GDPR-webinar hos Kromann Reumert for PLO-medlemmer og klinikpersonale

08-02-2023

Ved

- Pia Kirstine Voldmester, Partner hos Kromann Reumert
- Kia Hansen, Advokatfuldmægtig hos Kromann Reumert

PRAKTISERENDE
LÆGERS
ORGANISATION

Velkomst

PLO og Kromann Reumert byder indenfor til webinar om GDPR for alle PLO-medlemmer og klinikpersonale.

- Webinaret har til formål at hjælpe medlemmerne videre med arbejdet i egen klinik og svare på relevante juridiske og praktiske spørgsmål i relation til GDPR.

Baggrund for PLO's arbejde med GDPR:

- Alle aktører i sundhedsvæsenet skal efterleve reglerne i GDPR – og mange køber ydelsen dyrt ude i byen.
- PLO's bestyrelse ønsker, at PLO løfter så meget af arbejdet for den enkelte klinikejer som muligt med fælles skabeloner og information.
- Klinikken skal dog selv gøre arbejdet færdigt og tilpasse skabelonerne til de lokale forhold i klinikken for at komme helt i mål.
- Alle PLO's skabeloner og vejledninger til GDPR kan findes på PLO's hjemmeside under ***GDPR i almen praksis***
- Har man spørgsmål til PLO's arbejde med GDPR og hjælp til medlemmerne, kan man rette henvendelse til PLO's sekretariat. Alternativt til praktiserende læge Niels Ulrich Holm, medlem af PLO's bestyrelse og Digitaliseringsudvalg
- Spørgsmål vedrørende journalsystemet, kan rettes til jeres systemhus

Dagens program/Agenda

1.	Overordnede krav – og udleveret materiale fra PLO
2.	Introduktion til databeskyttelsesforordningen (GDPR)
3.	Grundlæggende principper og behandlingsregler
4.	Registreredes rettigheder
5.	Dataansvarlig og databehandler, roller og opgaver
6.	Sikkerhedsbrud
7.	Risikovurderinger

Hvad skal I som praktiserende læger have styr på?

Oplysning (privatlivspolitikker)

Patienterne skal oplyses om, hvordan deres personoplysninger behandles

Behandlingsoversigt (artikel 30-fortegnelse)

I skal dokumentere hvilke patientoplysninger, der behandles i jeres klinik, hvad de anvendes til, og hvem de deles med

Databehandleraftale

I skal sikre, at der foreligger en databehandleraftale mellem klinikken og dit systemhus, og at dens indhold lever op til kravene i forordningen

Tilsyn med databehandlere

Man skal kontrollere om databehandleren lever op til aftalen

Risikovurderinger og sikkerhedsforanstaltninger

I skal sikre, at risici ved behandlingen af personoplysninger er vurderet, og at de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger er implementeret

Sikkerhedsbrud

Sikre logning af sikkerhedsbrud, anmeldelse til Datatilsynet (hvis nødvendigt) og underretning af patienter (hvis nødvendigt)

Sletning

Slette personoplysningerne, når de opbevaring ikke længere er nødvendig

→ Forberedt til tilsynsbesøg

Datatilsynet kan komme på tilsynsbesøg, og her kan de bede om dokumentation for, at I lever op til kravene

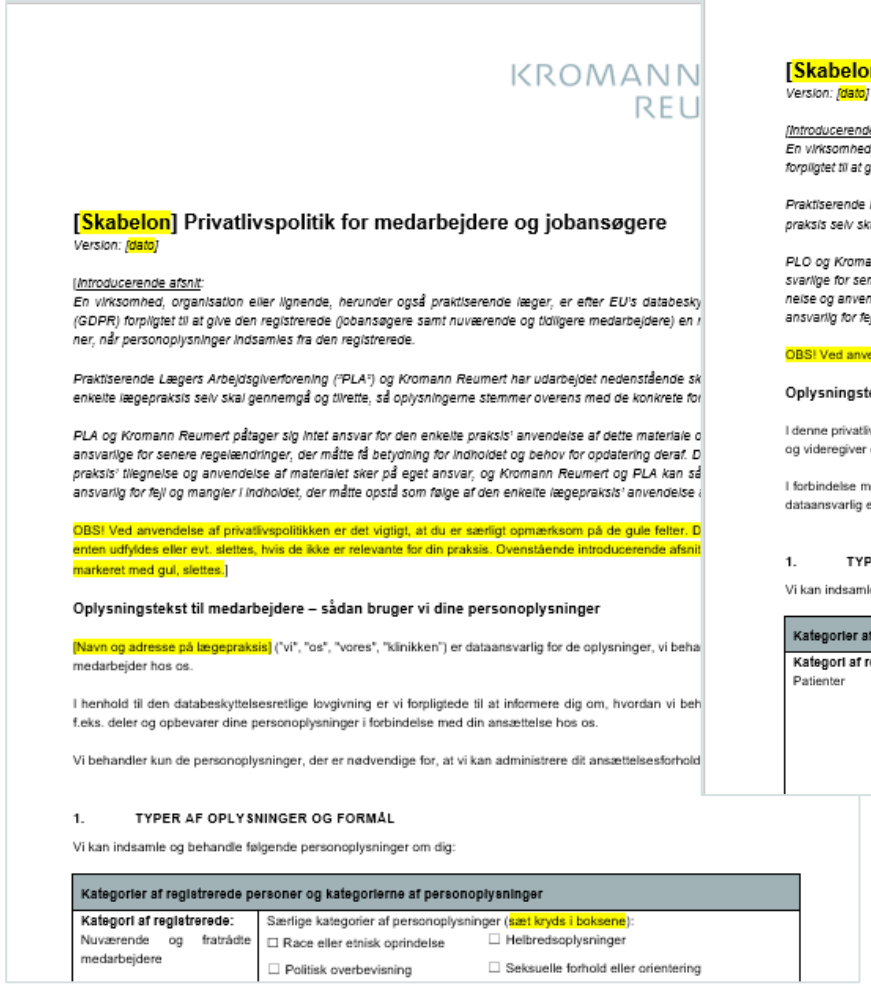
Bare rolig - I bliver hjulpet godt på vej

Udleveret materiale fra PLO:

Skabelon til privatlivspolitikker for både:

- Patienter

- Nuværende og tidligere medarbejdere samt jobansøgere



KROMANN REU

[Skabelon] Privatlivspolitik for medarbejdere og jobansøgere

Version: [dato]

[Introducerende afsnit:
En virksomhed, organisation eller lignende, herunder også praktiserende læger, er efter EU's databesky
(GDPR) forpligtet til at give den registrerede (jobansøgere samt nuværende og tidligere medarbejdere) en r
ner, når personoplysninger indsamles fra den registrerede.

Praktiserende Lægers Arbejdsgiverforening ("PLA") og Kromann Reumert har udarbejdet nedenstående sk
enkelte lægepraksis selv skal gennemgå og tilrette, så oplysningerne stemmer overens med de konkrete for

PLA og Kromann Reumert påtager sig intet ansvar for den enkelte praksis' anvendelse af dette materiale o
ansvarlige for senere regelændringer, der måtte få betydning for indholdet og behov for opdatering deraf. D
praksis' tilegnelse og anvendelse af materialet sker på eget ansvar, og Kromann Reumert og PLA kan så
ansvarlig for fejl og mangler i indholdet, der måtte opstå som følge af den enkelte lægepraksis' anvendelse

OBS! Ved anvendelse af privatlivspolitikken er det vigtigt, at du er særligt opmærksom på de gule felter. D
enten udfyldes eller evt. slettes, hvis de ikke er relevante for din praksis. Ovenstående introducerende afsnit
markeret med gul, slettes.]

Oplysningstekst til medarbejdere – sådan bruger vi dine personoplysninger

[Navn og adresse på lægepraksis] ("vi", "os", "vores", "klinikken") er dataansvarlig for de oplysninger, vi beha
medarbejder hos os.

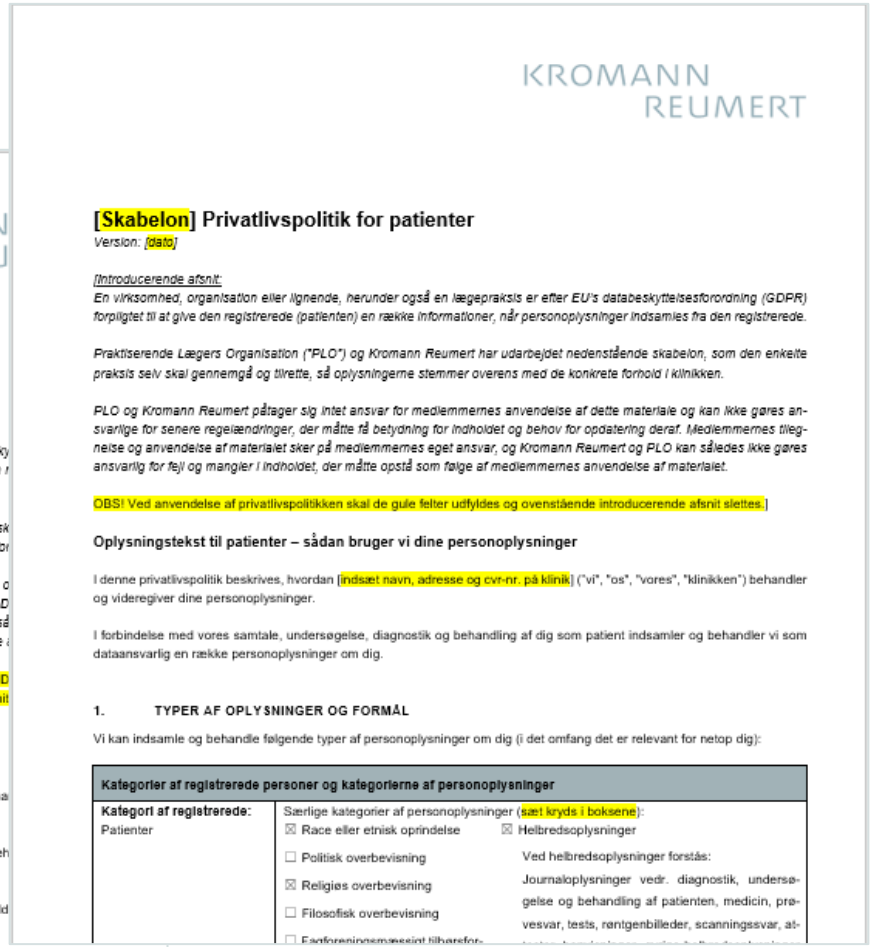
I henhold til den databeskyttelsesretlige lovgivning er vi forpligtede til at informere dig om, hvordan vi beh
f.eks. deler og opbevarer dine personoplysninger i forbindelse med din ansættelse hos os.

Vi behandler kun de personoplysninger, der er nødvendige for, at vi kan administrere dit ansættelsesforhold

1. TYPER AF OPLYSNINGER OG FORMÅL

Vi kan indsamle og behandle følgende personoplysninger om dig:

Kategorier af registrerede personer og kategorierne af personoplysninger	
Kategori af registrerede: Nuværende og fratrådte medarbejdere	Særlige kategorier af personoplysninger (sæt kryds i boksene): ☐ Race eller etnisk oprindelse ☐ Helbredsoplysninger ☐ Politisk overbevisning ☐ Seksuelle forhold eller orientering



KROMANN REUMERT

[Skabelon] Privatlivspolitik for patienter

Version: [dato]

[Introducerende afsnit:
En virksomhed, organisation eller lignende, herunder også en lægepraksis er efter EU's databeskyttelsesforordning (GDPR) forpligtet til at give den registrerede (patienten) en række informationer, når personoplysninger indsamles fra den registrerede.

Praktiserende Lægers Organisation ("PLO") og Kromann Reumert har udarbejdet nedenstående skabelon, som den enkelte praksis selv skal gennemgå og tilrette, så oplysningerne stemmer overens med de konkrete forhold i klinikken.

PLO og Kromann Reumert påtager sig intet ansvar for medlemmernes anvendelse af dette materiale og kan ikke gøres ansvarlige for senere regelændringer, der måtte få betydning for indholdet og behov for opdatering deraf. Medlemmernes tilegnelse og anvendelse af materialet sker på medlemmernes eget ansvar, og Kromann Reumert og PLO kan således ikke gøres ansvarlig for fejl og mangler i indholdet, der måtte opstå som følge af medlemmernes anvendelse af materialet.

OBS! Ved anvendelse af privatlivspolitikken skal de gule felter udfyldes og ovenstående introducerende afsnit slettes.]

Oplysningstekst til patienter – sådan bruger vi dine personoplysninger

I denne privatlivspolitik beskrives, hvordan [indsæt navn, adresse og cvr-nr. på klinik] ("vi", "os", "vores", "klinikken") behandler og videregiver dine personoplysninger.

I forbindelse med vores samtale, undersøgelse, diagnostik og behandling af dig som patient indsamler og behandler vi som dataansvarlig en række personoplysninger om dig.

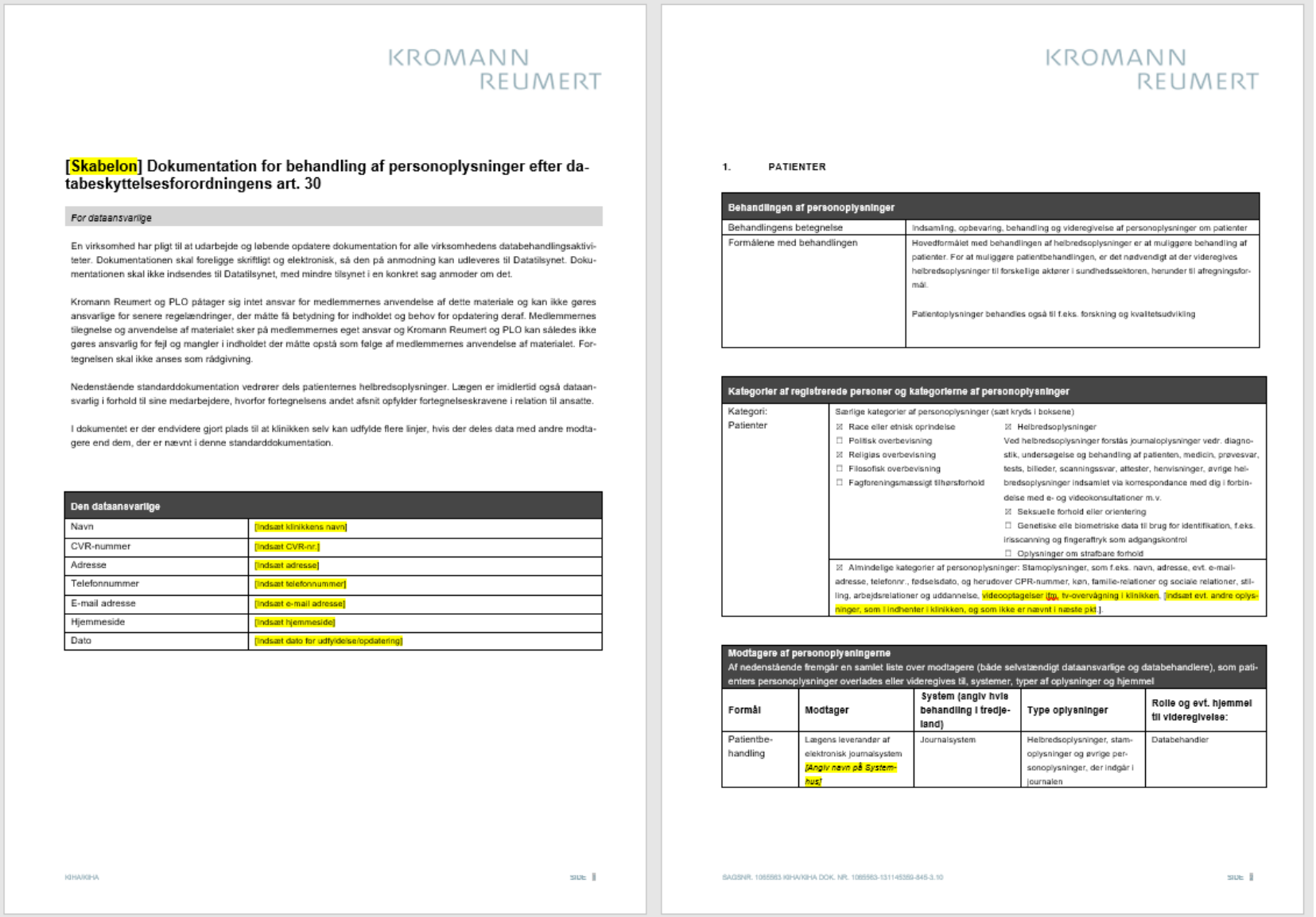
1. TYPER AF OPLYSNINGER OG FORMÅL

Vi kan indsamle og behandle følgende typer af personoplysninger om dig (i det omfang det er relevant for netop dig):

Kategorier af registrerede personer og kategorierne af personoplysninger	
Kategori af registrerede: Patienter	Særlige kategorier af personoplysninger (sæt kryds i boksene): ☒ Race eller etnisk oprindelse ☒ Helbredsoplysninger ☐ Politisk overbevisning ☒ Religiøs overbevisning ☐ Filosofisk overbevisning Ved helbredsoplysninger forstås: Journaloplysninger vedr. diagnostik, undersøgelse og behandling af patienten, medicin, prøvesvar, tests, røntgenbilleder, scanningssvar, at-

Udleveret materiale fra PLO:

Skabelon til dokumentation for behandling af personoplysninger (artikel 30-fortegnelse)



KROMANN REUMERT

[Skabelon] Dokumentation for behandling af personoplysninger efter databeskyttelsesforordningens art. 30

For dataansvarlige

En virksomhed har pligt til at udarbejde og løbende opdatere dokumentation for alle virksomhedens databehandlingsaktiviteter. Dokumentationen skal foreligge skriftligt og elektronisk, så den på anmodning kan udleveres til Datatilsynet. Dokumentationen skal ikke indsendes til Datatilsynet, med mindre tilsynet i en konkret sag anmoder om det.

Kromann Reumert og PLO påtager sig intet ansvar for medlemmernes anvendelse af dette materiale og kan ikke gøres ansvarlige for senere regelændringer, der måtte få betydning for indholdet og behov for opdatering deraf. Medlemmernes tilegnelse og anvendelse af materialet sker på medlemmernes eget ansvar og Kromann Reumert og PLO kan således ikke gøres ansvarlig for fejl og mangler i indholdet der måtte opstå som følge af medlemmernes anvendelse af materialet. Fortegnelsen skal ikke anses som rådgivning.

Nedenstående standarddokumentation vedrører dels patienternes helbredsoplysninger. Lægen er imidlertid også dataansvarlig i forhold til sine medarbejdere, hvorfor fortegnelsens andet afsnit opfylder fortegnelseskravene i relation til ansatte.

I dokumentet er der endvidere gjort plads til at klinikken selv kan udfylde flere linjer, hvis der deles data med andre modtagere end dem, der er nævnt i denne standarddokumentation.

Den dataansvarlige	
Navn	[indsæt klinikkens navn]
CVR-nummer	[indsæt CVR-nr.]
Adresse	[indsæt adresse]
Telefonnummer	[indsæt telefonnummer]
E-mail adresse	[indsæt e-mail adresse]
Hjemmeside	[indsæt hjemmeside]
Dato	[indsæt dato for udfyldelse/opdatering]

KIHA/KIHA

SIDE

KROMANN REUMERT

1. PATIENTER

Behandlingen af personoplysninger	
Behandlingens betegnelse	Indsamling, opbevaring, behandling og videregivelse af personoplysninger om patienter
Formålene med behandlingen	Hovedformålet med behandlingen af helbredsoplysninger er at muliggøre behandling af patienter. For at muliggøre patientbehandlingen, er det nødvendigt at der videregives helbredsoplysninger til forskellige aktører i sundhedssektoren, herunder til afregningsformål. Patientoplysninger behandles også til f.eks. forskning og kvalitetsudvikling

Kategorier af registrerede personer og kategorierne af personoplysninger		
Kategori: Patienter	Særlige kategorier af personoplysninger (sæt kryds i boksene) ☒ Race eller etnisk oprindelse ☐ Politisk overbevisning ☒ Religiøs overbevisning ☐ Filosofisk overbevisning ☐ Fagforeningsmæssigt tilhørsforhold	☒ Helbredsoplysninger Ved helbredsoplysninger forstås journaloplysninger vedr. diagnostik, undersøgelse og behandling af patienten, medicin, prøvesvar, tests, billeder, scanningssvar, attester, henvisninger, øvrige helbredsoplysninger indsamlet via korrespondance med dig i forbindelse med e- og videokonsultationer m.v. ☒ Seksuelle forhold eller orientering ☐ Genetiske elle biometriske data til brug for identifikation, f.eks. irisscanning og fingeraftryk som adgangskontrol ☐ Oplysninger om strafbare forhold
	☒ Almindelige kategorier af personoplysninger: Stamoplysninger, som f.eks. navn, adresse, evt. e-mail-adresse, telefonnr., fødselsdato, og herudover CPR-nummer, køn, familie-relationer og sociale relationer, stilling, arbejdsrelationer og uddannelse, videooptagelser (fx. tv-overvågning i klinikken, [indsæt evt. andre oplysninger, som I indhenter i klinikken, og som ikke er nævnt i næste pkt.].	

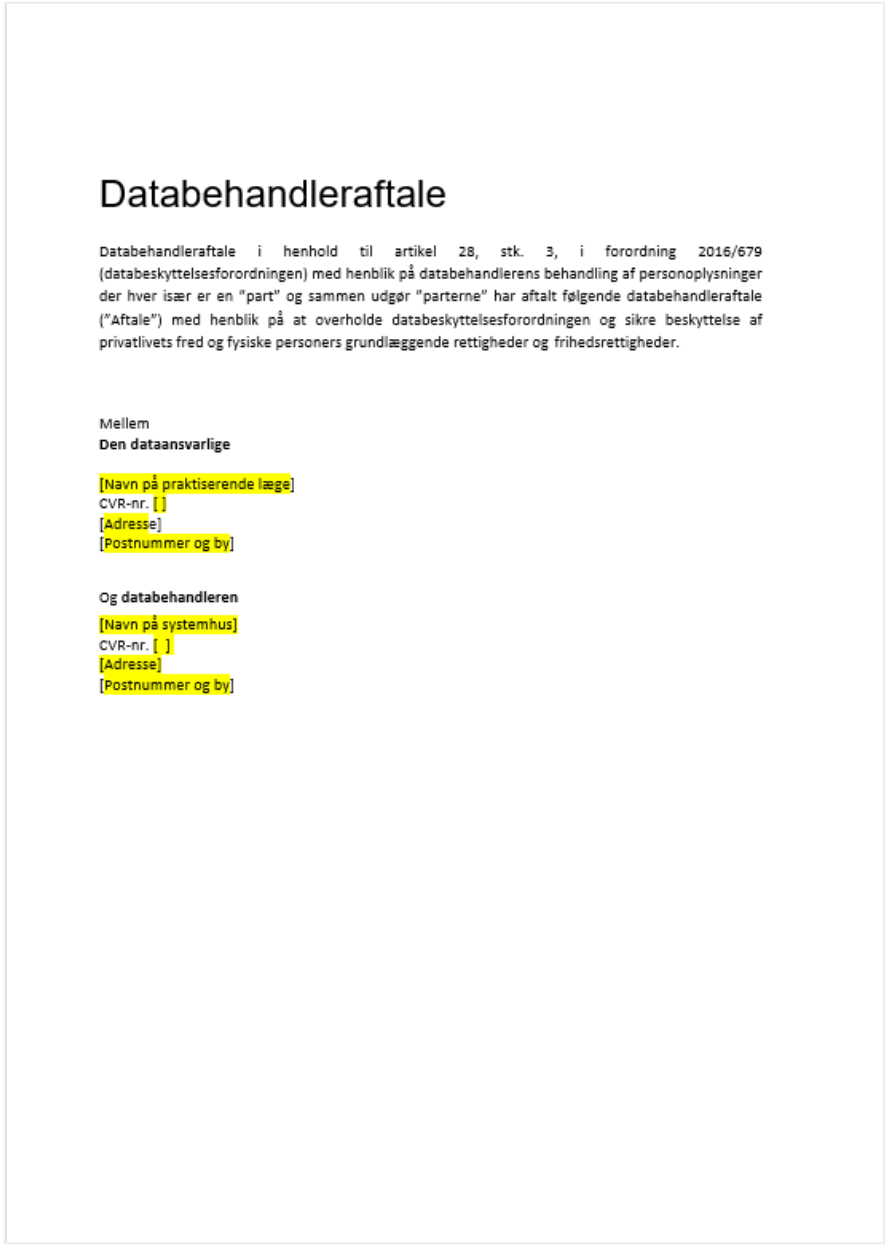
Modtagere af personoplysningerne Af nedenstående fremgår en samlet liste over modtagere (både selvstændigt dataansvarlige og databehandlere), som patienters personoplysninger overlades eller videregives til, systemer, typer af oplysninger og hjemmel				
Formål	**Modtager**	**System (angiv hvis behandling i tredjeland)**	**Type oplysninger**	**Rolle og evt. hjemmel til videregivelse:**
Patientbehandling	Lægens leverandør af elektronisk journalsystem *[Angiv navn på Systemhus]*	Journalsystem	Helbredsoplysninger, stamoplysninger og øvrige personoplysninger, der indgår i journalen	Databehandler

SAGSNR. 1065983 KIHA/KIHA DOK. NR. 1065983-131146389-845-3.10

SIDE

Udleveret materiale fra PLO:

Skabelon til databehandleraftale med systemhusene



Databehandleraftale

Databehandleraftale i henhold til artikel 28, stk. 3, i forordning 2016/679 (databeskyttelsesforordningen) med henblik på databehandlerens behandling af personoplysninger der hver især er en "part" og sammen udgør "parterne" har aftalt følgende databehandleraftale ("Aftale") med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder.

Mellem
Den dataansvarlige

[Navn på praktiserende læge]
CVR-nr. [ ]
[Adresse]
[Postnummer og by]

Og **databehandleren**

[Navn på systemhus]
CVR-nr. [ ]
[Adresse]
[Postnummer og by]

Udleveret materiale fra PLO:

Tilsynsrapporter for systemhusene

Alle tilsyn er afsluttet for 2021-2022

Udleveret materiale fra PLO:

Skabelon til risikovurderinger (omfatter al behandling af personoplysninger i klinikken)

Ledsaget af vejledning til jer

Risikovurdering af behandlingsaktiviteten: *2. Patientbehandling – journalsystem og attester*

Beskrivelse	
Eventuelle systeme	Lægeklinikkens journalsystem (leveres af systemhus)

Dato for udarbejdelse og godkendelse	
Risikovurdering udarbejdet eller genbesøgt:	*Dato, navn, titel*

Ref. ID	Risiko	Sandsynlighed for trussel før afhjælpende foranstaltninger (1-4)	Begrundelse for sandsynlighed før afhjælpende foranstaltninger	Konsekvens af trussel før afhjælpende foranstaltninger (1-4)	Konsekvens beskrivelse før afhjælpende foranstaltninger	Samlet risiko før afhjælpende foranstaltninger	Accepteres risikoen?
1	Indtastning af forkerte oplysninger i journal Der er en generel risiko for, at personoplysninger om patienter, herunder helbredsoplysninger, tastes forkert ind i en journal, f.eks. når oplysningerne gives via telefon eller videokonsultationer, men også ved konsultationer i klinikken.	2	Medarbejdere i lægeklinikken er meget opmærksomme på, at oplysninger skal indtastes korrekt i journalen, da dette er væsentligt for at sikre korrekt sygdomshistorik samt sikre, at f.eks. korrekt medicin ordineres. Det vurderes derfor, at sandsynligheden er lav, men der kan dog forekomme menneskelige fejl.	4	Det kan have kritiske konsekvenser for patienten, hvis truslen indtræffer, da det i værste fald kan betyde, at patienten vil modtage fejlbehandling eller helt manglende behandling	⚠ 8	Risikoen overvåges (Forekomsten af hændelser overvåges via sikkerhedsbrudslog)
2	Indtastning af korrekte oplysninger i forkerte felter Der er en generel risiko for, at personoplysninger om patienter, f.eks. talværdier, tastes ind i forkerte felter i journalen	2	Medarbejdere i lægeklinikken er meget opmærksomme på, at oplysninger skal indtastes i korrekte felter, da dette er væsentligt for at sikre en korrekt journal. Det vurderes derfor, at sandsynligheden er lav, men der kan dog forekomme menneskelige fejl.	4	Det kan have kritiske konsekvenser for patienten, hvis truslen indtræffer, da det potentielt kan betyde, at visse vigtige oplysninger om f.eks. patientens helbred ikke fremvises for lægen, hvilket kan medføre risiko for f.eks. fejlbehandling	⚠ 8	Risikoen overvåges (Forekomsten af hændelser overvåges via sikkerhedsbrudslog)
			Der er meget lav				

Udleveret materiale fra PLO:

Sikkerhedsbrudslog

Nr.	Dato, sted og tidspunkt for sikkerhedsbruddet	Hvornår blev sikkerhedsbruddet opdaget?	Hvad er årsagen til sikkerhedsbruddet?	Hvad skete der i forbindelse med buddet?	Hvilke typer personoplysninger omfattede sikkerhedsbruddet?	Hvilke konsekvens sikkerhedsbrudde registrerede (dvs. personoplysninge sikkerhedsbrudde
	Indsæt dato, tid og sted.	*Indsæt dato, tid og sted.*	*Beskriv årsagen til sikkerhedsbruddet f.eks. phishing eller tyveri.*	*Giv en overordnet beskrivelse af sikkerhedsbruddet.*	*F.eks. navn, kontaktoplysninger, helbredsoplysninger, CPR-nummer.*	*F.eks. kan sikkerhed identitetstyveri, skad økonomiske tab*
1						
2						
3						
4						
5						

Kommer snart fra PLO:

- Informationsbrev om sletning af personoplysninger i klinikkerne
- One-pager med gode råd om sletning
- Bilag med oversigt over vejledende sletteregler, der både omfatter personoplysninger om:
  - Jobansøgere
  - Tidligere og nuværende medarbejdere
  - Patienter

Dagens program/Agenda

1.	Overordnede krav – og udleveret materiale fra PLO
2.	Introduktion til databeskyttelsesforordningen (GDPR)
3.	Grundlæggende principper og behandlingsregler
4.	Registreredes rettigheder
5.	Dataansvarlig og databehandler, roller og opgaver
6.	Sikkerhedsbrud
7.	Risikovurderinger

Definitioner | Hvem er omfattet?

Registrerede personer

Fysiske personer (uanset nationalitet og bopæl)

- F.eks. patienter, medarbejdere, jobansøgere

GDPR beskytter ikke juridiske personer

- Bortset fra enkeltmandsvirksomheder og I/S'er

Hvem skal overholde forordningen?

- Private virksomheder (uanset selskabsform)
- Offentlige myndigheder
- Organisationer

- Private personer skal ikke overholde reglerne, når der er tale om rent personlige og familiemæssige aktiviteter

Hvad er personoplysninger?

Enhver form for information om en identificeret eller identificerbar fysisk person (”den registrerede”)

Eksempler:

- ✓ Navn, adresse, telefonnummer, stilling
- ✓ Køn, fødselsdato
- ✓ Sygdomslidelser / diagnoser
- ✓ Medicinforbrug
- ✓ Handicap
- ✓ Misbrug af narkotika, alkohol eller andre nydelsesmidler
- ✓ Sociale forhold
- ✓ Osv.

Hvad er en behandling?

Enhver aktivitet eller række af aktiviteter – med eller uden brug af automatisk behandling – som personoplysninger eller en samling af personoplysninger gøres til genstand for.

F.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse.

- Elektronisk behandling af personoplysninger
- Manuel behandling af personoplysninger i et register

Kategorier af personoplysninger

Almindelige personoplysninger	• Navn, adresse, telefonnummer, e-mail mv. • Alle andre oplysninger end de særlige kategorier (f.eks. er almindelige oplysninger også private forhold som ulykkestilfælde, selvmordsforsøg, adoptionsforhold mv.)
Særlige kategorier af personoplysninger	• F.eks. Racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold, helbredsmæssige og seksuelle forhold • Genetiske og biometriske data, ved behandling mhp. identifikation
Straffeattester mv.	• Behandling for private virksomheder kræver lovhjemmel • Samtykkets skæbne uvis

CPR-nr.	• Databeskyttelseslovens § 11: CPR-nummer kan bl.a. behandles, hvis:
	  • behandling er fastsat i lov
	  • hvis der er givet udtrykkeligt samtykke

Dagens program/Agenda

1.	Overordnede krav – og udleveret materiale fra PLO
2.	Introduktion til databeskyttelsesforordningen (GDPR)
3.	Grundlæggende principper og behandlingsregler
4.	Registreredes rettigheder
5.	Dataansvarlig og databehandler, roller og opgaver
6.	Sikkerhedsbrud
7.	Risikovurderinger

Grundlæggende principper for al behandling af personoplysninger

Ansvarlighed

Lovlighed, rimelighed og gennemsigtighed

- Lovlig, rimelig og gennemsigtig over for den registrerede

Datakvalitet

- Oplysningerne skal være rigtige og om nødvendigt ajourførte
- Der skal tages ethvert rimelig skridt for at sikre, at personoplysninger, der er urigtige, omgående slettes eller berigtiges

Formålsbegrænsning

- Indsamling af oplysninger skal ske til udtrykkeligt angivne og legitime formål, og senere behandling må ikke være uforenelig med disse formål.
- Statistiske formål (mv.) som udgangspunkt forenelige

Sletning

- Oplysningerne skal opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end formålet tilsiger

Dataminimering

- Oplysningerne skal være relevante, tilstrækkelige og begrænset til hvad der er nødvendigt i forhold til formålene
- ”Kan vi nå formålet med færre oplysninger?”

Integritet og fortrolighed

- Tilstrækkelig sikkerhed for personoplysninger, herunder mod ubemyndiget eller ulovlig behandling og mod hændeligt tab, ødelæggelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger

Behandling af patientoplysninger

Hvornår må I behandle patientoplysninger?

Udvalgte behandlingsgrundlag

1. **Samtykke**
   Patienten har givet sit udtrykkelige samtykke til, at personoplysningerne må behandles
   Sundhedslovens regler om videregivelse af patientoplysninger

2. **Retlig forpligtelse**
   Nødvendigt for at kunne opfylde en retlig forpligtelse. Journalføringsbekendtgørelsens regler om patientjournalens indhold. Receptbekendtgørelsens regler om receptens indhold

3. **Nødvendig, for at retskrav kan fastlægges, gøres gældende eller forsvares**
   Kun aktuelt, hvis der er en igangværende tvist

4. **Anden hjemmel i særlovgivning**

Behandling af oplysninger efter særlovgivning

Hvornår må I efter særlovgivningen behandle personoplysninger?

Udvalgte særlove

- **Oplysninger til brug for journalføring/patientbehandling**
  - Autorisationsloven kap. 6
  - Journalføringsbekendtgørelsen §§ 5-10
  - Sundhedslovens kap. 9
- **Arbejdsskader**
  - Arbejdsskadesikringsloven § 34
- **Indberetning af bivirkninger**
  - Bekendtgørelse vedr. indberetning af bivirkninger ved lægemidler §§ 4-5
- **Oplysninger vedr. recepter**
  - Sundhedsloven
  - Receptbekendtgørelsen
- **Indberetning til kliniske kvalitetsdatabaser**
  - Sundhedslovens §§ 195-196
  - Bekendtgørelse om indberetning af oplysninger til kliniske kvalitetsdatabaser mv.
- **Epikriser**
  - Sundhedslovens § 41

Samtykke som behandlingsgrundlag

Kravene til samtykke efter GDPR

Et samtykke skal være:

1. **Frivilligt |** Et reelt frit valg
2. **Specifikt |** Et afgrænset sæt behandlingsaktiviteter
3. **Informeret |** Patienten skal vide, hvad der gives samtykke til
4. **Utvetydigt** (nogle gange udtrykkeligt) **|** Der må ikke være tvivl om, hvorvidt patienten har afgivet samtykke

NB: Samtykke er ikke altid nødvendigt

Særligt om sletning af journaloplysninger

Efter journalføringsbekendtgørelsen

Udgangspunkterne (§§ 35 og 36)

- Opbevares i mindst 10 år fra seneste optegnelse i patientjournalen
- Røntgenbilleder og andet billeddiagnostisk materiale opbevares i mindst 5 år

Ved ophør af behandlingsstedet (uden overdragelse af behandlingsstedet til fortsat drift) (§§ 38 og 39):

- Overdrages til Styrelsen for Patientsikkerhed til fortsat opbevaring inden for opbevaringsperioden, eller
- Til patientens nye praktiserende læge til fortsat opbevaring, hvis patienten tilkendegiver, at patienten ønsker dette

Ved overdragelse af behandlingssted til fortsat drift (§§ 41-44):

- Patientjournaler overdrages til fortsat opbevaring hos den, der overtager behandlingsstedet, eller
- Hvis overdragelsen til fortsat drift ikke er effektueret, inden den sundhedsfaglige behandling på stedet er ophørt, kan journalen opbevares på behandlingsstedet i op til 6 måneder, indtil overdragelse har fundet sted.

Ved patientens skifte til nyt behandlingssted (uden ophør eller overdragelse af behandlingsstedet) (§ 46):

- Hvis patienten samtykker: Journalen overdrages til det nye behandlingssted til fortsat opbevaring indtil udløbet af opbevaringsperioden
- Hvis patienten ikke samtykker: Journalen opbevares fortsat i opbevaringsperioden:

Ved igangværende tvister (§ 35, stk. 5):

- Opbevares minimum i den normale opbevaringsperiode, og derefter så længe, at patientens sag verserer

Dagens program/Agenda

1.	Overordnede krav – og udleveret materiale fra PLO
2.	Introduktion til databeskyttelsesforordningen (GDPR)
3.	Grundlæggende principper og behandlingsregler
4.	Registreredes rettigheder
5.	Dataansvarlig og databehandler, roller og opgaver
6.	Sikkerhedsbrud
7.	Risikovurderinger

Registreredes rettigheder | Overblik

Oplysningspligt (udvidet)

Ret til – uden forespørgsel – at blive oplyst om behandling af oplysninger om ham/hende

Indsigt (udvidet)

Ret til – på forespørgsel – at få indsigt i hvilke personoplysninger, den dataansvarlige behandler

Berigtigelse

Ret til at få urigtige oplysninger berigtiget

Sletning

Ret til at få slettet oplysninger om ham/hende selv (”retten til at blive glemt”)

Begrænsning

Ret til at kræve begrænsning af behandling (”blokering”) i en periode

Dataportabilitet

Ret til at oplysninger afgivet af vedkommende selv med til en ny leverandør

Indsigelse

Ret til at gøre indsigelse mod behandling af hans/hendes personoplysninger

Automatisk individuel beslutningstagning

Ret til ikke at blive underlagt automatisk, individuel beslutningstagning

Oplysningspligt – hver skal der oplyses om?

1. Den dataansvarliges identitet og kontaktoplysninger
2. Formålene med behandlingen af oplysningerne
3. Behandlingsgrundlaget – f.eks. om afgivelsen af personoplysninger følger af lov eller er nødvendig for at indgå en kontrakt
4. De legitime interesser, som forfølges
5. Kategorierne af modtagere (f.eks. videregivelse til politi, skat mv.)
6. Evt. overførsler til tredjelande
7. Opbevaringsperioden eller, hvis det ikke er muligt, kriterierne herfor
8. Den registreredes rettigheder
9. Retten til at klage til en tilsynsmyndighed
10. Evt. brug af automatiserede beslutningsprocesser (profilering), meningsfuld information om den bagvedliggende logik og konsekvenserne/betydningen for den registrerede
11. Kilde til oplysninger – indsamles de hos den registrerede selv eller hos andre?

Indsigtsret efter GDPR og aktindsigt efter sundhedsloven

GDPR art. 15

Den registrerede har krav på at få oplyst, om der behandles oplysninger vedrørende den pågældende og – i bekræftende fald – også hvilke oplysninger, der behandles, og ”kontekstuelle oplysninger” om:

Formålene med behandlingen

- Kategorier af personoplysninger
- Kategorier af modtagere, navnlig modtagere i tredjelande eller internationale organisationer
- Opbevaringsperiode og, hvis det ikke er muligt, kriterierne herfor
- Retten til at anmode om berigtigelse eller sletning, begrænsning og retten til at gøre indsigelse
- Retten til at klage til en tilsynsmyndighed
- Tilgængelig information om kilderne til informationen
- Forekomsten af automatiske afgørelser, herunder profilering, og meningsfulde oplysninger om den bagvedliggende logik og de forventede konsekvenser for den registrerede
- Oplysning om overførsel til tredjelande og de trufne foranstaltninger efter overførselsreglerne

Sundhedslovens §§ 36-39

Patienten har på anmodning ret til aktindsigt i patientjournalen. Patienten har herudover på anmodning ret til på en let forståelig måde at få meddelelse om:

- Hvilke oplysninger der behandles i patientjournalen
- Formålet med behandlingen
- Kategorierne af modtagere af oplysningerne
- Tilgængelig information om, hvorfra disse oplysninger stammer

Aktindsigt kan enten gives elektronisk, eller ved at der gives adgang til gennemsyn af patientjournalen m.v. på stedet eller udleveres en afskrift eller kopi.

Pause – vi er tilbage om 5 minutter

Dagens program/Agenda

1.	Overordnede krav – og udleveret materiale fra PLO
2.	Introduktion til databeskyttelsesforordningen (GDPR)
3.	Grundlæggende principper og behandlingsregler
4.	Registreredes rettigheder
5.	Dataansvarlig og databehandler, roller og opgaver
6.	Sikkerhedsbrud
7.	Risikovurderinger

Eksempler på typiske databehandlere

Elektroniske journalsystemer hos eksterne leverandører (systemhusene)

Ekstern lønadministration

Databehandler og dataansvarlig | Definitioner

Hvorfor er det vigtigt, hvem der er dataansvarlig og databehandler?

1. Den dataansvarlige træffer beslutning om behandlingsform, -formål, og -omfang

2. Databehandleren følger beslutningerne, men har et -begrænset – råderum

3. Kravene til den dataansvarliges dokumentation for behandlingsaktiviteter er mere omfattende

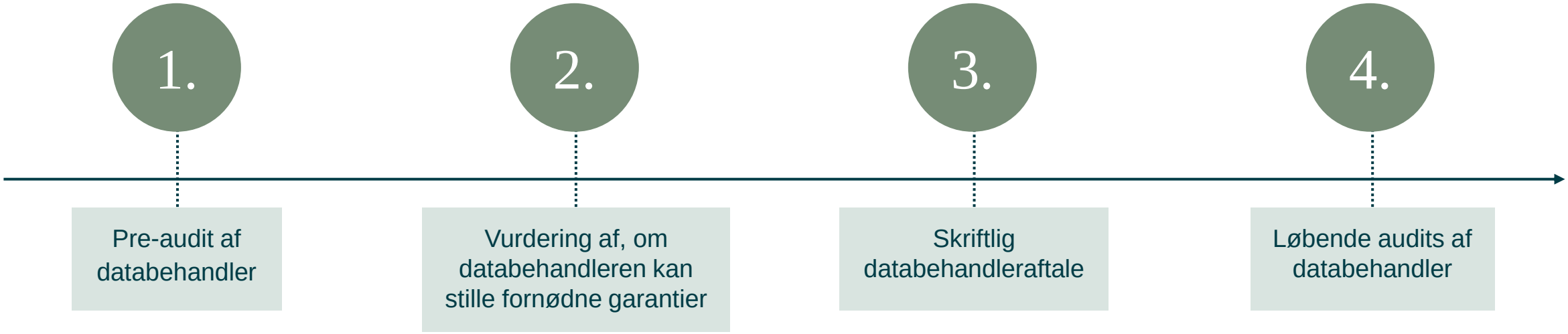
En dataansvarlig skal f.eks.

- foretage pre-audit af databehandleren
- indgå en skriftlig aftale med lovpligtigt indhold med databehandleren
- løbende auditere databehandleren i aftaleforholdet

En databehandler skal f.eks.

- stille sig til rådighed for inspektioner og audits
- indgå underdatabehandleraftaler med sine leverandører
- give information til dataansvarlig f.eks. ved sikkerhedsbrud
- bidrage til dataansvarliges konsekvensanalyser

GDPRs krav for brug af databehandlere



Indholdet i databehandleraftalen

Databehandleraftalen skal indgås skriftligt, og indeholde følgende:

- ✓ Genstanden for behandlingen/hvad er det der skal behandles
- ✓ Varigheden af behandlingen
- ✓ Behandlingens karakter og formål
- ✓ Typen af personoplysninger
- ✓ Kategorier af registrerede
- ✓ Parternes rettigheder og forpligtelser (næste slide)

Indholdet i databehandleraftalen

1. Behandling skal ske efter dokumenteret instruks

2. Personer, der er autoriseret til at behandle oplysninger skal være underlagt fortrolighed (i aftale eller lov)

3. Foranstaltninger for behandlingssikkerhed

4. Slette eller tilbagelevere personoplysninger til den dataansvarlige, når tjenesten er ophørt.
   U: EU-ret eller national ret

5. Stille alle oplysninger til rådighed og give mulighed for inspektioner

6. Omgående underrette den dataansvarlige om instrukser i strid med GDPR, EU-ret eller national ret

Dagens program/Agenda

1.	Overordnede krav – og udleveret materiale fra PLO
2.	Introduktion til databeskyttelsesforordningen (GDPR)
3.	Grundlæggende principper og behandlingsregler
4.	Registreredes rettigheder
5.	Dataansvarlig og databehandler, roller og opgaver
6.	Sikkerhedsbrud
7.	Risikovurderinger

Sikkerhedsbrud

1. **Sikkerhedsbrud**
   - Kendskab til sikkerhedsbrud
   - Eventuel databehandler underretter straks dataansvarlig
2. **Undersøgelse og beskrivelse**
   - Undersøgelser og beskrive kategorier af data, antal af registrerede omfattet af bruddet, foranstaltninger, konsekvenser for registrerede, mv.
3. **Anmeldelse til Datatilsynet**
   - Den dataansvarlige anmelder til Datatilsynet senest 72 timer efter kendskab *(medmindre at det er **usandsynligt**, at bruddet indebærer en risiko for fysiske personers rettigheder)*
   - Evt. trinvis anmeldelse, hvis det ikke er muligt at give oplysningerne samlet
4. **Underretning til registrerede**
   - Den dataansvarlige underretter den registrerede, hvis sikkerhedsbruddet sandsynligvis indebærer en **høj risiko**
5. **Log**
   - Tilføje til loggen over sikkerhedsbrud (I har fået skabelon af PLO)

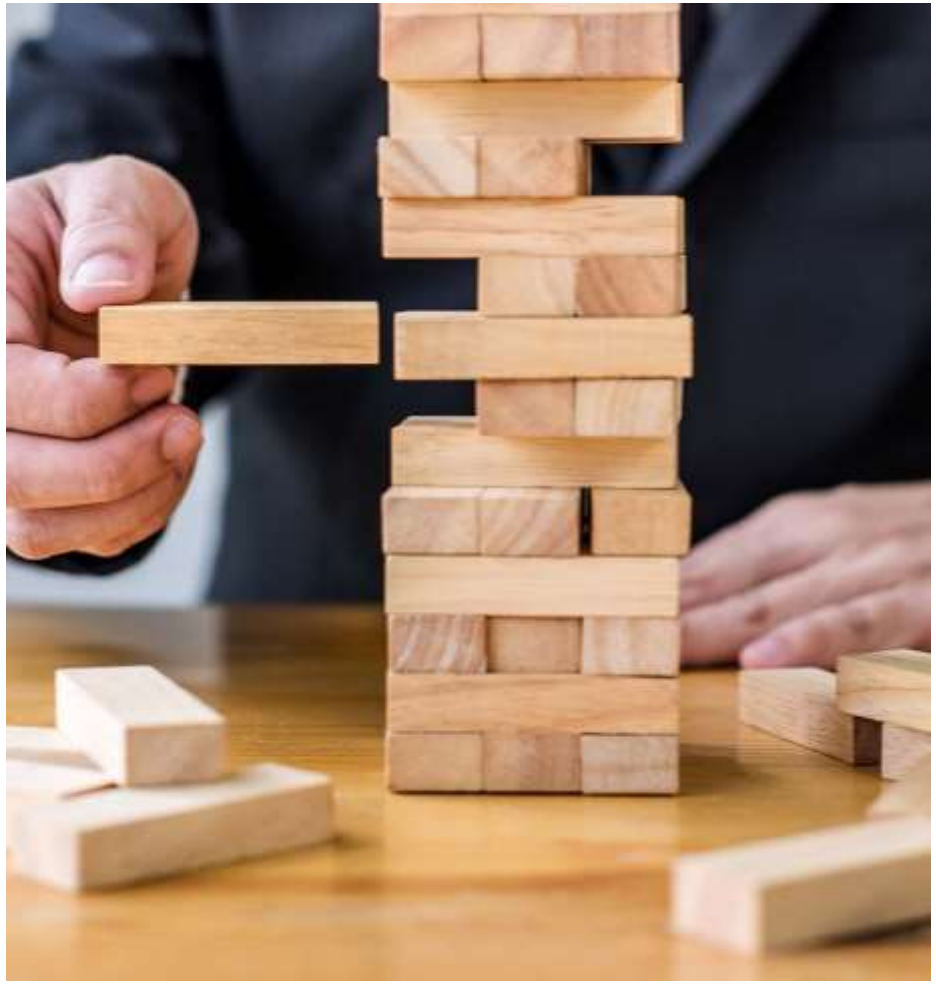
Dagens program/Agenda

1.	Overordnede krav – og udleveret materiale fra PLO
2.	Introduktion til databeskyttelsesforordningen (GDPR)
3.	Grundlæggende principper og behandlingsregler
4.	Registreredes rettigheder
5.	Dataansvarlig og databehandler, roller og opgaver
6.	Sikkerhedsbrud
7.	Risikovurderinger

Risikovurderinger

Hvorfor skal vi lave dem?

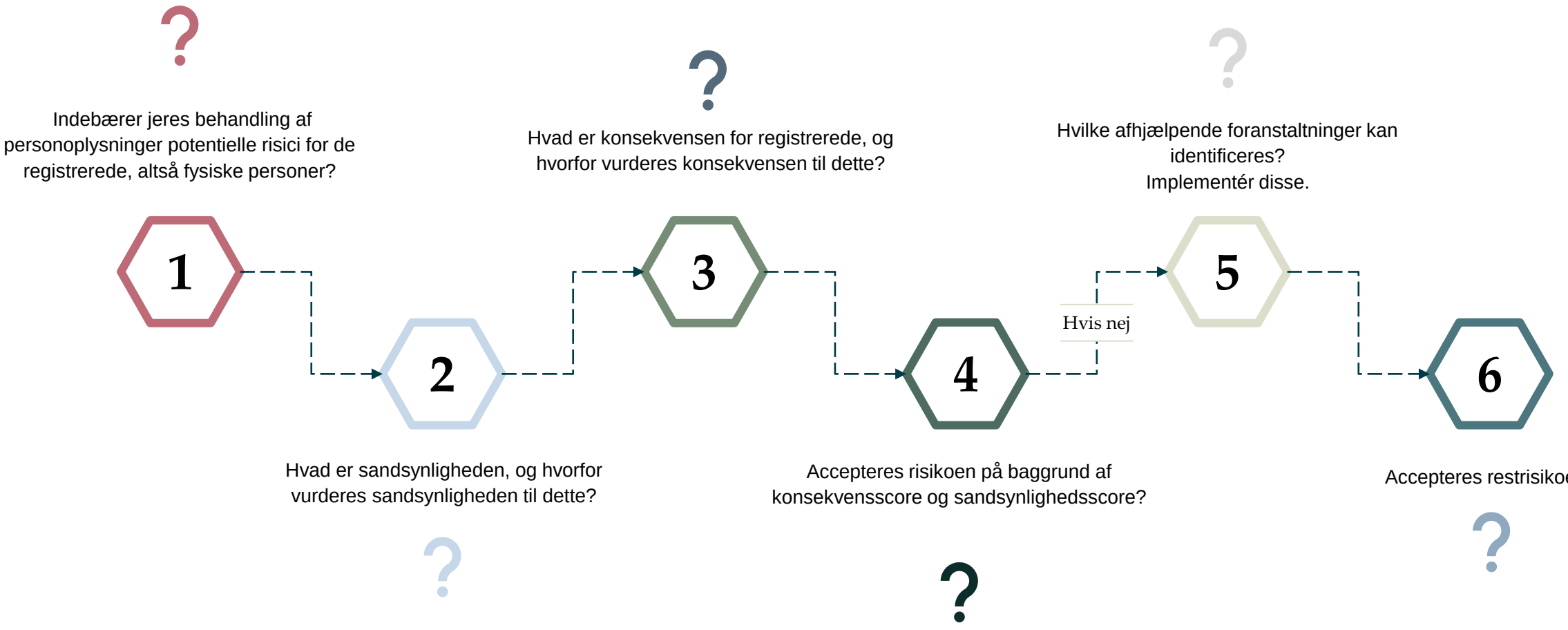
- Risikovurderingen er nødvendig for, at det kan vurderes, hvilke sikkerhedsforanstaltninger der skal implementeres
- En risikobaseret tilgang → Den dataansvarlige skal fastlægge de foranstaltninger, som er relevante henset de konkrete risici, som de registrerede udsættes for ved behandlingen af personoplysninger
- Betydningen af risikovurderinger ses særligt i sager om sikkerhedsbrud



Fokuspunkter ved udarbejdelsen

- Persondataretlige risikovurderinger skal tage udgangspunkt i de risici, der er for fysiske personer (de registrerede), og ikke de risici, der kan være for jer som klinik
  - Den registrerede udsættes for en risiko, hvis **fortroligheden**, **tilgængeligheden** eller **integriteten** af personoplysningerne påvirkes.
  - Det er vigtigt at identificere de risici, som en hændelse indebærer.
- Det er risikoen for den registrerede, der skal identificeres og vurderes → Det gør man ved at se på sandsynligheden og konsekvensen
- Man skal ”skrive sine tanker ned” – hvorfor er konsekvensen og sandsynligheden vurderet som de er?
- Hvis risikoen er for høj: Afhjælpende sikkerhedsforanstaltninger skal identificeres klart og tydeligt

Fremgangsmåden



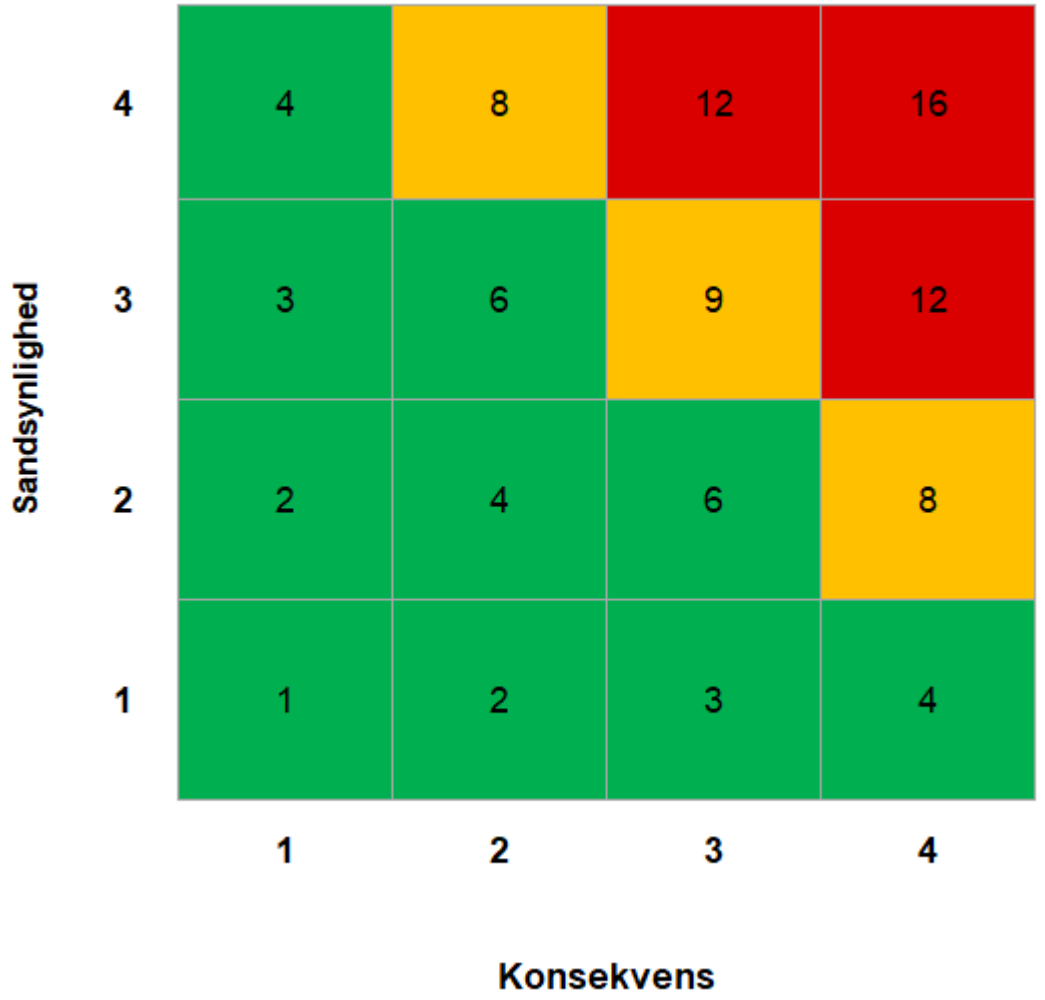
Nu til de risikovurderinger, I har fået fra PLO

Intro – hvad har I modtaget fra PLO?

Risikovurderingerne tager udgangspunkt i de her overordnede behandlingsaktiviteter:

1. Personale, rekruttering og klinikadministration
2. Patientbehandling – journalsystem og attester
3. Patientbehandling – integrationer til eksterne systemer
4. Fysiske rammer i klinikken og sikkerhed omkring lægeklinikkens PC'er
5. Kommunikation med patienter
6. Kvalitetsudvikling og forskning

Vejledning – step by step guide til gennemgang/udfyldelse



Risikovurdering af behandlingsaktiviteten: *1. Personale, rekruttering og klinikadministration*

Beskrivelse	
Eventuelle systemer	Mailsystem Lønsystem (Bluegarden)

Dato for udarbejdelse og godkendelse	
Risikovurdering udarbejdet eller genbesøgt:	*Dato, navn, titel*

Ref. ID	Risiko	Sandsynlighed for trussel før afhjælpende foranstaltninger (1-4)	Begrundelse for sandsynlighed før afhjælpende foranstaltninger	Konsekvens af trussel før afhjælpende foranstaltninger (1-4)	Konsekvens beskrivelse før afhjælpende foranstaltninger	Samlet risiko før afhjælpende foranstaltninger	Accepteres risikoen?
2	E-mail sendes til forkert modtager: Der er risiko for, at e-mails stiles til den forkerte modtager, f.eks. ved at adressefeltet autoudfyldes. Personoplysninger, herunder fortrolige og følsomme oplysninger, om medarbejdere og ansøgere kan derfor tilflyde utilsigtede modtagere, hvis der ikke udvises fornøden varsomhed ved afsendelse af e-mails - f.eks. ved modtagelse af ansøgninger per e-mail og besvarelse heraf, samt ved anden kommunikation med medarbejdere via e-mail, herunder om sygdom.	3	Det vurderes som sandsynligt, da der nemt kan ske menneskelige fejl, navnlig hvis autoudfyld ikke er slået fra.	3	Konsekvensen vurderes at være alvorlig, da oplysninger kan bruges til f.eks. identitetstyveri, og idet fortrolighedstabet af visse oplysninger i sig selv kan være indgribende for de registrerede.	9	Risikoen overvåges (Forekomsten af hændelser overvåges via sikkerhedsbrudslog)

Risikovurdering af behandlingsaktiviteten:	*2. Patientbehandling – journalsystem og attester*

Beskrivelse	
Eventuelle systemer	Lægeklinikkens journalsystem (leveres af systemhus)

Dato for udarbejdelse og godkendelse	
Risikovurdering udarbejdet eller genbesøgt:	*Dato, navn, titel*

Ref. ID	Risiko	Sandsynlighed for trussel før afhjælpende foranstaltninger (1-4)	Begrundelse for sandsynlighed før afhjælpende foranstaltninger	Konsekvens af trussel før afhjælpende foranstaltninger (1-4)	Konsekvens beskrivelse før afhjælpende foranstaltninger	Samlet risiko før afhjælpende foranstaltninger	Accepteres risikoen?
1	Indtastning af forkerte oplysninger i journal Der er en generel risiko for, at personoplysninger om patienter, herunder helbredsoplysninger, tastes forkert ind i en journal, f.eks. når oplysningerne gives via telefon eller videokonsultationer, men også ved konsultationer i klinikken.	2	Medarbejdere i lægeklinikken er meget opmærksomme på, at oplysninger skal indtastes korrekt i journalen, da dette er væsentligt for at sikre korrekt sygdomshistorik samt sikre, at f.eks. korrekt medicin ordineres. Det vurderes derfor, at sandsynligheden er lav, men der kan dog forekomme menneskelige fejl.	4	Det kan have kritiske konsekvenser for patienten, hvis truslen indtræffer, da det i værste fald kan betyde, at patienten vil modtage fejlbehandling eller helt manglende behandling	⚠ 8	Risikoen overvåges (Forekomsten af hændelser overvåges via sikkerhedsbrudslog)

Hvad hvis den samlede risiko ender i rød?

OBS: Disse kolonner udfyldes kun, hvis risikoen skal nedbringes					
Afhjælpende foranstaltninger (hvis risikoen skal nedbringes) *Det kan f.eks. være tekniske sikkerhedsforanstaltninger eller organisatoriske sikkerhedsforanstaltninger (f.eks. retningslinjer)*	Sandsynlighed for trussel efter afhjælpende foranstaltninger	Begrundelse for sandsynlighed efter afhjælpende foranstaltninger	Indsæt konsekvens værdi efter afhjælpende foranstaltninger	Konsekvens beskrivelse efter afhjælpende foranstaltninger	Samlet risiko efter afhjælpende foranstaltninger
					✔ 0

Opsamling på spørgsmål

Tak for i dag