should be written in a way that includes all necessary information while remaining concise.

Certified Organizations

SAI expects that, in dealing with SA8000 certified or applicant organizations where employees are or may be EU citizens, CBs require such organizations to communicate Employee Privacy Notices similar to that outlined above. Such communication should address not only data shared with the CB, but also data that may be shared with SAI as part of its scheme management, oversight and accreditation activities. All new certification agreements with prospective organizations must cover the implementation of employee notices with regards to the expectations outlined above.