Contract on the affiliation of <service> to WAYF

Service provider logo

Certified translation

Signatories:

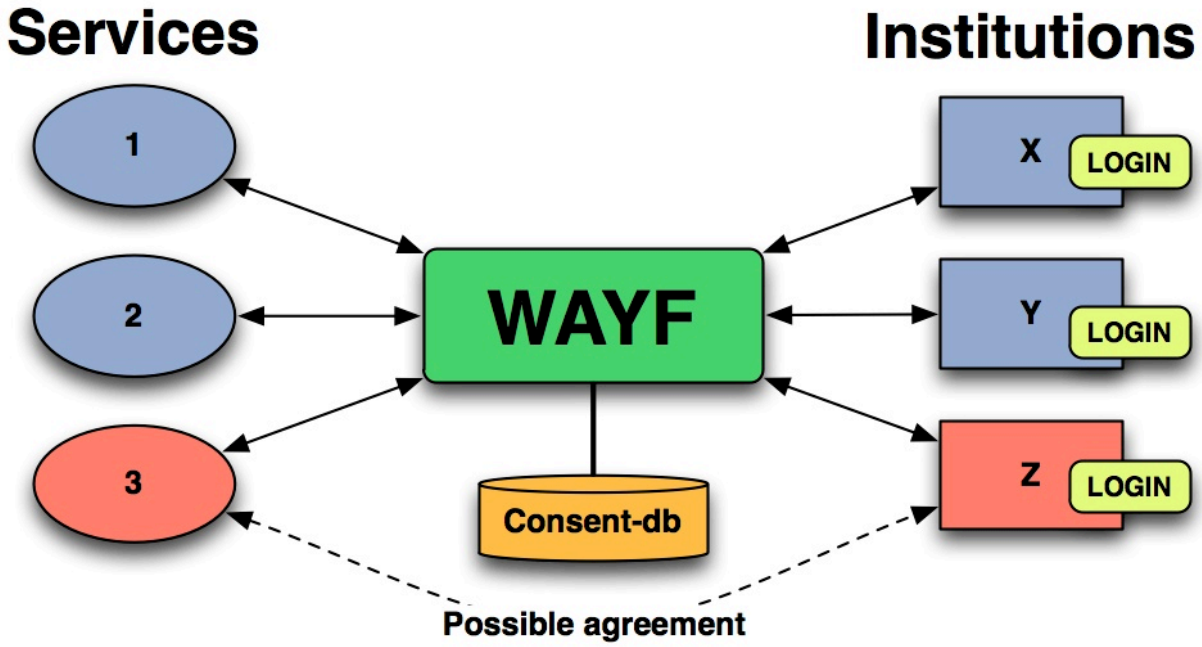
1 – **D**anish **e**-**I**nfrastructure **C**ooperation (legal base of the WAYF Secretariat)

2 – <service provider>

<date>

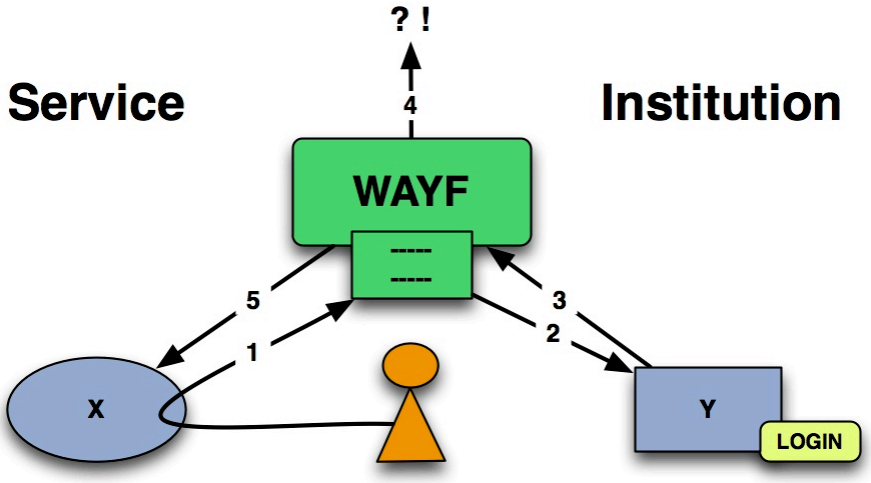
1 Background

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 visits 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 no. 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 service provider is responsible for data in respect of the data about users that are received via the WAYF service. The WAYF organisation is the data processor in accordance with the Danish Personal Data Act on behalf of both the affiliated institutions and the service provider.

This provision is only relevant for the service provider if the service provider receives personal data via the WAYF service as defined in the Danish Personal Data Act. If the service provider does not receive personal data via the WAYF service, the service provider can ignore this provision.

The rules in section 41 (3)-(5) of the Danish Personal Data Act also apply to the WAYF organisation. The WAYF organisation's processing of data must in general take place solely in response to an instruction from an individual institution or individual service provider, 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 service provider 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*.

Please note that service providers are subject to the Danish Personal Data Act, which includes the following:

1 – The service provider must, if requested to do so by a given user, delete all personal data relating to the user, if this is a requirement under legislation, including the Danish Personal Data Act.

2 – Personal data that have been obtained for the purpose of providing the user with access to the above service and/or for the service's own purpose must not be passed on in any way or in any form to a third party.

The service provider 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. If the service provider is established in another EU member state, the provisions on security measures as set out in legislation in the member state where the service provider is established shall apply to the service provider.

5 The WAYF organisation'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 service provider 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

The WAYF organisation is obliged to make documentation available to the service provider 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 service provider within 21 working days of receipt of this signed contract. In the event that this deadline cannot be observed, the service provider 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 service provider fulfil his obligations (see clause 6).

5.5 Changes in policies

Any changes in policies (e.g. logging policy, certification policy, etc.) are announced at *www.wayf.dk*.

6 The service provider's obligations

6.1 Registration of contact persons

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

6.4 Logging and certificate policy
The service provider is obliged to comply with the logging policy, certificate policy etc. in force at any time. The policies are available at *www.wayf.dk* (see clause 5.5).

6.5 Security
It is the responsibility of the service provider to ensure that there is sufficient (IT) security within its own organisation. If the WAYF organisation believes that a solution may significantly compromise security, this is considered to constitute a breach of the terms of affiliation (see clause 8).

6.6 The service provider's supplier
If the service provider uses a third party in connection with its affiliation with the WAYF service, it is the service provider'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 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 service provider is able to organise resources to implement any changes that may be necessary. The service provider is obliged to bear any costs in connection with changes and modifications to its own system in connection with a change of supplier.

7 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 service provider 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.

8 Breach of contract and liability
The general rules of Danish law on breach of contract and breach remedies are applied, with the additions specified in clause 8.1.

8.1 Notification 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.

9 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 service provider might incur as a consequence of delays, faults or deficiencies in the WAYF service.

10 Jurisdiction

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

11 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 service provider 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.

12 Service-specific data

12.1 The purpose of the service

The purpose of <service> is <purpose, typically as an infinitive or a gerund>.

12.2 Agreed volume of personal data supplied to <service> from the WAYF service

The WAYF service always delivers the following data about each individual user who tries to access <service>:

- *eduPersonPrincipalName (User ID at the home organisation)*
- *schacHomeOrganization (the home organisation's unique ID)*

…

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 8.

15 Contact information, WAYF organisation

WAYF-sekretariatet
Rued Langgaards Vej 7, 5.
DK-2300 København S
FAO: David Simonsen

E-mail: sekretariat@wayf.dk
Telephone: +45 3373 3358

16 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 service provider:	<service provider>
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: