

# Data protection good practice for Home Organisations



These are commonly approved good practices for Home Organisations based on the data protection directive.

A proper attribute release module installed to the Identity Provider server may help a Home Organisation to implement this good practice. See [Notes on Implementation of INFORM/CONSENT GUI Interfaces](#) for details.

## Contents

- [Home Organisations may consider taking the following steps to reduce their risks](#)
- [Deferred until Phase 2 of the Code of Conduct](#)

## Home Organisations may consider taking the following steps to 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. See [Introduction to Data protection directive](#) for details on sensitive personal data.
- 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 [SAML 2 Profile for the Code of Conduct](#) 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 requested in SAML metadata (see [SAML 2 Profile for the Code of Conduct](#) for details on how this is done)
  - see [What attributes are relevant for a Service Provider](#) for information and suggestions on Attribute use
- If the Service Provider requests only **a particular Attribute value**, release only that value and no other values
  - for instance, if the Service Provider requests only eduPersonAffiliation="member", do not release eduPersonAffiliation="faculty"
  - for instance, if the Service Provider requests only eduPersonEntitlement="http://xstor.com/contracts/HEd123", do not release eduPersonEntitlement="urn:mace: washington.edu:confocalMicroscope"
  - see [SAML 2 Profile for the Code of Conduct](#) for details on SAML metadata for requesting only particular values
- **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 (mdui:DisplayName and mdui:Logo, if available, for better usability and look-and-feel)
    - the purpose of processing (mdui:Description)
    - a clickable link to the Service Provider's Privacy Policy 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 s/he checks it, the information above is not provided next time s/he logs in to this Service Provider.
  - see [Notes on Implementation of INFORM/CONSENT GUI Interfaces](#) 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 [SAML 2 Profile for the Code of Conduct](#) for details on how this is done)
  - see [Introduction to Data protection directive](#) for reasoning
  - however, in certain jurisdiction (e.g. Switzerland) user consent may be needed for attribute release

## Deferred until Phase 2 of the Code of Conduct

**Note:** [Introduction to Code of Conduct](#) proposes to defer support to optional extra Attributes to Phase 2.

- If the user consents to, **release extra Attributes that are purely optional** but provide a higher service level to the user
  - flagged as REQUIRING CONSENT
  - If several Attributes are released based on consent, the user **MUST** be able to give his/her consent individually to each Attribute or each group of similar Attributes (for instance, a user could be asked to consent to release "name", and this single consent would allow the release of cn, sn, givenName and displayName).
  - user can be provided a checkbox "remember my consent". If s/he checks it, consent is not asked next time
  - if Attribute release is based on consent, the user must be able to view and withdraw his/her previously given consents any time

- see [What attributes are relevant for a Service Provider](#) for details on the Attributes
- see [SAML 2 Profile for the Code of Conduct](#) for details on SAML metadata for flagging Attributes as necessary
- see [Notes on Implementation of INFORM/CONSENT GUI Interfaces](#) for details and GUI recommendations on how to ask user consent