DANISH AGENCY FOR DIGITAL GOVERNMENT

NemLog-in

Annex 2 Service Provider terms and conditions for using NemLog-in Services

Version 1.1

Contents

1 Introduction

This Annex, together with the Terms and Conditions, cf. clause 7.2 of the Terms and Conditions, contains the terms (Service Provider Terms and Conditions) that Service Providers must comply with to use the NemLog-in Services. The Supplier must incorporate the provisions of the Annex into its agreements with Service Providers, so that Service Providers are bound by them.

The Service Provider Terms and Conditions in this Annex may be amended and updated periodically, cf. clause 17 of the Terms and Conditions. Any amendments to the Service Provider Terms and Conditions must be communicated to the Supplier, who will in turn communicate the amendments to the Service Providers as appropriate, and the Supplier will ensure that the amendments are implemented in the agreements with Service Providers.

Public-Sector Service Provider' usage of NemLog-in Services is regulated by the Act on MitID and NemLog-in, inclusive of the decree concerning the provision and use of the MitID solution and NemLog-in. The matters referred to in points 2 to 6 are regulated in the decree and therefore must not to be covered by the Supplier's agreements with Public-Sector Service Provider.

2 Security requirements

The Service Provider must comply with the security requirements specified on the Service Provider Site. Service providers are furthermore not to expose NemLog-in and associated solutions, including the MitID solution, to security risks in terms of authenticity, integrity and confidentiality in any other context.

The Service Provider is obliged to notify End Users and the Supplier of any security breaches related to NemLog-in.

3 Technical requirements

The Service Provider is obliged to comply with the technical requirements set out on the Service Provider Site intended for Service Providers.

4 Use of Assurance Levels

The Service Provider may not use Authentication that is received by the Supplier from NemLog-in for the Service Provider’s Digital Self-Service Solutions, which require a higher Level of Assurance than specified by the authentication response in accordance than what appears from the authentication response from NemLog-in.

5 Use of distinctive features

The visual identity and the design elements made available to the NemLog-in infrastructure may only be used in connection with Authentication via NemLog-in. The Service Provider is not permitted to use them for supporting its own or third-party services.

The Service Provider is required to comply with the applicable terms for using the NemLog-in and MitID Marks (hereinafter referred to as the distinctive features), including names, logos and domain names, as well as other material related to the Partnership and MitID.

Guidelines for UX/UI and communication related to NemLog-in and MitID are provided on the Service Provider Site.

Service Providers have a right to use distinctive features and are required to use such distinctive features in connection with Authentication through the NemLog-in solution and marketing thereof.

The guidelines may be amended and the distinctive features may be altered entirely or partially. The Service Provider is obligated to stay updated to that effect and comply with the guidelines applicable at any time.

On termination of the agreement on the use of Authentication from NemLog-in, the Service Provider is required to remove any reference to distinctive features and stop using them unless another agreement is entered into with a rights holder.

6 Suspension of access to NemLog-in

The Service Provider's access to Authentication and additional services may be suspended or revoked by the Supplier if the Service Provider to a significant extent fails to comply with the Supplier's requirements for the Service Provider, or if the Service Provider's behaviour otherwise represents a security risk, or if the Service Provider engages in behaviour that significantly affects or is likely to negatively affect the End Users' perception of NemLog-in and associated solutions, including the MitID solution.

The Supplier is additionally entitled to continue to suspend or revoke access from the Agency for Digital Government including suspensions justified on significant security grounds.

7 Terms and conditions for the Service Provider’s charging fees

Service Provider is not authorised to charge End Users fees for Authentication or signature using NemLog-in.

8 Processing of personal data

The Service Provider's data processing agreement with the Supplier must stipulate that the Supplier as data processor processes the following information about the End User as part of the receipt of the Authentication response from NemLog-in:

- Name and CPR number (if a CPR number is registered)
- Email address (Business Users)
- Pseudonym (Business Users)
- PID and RID
- CVR number (Business Users)
- Level of Assurance
- NemLog-in identification number of the electronic identity (UUID)

Further details about the relevant data are provided in the latest version of OIOSAML Web SSO Profile.

The Supplier may not process Authentication responses in any way or for any purpose other than set out in the Danish Act on MitID and NemLog-in, unless the Service Provider has independent legal authority to process Authentication responses.

9 Certificates and signature

9.1 Use of NemLog-in Digital Signature

If the Service Provider reasonably relies on a qualified electronic signature or a qualified electronic seal and related certificate from NemLog-in’s digital signature, the Agency for Digital Government is liable under the general provisions of Danish law.

The Agency for Digital Government is liable for loss in the circumstances set out in requirements 9.6.1-04 of the Certificate Policy unless the Digitisation Board can prove that it did not act intentionally or negligently.

The Agency for Digital Government's total liability is limited to DKK 100,000 for each loss-making event, and is in any event maximised at DKK 100,000 per year. A loss-making event is considered as any matter arising from the same continued or repeated actionable matter.

The above limitation only applies if the breach cannot be attributed to gross negligence or intentional circumstances.

9.2 Service provider's obligation on receiving a certificate

Prior to trusting a certificate from Den Danske Stat Tillidstjenester , the Service Provider as recipient of a signature must ensure the following:

- That the certificate is valid - i.e. not listed on Den Danske Stat Tillidstjenester list of revoked certificates at the time of signature,
- that the purpose for which the certificate is to be used is suitable in respect of any use limitations in the certificate and
- that the use of the certificate is otherwise suitable in terms of the level of security described in the certificate policy for the certificate in question

The Service Provider, as the recipient of a signature, must ensure the following before accepting a time stamp (if a time stamp is included in the signed document):

- that the time-stamp is correctly signed and that the private key used to sign the time-stamp has not been marked as compromised at the time of the verification,
- that use takes place within the framework of any limitations on the use of the time-stamp indicated by the time-stamp policy and
- that other measures specified in agreements or similar are satisfied.

10 Service Provider claims

Any Service Provider claim relating to NemLog-in Services shall be directed to the Supplier. However, claims relating to errors in signatures or seals from NemLog-in Digital Signature, which must be addressed to the Agency for Digital Government, are excluded.

11 Special Conditions for Public-Sector Service Providers

Public-Sector Service Providers' receiving Authentication from NemLog-in via the Supplier is regulated by the Act on MitID and NemLog-in, including the Decree concerning the provision and use of the MitID solution and NemLog-in. The powers held by the Agency for Digital Government under the Decree apply irrespective of whether Authentications are received via the Supplier. The authority and powers may be exercised by the Agency for Digital Government through the Supplier.