DANISH AGENCY FOR DIGITAL GOVERNMENT

NemLog-in

Terms and Conditions for Private Service Providers

Version 1.1

The terms and conditions are written in Danish and English.

The Danish language version of terms and conditions shall be controlling in all respects and shall prevail in case of any inconsistencies with the English version, if any.

Contents

1 Introduction 4
2 Definitions 4
3 Correct organisational classification of Service Provider 7
4 NemLog-in Services 7
4.1 Introduction 7
5 Completion of connection 8
5.1 General conditions 8
5.2 The Service Provider's using a technical collaborative partner 8
6 Use of Authentication in Digital Self-Service Solutions 8
6.1 Login and authentication 8
6.2 Restriction on the use of Authentication from NemLog-in 9
6.3 Information in the authentication response 9
6.4 Information from Attribute Service after Authentication of the End User 9
6.5 NemLog-in CPR match service 9
6.6 End User's access rights 10
6.7 Use of Authentication outside the specified time period 10
6.8 Risk data in the use of MitID as a authenticator. 10
6.9 Authentication using NemID 10
6.10 Signature through NemLog-in 10
7 Use of MitID's distinctive features 10
8 Management of security breaches 11
9 Service Levels 11
10 Support 11
10.1 End User Support 11
10.2 Technical support 11
11 Fees and payment 12
11.1 Fees for using the services 12
11.2 Terms of payment 12
11.3 Fees from End Users 12
12 Breach and remedies for breach 12
12.1 Remedial action 12
12.2 Termination in general 12
12.3 Termination by the Agency for Digital Government 12
12.4 Suspension of the Service Provider access to NemLog-in's services 13
13 General Services Shutdown 13
14 Liability and compensation 13

14.1 General provisions 13
14.2 Liability for qualified electronic signatures and seals 14
15 Maintenance of information regarding the Service Provider in NemLog-in 14
16 Duty of confidentiality 14
17 Processing of personal data 15
18 Term and termination 15
19 Change of terms and Services 15
19.1 General 15
19.2 Changes to services or functionality 15
19.3 Special circumstances concerning signature services 15
20 Governing law and disputes 16
20.1 Governing law 16
20.2 Disputes, mediation and arbitration 16

Changelog

Date	Version	Change description	Initials
21/9/2021	1.0	Version for publication	ACB
16/1/2023	1.1	Updated to accommodate new setup for terms where terms for service providers are underlying terms for IT system providers. General updates related to use of terms and description of infrastructure.	ACB
28/2/2023	1.2	The provision of liability in paragraph 14.2 regarding Qualified certificates are updated. Definition of Certificate Policy has been added.	ACB

1 Introduction

These Terms for Service Providers regulate Private Service Provider use of Login and Authentication and digital signature from NemLog-in. Service Provider Terms and Conditions are agreed and included as part of the terms for IT system providers and are accepted together when connecting to NemLog-in.

As the Broker, NemLog-in supplies Authentication and related functionality for Service Providers who want to authenticate End Users based on MitID, NemID (for a period) and a number of other NSIS-registered Authenticators.

NemLog-in is a certified MitID Broker and passes on Authentications carried out using MitID based on individual agreement with the MitID supplier (Nets DanID A/S).

Public authorities and public law bodies using NemLog-in as Service Providers are subject to Decree no. 968 of 10 June 2022 on the provision and use of the MitID solution and NemLog-in for public authorities and public law bodies, are not bound by these Terms.

The Terms and Conditions contain several references to the Service Provider Site, where a number of technical requirements and policies are provided. These requirements and policies include detailed requirements and service descriptions and are an integral part of the Terms and Conditions.

When connecting to NemLog-in, the Service Provider must be particularly aware of the organisational classification of the Service Provider, cf. clause 3, and the requirement to conclude a separate NemID service provider agreement with Nets DanID A/S, cf. clause 6.9.

All Services described in the Terms are not necessarily available at the time of the Service Provider's acceptance of the same. On the Service Provider Site, the Service Provider must check the descriptions of which Services are available and any time schedules for introduction of new Services.

2 Definitions

Term	Description
Authentication	An electronic procedure that recognises and verifies the identity of an End User.
Attribute Service	A NemLog-in service, in which the Service Provider has the possibility of requesting information about the End User after completion of the authentication but within the same session.
Administration Module	A self-service solution in NemLog-in, in which Service Providers may manage the connection of their Digital Self-Service Solutions to NemLog-in, including which attributes must be delivered to the Service Provider in the authentication response and certificates and other technical information of relevance to the integration.

Term	Description
Broker	A Legal Entity that passes on Authentication of digital identities to third parties based on Authentication verified by the broker itself or any third parties (brokers in more than one layer). A broker serves as a trusted third party. Brokers connected to NemLog-in are NSIS-notified. NemLog-in's login service within the login and authentication service area operates based on an agreement with the MitID Supplier as a MitID Broker by providing MitID authentications.
Certificate Policy	The basic rules for each certificate type that must be met by the Danish State Trust Services as issuer of certificates. The certificate policies can be read at https://certifikat.gov.dk/.
Digital Self-Service Solution	An IT system in which private individuals or Business Users with digital identities may access digital self-service after having been authenticated. Also referred to as service or IT System.
The eIDAS regulation	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
Business User	A natural person who is associated with a Legal Entity and who has been created with a Business User in NemID Erhverv or MitID Erhverv (referred to as NemLog-in Erhvervsadministration in the Danish Act on MitID and NemLog-in).
Authenticator	An authenticator is characterised as a material unit, an immaterial unit or a combination thereof used for online authentication. The Authenticator must be under the control of the natural or Legal Entity issued with it. The Authenticator, that may be authenticated through NemLog-in will either be based on a NemID, MitID or NSIS-notified authenticator from a local IdP.
IT System	Used as a synonym for Digital Self-Service Solution supplied by a Service Provider.
IT system Provider	Collective term for organisations with a CVR number that connect IT systems to NemLog-in as a Service Provider, Multi-tenant Supplier or Broker.
Qualified Electronic Signature	A qualified electronic signature provided in the Signature Solution based on a qualification certificate. Unless otherwise specifically stated, the term also covers qualified electronic seal, which may also be given in the Signature Solution. Qualified electronic signatures correspond to signatures provided by natural persons, whereas qualified electronic seals are provided by businesses and serve as evidence that the sealed data stem from the business.
Local IdP	Local authentication service through which a user organisation may provide authentication of its own business users, which can be passed on to NemLog-in's underlying Service Providers through NemLog-in.

Term	Description
MitID	The national digital identity of a private individual and related electronic Authenticator that may be attached to the digital identities of private individuals and business users.
MitID Broker	A Broker in the MitID infrastructure which provides authentication based on MitID, if possible supplemented by further services. NemLog-in's login service in the login and authentication service area operates based on an agreement with the MitID Supplier as an MitID Broker.
MitID Erhverv	The Erhvervsadministration area for user organisations in NemLog-in, which i.a. makes it possible to create and administer digital business identities and certificates.
Multi-tenant	An IT system connected to NemLog-in and providing the foundation for a Digital Self-Service solution used by one or more Service Providers for which the Supplier of the system receives Authentication from NemLog-in as an integrated service.
Nets DanID A/S	Nets DanID A/S, Lautrupbjerg 10, P.O. Box 500, 2750 Ballerup
The MitID solution	The Danish national eID-solution to replace NemID. The solution provides electronic identification and authentication of natural persons and natural persons representing legal entities.
MitID authentication request	A request for authentication with MitID from a Service Provider as a result of an End User wanting access to a Digital Self-Service Solution.
NemID	A national identification scheme which issues Authenticator to Danish citizens and to employees and businesses (NemID Erhverv). For citizens, NemID issues one common log-in to both public and private self-service solutions and to online banking services.
NemLog-in	The joint-public digital infrastructure solution that enables private individuals and Business Users with digital identities able to interact with Digital Self-Service solutions, including as a Broker for Service Providers and other brokers. NemLog-in is also the national identity guarantor for business users.
NSIS	National Standard for Identity Level of Assurance
Services	Connection services and the provision of Authentication and signatures, and additional services further defined in the Terms, which the Agency for Digital Government provides to the Service Provider.
Signature solution	Signature solution from Den Danske Stat Tillidstjenester(the Danish State Trust Services) at the Agency for Digital Government issuing qualified electronic signatures and seals with associated qualified certificates.
Level of Assurance	The degree of trust in an authenticated Identity (Leve of Assurance) also referred to as level of identity assurance. Three Levels of Assurance are used: Low, Substantial and High.

Term	Description
End User	A natural person in the form of a private individual or a Business User, who may use an authenticator as the basis for Authentication vis-a-vis a Service Provider.
Security Token Service (STTS)	A NemLog-in service that handles authentication and authorisation of system users/clients through the issue of 'security tokens' that may be used when calling APIs provided by Service Providers connected to NemLog-in's STS. Is included as part of the authentication services supplied by NemLog-in.
Service Provider	An organisation which provides one or more Digital Self-Service Solutions to End Users. The Service Provider is registered as an IT system provider in NemLog-in.
Agreement	The agreement concluded between the Service Provider and the Agency for Digital Government on the Service Provider's acceptance of these terms.
Service Provider Site	NemLog-in's portal for Service Providers at https://tu.nemlog-in.dk/ The Service Provider Site includes a description of technical requirements for Service Providers' usage of NemLog-in and a range of supporting policies. Reference to the Service Provider Site is at the same time a reference to the technical requirements and related policies available on the Site.

3 Correct organisational classification of Service Provider

Connecting to NemLog-in results in an immediate and automatic classification of the Service Provider as a Public-Sector Service Provider or a Private Service Provider. Public-Sector Service Providers include public authorities and bodies governed by public law, as further detailed in the Act on MitID and NemLog-in.

The Service Provider must ensure that the classification is correct in accordance with the law and must contact the Agency for Digital Government if it is determined that there is a need to change the automatically determined classification, so the Service Provider is correctly registered in NemLog-in.

4 NemLog-in Services

4.1 Introduction

By accepting these terms, the Service Provider gains access to the following Services through NemLog-in:

- Login and Authentication (including search services)
- Security Token Service
- Digital signature

The individual Services are described in detail in clause5 and clause6 respectively. A detailed technical description is also provided on the Service Provider Site.

No access is granted to single sign-on functionality through NemLog-in between private Service Providers, for which reason an End Users must always authenticate themselves actively when the End User accesses the Service Provider.

5 Completion of connection

5.1 General conditions

The technical connection and testing of a Digital Self-Service solution to NemLog-in shall take place in accordance with what is stated on the Service Provider Site. The Service Provider Site outlines the technical standards and policies that the Service Provider is required to comply with.

Connection to NemLog-in is subject to payment of a fees as specified in clause11 and prices published on the Service Provider Site.

5.2 The Service Provider's using a technical collaborative partner

Service Providers may through the NemLog-in administration module, attach a technical collaborative partner (called IT provider in NemLog-in) to assist with the connection and ongoing maintenance of the Digital Self-Service Solution, integrations etc.

Vis-a-vis the Agency for Digital Government, the Service Provider is responsible for the actions performed by a technical collaborative partner in NemLog-in.

The Service Provider is required to deregister a technical collaborative partner from NemLog-in when this partner no longer performs services for the Service Provider.

The technical collaborative partner must accept separate terms and conditions from the Agency for Digital Government that reflect this clause when registering in NemLog-in. Additionally, specific technical and organisational security requirements must be accepted. The Service Provider must ensure that the obligations in the terms of the technical collaborative partner are also included in the mutual agreement between the Service Provider and technical collaborative partner. The Terms and Conditions are published on the Service Provider Site.

6 Use of Authentication in Digital Self-Service Solutions

6.1 Login and authentication

The Service Provider is granted access to the NemLog-in login service for Authentication of End Users wishing to use the Digital Self-Service Solutions connected through the Service Provider.

Authentication of End Users is provided with the following Authenticators:

- Private individuals who use NemID or MitID
- Business Users using a private MitID or separate MitID for business use
- Business Users that use a NemID Private for Business or an MitID Private to
- Business Users that use a NemID employee certificate (MOCES)
- Business Users that log on through a NSIS-registered local IdP and use NSIS-registered authenticator issued by a local identity guarantor (local IdP) connected to MitID Erhverv.

When using the Service, an authenticated private identity or Business User is provided, and it is checked if the End User's authenticator is valid, and has not expired or been revoked. The Service Provider is required in accordance with the Service Provider Site to verify the authentication response received from NemLog-in, cf. also clause 6.3below.

Also, reference is made to Service Provider Site for requirements on the reporting to the Agency for Digital Government concerning the Service Provider's use patterns, including peak periods in the use of NemLog-in's login service.

6.2 Restriction on the use of Authentication from NemLog-in

The Service Provider may only use Authentication from NemLog-in for Authentication of End Users in its own Digital Self-Service Solutions.

Accordingly, the Service Provider is not permitted to issue or sign its own authentication responses to third parties and consequently enter the chain of trust with respect to End Users.

A third party means a legal entity with a CVR number which is different from that of the Service Provider.

The Service Provider must ensure that the use of Authentication is planned in such a way that the End User does not circumvent the security, knowingly or not-knowingly, of the NemLog-in Authentication, and does not risk compromising the security attaching to the End User's Authenticator.

6.3 Information in the authentication response

On connection of a Digital Self-Service Solution, the Service Provider must determine the attributes in the administration module which should be provided by NemLog-in based on the End User's Authentication in the relevant Digital Self-Service Solution.

As the data controller, the Service Provider is required to ensure, in compliance with the general principle on data minimisation, that the collection of information through attributes is limited to what is relevant and necessary taking into consideration the purpose for which they are collected and processed by the Service Provider.

In the authentication response, the Service Provider is informed of the Level of Assurance obtained for the completed Authentication of the End User. It is the responsibility of the Service Provider to check the Level of Assurance and determine whether and to which extent access shall be granted on that basis to the Service Provider's Self-Service Solution.

The Service Provider is recommended to complete a risk assessment for the purpose of uncovering which Level of Assurance grants access to the Digital Self-Service Solution. The Service Provider may use tools and guidelines published by the Agency for Digital Government to assist with this risk assessment.

A more detailed description of information in the authentication response is provided on the Service Provider site.

6.4 Information from Attribute Service after Authentication of the End User

After authentication of the End User, but within the said session, the Service Provider may request further attributes from NemLog-in's Attribute Service. In this connection, the Service Provider must observe the principle of data minimisation as described in clause 6.3.

6.5 NemLog-in CPR match service

The Agency for Digital Government makes available a match service to the Service Provider, in which it is possible to check if a civil registration number stated by the End User matches the civil registration number registered by the Agency for Digital Government for the End User.

A more detailed description of the match service is available on the Service Provider Site.

The Service Provider warrants that a valid consent from the End User or other authority for processing is available before the information is obtained from NemLog-in.

6.6 End User's access rights

In MitID Erhverv, User Organisations may grant Intellectual property rights to End Users to be used in public Digital Self-Service Solutions. It is not possible for Private Service Providers to request and be granted such Intellectual property rights.

6.7 Use of Authentication outside the specified time period

Authentications via NemLog-in are subject to specific session lengths as further described on the Service Provider Site. The Service Provider is the sole responsible party and bears the risk of the validity of such Authentications and quality in terms of security, and the Agency for Digital Government may in no way be made liable for security or other matters to that end.

6.8 Risk data in the use of MitID as an authenticator.

The MitID solution collects risk data concerning an End User's use of their MitID authenticator. The MitID solution may pass on this risk data to MitID brokers for the purpose of the brokers' assessment of risks related to actual authentications with connected Service Providers.

NemLog-in does not use risk data and it is not disclosed to Service Providers.

6.9 Authentication using NemID

Through NemLog-in, End Users may for a period authenticate themselves to the Service Provider's Digital Self-Service Solution using NemID. The Service Provider is required to conclude a separate Service Provider Agreement with Nets DanID A/S to that effect.

Fees for receipt of Authentications based on NemID are settled directly with Nets DanID A/S. Invoicing is made on the basis of the settlement model "session settlement" according to which payment is made for each individual NemID transaction made through NemLog-in Broker.

If Service Providers does not want to receive Authentications based on NemID, they may opt out by contacting the Agency for Digital Government. Opting out of this option for Authentication on the basis of NemID shall be paid according to the fixed prices for support at Nets DanID A/S.

6.10 Signature through NemLog-in

The Service Provider has the possibility of integrating up to two different signature services with NemLog-in:

- Signature service based on OCES certificates by means of NemID (NemLog-in's NemID Signature Service)
- Signature solution from Den Danske Stat Tillidstjenester is based on qualified certificates.

Please refer to clause 19.3on special provisions for the discontinuation of the NemID based on OCES certificates.

End User use of the signature is subject to separate terms.

7 Use of MitID's distinctive features

The visual identity and the design elements made available to the Service Provider in the MitID and NemLog-in infrastructure may only be used in connection with Authentication of MitID. 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 provisions for the use of the distinctive features of the MitID solution and MitID, including names, logos and domain names and other material related to MitID.

Service Providers have a right of use of MitID's distinctive features and are required to use MitID's distinctive features in connection with Authentication through the MitID solution and marketing thereof.

UX Scheme" and the design manuals are available at Service Provider Site and the Service Provider is required to stay updated to that effect and comply with the guidelines applicable from time to time.

The Service Provider is obliged, when disconnecting the Digital Self-Service solution from NemLog-in, to remove any reference to MitID's distinctive features and cease using them, unless another agreement is concluded with a rights holder.

8 Management of security breaches

The Service Provider must immediately notify relevant End Users and the Agency for Digital Government of any security breaches.

A security breach is an event which may constitute a security flaw/risk, including unauthorised access to and/or loss of personal data, confidential information, financial information or similar critical information.

If a security breach relates to a breach of the personal data security, the Service Provider is specifically required to act in compliance with the data protection rules, including reporting to the Danish Data Protection Agency. The Provider is required to inform the Agency for Digital Government of all such communication with the Danish Data Protection Agency related to the use of Services from NemLog-in.

In connection with general threats or attacks against NemLog-in and related security infrastructures, the Service Provider is required to reasonably assist the Agency for Digital Government or other competent authority in troubleshooting etc., even if the Service Provider is not covered by the said threat or a specific attack.

9 Service Levels

Unless otherwise specified in these terms, all Services are covered by these terms at normal operation and available all hours on all days of the year, except for service windows.

Detailed description of Service objectives is provided on the Service Provider Site.

The Agency for Digital Government is not responsible for compliance with the Service Levels.

10 Support

10.1 End User Support

The Service Provider is responsible for supporting End Users with regard to the use of the Service Provider's Digital Self-Service Solutions, including the actual implementation of NemLog-in with the Service Provider.

10.2 Technical support

Technical support in connection with the usage of NemLog-in by the Digital Self-Service Solution may be provided by Nets DanID A/S subject to payment of the fees stated on the Service Provider Site.

Detailed description of technical support is also provided on the Service Provider Site.

11 Fees and payment

11.1 Fees for using the Services

Service Provider shall pay the fees provided on the Service Provider Site for the usage of Services from NemLog-in. The actual use of Services registered and calculated by Nets DanID A/S on behalf of the Agency for Digital Government.

11.2 Terms of payment

The Service Provider is invoiced on a monthly basis for Services covered by these terms, including MitID authentication requests.

Invoicing is made on behalf of the Agency for Digital Government by Nets DanID A/S, which also manages the practical matters concerning payments and any adjustments.

Invoicing for NemID transactions is made directly from Nets DanID A/S, cf. clause 6.9.

The Service Provider must make the payment no later than thirty (30) days after the invoice is sent. For payments received after the due date, the Danish Agency for Digital Government is entitled to default interest under the Danish Interest Act. Nets DanID A/S will send, on behalf of the Danish Agency for Digital Government, the first and second reminders, after which any outstanding balances will be transferred to the Danish Debt Collection Agency for the purpose of public debt collection.

The Agency for Digital Government is entitled to deny delivery of Services to the Service Provider, if it has a substantial arrears related to Services provided under these Terms for two consecutive months.

11.3 Fees from End Users

The Service Provider is not permitted to collect fees from End Users for Authentication with Authenticators from NemLog-in, including MitID.

12 Breach and remedies for breach

12.1 Remedial action

The parties are required, without undue delay after the other party's written complaint, to make remedial action regarding errors and defects in the party's obligations.

12.2 Termination in general

Either party may terminate the Agreement if the other party is in material breach of any obligation, and in particular in relation to security, and has failed to remedy the breach or breaches without undue delay.

The Agency for Digital Government may also terminate the Agreement if the Service Provider is declared bankrupt, files a petition for bankruptcy or initiates restructuring administration to the extent that the provisions of the Danish Bankruptcy Act do not prevent this.

The termination takes effect from the time when the termination notice is received and applies to any Services thereafter.

The Agency for Digital Government may also terminate the agreement as further provided in clause 12.3.

12.3 Termination by the Agency for Digital Government

The Agency for Digital Government is entitled to terminate the Service Provider Agreement if one or more of the following circumstances apply:

- The Service Provider breaches its reporting obligation in relation to security events
- The Service Provider breaches its payment and remuneration obligations, cf. clause 11
- The Agency for Digital Government may properly ascertain that the Service Provider's use of services from NemLog-in is of such a nature that it entails a risk of compromising NemLog-in or related infrastructures, including MitID.
- Non-compliance with applicable law, including the Danish Data Protection Act and the General Data Protection Regulation
- The Service Provider exhibits conduct which has a substantial negative influence on or is suited to negatively influence the End Users' perception of NemLog-in and/or related infrastructures, including the MitID solution.
- Service provider uses logo and distinctive features in breach of the applicable provisions, cf. clause7

Termination according to this clause may, however, not take place until the Agency for Digital Government has pointed out the said matter in writing to the Service Provider giving a reasonable deadline for remedying the said matter and this has not taken place within the deadline. The Agency for Digital Government may suspend the Service Provider's access to NemLog-in during this period, cf. clause 12.4, paragraph 3.

In the event of termination, the Service Provider's IT systems will be disconnected from NemLog-in.

12.4 Suspension of the Service Provider access to NemLog-in's services

The Agency for Digital Government may suspend the Service Provider's access to Services covered by these terms if the Agency for Digital Government finds that the Service Provider does not materially perform the obligations set out in the terms and conditions or otherwise uses NemLog-in's Services or MitID in such a way that it is harmful to the security and reputation of the infrastructure.

The Agency for Digital Government must give reasonable and to the extent possible 14 days' notice to the Service Provider for the purpose of remedying the said matter.

In extraordinary cases, suspension of the access to NemLog-in may take place at shorter or without notice if the consideration for the integrity of the infrastructure, other Service Providers or End Users so warrants, or if the said use constitutes a security risk. In all cases, the Agency for Digital Government must give an actual reason for the decision to suspend.

In case of suspension, the Service Provider is excluded from NemLog-in until the Agency for Digital Government reopens the connection or uses its other powers under these terms, including the right to cancellation.

13 General Services Shutdown

The Agency for Digital Government may generally suspend Service Providers' access to services for operational reasons, including out of consideration for maintaining a high security level in the infrastructure.

The Service Providers affected shall be notified of the shutdown to the extent possible.

14 Liability and compensation

14.1 General provisions

The parties are liable according to the general provisions of Danish law and in accordance with the provisions of this clause.

In no event is the Danish Agency for Digital Government liable for business interruption, loss of profits, consequential damage or other indirect loss. Losses related to suspension and revocation under clauses 12.4 and 13 can be characterised as indirect losses.

The Danish Agency for Digital Government is not liable for any losses as a result of non-availability of NemLog-in, including the performance of the service levels outlined on the Service Provider site.

The Parties' 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 of the parties.

Liability issues related to the End User's purchase and use of an MitID are regulated by MitID End User Terms which the End User accepts on the issuance of MitID. Claims related to MitID can only be made to the MitID supplier if the legislation mandatorily prescribes that a Service Provider or an End User may make such a claim.

14.2 Liability for qualified electronic signatures and seals

If the Service Provider reasonably rely on a qualified electronic signature or a qualified electronic seal and related certificate from Den Danske Stat Tillidstjeneste, or 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 The Agency for Digital Government can lift the burden of proof of not acting intentionally or negligently.

Under this provision, the Danish Agency for Digital Government's liability is subject to the financial limitation of liability specified in clause 14.1.

15 Maintenance of information regarding the Service Provider in NemLog-in

The Service Provider is required to ensure that registered information on the Service Provider in NemLog-in, including names of administrators, is always correct and accurate.

16 Duty of confidentiality

The Parties, including employees, subcontractors, consultants etc. must observe unconditional confidentiality with regard to information received from the other Party as a result of the Service Provider's connection to NemLog-in, and on the condition that the information concerns the said Party's trade secrets, concepts, relations and other confidential information. The parties must particularly ensure confidentiality about personal data, technical integrations and security-related issues.

The rules for employees in public administration apply to the staff of the Danish Agency for Digital Government. A similar obligation as regards information about the Service Provider's affairs that apply to the Service Provider regarding the affairs of the Agency for Digital Government is imposed on consultants and others that assist the Agency.

The duty of confidentiality also apply after termination of the Agency for Digital Government's provision of Services, regardless of whether the Service Provider Agreement has been terminated, cancelled or otherwise lapsed.

17 Processing of personal data

The Service Provider is the data controller of data contained in the authentication response from NemLog-in and data which, based on the Authentication, is subsequently requested from NemLog-in's attribute service, cf. clause 6.4 and 6.5. The Service Provider is also the data controller for personal data disclosed to the Service Provider in the course of using the signing services, as referred to in cf. clause6.10.

Privacy of personal information the Service Provider must ensure that there is a necessary basis for processing prior to processing.

18 Term and termination

The Agreement will remain in force until it is terminated. The Agreement may be terminated by either party giving 6 months' written notice.

On expiry of the Agreement duration, the Service Provider's IT systems will be disconnected from NemLog-in.

19 Change of terms and Services

19.1 General

The Agency for Digital Government may change the terms and applicable policies of the Service Provider Site by giving 3 months' notice.

In case of major changes, including changes that are assessed to impact the Service Provider's IT systems, the Agency for Digital Government will strive to give six (6) months' notice.

If the Danish Agency for Digital Government finds that changes are material for operational purposes, including security, changes may be made at shorter notice, including with effect from the time of notification. This also applies to changes that the Agency for Digital Government is required to implement as a result of the agreement with the MitID supplier for the delivery of MitID broker services.

The Service Provider will be notified of changes to terms and included policies after which they will take effect after expiry of the notice.

The notice will sent by email to the addresses specified in the Administration Module.

19.2 Changes to Services or functionality

Any addition of new services or functionalities that do not impact the current operational circumstances of the Service Provider may take place without notice.

The Danish Agency for Digital Government may on an ongoing basis and without notice change the range of supported authenticators in NemLog-in, including as a result of decisions made by identity providers connected to NemLog-in..

19.3 Special circumstances concerning signature services

Signature service based on OCES certificates by means of NemID (NemLog-in's NemID Signature Service) are expected to be discontinued during 2023. The Danish Agency for Digital Government may discontinue this service giving one month's notice.

On discontinuation of NemLog-in's NemID Signature Service, the terms for new Service Providers will be updated.

20 Governing law and disputes

20.1 Governing law

Any matters subject to these terms and their severability must be settled according to Danish law.

20.2 Disputes, mediation and arbitration

In the event that any disputes should arise between the Parties, the Parties must first endeavour to solve such dispute by mutual and loyal settlement negotiations.

Any disputes and disagreements directly or indirectly arising out of these Terms and Conditions must be settled with final and binding effect by arbitration in accordance with the Rules of Procedure of the Danish Institute of Arbitration and according to Danish law. The place of arbitration is Copenhagen.

Each Party appoints an arbitrator while the umpire of the arbitration tribunal is appointed by the Institute, provided that the arbitrators appointed by the Parties fail to agree on an umpire within 14 days after their appointment.

In the event that a Party has not appointed its arbitrator within 30 days after having given or received notification of a request for arbitration, such arbitrator will be appointed by the Institute in accordance with the above provisions.

However, this clause 20.2 shall not prevent the Parties from bringing cases regarding breaches of these terms before the courts of law with a view to taking preliminary legal action.