

DIGITALISERINGSSTYRELSEN



Bilag 2 Brokers behandling af personoplysninger

Version 1.1

Indholdsfortegnelse

1	Indledning.....	2
2	Omfattede personoplysninger	2
3	Videregivelseshjemmel	2
3.1	Digitaliseringsstyrelsens videregivelse af personoplysninger	2
4	Behandlingshjemmel	2
4.1	Brokers modtagelse af personoplysninger.....	2
4.2	Brokers videregivelse af personoplysninger.....	2
4.3	Slettefrist	3
4.4	Brokers forpligtelser ved behandling	3

1 Indledning

Dette bilag regulerer Brokerens behandling af personoplysninger, når NemLog-in videregiver personoplysninger til Brokeren, og når Brokeren videregiver eventuelle personoplysninger til Tjenesteudbyderen, og de nærmere vilkår herfor, jf. Brokeraftalens punkt 14.

Brokeren er selvstændig dataansvarlig i forbindelse med modtagelse af personoplysninger fra NemLog-in og den efterfølgende behandling heraf, herunder i forhold til eventuel videregivelse af personoplysninger fra Broker til Tjenesteudbyder.

2 Omfattede personoplysninger

Brokerens behandling af personoplysninger fra NemLog-in omfatter nedenstående typer af oplysninger:

- Autentifikationsvar, der indeholder oplysninger om Slutbrugeren, der logger ind:
 - 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.

3 Videregivelseshjemmel

3.1 Digitaliseringsstyrelsens videregivelse af personoplysninger

Digitaliseringsstyrelsen har i medfør af lov om MitID og NemLog-in hjemmel til at videregive Autentifikationsvar til Broker.

4 Behandlingshjemmel

4.1 Brokers modtagelse af personoplysninger

Brokeren har i medfør af lov om MitID og NemLog-in hjemmel til at modtage og behandle autentifikationsvar.

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

4.2 Brokers videregivelse af personoplysninger

Brokeren har i medfør af lov om MitID og NemLog-in hjemmel til at videregive det af Brokeren modtagne behandlede autentifikationsvar til en Tjenesteudbyder, der har indgået en aftale med den pågældende Broker om at modtage autentifikationsvar. Ved videregivelsen bliver Tjenesteudbyder selvstændig dataansvarlig for behandlingen af autentifikationsvaret.

Formålet med Brokerens videregivelsen af autentifikationsvaret til en Tjenesteudbyder er at sikre, at Slutbrugeren kan logge ind på den pågældende Tjenesteudbyders tjeneste.

Det kan ligeledes udledes af Lov om MitID og NemLog-in, at ved Brokerens videregivelse af autentifikationssvar til en tilsluttet til Broker (Brokere i flere led), så bliver den tilsluttede Broker selvstændig dataansvarlig for behandling af autentifikationssvaret.

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

Ved videregivelse af autentifikationssvar til en Tjenesteudbyder tilsluttet via en Multi-tenant Leverandør, er Multi-tenant leverandøren databehandler for Tjenesteudbyder. Krav til databehandleraftale mellem Tjenesteudbyder og Multi-tenant Leverandør fremgår af Bilag 3.

4.3 Slettefrist

Brokeren skal fastsætte relevante slettefrister for personoplysninger.

4.4 Brokers forpligtelser ved behandling

Brokeren er til enhver tid forpligtet til at sikre, at den til enhver tid gældende databeskyttelseslovgivning overholdes, for nuværende særligt Europa-Parlamentets og Rådets forordning (EU) nr. 2016/679 af 27. april 2016 (databeskyttelsesforordningen). Brokeren er endvidere forpligtet til at efterleve supplerende dansk lovgivning til databeskyttelsesforordningen og regler udstedt i medfør heraf, for nuværende særligt lov nr. 502 af 23. maj 2018 (databeskyttelsesloven).

Dette indebærer bl.a., at Brokeren i forbindelse med behandling af personoplysninger skal overholde forpligtelserne som selvstændig dataansvarlig. Brokers forpligtelser som selvstændig dataansvarlig for omfatter blandt andet nedenstående forpligtelser:

- Brokeren skal træffe passende foranstaltninger til at opfylde sin oplysningspligt efter databeskyttelsesforordningens artikel 13-14 og give enhver meddelelse i henhold til artikel 15-22 og 34 om behandling til den registrerede, jf. databeskyttelsesforordningens artikel 12
- Brokeren skal gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre og være i stand til at påvise, at behandling er i overensstemmelse med databeskyttelsesforordningen, jf. databeskyttelsesforordningens artikel 24.
- Brokeren skal føre en fortegnelse over alle behandlingsaktiviteter af personoplysninger, der foretages af Brokeren, jf. databeskyttelsesforordningen artikel 30. Fortegnelsen skal indeholde en beskrivelse af den behandlingshjemmel, der danner grundlag for behandling af de pågældende personoplysninger (autentifikationsdata og risikodata).
- Brokeren skal efter anmodning fra Digitaliseringsstyrelsen til enhver tid stille fortegnelsen efter databeskyttelsesforordningens artikel 30 til rådighed for Digitaliseringsstyrelsen eller Datatilsynet.
- Brokeren skal gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til risiciene, jf. databeskyttelsesforordningens artikel 32.