Bilag 9C – Forpligtelser for Brokerens behandling af personoplysninger i downstream dataflowet

Version 2.0

Version	Ændringer	Dato

[Broker bedes indsætte virksomhedsnavn]

Indholdsfortegnelse

1. Indledning

Dette bilag regulerer Brokerens behandling af personoplysninger i "downstream dataflowet", når MitID-løsningen videregiver personoplysninger til Brokeren, og når Brokeren videregiver eventuelle personoplysninger til Tjenesteudbyderen, og de nærmere vilkår herfor, jf. Brokeraftalens punkt 11.

Brokeren er selvstændig dataansvarlig i forbindelse med modtagelse af personoplysninger fra MitID-løsningen og den efterfølgende behandling heraf, herunder i forhold til eventuel videregivelse af personoplysninger fra Broker til Tjenesteudbyder. Dette gælder, uanset hvilken en af anvendelsesmodellerne, jf. Bilag 3, som Brokeren anvender.

1.1 Omfattede personoplysninger

Brokerens behandling af personoplysninger i "downstream dataflowet" omfatter følgende typer af personoplysninger:

- Autentifikationssvar, herunder risikodata

Autentifikationssvaret indeholder oplysninger om Slutbrugeren, der logger ind.

Risikodata indeholder følgende oplysninger:

- Lokationsbaserede risikoparametre – GeoIP koordinater,
- Netværksbaserede risikoparametre – IP-nummer,
- Devicebaserede risikoparametre – Information om den anvendte mobiltelefon eller browser og
- Identitetsbaserede risikoparametre – Information om identiteten og sidste anvendelse af Identifikationsmidlet.

Disse risikodata indsamles af MitID-løsningen i forbindelse med hvert enkelt log-in og videregives sammen med tidligere observerede risikodata i autentifikationssvaret til den Broker, der formidler Autentifikation til en given selvbetjeningsløsning i forbindelse med log-in hos en tjeneste.

Formålet med behandlingen af disse oplysninger er, at Brokeren kan vurdere og afgøre om risikodataene af sikkerhedsmæssige årsager skal umuliggøre log-in på den pågældende tjeneste.

2. Videregivelseshjemmel

2.1 Digitaliseringsstyrelsens videregivelse af personoplysninger

Digitaliseringsstyrelsen har i medfør af lov om MitID og NemLog-in hjemmel til at videregive autentifikationssvar, herunder risikodata vedrørende den konkrete og enkelte Autentifikation fra MitID-løsningen til Brokeren.

3. Behandlingshjemmel

3.1 Brokerens modtagelse af personoplysninger

Brokeren har i medfør af lov om MitID og NemLog-in hjemmel til at modtage og behandle autentifikationssvar, herunder risikodata til vurdering af risikoen ved den konkrete og enkelte transaktion.

Brokeren må ikke behandle autentifikationssvar og risikodata 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 autentifikationssvar og risikodata.

3.2 Brokerens videregivelse af personoplysninger

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

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

Videregivelse af risikodata til Tjenesteudbyder forudsætter, at Tjenesteudbyder har et selvstændigt hjemmelsgrundlag til at modtage og behandle risikodata.

Tjenesteudbyderen må ikke behandle autentifikationssvar, herunder eventuelle risikodata 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.

3.3 Slettefrist

Såfremt Brokeren ikke har et særskilt hjemmelsgrundlag til videre behandling af autentifikationssvar, herunder risikodata (end hvad der er angivet i lov om MitID og NemLog-in) skal Brokeren fastsætte relevante slettefrister for disse personoplysninger

Brokeren skal sikre, at tilsvarende slettefrister fastsættes hos Tjenesteudbyderen.

3.4 Forpligtelser ved behandling

Nedenstående forpligtelser skal iagttages og overholdes af Brokeren.

3.4.1 Almindelige forpligtelser som dataansvarlig

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 i "downstream dataflowet" skal overholde forpligtelserne som selvstændig dataansvarlig. Brokers forpligtelser som selvstændig dataansvarlig for "downstream dataflow" 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.