

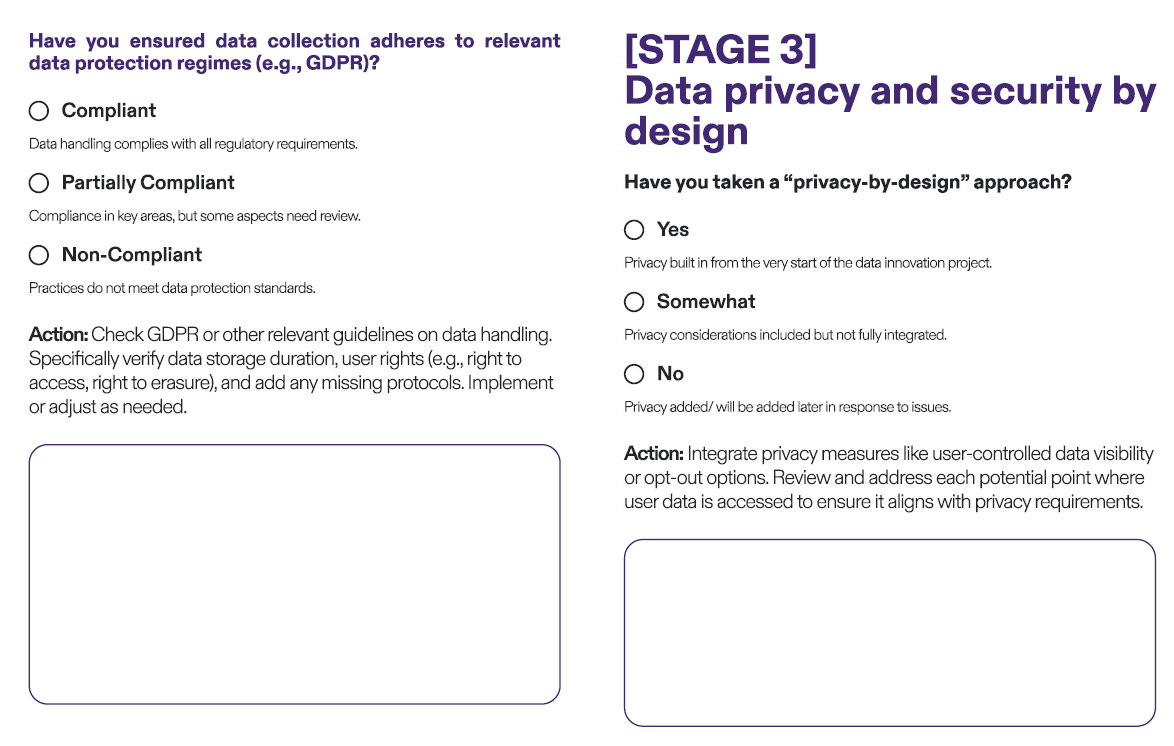
Example

Partially

Consent forms lacked specifics on third-party data sharing, so reconsent

may be necessary to cover this issue.

xxxxxxx



Example

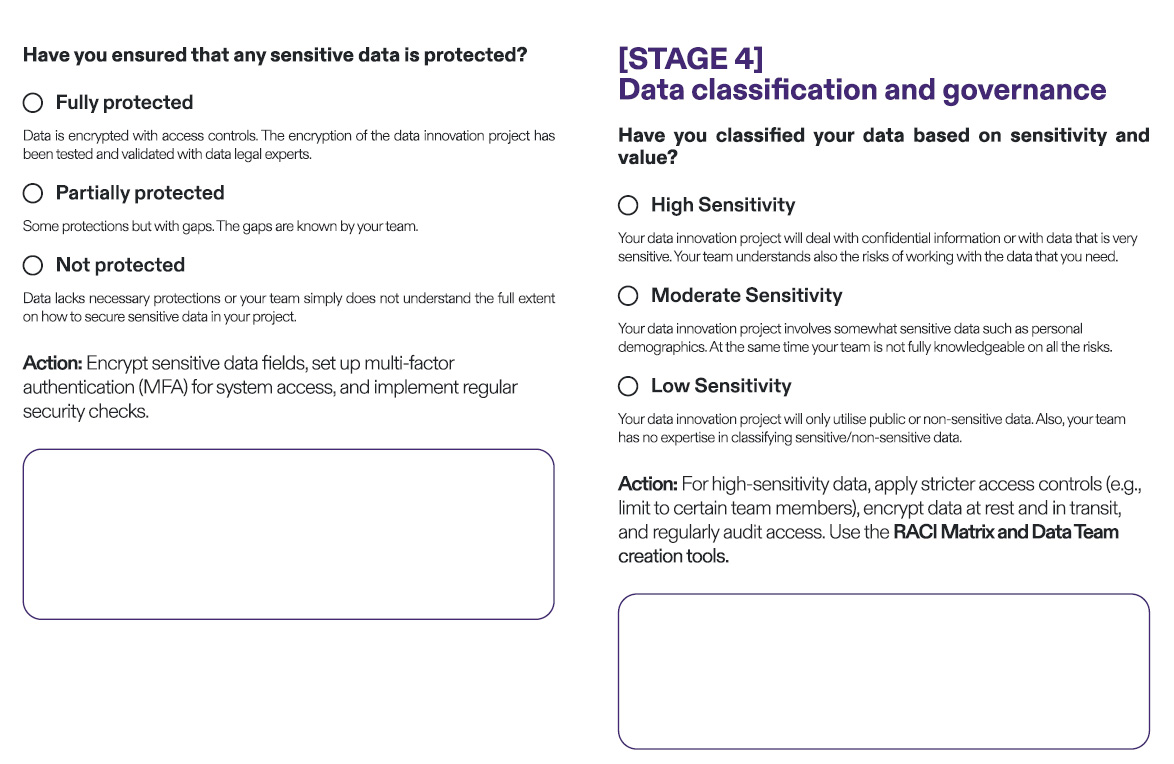
Partially Compliant

Data storage periods exceed GDPR limits. Action: Adjust data retention policy to comply with GDPR, ensuring data is deleted after the legally specified timeframe.

Example

Somewhat

Users can't currently request data deletion. So a possible action is to develop an easy-to-use “Delete My Data” option in your upcoming solution and integrate it into user settings, so users can directly request data removal - also state that during data collection procedure



Example

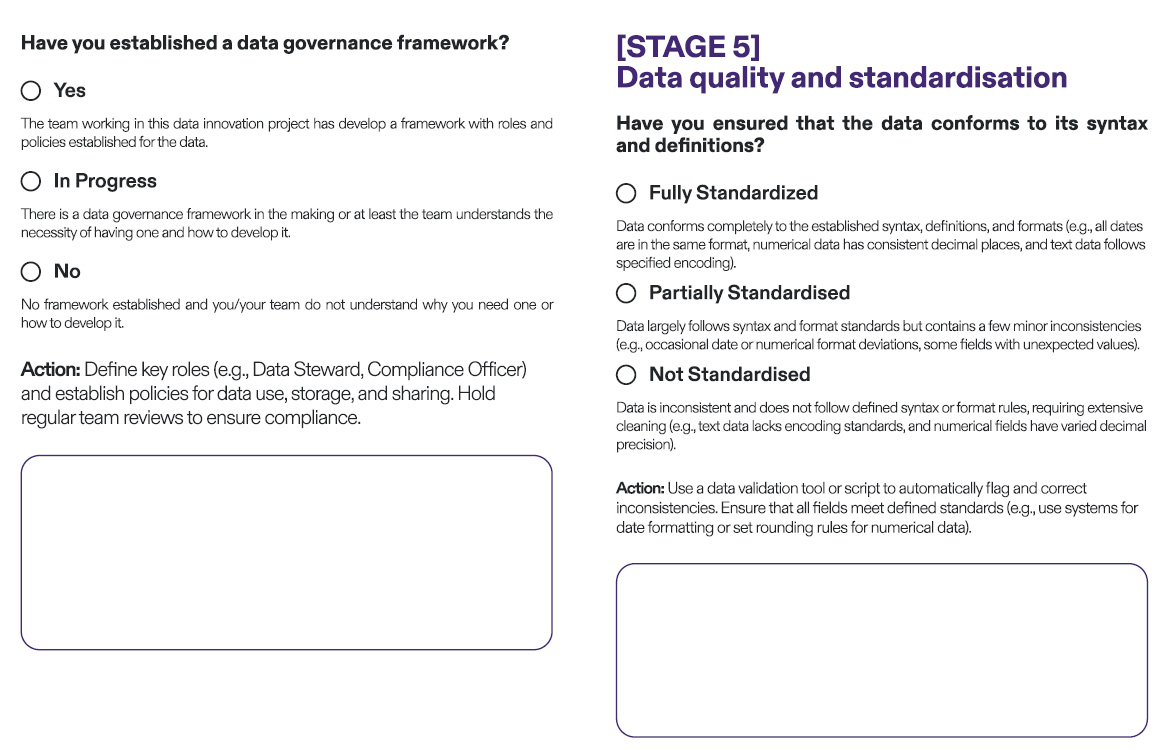
High Sensitivity

Health data classified as high sensitivity. Your team will need to store data in a secure server with encryption and restrict access to specific authorised personnel.

Example

Partially Protected

Sensitive data is stored securely, but access lacks MFA. An action could be to enable MFA on all systems handling this data and schedule quarterly security audits.



Example

Partially Standardised

Dates are mostly in “YYYY-MM-DD” format, but a few entries use “MM/ DD/YYYY.” Action: Run a data cleaning script to convert all dates to

Example

No

Roles are unclear and the team is also not fully aware of your data policies. In this case, it may be necessary to assign data stewardship roles to team members, document responsibilities, and set monthly meetings to ensure data policies are followed.