DIGITALISERINGSSTYRELSEN

NemLog-in

Bilag 2 Regler og vilkår for Tjenesteudbyderes brug af NemLog-in Services

Version 1.2

Indholdsfortegnelse

1 Indledning

Dette bilag indeholder sammen med Vilkårene, jf. Vilkårenes punkt 7.2, de vilkår (Tjenesteudbydervilkår), som Tjenesteudbydere skal opfylde for at anvende Services fra NemLog-in. Leverandøren skal indarbejde det i bilaget anførte i sine aftaler med Tjenesteudbydere, således at Tjenesteudbyderne bliver forpligtet heraf.

Tjenesteudbydervilkårene i dette bilag kan ændres og opdateres løbende, jf. Vilkårenes punkt 17. Ændringer i tjenesteudbydervilkårene kommunikeres til Leverandøren, som i fornødent omfang skal kommunikere ændringer til Tjenesteudbyderne, ligesom Leverandøren skal sikre, at ændringerne gennemføres i aftaler med Tjenesteudbydere.

Offentlige Tjenesteudbyderes anvendelse af Services fra NemLog-in er i reguleret af Lov om MitID og NemLog-in, herunder bekendtgørelse om tilrådighedsstillelse og anvendelse af MitID-løsningen og NemLog-in. De i punkt 2.1 til 2.5 anførte forhold er reguleret i bekendtgørelsen og skal derfor ikke omfattes af Leverandørens aftaler med Offentlige Tjenesteudbydere.

2 Krav til indhold af Leverandørens aftale med Tjenesteudbyder

2.1 Sikkerhedskrav

Tjenesteudbyder skal opfylde de sikkerhedskrav, der er anført på Tjenesteudbydersitet. Tjenesteudbydere må desuden ikke i anden sammenhæng udsætte NemLog-in og tilknyttede løsninger, herunder MitID-løsningen for sikkerhedsrisiko med hensyn til ægthed, integritet og fortrolighed.

Tjenesteudbyder er forpligtet til at underrette Slutbrugere og Leverandøren om eventuelle sikkerhedsbrud relateret til anvendelsen af NemLog-in.

2.2 Tekniske krav

Tjenesteudbyder er forpligtet til at opfylde de tekniske krav anført på Tjenesteudbydersitet, der retter sig mod Tjenesteudbydere.

2.3 Anvendelse af Sikringsniveauer

Tjenesteudbyder må ikke anvende Autentifikation, der modtages af Leverandøren fra NemLog-in, til Tjenesteudbyders Digitale Selvbetjeningsløsninger, der kræver et højere Sikringsniveau end hvad der fremgår af autentifikationssvaret fra NemLog-in.

2.4 Anvendelse af kendetegn

Den visuelle identitet og de designkomponenter, der stilles til rådighed NemLog-in infrastrukturen, må alene anvendes i forbindelse med Autentifikation via NemLog-in. Det er ikke tilladt for Tjenesteudbyderen at anvende disse til understøttelse af egne eller tredjeparts services.

Tjenesteudbyderen er forpligtiget til at overholde de gældende regler for brug af NemLog-in's og MitID's kendetegn (herefter blot kendetegn), herunder navne, logoer og domænenavne samt øvrigt materiale med tilknytning til Partnerskabet og MitID.

Retningslinjer for UX/UI og kommunikation relateret til NemLog-in og MitID fremgår af Tjenesteudbydersitet.

Tjenesteudbydere har en brugsret til kendetegn og er forpligtet til at anvende disse kendetegn i forbindelse med, at der tilbydes Autentifikation via NemLog-in løsningen og markedsføring heraf.

Retningslinjerne kan ændres, og kendetegn kan ændres helt eller delvist. Tjenesteudbyderne er forpligtet til løbende at holde sig opdateret herom og opfylde de til enhver tid gældende retningslinjer.

Tjenesteudbyderen er ved ophør af aftale om brug af Autentifikation fra NemLog-in forpligtet til at fjerne enhver henvisning til kendetegn og ophøre med brugen heraf, medmindre anden aftale indgås med en rettighedshaver.

2.5 Spærring af adgang til NemLog-in

Tjenesteudbyders adgang til Autentifikation og øvrige ydelser kan spærres af Leverandøren, hvis Tjenesteudbyderen i væsentligt omfang ikke opfylder Leverandørens krav til Tjenesteudbyderen, eller hvis Tjenesteudbyderens adfærd i øvrigt udgør en sikkerhedsrisiko eller såfremt Tjenesteudbyderen udviser en adfærd, der i væsentligt omfang påvirker eller er egnet til at påvirke Slutbrugernes opfattelse af NemLog-in og tilknyttede løsninger, herunder MitID-løsningen negativt.

Leverandøren er i øvrigt berettiget til at videreføre en spærring fra Digitaliseringsstyrelsen, herunder spærringer der er begrundet i væsentlige sikkerhedsmæssige grunde.

2.6 Vilkår for Tjenesteudbyders opkrævning af vederlag

Tjenesteudbyder er ikke berettiget til at opkræve vederlag fra Slutbrugere for Autentifikation eller signering fra NemLog-in.

2.7 Certifikater og signering

2.7.1 Anvendelse af NemLog-in Digital Signering

Såfremt Tjenesteudbyder med rimelighed forlader sig på en kvalificeret elektronisk signatur eller et kvalificeret elektronisk segl og tilhørende certifikat fra NemLog-in Digital Signering, er Digitaliseringsstyrelsen erstatningsansvarlig for tab efter dansk rets almindelige regler.

For de i Certifikatpolitikkens krav 9.6.1-04 anførte forhold er Digitaliseringsstyrelsen ansvarlig for tab, medmindre Digitaliseringsstyrelsen kan løfte bevisbyrden for ikke at have handlet forsætligt eller uagtsomt.

Digitaliseringsstyrelsens erstatningsansvar efter denne bestemmelse er begrænset til 100.000 kr. for hver tabsgivende begivenhed og er i alle tilfælde maksimeret til 100.000 kr. årligt. Ved en tabsgivende begivenhed anses alle forhold, der udspringer af samme fortsatte eller gentagne ansvarspådragende forhold.

Ovenstående begrænsning er kun gældende, såfremt misligholdelsen ikke kan henføres til grov uagtsomhed eller forsætlige forhold.

2.7.2 Tjenesteudbyders pligt ved modtagelse af et certifikat

Forud for at have tillid til et certifikat fra den Danske Stat – Tillidstjenester, skal Tjenesteudbyder som modtager af en signatur sikre sig følgende:

- At certifikatet er gyldigt - dvs. ikke opført på Den Danske Stats Tillidstjenesters spærreliste på tidspunktet for signeringen,
- at det formål, certifikatet søges anvendt til, er passende i forhold til evt. anvendelsesbegrænsninger i certifikatet samt
- at anvendelsen af certifikatet i øvrigt er passende i forhold til niveauet af sikkerhed, som er beskrevet i certifikatpolitikken for det pågældende certifikat

Inden et tidsstempel (såfremt et tidsstempel indgår i det signerede dokument) accepteres, skal Tjenesteudbyder som modtager af en signatur sikre sig følgende:

- at tidsstemplet er korrekt signeret, og at den private nøgle, der bruges til at signere tidsstemplet, ikke er blevet markeret som kompromitteret på kontroltidspunktet,
- at anvendelsen sker inden for eventuelle begrænsninger for brugen af tidsstemplet angivet i tidsstempelpolitikken og
- at andre forholdsregler, der er angivet i aftaler eller lignende, er opfyldte.

2.8 Krav fra Tjenesteudbydere

Ethvert krav fra Tjenesteudbydere, der relaterer sig til NemLog-in Services skal rettes mod Leverandøren. Undtaget herfra er dog krav, der relaterer sig til fejl i signaturer eller segl fra NemLog-in Digital Signering, der skal rettes mod Digitaliseringsstyrelsen.

3 Krav til databehandleraftale

Det skal af Leverandørens databehandleraftale med Tjenesteudbydere fremgå, at Leverandøren som databehandler behandler følgende oplysninger om Slutbruger som led i modtagelsen af Autentifikationssvaret fra NemLog-in:

- Navn og CPR-nummer (hvis CPR-nummer er registreret),
- E-mailadresse (erhvervsbrugere)
- Pseudonym (erhvervsbrugere)
- PID og RID
- CVR-nummer (erhvervsbrugere)
- Sikringsniveau
- NemLog-in identifikationsnummer på den elektroniske identitet (UUID)

Nærmere detaljer om de pågældende oplysninger fremgår af seneste version af OIOSAML Web SSO Profile.

Leverandøren må ikke behandle autentifikationssvar på anden måde eller til andre formål end hvad der følger af lov om MitID og NemLog-in, medmindre Tjenesteudbyder har et selvstændigt hjemmelsgrundlag for behandlingen af autentifikationssvar.

4 Særlige forhold for Offentlige Tjenesteudbydere

Offentlige Tjenesteudbyderes modtagelse af Autentifikation fra NemLog-in via Leverandøren er reguleret af Lov om MitID og NemLog-in, herunder bekendtgørelse om tilrådighedsstillelse og anvendelse af MitID-løsningen og NemLog-in. De beføjelser, som Digitaliseringsstyrelsen har i medfør af Bekendtgørelsen er gældende uanset, at Autentifikationer modtages via Leverandøren. Beføjelserne kan udmøntes af Digitaliseringsstyrelsen gennem Leverandøren.