

NSP Serviceaftale for Anvendersystem- leverandør

Definitioner

I denne NSP Serviceaftale anvendes følgende definitioner:

- Serviceudbyder/Serviceformidler: den der udbyder eller formidler en service
- Serviceaftager: den der er umiddelbart aftager af servicen og aftalepart
- Serviceanvender/Serviceanvenderorganisation/Servicebruger: den der faktisk bruger/anvender servicen i det daglige arbejde – herunder også slutbruger.

Aftaleparter

Nærværende aftale om at anvende den Nationale Serviceplatform (NSP) er indgået mellem Sundhedsdatastyrelsen (SDS) som systemansvarlig organisation for NSP og Serviceaftager på vegne af de i bilag 1 oplyste Serviceanvendere af data og/eller services der udbydes på NSP.

NSP Serviceaftalekoncept

Aktører på sundhedsområdet, der ønsker at anvende data og services, der udbydes på NSP, skal indgå en NSP Serviceaftale (nærværende aftale) før adgangen etableres. NSP Serviceaftalen regulerer forholdet mellem SDS, som systemansvarlig organisation for NSP og Serviceaftager. Da Serviceaftager agerer som leverandør for andre organisationer (med andet CVR-nummer) skal Serviceaftager til hver en tid kunne dokumentere, hvilke Serviceanvenderorganisationer vedkommende handler på vegne af, samt at der er indgået aftaler svarende til denne NSP Serviceaftale mellem Serviceaftager og de pågældende Serviceanvenderorganisationer.

Aftalen omfatter de til enhver tid gældende vilkår for brug af NSP services, som parterne hermed forpligter sig til, herunder at sætte sig ind i de til enhver tid gældende vilkår.

SDS publicerer de til enhver tid gældende vilkår for benyttelse af NSP platformen under punktet "Servicedeclaration for NSP" på <https://www.nspop.dk>. På denne adresse er servicemål for NSP platformen også tilgængelig.

Serviceaftager har adgang til oversigt over aftaler og forbrug af services via brugernavn og password. Adgang fås i forbindelse med accept af denne serviceaftale på nspop.dk.

Specifikke vilkår for Serviceaftager og Serviceanvenderorganisationer ifm. anvendelse af data og services på NSP

Serviceaftager indestår, som databehandler for Serviceanvenderorganisationer, for til enhver tid at overholde gældende love, regler mv. omkring håndtering af persondata. Serviceaftager er forpligtet til at holde sig orienteret omkring den nationale sikkerhedsinfrastruktur samt til at sikre, at incidents i et Serviceaftagers system ikke medfører afledte incidents i andre systemer eller i infrastrukturen. Serviceaftager er således forpligtet til at opretholde det fornødne support-beredskab til at kunne håndtere incidents på forsvarlig vis, og er forpligtet til at orientere SDS uden ugrundet ophold, hvis der forekommer incidents, der kan have betydning for den nationale infrastruktur eller andre systemer. I tilfælde af konkrete incidents skal Serviceaftager kunne afbryde adgangen til den nationale infrastruktur

for de enkelte Serviceanvendere/-organisationer som anvender Serviceaftagers it-løsning for at sikre, at et incident begrænses til færrest muligt lokationer.

Serviceaftager indestår for, at der i Serviceaftager kundevilkår for Serviceanvendere/-organisationer optages bestemmelser, der på tydelig vis forpligter de Serviceanvendere som anvender Serviceaftagers it-løsning til at

- overholde de generelle NSP servicevilkår, samt de specifikke servicevilkår der er gældende for de services som Serviceaftager udbyder sin it-løsning til,
- overholde de fastlagte regler for brug af Sundhedsdatanettet¹,
- varetage brugeradministration og vedligehold heraf i overensstemmelse med lovkrav og indgåede aftaler,
- sikre den fornødne netværkssikkerhed, herunder løbende opdatering af firewalls, antivirus-og anti-malwareprogrammer, og
- at rette henvendelse til Serviceaftager i tilfælde af formodede eller konstaterede sikkerhedsbrud med henblik på at sikre størst mulig begrænsning af skaden.

I forhold til NSP optræder den enkelte Serviceanvenderorganisation, fx apotek, tandlægepraksis m.fl. som Serviceanvender. Denne forståelse anvendes i det følgende.

Adgangen til NSP, og de data og services der udbydes på NSP, etableres under forudsætning af, at de i bilag 1 nævnte Serviceanvendere har indgået databehandleraftaler med Serviceaftager, hvoraf det fremgår, at Serviceaftager (databehandler) alene handler efter instruks fra Serviceanvender (sundhedsorganisationer eller sundhedspersoner dvs. den dataansvarlige), og at reglerne i databeskyttelsesforordningen § 32 ligeledes gælder for behandlingen ved databehandleren.

Såfremt en ønsket databehandler er etableret i et land, der ikke er omfattet af forordningen, skal forordningens regler i kapitel 5 vedr. databehandlere i 3. lande overholdes. SDS skal derfor inddrages konkret i forhold til evt. indgåelse af aftale.

Det skal fremgå af den indgåede aftale mellem Serviceanvender (den dataansvarlige) og databehandleren, at de procedurer, der er beskrevet i bilag 2, skal overholdes.

SDS kan på ethvert tidspunkt udbede sig databehandleraftalerne.

Adgangen etableres derfor under forudsætning af, at Serviceaftager ikke under nogen omstændigheder anvender oplysningerne til egne formål.

¹ Anført i Bilag 1: Betingelser for tilslutning til og brug af SDN i Tilslutningsaftale for Sundhedsdatanettet (SDN) - se <https://www.medcom.dk/systemforvaltning/sundhedsdatanet-sdn/startpakke>

Hvis en Serviceanvender, eller dennes databehandler, ikke retter sig efter de i denne aftale udstukne retningslinjer for sikkerhed eller overtræder reglerne i databeskyttelseslovgivningen, forbeholder SDS sig ret til at fratage adgangen, indtil SDS finder at der fra Serviceanvender og Serviceaftager side, er etableret betryggende sikkerhed for overholdelse af kravene. Det samme gælder, hvis der i øvrigt konstateres misbrug af adgangen.

Serviceaftager har ansvaret for, at bilag 1 udfyldes i overensstemmelse med de anførte krav. Bilaget skal til enhver tid være opdateret og skal sendes til SDS to gange årligt, nærmere bestemt hvert år den 1. marts og den 1. september. SDS kan dog til enhver tid kræve en komplet og opdateret liste.

Serviceaftager må ikke overdrage rettigheder og forpligtelse i medfør af denne aftale til tredjemand uden SDS' forudgående skriftlige samtykke.

Ændring i aftalemæssige forhold

SDS kan foretage ændringer i vilkårene for tilslutning til NSP. Ændringer i vilkår træder i kraft med minimum 6 måneders varsel, med mindre ændringerne er nødvendige at implementere hurtigere af lovgivningsmæssige eller sikkerhedsmæssige årsager, der nødvendiggør et kortere eller intet varsel.

Aftaleindgåelse

Så snart aftalen er underskrevet af Serviceaftager og godkendt af SDS, foretager SDS de nødvendige foranstaltninger for at Serviceaftager får adgang til NSP. Så snart dette er iværksat sender SDS besked via e-mail til den i aftalen angivne kontaktperson, hvorefter aftalen træder i kraft.

Aftalen kan opsiges af begge parter med 6 måneders varsel.

Kontaktdata

Normalt vil man kunne orientere sig om driftsmæssige forhold og varslinger på NSPOP Driftsstatus:

<https://www.nspop.dk/display/driftsstatus/Driftsstatus>

Ved særlige driftsmæssige forhold eller kritiske incidents, kan der være behov for at kontakte Servicedesk eller ansvarligt teknisk personale hos Serviceaftager. I forbindelse med indgåelse af aftalen skal disse kontaktdata anføres på nspop.dk.

Underskrift

Serviceaftager giver med sin accept af denne aftale på nspop.dk tilsagn om overholdelse af denne aftale, på vegne af de i bilag 1 oplistede Serviceanvendere.

Bilag 1: Liste over de Serviceanvendere/-organisationer Serviceaftager har indgået denne aftale med Sundhedsdatastyrelsen på vegne af.

Instruks for listens indhold og opdatering:

Bilaget skal udfyldes i excel/csv med navn og CVRnr. For samtlige Serviceanvendere (sundhedsorganisationer eller sundhedspersoner), som oplysningerne vil blive givet til.

Bilaget i excel/csv opdateres den 1. marts og den 1. september hvert år via <https://www.nspop.dk/display/resources/Supporthenvendelse>

Bilag 2: Sikkerhedsforanstaltninger hos Serviceanvender

Serviceaftager (databehandleren) er forpligtet til at informere Serviceanvender om nedenstående krav, som stilles af SDS (den dataansvarlige) for at kunne tilgå de ønskede services på NSP.

Instruks for adgangskontrol

Betingelser for adgang

En slutbruger ved den enkelte Serviceanvender har alene adgang til oplysningerne om en person når:

- Slutbrugeren har person i aktuel behandling og
- Oplysningerne er relevante som led i behandlingen

Data og Services stilles til rådighed for normal og løbende forretningsanvendelse.

Samtlige disse betingelser skal være opfyldt, og Serviceanvender skal til enhver tid kunne dokumentere, at betingelserne er opfyldt.

Adgangskontrol

Serviceanvender skal sikre behørig adgangskontrol til data og services der udbydes på NSP i overensstemmelse med følgende retningslinjer:

- Kun den slutbruger, der autoriseres hertil, skal have adgang til data og services der udbydes på NSP. Kun sundhedsorganisationen eller sundhedspersonen selv eller dennes medhjælp må autoriseres som slutbruger.
- For slutbrugere, som ikke længere har behov for de autorisationer, de har fået udstedt, skal autorisationerne straks inddrages. Det gælder f.eks. medarbejdere, som flytter til andet arbejdsområde, eller hvis ansættelsesforhold ophører.
- Der skal etableres en teknisk adgangskontrol i systemet, således at autoriserede personer skal identificere sig entydigt over for systemet for at få adgang til data og services der udbydes på NSP. Man må ikke anvende andre adgangsoplysninger end sine egne.
- Serviceanvender skal ved adgangskontrollen sikre sig, at den, der forsøger at få adgang, er berettiget til at foretage opslag.
- Der skal foretages registrering af alle afviste adgangsforsøg.

Netværkssikkerhed

Serviceanvender er forpligtet til at sikre den fornødne netværkssikkerhed, herunder:

- overholde de fastlagte regler for brug af Sundhedsdatanettet²
- sikre den fornødne netværkssikkerhed, herunder løbende opdatering af firewalls, antivirus-og anti-malwareprogrammer

² Anført i Bilag 1 startpakke: Betingelser for tilslutning til og brug af SDN i Tilslutningsaftale for Sundhedsdatanettet (SDN) - se <https://www.medcom.dk/systemforvaltning/sundhedsdatanet-sdn/startpakke>

- sikre opdatering af operativsystemer og anvendt software på de arbejdspladser, der anvendes til at tilgå NSP.

Bistand til den dataansvarlige

Serviceaftager (databehandleren) og/eller Serviceanvender bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige, med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel 3.

Dette indebærer, at Serviceaftager (databehandleren) og/eller Serviceanvender så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

- a) oplysningspligten ved indsamling af personoplysninger hos den registrerede
- b) oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
- c) den registreredes indsigtsret
- d) retten til berigtigelse
- e) retten til sletning (»retten til at blive glemt«)
- f) retten til begrænsning af behandling
- g) underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
- h) retten til dataportabilitet
- i) retten til indsigelse
- j) retten til at gøre indsigelse mod resultatet af automatiske individuelle afgørelser, herunder profilering

Serviceaftager (databehandleren) og/eller Serviceanvender bistår den dataansvarlige med at sikre overholdelse af den dataansvarliges forpligtelser i medfør af databeskyttelsesforordningens artikel 32-36 under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, jf. art 28, stk. 3, litra f.

Dette indebærer, at Serviceaftager (databehandleren) og/eller Serviceanvender under hensyntagen til behandlingens karakter skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

- a) forpligtelsen til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er forbundet med behandlingen.
- b) forpligtelsen til at anmelde brud på persondatasikkerheden til tilsynsmyndigheden (Datatilsynet) uden unødigt forsinkelse og om muligt senest 72 timer, efter at den dataansvarlige er blevet bekendt med bruddet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.
- c) forpligtelsen til - uden unødigt forsinkelse - at underrette den/de registrerede om brud på persondatasikkerheden, når et sådant brud sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder.
- d) forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder.

- e) forpligtelsen til at høre tilsynsmyndigheden (Datatilsynet) inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen

Sikkerhedsbrud

Serviceanvender er forpligtet til at rette henvendelse til Serviceaftager uden unødigt ophold i tilfælde af formodede eller konstaterede sikkerhedsbrud med henblik på at sikre størst mulig begrænsning af skaden.

Serviceanvender er forpligtet til at hjælpe Serviceaftager og SDS med at udrede og afhjælpe evt. sikkerhedsbrud.

Såfremt der er tale om brud på persondatasikkerheden i forhold til anvendelse af services på NSP, skal Serviceanvender underrette Sundhedsdatastyrelsen uden unødigt ophold og senest 24 timer efter, at bruddet er konstateret på adressen databeskyttelse@sundhedsdata.dk.

Tilsyn og kontrol

SDS kan i samarbejde med Serviceaftager, føre tilsyn med Serviceanvenders varetagelse af sikkerheden, herunder adgangskontrollen og ajourføring af autorisationer.

Serviceanvender er forpligtet til at stille alle nødvendige oplysninger til rådighed for SDS i forbindelse med denne kontrol.

Der henvises i øvrigt til bestemmelserne i databeskyttelsesforordningen³ og databeskyttelseslovens⁴ vedrørende denne databehandling.

³ EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse).

⁴ Lov nr. 502 af 23/05/2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.