Handling SP's non-compliance

Assumptions

This Data protection Code of Conduct relies on the following principles

- The Service Provider has an Entity Category element in its SAML 2.0 metadata that indicates it has committed to and believes that its Service is being operated in a manner consistent with the Code of Conduct.
- The Service Provider informs the Home federation operator (Registrar) about any material changes that may influence their ability to commit to the Code of Conduct for Service Providers.
- Reminding the Service Provider of a potential non-compliance issue is not expected to make the reminding party a joint data controller which shares legal responsibility with the Service Provider.
- The federation(s) provides a trusted SAML 2.0 metadata exchange service to the Identity and Service Providers.

Examples of SP non-compliance

There are various ways a Service Provider can violate the Code of Conduct for Service Providers. For instance,

- request attributes which are not relevant for the service.
- omit publishing a privacy notice or publish an insufficient privacy notice.
- omit installing security patches.
- etc.

Possible actions in case of doubts of SP compliance

If anyone (such as an end user, Home Organisation or a Federation Operator) has doubts that a Service Provider is not complying with the Code of Conduct to which it has committed, the following alternative, mutually non-exclusive actions are suggested:

- Contact the Service Provider directly (with a cc to the Service Provider's Home Federation), describe the suspected problem, and ask the SP to check if it has a compliance problem.
- Contact the Service Provider's Home Federation, and ask it to contact the Service Provider and ask the Service Provider to check if it has a compliance problem.
    - The Home federation operator (Registrar) has the right to remove the Code of Conduct Entity Category element if the Service Provider can no longer demonstrate commitment to the Code of Conduct.
    - Depending on the Home Federation's policy, there may be also additional measures available for the the Home Federation for handling non-compliance.
- Lodge a complaint with the competent Data Protection Authority, as defined in the SP's Privacy Notice and Articles 55 and 56 of the GDPR.