



Purpose

This procedure provides a customer-facing summary of how Senso.cloud detects, investigates, contains, records and notifies data incidents and personal data breaches. It is based on the Supplier Security Assessment breach policy content, EULA data breach clause and Australia Addendum.

Stage	Process summary
1. Identify and report	Any discovered or suspected data breach is reported internally to the Data Protection Officer/privacy owner using a breach report process.
2. Initial containment	The DPO/privacy owner determines whether the breach is still occurring and takes immediate steps to minimise effects and stop the breach.
3. Initial assessment	Assess severity, data types involved, categories of data subjects, whether special category/sensitive data is involved, number of affected subjects and likely consequences.
4. Containment and recovery	Recover, amend, restrict or revoke access where practicable, including access permission changes or temporary unavailability of affected data.
5. Investigation	Investigate as soon as reasonably possible and, according to the source breach policy, within 24 hours of discovery/reporting where applicable.
6. Notification decision	Determine whether to notify affected data subjects, the ICO, police, insurers, affected commercial partners and/or customer organisations.
7. Customer notification	Where Renato/Senso becomes aware of a personal data breach affecting Customer Data, it notifies the Customer without undue delay in accordance with the EULA.
8. Regulator notification	Where ICO notification is required, the source breach policy states this must be done within 72 hours of becoming aware of the breach where feasible. For Australian schools, the Australia Addendum references the Notifiable Data Breaches scheme and OAIC notification where required.
9. Breach register	All data breaches are recorded regardless of whether notification is required, with notification decisions documented.
10. Post-incident review	Review root cause, effectiveness of response and whether systems, policies, procedures, training or DPIAs need to change.

Information provided to customers

- A description of the incident and how/when it was identified, where known.
- Categories and approximate number of affected data subjects and records, where known.
- Likely consequences and risk assessment, where known.
- Measures taken or proposed to contain, investigate, remediate and mitigate adverse effects.
- Recommended customer actions, where relevant.
- Relevant contact point for further information.

Source basis

- Senso Terms of Service and End User Licence Agreement, Revised Oct 2023 V7, <https://senso.cloud/eula/>
- Senso.cloud Privacy Notice Australia Addendum for Schools, effective 1 October 2025
- Supplier Data Security Assessment Questionnaire, completed 10 May 2023