Digifys DK A/S

Databehandleraftale

Mellem

Klinikker i Danmark, der anvender www.digifys.com,
(herefter "Klinikken")

og

Digifys DK A/S
Brovej 20A
8800 Viborg
CVR: 36401702
(herefter "Leverandøren")

gælder nedenstående databehandleraftale (herefter "Aftalen") om Leverandørens behandling af personoplysninger på vegne af Klinikken:

Indhold

1. Generelt

1.1 Den 25. maj 2018 erstattes Persondataloven af Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 (herefter Databeskyttelsesforordningen). Denne aftale vedrører leverandørens forpligtelse til at efterleve de sikkerhedskrav, som fremgår af Databeskyttelsesforordningen og Databeskyttelsesloven.

1.2 I Aftalen er indarbejdet de krav, som Databeskyttelsesforordningen stiller til databehandleraftaler.

2. Formål

2.1 Leverandøren behandler i medfør af Klinikkens køb af adgang til www.digifys.com personoplysninger for Klinikken.

3. Klinikkens rettigheder og forpligtelser

3.1 Klinikken er dataansvarlig for de personoplysninger, som Klinikken instruerer Leverandøren om at behandle.

3.2 Klinikken har de rettigheder og forpligtelser, som er givet en dataansvarlig i medfør af lovgivningen, jf. Aftalens pkt. 1.1 og 1.2.

4. Leverandørens forpligtelser

4.1 Leverandøren er databehandler for de personoplysninger, som Leverandøren behandler på vegne af Klinikken, jf. pkt. 6 og bilag 3.

4.2 Leverandøren behandler alene de overladte personoplysninger efter instruks fra Klinikken, jf. pkt. 6 og bilag 3, og alene med henblik på opfyldelse af Klinikkens anvendelse af www.digifys.com.

4.3 Leverandøren skal sikre personoplysningerne via tekniske og organisatoriske sikkerhedsforanstaltninger, som beskrevet i Sikkerhedsbekendtgørelsen og Sikkerhedsvejledningen Databeskyttelsesforordningen jf. bilag 1 – Sikkerhed.

4.4 Leverandøren skal på opfordring fra Klinikken hjælpe med at opfylde Klinikkens forpligtelser i forhold til den registreredes rettigheder, herunder besvarelse af anmodninger fra patienter om indsigt i egne oplysninger, udlevering af patientens oplysninger, rettelse og sletning af oplysninger, begrænsning af behandling af patientens oplysninger, samt Klinikkens forpligtelser i forhold til underretning af den registrerede ved sikkerhedsbrud, jf. Databeskyttelsesforordningens kap. III samt artikel 34.

4.5 Leverandøren skal hjælpe Klinikken med at efterleve dennes forpligtelser efter Databeskyttelsesforordningens artikel 32-36.

4.6 Leverandøren garanterer at levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at implementere passende tekniske og organisatoriske foranstaltninger sådan, at Leverandørens behandling af Klinikkens personoplysninger opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.

5. Underleverandør (underdatabehandler)

5.1 Ved underdatabehandler forstås en underleverandør, til hvem Leverandøren har overladt hele eller dele af den behandling, som Leverandøren foretager på vegne af Klinikken.

5.2 Leverandøren må ikke uden udtrykkelig skriftlig godkendelse fra Klinikken anvende andre underdatabehandlere end dem, der er angivet i bilag 2, herunder foretage udskiftning af disse, til at behandle de personoplysninger, som Klinikken har overladt til Leverandøren i medfør af Aftalen.

5.3 Hvis Leverandøren overlader behandlingen af personoplysninger, som Klinikken er dataansvarlig for, til underdatabehandlere, skal Leverandøren indgå en skriftlig (under)databehandleraftale med underdatabehandleren.

5.4 Underdatabehandleraftalen, jf. pkt. 5.3, skal pålægge underdatabehandleren de samme databeskyttelsesforpligtelser, som Leverandøren er pålagt efter Aftalen, herunder, at underdatabehandleren garanterer at kunne levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at kunne implementere de passende tekniske og organisatoriske foranstaltninger således, at underdatabehandlerens behandling opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.

5.5 Når Leverandøren overlader behandlingen af personoplysninger, som Klinikken er dataansvarlig for, til underdatabehandlere, har Leverandøren over for Klinikken ansvaret for underdatabehandlernes overholdelse af disses forpligtelser, jf. pkt. 5.3.

5.6 Klinikken kan til enhver tid forlange dokumentation fra Leverandøren for eksistensen og indholdet af underdatabehandleraftaler for de underdatabehandlere, som Leverandøren anvender i forbindelse med opfyldelsen af sine forpligtelser over for Klinikken.

6. Instrukser

6.1 Leverandørens behandling af personoplysninger på vegne af Klinikken sker udelukkende efter dokumenteret instruks, jf. bilag 3.

6.2 Leverandøren giver omgående besked til Klinikken, hvis en instruks efter Leverandørens vurdering er i strid med lovgivningen, jf. pkt. 1.1.

7. Tekniske og organisatoriske sikkerhedsforanstaltninger

7.1 Leverandøren skal jf. bilag 1, træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at personoplysninger:

(i) tilintetgøres, mistes, ændres eller forringes,
(ii) kommer til uvedkommendes kendskab eller misbruges, eller
(iii) i øvrigt behandles i strid med lovgivningen, jf. pkt. 1.1

7.2 Leverandøren skal jf. bilag 1, iværksætte alle sikkerhedsforanstaltninger, der kræves for at sikre et passende sikkerhedsniveau.

7.3 Leverandøren er forpligtet til straks at underrette Klinikken om ethvert sikkerhedsbrud uanset, om dette sker hos Leverandøren eller hos en underdatabehandler.

8. Overførsler til andre lande

8.1 Leverandørens overførsel af personoplysninger til lande, der ikke er medlem af EU (tredjelande), f.eks. via en cloudløsning eller en underdatabehandler, skal ske i overensstemmelse med Klinikkens instruks herfor, jf. bilag 3.

9. Tavshedspligt og fortrolighed

9.1 Leverandøren skal sikre, at alle, der behandler oplysninger omfattet af Aftalen, herunder ansatte, tredjeparter (f.eks. en reparatør) og underdatabehandlere, forpligter sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

10. Kontroller og erklæringer

10.1 Leverandøren stiller alle oplysninger, der er nødvendige for at påvise Leverandørens overholdelse af databeskyttelsesforordningens artikel 28 og Aftalen, til rådighed for Klinikken.

10.2 Klinikken, en repræsentant for Klinikken eller dennes revision (såvel intern som ekstern) har adgang til at foretage inspektioner og revision hos Leverandøren, med henblik på at konstatere, at Leverandøren overholder de krav, der følger af denne Aftale.

10.3 Klinikkens tilsyn med underdatabehandlere sker som udgangspunkt gennem Leverandøren. Klinikken skal have samme ret til oplysninger, kontrol og revision overfor underleverandørerne som overfor Leverandøren.

11. Ændringer i Aftalen

11.1 I det omfang ændringer i lovgivningen, jf. pkt 1.1 og 1.2, eller tilhørende praksis, giver anledning til dette, er Klinikken med et varsel på 30 dage og uden at dette medfører krav om betaling fra Leverandøren, berettiget til at foretage ændringer i Aftalen.

12. Sletning af data

12.1 Klinikken træffer beslutning om, hvorvidt der skal ske sletning eller tilbagelevering af personoplysningerne efter, at behandlingen af personoplysningerne er ophørt i medfør af Klinikkens anvendelse af www.digifys.com.

12.2 Klinikken skal senest 30 dage inden anvendelsens ophør skriftligt meddele Leverandøren, hvorvidt alle personoplysningerne skal slettes eller tilbageleveres til Klinikken. I det tilfælde, hvor personoplysningerne tilbageleveres til Klinikken, skal Leverandøren ligeledes slette eventuelle kopier. Leverandøren skal sikre, at eventuelle underdatabehandlere ligeledes efterlever Klinikkens meddelelse.

13. Formkrav

13.1 Aftalen skal foreligge skriftligt, herunder elektronisk på www.digifys.com og hos Leverandøren.

For Leverandøren
Dato: 22/5-18

Navn: Niels Heuer
Titel: Direktør

Bilag:

Bilag 1 – Sikkerhed
Bilag 2 – Oplysninger om lokationer for behandling og underleverandører (underdatabehandlere)
Bilag 3 – Instruks

Bilag 1 – Sikkerhed

Indledning

Dette bilag indeholder en beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, som Leverandøren i medfør af Aftalen har ansvar for at gennemføre, overholde og sikre overholdelse af hos dennes underdatabehandlere, som er angivet i bilag 2.

Generelle sikkerhedsforanstaltninger

Leverandøren gennemfører følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til de aftalte behandlinger, jf. Instruks (bilag 3), og som dermed opfylder Databeskyttelsesforordningens artikel 32.

Sikkerhedsniveauet skal afspejle, at der er tale om behandling af en stor mængde personoplysninger omfattet af databeskyttelsesforordningens artikel 9 om "særlige kategorier af personoplysninger", herunder særligt helbredsoplysninger, hvorfor der skal etableres et "højt" sikkerhedsniveau.

Autorisation og adgangskontrol

Digifys kan kun tilgås af personer med korrekt brugernavn og kodeord.

En klinikbruger (fysioterapeut, receptionist, klinikejer) er alle identificeret via sin e-mailadresse.
Klinikbrugere tildeles et 6 cifret autogenereret kodeord bestående af store og små karakterer inkl. tal. Såfremt en bruger glemmer sit kodeord, kan et nyt kodeord bestilles, hvorved processen med oprettelse af kodeord gentages.

En patient er identificeret via sin e-mailadresse eller sit CPR-nummer.
Patientbrugere tildeles et link i sin velkomst-email, hvor patienten kan angive et kodeord efter eget valg.

Klinikbrugere kan kun tilgå patienter oprettet på klinikken.

Patienter kan kun tilgå egne data.

Udover de brugere, som Klinikken giver adgang til data, er det udelukkende Digifys systemadministrator og Digifys-projektleder, der kan have adgang til data. I tilfælde af support-sager, hvor det af hensyn til at kunne genskabe fejl er nødvendigt, at produktive data tilgås af programmører, bliver data anonymiseret før programmøren tilgår data. Efter end fejlanalyse slettes data umiddelbart.

Omfang af data

En klinik-administrator tildeler autorisation til de enkelte brugere på den enkelte klinik.
En klinik-bruger har adgang til patienter tilhørende kontoen han arbejder på.
En patient har udelukkende adgang til data vedrørende patienten selv.
En klinik-bruger kan udtrække statistik på aktiviteten på sin egen konto (oplys.skemaer, journaler, programmer).
Digifys-administrative brugere (interne brugere, support) har adgang til alle brugeres data.

Eksterne kommunikationsforbindelser

Al kommunikation over internettet sker via krypteret dataoverførsel.
Digifys kører med https/SSL-kryptering.

Overvågning af forsøg på uretmæssig systemadgang

Underdatabehandleren ITPilot ApS foretager overordnet overvågning af netværket, herunder angreb af forskellig art. Det være sig DDoS-angreb, Brute force-angreb, botnet-aktivitet eller forsøg på inficering af websider på netværket ved for eksempel fjern-inklusion af malware og lignende.

Derudover foregår der konstant overvågning af serveren ved hjælp af værktøjer, der måler trafikmængde, forespørgsler og ydeevne. Ved atypiske mønstre notificeres serveradministratorer. Dette er med til at forebygge og forhindre forsøg på uretmæssig adgang.

Ved forgæves loginforsøg låses konti automatisk. Konto kan låses op ved kontakt til Digifys systemadministrator.

Sikkerhedskopiering
Der foretages dagligt sikkerhedskopiering af data liggende i Digifys-systemporteføljen. Dette gælder både databaser og filer, således at eventuelt mistet data vil kunne genskabes. Sikkerhedskopieringer foretages både til en lokal backup-server og til en fjernlokation (remote).

Sikkerhedskopier beholdes i 14 dage.

IT-revision
Digifys hostes af ITPilot ApS, som er underlagt revision af BDO Statsautoriseret aktieselskab.

Som en del af revisionen af et årsregnskab vurderer BDO de risici, som anvendelsen af it indebærer i forhold til regnskabet, og hvordan virksomheden har reageret herpå ved at indføre interne kontroller. I kontrollen af selskabet vurderer BDO, om forsvarlige procedurer er implementerede inden for drift, adgangssikkerhed samt anskaffelse og vedligeholdelse af it-systemer.

It-revision omfatter også en undersøgelse og vurdering af, om det er muligt at fortsætte forretningsdriften i tilfælde af en katastrofe eller et kritisk it-nedbrud, og om relevant lovgivning og regulativer overholdes.

Bilag 2 – Oplysninger om lokationer for behandling og underleverandører (underdatabehandlere)

1. Lokation(er) for behandlingen.

www.Digifys.com-website og database afvikles på egne servere, der fysisk er placeret hos ITPilot ApS, Livøvej 21, 1. sal, 8800 Viborg.

www.Digifys.com-serverne driftes og vedligeholdes af vores underdatabehandlere ITPilot ApS, Livøvej 21, 1.sal., 8800 Viborg.

ITPilot APS anvender en underleverandør til ekstern backup. Den eksterne backuplokation er:

UAB Interneto vizija (Time4VPS)

J. Kubiliaus st. 6

08234 Vilnius

Litauen

Data transmitteres dertil fra datacenter på Livøvej 21, 1.sal, 8800 Viborg via backupsoftware, som krypterer data inden transmission.

www.Digifys.com videreudvikles, vedligeholdes og supporteres af Adevo ApS, Brovej 20A, 8800 Viborg og dennes datterselskaber.

Køb af tilgang til www.Digifys.com faktureres via Visma e-conomic A/S, Langebrogade 1, 1411 København K.

2. Angivelse af underleverandører

Her angiver Leverandøren navn, adresse, cvr-nummer m.m. på underdatabehandlere, jf. pkt. 5.2 i Aftalen.

ITPilot ApS
Livøvej 21, 1.sal
8800 Viborg
CVR-nr.: 30568656
Att. Kenneth Løwe

Adevo ApS
Brovej 20A
8800 Viborg
CVR-nr.: 35633413
Att. Kim Nielsen

Visma e-conomic A/S
Langebrogade 1
1411 København K.
CVR-nr.: 29403473

Bilag 3 – Instruks

Instruks
Klinikken instruerer hermed Leverandøren om at foretage behandling af Klinikkens oplysninger til brug for Klinikkens anvendelse af www.digifys.com.

Overlader Leverandøren behandling af Klinikkens oplysninger til underdatabehandlere, er Leverandøren ansvarlig for at indgå skriftlige (under)databehandleraftaler med disse. Leverandøren er ansvarlig for, at Klinikkens instruks fremsendes til eventuelle underdatabehandlere.

1.1 Behandlingens formål
Behandling af Klinikkens oplysninger sker i henhold til formålet i Klinikkens anvendelse af www.digifys.com.

Leverandøren må ikke anvende oplysningerne til andre formål.

Oplysningerne må ikke behandles efter instruks fra andre end Klinikken.

1.2 Generel beskrivelse af behandlingen
Den typiske proces

En patient henvender sig til en Klinik, patienten oplyser stamdata til klinikken indeholdende navn og CPR-nummer.

Klinikken fremsender adgang til et oplysningsskema til patienten ved at anvende www.digifys.com.

Patienten udfylder oplysningsskemaet ved anvendelse af www.digifys.com.

Ved patientens besøg på klinikken tager terapeuten i sin journalføring i www.digifys.com afsæt i patientens fremsendte oplysningsskema.

Ved den fortsatte kontakt mellem patient og fysioterapeut vedligeholdes patientens journal i www.digifys.com.

Fysioterapeuten kan med www.digifys.com udarbejde et træningsprogram. Træningsprogrammet kan bestå af både video-baserede træningsøvelser optaget af Digifys DK A/S, og fysioterapeuten kan selv optage øvelser med eller uden den specifikke patient til anvendelse i træningsprogrammet.

Patienten tilgår sit træningsprogram i www.digifys.com.

Patienten vil periodisk modtage nye oplysningsskemaer til opfølgning på helbredelse/udvikling fra www.digifys.com.

Efter endt behandling modtager patienten fra www.digifys.com et kundetilfredshedsspørgeskema, der vurderer oplevelsen med klinikken.

Af hensyn til fysioterapeutens pligt til journalføring gemmes data om hver enkelt patient frem til patienten ønsker data slettet. Dette kan tidligst ske 5 år efter endt behandlingsforløb, og vil kun ske efter instruktion fra klinikken.

Patient

Leverandøren behandler følgende oplysninger om patienter:

- Navn
- CPR-nummer
- E-mail
- Telefonkontaktoplysninger
- Helbredsoplysninger omkring patientens lidelse
- Fysioterapeutens journaldata omkring patienten

- Træningsprogram og træningstidspunkter
- Andre helbredsoplysninger

Medarbejdere

Leverandøren behandler oplysninger om medarbejdere, der anvender www.digifys.com.

Som unik nøgle anvendes medarbejderens email-adresse.

Leverandøren behandler følgende oplysninger om medarbejdere:

- Navn
- E-mail
- Telefonkontaktoplysninger

Brugerstyringen foretages af Klinikken.

1.3 Typen af personoplysninger

Behandlingerne indeholder personoplysninger i de nedenfor afkrydsede kategorier. Leverandørens og eventuelle underdatabehandleres niveau for behandlingssikkerhed bør afspejle oplysningernes følsomhed.

Almindelige personoplysninger (jf. Databeskyttelsesforordningens artikel 6)

☒ Almindelige personoplysninger

Følsomme personoplysninger (jf. Databeskyttelsesforordningens artikel 9):

☐ Racemæssig eller etnisk baggrund

☐ Politisk overbevisning

☐ Religiøs overbevisning

☐ Filosofisk overbevisning

☐ Fagforeningsmæssige tilhørsforhold

☒ Helbredsforhold, herunder misbrug af medicin, narkotika, alkohol m.v.

☐ Seksuelle forhold

Oplysninger om enkeltpersoners rent private forhold (jf. Databeskyttelsesforordningens artikel 6 og 9):

☐ Strafbare forhold

☐ Væsentlige sociale problemer

☐ Andre rent private forhold, som ikke er nævnt ovenfor

_____

_____

Oplysninger om cpr-nummer (jf. Databeskyttelsesforordningens artikel 87)

☒ CPR-numre

1.4 Kategorier af registrerede
Der behandles oplysninger om følgende kategorier af registrerede:

A) Patienter, der har henvendt sig til Klinikken.

B) Medarbejdere i Klinikken

1.5 Tredjelande (ikke EU-medlemslande)
Leverandøren overfører ikke personoplysninger til tredjelande.