eduGAIN Service Provider Code of Practice draft v0.03

In order to provide Identity Providers with confidence that attributes they release will be processed in accordance with European data protection law (in particular Directive 95/46/EC), Service Providers are invited to follow this Code of Practice. Those who commit to doing so may indicate this fact on their websites[1] and in the signed metadata they provide to their own federations and to eduGAIN.[2]

1. Data Minimisation
    a. The Service Provider will only request those attributes that are *strictly necessary for the specific service explicitly requested by the user*.[3,4]
    b. Where a number of different attributes could be used to deliver the service, the Service Provider will use the least intrusive attributes possible (e.g. pseudonymous identifiers rather than names/e-mail/etc; type of user rather than identifiers)
2. Grounds for Processing
    a. The Service Provider will only request and process attributes as is *necessary in the legitimate interests* of providing the service;[5]
    b. The Service Provider will not perform additional requests or processing on the grounds of the user's *consent*.[6]
3. Privacy Statement
    a. The Service Provider will publish a Privacy Statement,[7] containing at least
        i. *The (legal) identity of the Service Provider*;
        ii. *The purposes of processing* the requested attributes;
        iii. *The categories of attributes concerned*;
        iv. *The recipients or categories of recipients* (if attributes are transferred to others);
        v. *The existence of the rights to access and rectify the attributes held about them.*[8]
    b. The Service Provider will provide the Privacy Statement[9] to the user no later than the user's first use of the service;

[1] #How? E.g. pdf of ink-signed declaration

[2] #How? What's the flag?

[3] Directive 2009/136/EC, Recital 66

[4] #Could provide a link to the REFEDs paper on what necessary means

[5] Directive 95/46/EC, Article 7f

[6] Directive 95/46/EC, Article 7a

[7] Guidance on Privacy Statements is available from the UK Information Commissioner: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_notices_cop_final.pdf

[8] Directive 95/46/EC Article 11

    c. The Service provider will provide each Identity Provider with a machine-readable link to the Privacy Policy.[10]
4. Purpose of Processing
    a. The Service Provider will only use or disclose attributes for controlling access to, or personalisation of, the service requested by the user, and not for any secondary purposes;
5. Information Security
    a. *The Service Provider will take appropriate organisational and technical measures to protect information against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access*.[11]

[9] For example by statement on, or obvious hyperlink from, the service landing page

[10] #Ref to MDUI SAML standard on how to do that

[11] Directive 95/46/EC, Article 17