Good practice for Home organisations

Home Organisations managing Identity Provider servers do not commit to the Code of Conduct for Service Providers. However, Home Organisations as data controllers of their End users may consider taking the following steps to manage the attribute release to the Service Providers and reduce their risks

- Study Code of Conduct for Service Providers and, based on the Home Organisation's local risk management procedures, decide if a Service Provider's unilateral commitment to the Code of Conduct provides the Home Organisation with sufficient guarantees for an Attribute release
    - For instance, a Home Organisation may reduce its risks by releasing only non-sensitive attributes.

- Ensure that the Service Provider has **committed to the Data Protection Code of Conduct for Service Providers**
    - see Code of Conduct for Service Providers for details on the Code of Conduct
    - see Code of Conduct 2.0 Entity Category for details on SAML metadata indicating SP's commitment
    - Tools may be available to scan the Federation metadata and identify the Service Providers which have committed to the Code of Conduct.

- Ensure that the Service Provider's Purpose of Processing is consistent with the Home Organisation's Purpose of Processing (typically, "support Research and Instruction").
    - the Code of Conduct does not provide support to this directly
    - the Entity Category SAML Entity Metadata Attribute work may assist a Home Organisation with filtering out Service Providers with a conflicting purpose of processing

- Release only Attributes that are **adequate, relevant and not excessive** for the Service Provider
    - flagged as required in SAML metadata (see Code of Conduct 2.0 Entity Category for details on how this is done)

- **Inform the end user** on the Attribute release
    - by providing the following information to the user when s/he is accessing a new Service Provider for the first time
        - the identity of the Service Provider Organisation (mdui:DisplayName and mdui:Logo, if available, for better usability and look-and-feel)
        - the purpose of the service (mdui:Description)
        - a clickable link to the Service Provider's Privacy Notice document (mdui:PrivacyStatementURL)
        - for each Attribute, the Attribute name, description and value
        - an easily understood label can be displayed instead of displaying several closely related Attributes (eg the various name Attributes)
    - user can be provided a checkbox "don't show this information again". If they check it, the information above is not provided next time they log in to this Service Provider.
    - see How the Home organisation should inform the End user for details and GUI recommendations on how to inform the end user

- use the **data controller's legitimate interests** as the legal grounds for attribute release
    - release only attributes that are flagged as NECESSARY (see Code of Conduct 2.0 Entity Category for details on how this is done)
    - however, in certain jurisdiction (e.g. Switzerland) user consent may be needed for attribute release