Data processor contract

Affiliation of <institution> to the WAYF service

Institution's logo

Certified translation

Signatories:

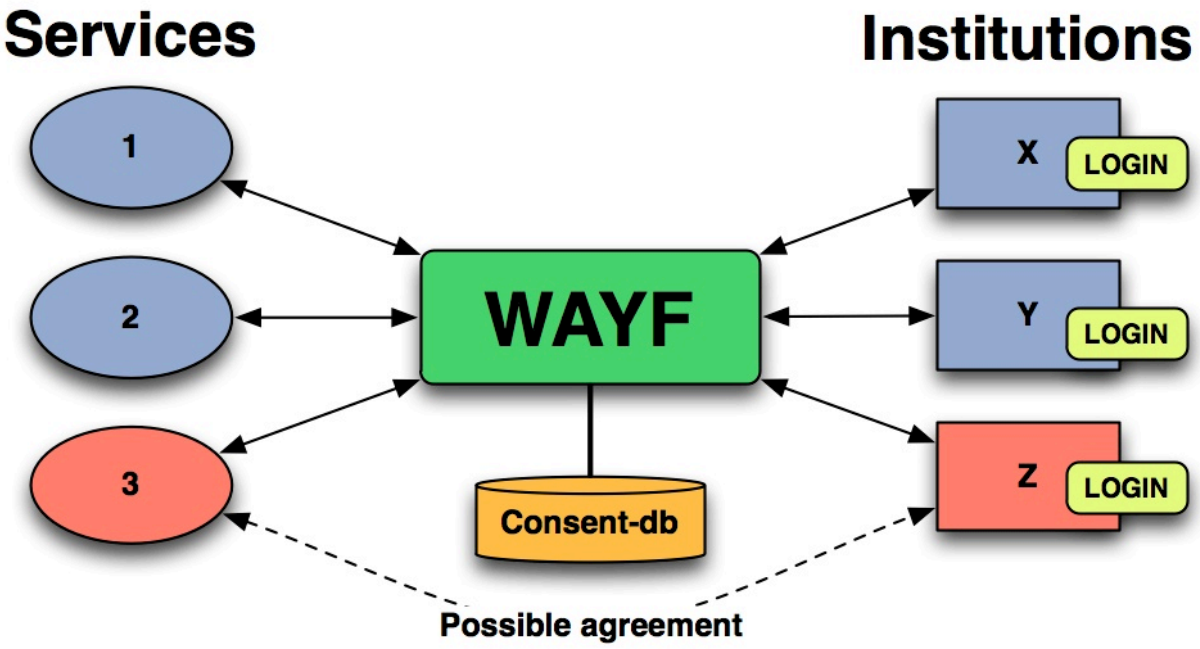
1 – **D**anish **e**-**I**nfrastructure **C**ooperation (legal base of the WAYF Secretariat)

2 – <institution>

<date>

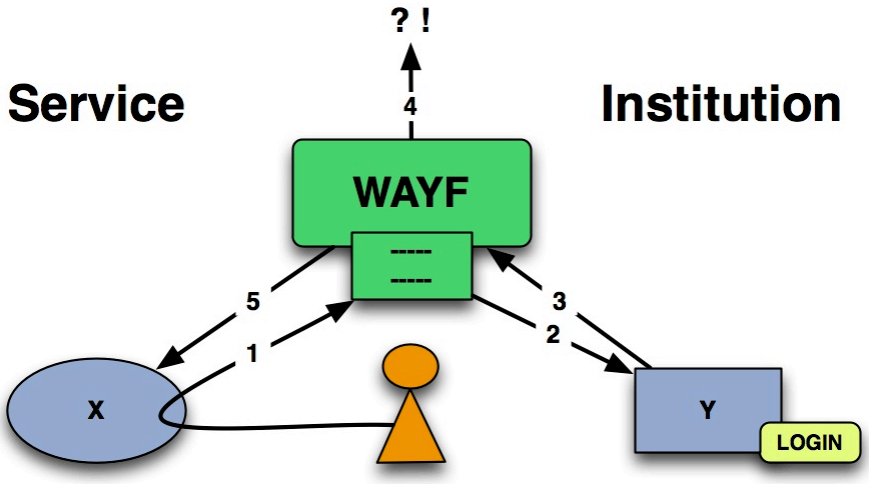
1 Background

The purpose of the “Where Are You From service” (hereinafter the “WAYF service”) is enable roll-based access management and reuse of login-systems.



2 Description of WAYF

The WAYF service is a technical connecting link between institutions and services. In future the WAYF service will also be a connecting link to other WAYF-style services both in Denmark and abroad. In technical terms, the WAYF service is located between institutions and services.



1. The user accesses a web based service that requires a login. The service's login function sends the user to the WAYF website, where the user selects his/her institution.

2. If the user is not already logged in, the user is transferred to the institution's login page.

3. After the user has logged into the institution, data about the user is sent to WAYF.

4. The WAYF website is displayed to the user with the data that will be forwarded to the web based service. The user gives his/her consent by clicking on a button. The user can tick a box to denote that this consent may be remembered for future isits to the same web based service.

5. WAYF sends the data to the web based service. If the web based service can approve the user on the basis of this data, access is granted.

The institution's login system sends information about the user to the WAYF service. This is called the user's "attributes". The WAYF service selects the attributes that the service provider needs (the number of attributes is agreed when the service is affiliated to WAYF) and forwards them to the service provider. The user is asked in advance to provide consent for the data to be sent to the service provider for their use in connection with the web based service.

On the basis of the data about the user, the service provider either grants or refuses access to the service. The service provider itself can thus manage access controls to its service.

This model makes it possible for service providers to provide access to users without knowing their name, civil registration number or other personal data. Service providers can now use role-based access control via WAYF, in which access is provided, for example, if the user is associated with a given institution. It is possible to transfer personal data, but this is only done if it is relevant for the service.

The benefit for users is that they can use one single username and password to gain access to a large number of services, wherever they happen to be.

The benefit for the institution is that it provides users with access to a large number of services beyond the normal institutional domains.

The benefit for service providers is that they gain access to a number of users whose identity and affinity are vouched for by the affiliated institutions.

Both service providers and institutions benefit from the fact that they only need to sign up to the WAYF service to establish technical access to everyone else who is also signed up to the WAYF service. WAYF protects sensitive personal data, and the WAYF service never sees the user's login details (users always log in at the institutions). The WAYF service does not save users' attributes or other sensitive data – they only pass WAYF on the way from institution to service, although please note the comment below.

Every single user can save his/her consents with WAYF. A consent is an authorisation to send data about the user to the service. The consent is saved at WAYF in the form of a digital 'fingerprint' (hash value), which is in practice one-way encryption. This means that the original data cannot be restored in any way by WAYF alone.

One example of such a 'fingerprint' for consent is:
'e2a67df2a8d2c7ea3891ab66f75acf4f8780850d'

This data can only point back to the user if WAYF and the user's institution co-operate on a review of the entire institution's user database, something that would only happen in connection with police cases or other very serious cases of abuse.

The next time the user accesses the same service, WAYF calculates the 'fingerprint' on the basis of the data that are transferred from the institution and checks whether it is already in the database. If this is the case, the user has previously given consent to the data being passed on and does not therefore have to be asked once more. All consents can be withdrawn via the consent administration function, which can be accessed via *www.wayf.dk*.

When a service is affiliated to the WAYF service, its purpose is defined. On the basis of the purpose, the service provider determines in collaboration with the WAYF secretariat what data can be transferred to the service. In accordance with the Danish Personal Data Act, which implements Council Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, service providers may only receive a minimum of personal data with due reference to the purpose of the service.

Data about users are stored at the affiliated institutions. The quality of the data is guaranteed by such means as the institution's compliance with governmental security standard DS-484 or similar and the Danish National Audit Office's control that the requirements of DS-484 or similar have been satisfied.

Agreements on any payment for using the affiliated web-based services are concluded directly between the service provider and the institutions.

As a basic principle all services are available to all affiliated institutions. The institutions have the facility to deselect services individually. At least two weeks before a new service becomes available, the institutions are notified of its purpose, data profile, terms of payment (if relevant), etc.

The WAYF organisation has its legal base with Danish e-Infrastructure Cooperation (DeIC, *www.deic.dk*) and uses the CVR number of the Technical University of Denmark, to which the tasks of DeIC have been assigned. The WAYF organisation is also funded by DeIC.

Further information: *www.wayf.dk*.

3 Definition

A *service provider* is a legal person (company, authority, institution, etc.) that offers one or more services.

An *institution* is a legal person (typically an institution) that creates, maintains and closes down electronic accounts with associated data about its affiliated persons (employees, students, etc.). In certain contexts the synonymous term 'identity provider' is used.

4 Responsibility according to and relationship with the Danish Personal Data Act

The institution is responsible for data in connection with the processing of personal data in accordance with the Danish Personal Data Act. If the institution's base data are formed by aggregating data from third parties, the institution is also responsible for the data.

The WAYF organisation is the data processor on behalf of the affiliated institutions in accordance with section 3 (5) of the Danish Personal Data Act.

The rules in section 41 (3)-(5) of the Danish Personal Data Act also apply to the WAYF organisation, cf. Section 42 (2). The WAYF organisation's processing of data may in general only take place subject to instructions issued by the individual institution, cf. Section 42 (2) of the Danish Personal Data Act.

The WAYF organisation must therefore implement the necessary technical and organisational security measures to prevent data from being accidentally or illegally destroyed, lost or damaged, and also from being made available to unauthorised parties, being abused or otherwise being handled in breach of the Danish Personal Data Act, in accordance with the rules issued under the Danish Personal Data Act. Please refer to the Danish Data Protection Agency's security guidelines no. 37 of 2 April 2001 on measures to protect personal data.

The provisions contained in the Ministry of Justice's Executive Order no. 528 of 15 June 2000 (as amended by Executive Order no. 201 of 22 March 2001 and any amendments that might subsequently be adopted) on security measures to protect personal data that is processed for public administration also apply to the WAYF organisation.

As the party responsible for the data, the institution must comply with the rules on registration in the Danish Personal Data Act. Any application must be made to the Danish Data Protection Agency via the Danish Data Protection Agency's website at *www.datatilsynet.dk*.

The institution and the WAYF organisation must in general comply with the relevant rules governing a party responsible for data and a processor of data under the Danish Personal Data Act as well as rules issued under this act.

5 WAYF's obligations

5.1 Downtime and operational disruption

The WAYF organisation concludes an agreement with one or more operators on the delivery of systems and operations. It is the responsibility of the WAYF organisation to notify the institution without undue delay of any circumstances that might affect the functionality or operation of the WAYF service. Planned downtime, updates, cessation of operation, legal changes or practical changes must also be announced without undue delay.

5.2 Assistance in connection and support
If required, the WAYF organisation advises the institution to guarantee the best possible connection to the WAYF service.

5.3 Emergency preparedness
The WAYF organisation is obliged to maintain a level of emergency preparedness to ensure that any downtime can be minimised by means of defined processes and procedures.

5.4 Connection time
The WAYF organisation strives to connect the institution within 21 working days of receipt of this signed contract. In the event that this deadline cannot be observed, the institution is notified immediately of why the deadline cannot be observed and when connection will take place.

For this deadline to be observed, it is essential that the institution fulfil his obligations (see clause 6).

5.5 Attribute form
The WAYF organisation maintains and develops the WAYF attribute form (see *www.wayf.dk*).

5.6 Changes in policies
Any changes in policies (certificate, logging, etc.) are announced at *www.wayf.dk*.

6 The institution's obligations
6.1 Registration of contact persons
The institution is obliged to designate at least one technical and at least one organisational contact person, and to make sure that the contact details are kept up to date on an ongoing basis by sending the necessary details and any changes to the WAYF organisation.

6.2 Testing
The institution is obliged to test the connected solutions and to conduct and pass all tests specified by the WAYF organisation when connecting to the service (see details at *www.wayf.dk*).

6.3 Resources
The institution undertakes to make all necessary resources available in connection with the testing of its own solutions and services. The institution bears the costs of development, creation, integration, operation, etc. of its own installations.

6.4 Logging and certification
The institution is obliged to comply with the logging policy and certificate policy in force at any time. The policies may be found on the WAYF organisation's website (see clause 5.6).

6.5 Security
It is the responsibility of the institution to ensure that (IT) security in its own organisation complies with the prevailing rules and good IT practice. If the WAYF organisation believes that a solution (IT system with direct or indirect connection to the WAYF service) may significantly compromise security, this is considered to constitute a breach of the terms of affiliation (see clause 9).

6.6 The institution's supplier
If the institution receives systems or other items that are used to connect to the WAYF service from a supplier, it is the institution's responsibility to ensure that the supplier complies with and assumes responsibility for all of the clauses in this contract.

6.7 Change of WAYF service supplier
Any changes in the setup of the WAYF service as a consequence of a new supplier, etc. must be announced at least 90 days before any changes are made, so that the institution is able to organise resources to implement any changes that may be necessary. The institution is obliged to bear any costs in connection with changes and modifications to its own system in connection with a change of supplier.

6.8 Information page about WAYF
The institution must produce a page on its local website to explain to users how the WAYF service interacts with the local login service. The page must also explain to users the rationale behind the partnership with WAYF and remain available as an element of the general support material aimed at end users.

7 Attributes and user administration
7.1 Attributes
All WAYF attributes labelled 'MUST' are mandatory for delivery to the WAYF service in connection with an approved user login (see list of WAYF attributes at *www.wayf.dk*). Attributes labelled 'MAY' can be delivered to the WAYF service, but are not required. MAY information can be delivered to WAYF if the institution wants its users, either now or in the future, to be able to access services where there attributes are required in order to gain access. The institution is obliged to inform the WAYF organisation of which attributes (in addition to the MUST attributes) are delivered to the WAYF service.

The WAYF organisation maintains and develops the WAYF attribute form (see clause 5.5) and the institution is obliged to comply with the requirements of the form.

Attributes can be organised as preferred locally at the institution; it must, however, be borne in mind that certain connection types may place demands on the local data structures.

When the WAYF organisation introduces new attributes, the definition of the attribute is valid from the time when it is announced. When introducing MUST attributes (mandatory WAYF attributes), the institution is obliged to comply with the new requirements as quickly as possible, and within 12 months of the announcement date. If this deadline is not observed, it is considered to constitute breach of contract (see clause 9).

7.2 Data quality
The quality of user data in the administrative systems at the institution must always comply with prevailing legislation, audit requirements and other relevant rules.

The WAYF organisation can at any time request a description of routines and procedures for user administration applied by the institution.

Changes in the data that the WAYF service receives (e.g. student -> alumnus) must be reflected in the data delivered to WAYF within a maximum of 24 hours of the formal change having come into force.

7.3 Procedures and routines for user administration

Below is a list of the roles that can be used from the institution's identity management system.

1 - student
2 - faculty
3 - staff
4 - affiliate
5 - alum
6 - library-walk-in
7 - employee
8 - member

The following four questions are answered for each role.

a – Was the role delivered from another system? If so, which one?
b – How and when is the role enabled?
c – How and when is a decision made to disable the role?
d – Do procedures exist for a periodical review of the user role?
If so, which?

When and if procedures, etc. are changed, notification of this must be forwarded to WAYF.

7.4 Authentication strength

Please answer the following questions:

1 – How is the identity of people allocated user accounts verified?

2 – Are there routines for cancelling or reassessing users?
If so, what are they?

3 – Which login methods are used?
(Username/password, digital signature, etc.?)

4 – Are there any rules for the allocation of usernames?
(E.g.: no repeat use within X years?)

8 Payment

The WAYF organisation bears the costs of development, operation and administration of the WAYF service's systems at least until the end of 2012.

The institution itself bears the costs of affiliation to the WAYF service as regards the development, creation, integration, testing, operation, etc. of its own solution.

There shall be no payment between the parties. The WAYF service is thus made available free of charge.

9 Breach of contract and liability

The general rules of Danish law on breach of contract and breach remedies are applied, with the additions specified below.

9.1 Notification and termination in connection with breach of contract
If a party is in significant breach of its obligations and does not cease to be so within ten days of having received written notification of this, the other party may terminate the contract in writing with immediate effect.

10 Exclusion of liability

The WAYF organisation accepts no liability for losses (including direct and indirect consequential damage such as operating losses, loss of profits, loss of interest and loss of savings) that the institution might incur as a consequence of delays, faults or deficiencies in the WAYF service.

11 Jurisdiction

This contract is concluded and is at all times subject to prevailing Danish law.

12 Resolution of disputes

An attempt should be made to resolve any dispute through negotiation. If no solution has been reached within four weeks of the first written notification, and the institution is not a part of the Danish state, either party may bring the case before a court of law, although in such a way that Copenhagen is the venue for a possible court case.

13 Commencement

This contract comes into force once it has been signed by both parties.

14 Notice and termination

Either party may terminate the contract by serving one month's written notice of the end of a month. This deadline does not apply in the event of breach of contract, cf. clause 9.

15 Signatures

The undersigned confirm with their signatures that they accept the terms of this contract. The contract is issued in two copies, each party retaining one.

Name of institution: <institution>
CVR no.: <CVR no. or other applicable legal identifier>
Name of signatory:

Place and date:
Signature:

On behalf of the WAYF organisation

CVR no.: 30060946 (Technical University of Denmark)
Name of signatory: **David Simonsen**

Place and date:
Signature: