STATENS SERUM INSTITUT | NATIONAL SUNDHEDS-IT

NSP Servicevilkår for
Indirekte GW LEVERANDØR

Parter

Denne aftale om at anvende den Nationale Serviceplatform (NSP) er indgået mellem Statens Serum Institut (SSI) v/National Sundheds-it (NSI) som systemansvarlig organisation for NSP og LPS leverandør

LEVERANDØRNAVN
ADRESSE
POSTNR BY
CVR

på vegne af de i bilag 1 oplistede serviceanvendere af data og/eller services der udbydes på NSP.

Specifikke vilkår for LPS-leverandører og deres kunder ifm. anvendelse af data og services på NSP

LPS-leverandør indestår for til enhver tid at overholde gældende love, regler mv. omkring håndtering af persondata. LPS-leverandøren er forpligtet til at holde sig orienteret omkring den nationale sikkerhedsinfrastruktur samt til at sikre, at incidents i et LPS-system ikke medfører afledte incidents i andre systemer eller i infrastrukturen. LPS-leverandøren er således forpligtet til at opretholde det fornødne support-beredskab til at kunne håndtere incidents på forsvarlig vis, og er forpligtet til at orientere NSI uden ugrundet ophold, hvis der forekommer incidents, der kan have betydning for den nationale infrastruktur eller andre systemer. I tilfælde af konkrete incidents skal LPS-leverandøren kunne afbryde adgangen til den nationale infrastruktur for de enkelte lægepraksis (serviceanvender) som anvender LPS-leverandørens it-løsning for at sikre, at et incident begrænses til færrest muligt lokationer.

LPS-leverandør indestår for, at der i LPS-leverandørens kundevilkår optages bestemmelser, der på tydelig vis forpligter de lægepraksis som anvender LPS-leverandørens it-løsning (herefter benævnt serviceanvender) til at

- overholde de generelle NSP servicevilkår, samt de specifikke servicevilkår der er gældende for de services som LPS-leverandøren udbyder sin it-løsning til,

- overholde de fastlagte regler for brug af Sundhedsdatanettet[1],

- 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 LPS-leverandøren i tilfælde af formodede eller konstaterede sikkerhedsbrud med henblik på at sikre størst mulig begrænsning af skaden.

I forhold til NSP optræder den enkelte lægepraksis som service anvender. 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 LPS-leverandøren, hvoraf det fremgår, at LPS-leverandøren (databehandler) alene handler efter instruks fra Serviceanvender (sundhedsorganisationer eller sundhedspersoner dvs. den dataansvarlige), og at reglerne i persondatalovens § 41, stk. 3-5, ligeledes gælder for behandlingen ved databehandleren.

Hvis databehandleren er etableret i en anden medlemsstat, skal det fremgå af aftalen, at de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den medlemsstat, hvor databehandleren er etableret, gælder for denne, og at de procedurer, der er beskrevet i bilag 2, overholdes. NSI kan på ethvert tidspunkt udbede sig databehandleraftalerne.

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

[1] http://www.medcom.dk/wm111781

Hvis en Serviceanvender, eller dennes databehandler, ikke retter sig efter de i denne aftale udstukne retningslinjer for sikkerhed eller overtræder persondataloven, forbeholder NSI sig ret til at frakoble adgangen, indtil NSI finder at der fra Serviceanvender og LPS-leverandørs side, er betryggende sikkerhed for overholdelse af kravene. Det samme gælder, hvis der i øvrigt konstateres misbrug af adgangen.

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

LPS-leverandøren må ikke overdrage rettigheder og forpligtelse i medfør af denne aftale til tredjemand uden NSI's forudgående skriftlige samtykke.

Underskrift

For LPS-leverandør på vegne af de i bilag 1 oplistede modtagere af data og/eller services.

Dato	
Navn	
E-mail	
Titel og organisatorisk placering	
Underskrift	

For NSI

Dato	
Navn	
E-mail	
Titel og organisatorisk placering	Systemejer, NSP – National Service platform It udvikling og projekter Sektor for National Sundheds-it
Underskrift	

Bilag 1

Liste over de LPS Kunder (serviceanvendere), som LPS leverandør har indgået denne aftale med NSI på vegne af.

Instruks for listens indhold og opdatering:

Bilaget skal udfyldes med navn, adresse og CVRnr./autorisations-ID for samtlige Serviceanvendere (sundhedsorganisationer eller sundhedspersoner), som oplysningerne vil blive givet til.

Bilag 2

Instruks for adgangskontrol

Sikkerhedsforanstaltninger hos Serviceanvender

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 over for systemet for at få adgang til data og services der udbydes på NSP i overensstemmelse med krav til certifikater i relation til SOSI infrastruktur på NSP.

- Bliver slutbrugeren bekendt med, at certifikatet er blevet kompromitteret, skal den pågældende uden unødigt ophold sikre, at certifikatet spærres.

- 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.

Der henvises i øvrigt til Datatilsynets vejledning til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning for nærmere detaljer med hensyn til krav til autorisation mv.

NSI kan føre kontrol med Serviceanvenders varetagelse af sikkerheden, herunder adgangskontrollen og ajourføring af autorisationer.