PSYKOLOG FÖRETAGARNA

GDPR

Vägledning för psykologföretagare

Innehåll

Inledning

Följande vägledning med bilagor kan användas av dig som är psykolog och egenföretagare i Följande vägledning med bilagor kan användas av dig som är psykolog och egenföretagare i arbetet med att anpassa din verksamhet till de krav dataskyddsförordningen (GDPR) ställer från den 25 maj 2018. Förordningen gäller all personuppgiftsbehandling, både patienters uppgifter och andras, om du t.ex. har anställda, men specialregler kan ersätta eller komplettera GDPR:s bestämmelser.

För journaluppgifter gäller framförallt specialreglerna i Patientdatalagen (PDL) som kompletterar GDPR:s regler. Journalföringsreglerna i PDL är i det stora hela oförändrade mot tidigare oavsett att GDPR börjat gälla. När det gäller de delar av GDPR som inte regleras i PDL innebär GDPR:s ikraftträdande att vissa nya regler börjar gälla. Vägledningen syftar framförallt till att ge dig som egenföretagare information om de förändringarna.

Observera att vägledningen inte kan vara helt uttömmande i alla delar och vi rekommenderar att du vid osäkerhet tar kontakt med Datainspektionen eller Psykologföretagarnas medlemsrådgivning. Till den finns även ett antal bilagor som texten refererar till. Vägledningen kommer att uppdateras löpande.

Det är Datainspektionen som är tillsynsmyndighet i Sverige. Regeringen har föreslagit att Datainspektionen under 2018 byter namn till Integritetsskyddsmyndigheten.

Några viktiga definitioner:

En personuppgift är enligt GDPR varje upplysning som avser en identifierad eller identifierbar fysisk levande person (nedan kallad en registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras genom namn, bild, personnummer m.m. Avidentifierade uppgifter omfattas således inte av GDPR:s regler. Även personuppgifter på papper omfattas av GDPR:s regler om uppgifterna är sökbara, som t.ex. ett alfabetiskt ordnat patientjournalsystem i hängmappar.

En behandling är en ”åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter”. En åtgärd är all tänkbar hantering av en personuppgift, exempelvis insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, läsning, användning, utlämning. Det har här alltså inget att göra med behandling i meningen ”vård” av något slag utan gäller hantering av en personuppgift.

Personuppgiftsansvarig bestämmer ändamålen med och medlen för behandlingen av personuppgifter, ensam eller tillsammans med andra. Om du har en enskild firma är det du själv som är personuppgiftsansvarig. Har du ett bolag är det bolaget.

Ett personuppgiftsbiträde behandlar personuppgifter åt den personuppgiftsansvariga. Biträdet agerar på uppdrag av den personuppgiftsansvariga, och bestämmer alltså inte ändamål och medel för en behandling. Biträdet kan vara en fysisk eller juridisk person.

1. Gör en kartläggning och en förteckning

Ett första och viktigt steg i att uppfylla kraven i dataskyddsförordningen är att ha kontroll över vilka personuppgifter som hanteras i din verksamhet. Av det skälet kan en **kartläggning** av de personuppgiftsbehandlingar som förekommer i din verksamhet vara ett viktigt första steg.

Enligt GDPR är du som psykologföretagare skyldig att ha en **förteckning** som beskriver de olika sätt som du hanterar personuppgifter på. Samtidigt som kartläggningen görs kan lämpligen också förteckningen göras. Förteckningen ska inte skickas in till någon myndighet, men behöver finnas tillhands om tillsynsmyndigheten skulle göra en tillsyn. Den är också mycket bra att använda internt i verksamheten för att få överblick och kontroll på de behandlingar som sker.

Förteckningen[1] ska innehålla:

- kontaktuppgifter till den som är ansvarig för hanteringen av personuppgifterna (du själv om du har en enskild firma eller enskilt företag)
- vad uppgifterna används till (till exempel patientjournal, kontaktuppgifter på webbplats)
- vilka kategorier av personer och uppgifter som förekommer (till exempel patienter eller anställda)
- tidsgräns för borttagning av uppgifter, om möjligt
- om uppgifterna överförs till ett land utanför EU ska information finnas om det
- beskrivning av säkerhetsåtgärder som används vid behandling, om möjligt.

Tips!

- Förteckningen kan du till exempel ha i ett Excel-kalkylark.
- Tänk på att du kan behöva uppdatera förteckningen med jämna mellanrum.

2. Tänk på att du måste ha ett ändamål med alla behandlingar

Att ha ett ändamål/syfte med personuppgiftsbehandlingen är ett grundläggande krav enligt GDPR. Det är ändamålet med behandlingen som avgör om den är laglig överhuvudtaget. Ändamålet med behandlingarna måste antecknas i förteckningen, vilket också säkerställer

[1] Exempel på förteckning, se ”Exempel på förteckning och register över personuppgifter”. Nedladdningsbar excelfil finns på hemsidan.

att alla behandlingar görs med ett syfte. Ändamålet styr vilka uppgifter som får behandlas, uppgifterna måste kunna kopplas till syftet med behandlingen. Ändamålet styr också när uppgifterna ska raderas. Så snart ändamålet har upphört ska radering ske[2].

3. Tänk på att en ”rättslig grund” alltid måste finnas för behandlingen

I GDPR anges att alla personuppgiftsbehandlingar, även journaluppgifter, måste ha en s.k. ”rättslig grund”. Tänk på att du bara behöver använda en av dessa grunder för en behandling, där samtycke som rättslig grund (se nedan) enligt vår bedömning endast behöver användas i undantagsfall.

Följande rättsliga grunder är de vanligaste inom en psykologföretagares verksamhet. Information om övriga rättsliga grunder hittar du på tillsynsmyndighetens hemsida.

- Behandlingen är nödvändig för att utföra en uppgift av **allmänt intresse** enligt svensk **lag**.

Den här rättsliga grunden tillämpas på den dokumentation i patientjournaler som sker enligt patientdatalagens bestämmelser.

- Behandlingen är nödvändig för att **fullgöra ett avtal**.

Den här grunden kan tillämpas t.ex. när det gäller uppgifter om anställda i personaladministrativa system. Den kan också användas om personuppgifter behandlas i samband med andra avtal, som t.ex. leverantörsavtal eller hyresavtal. Denna grund används också vid fakturering.

- Behandlingen är nödvändig för att fullgöra en **rättslig förpliktelse**.

Den här grunden kan användas t.ex. vid användning av ekonomisystem för att följa bokföringslagens krav eller för att uppfylla krav som ställs i skattelagstiftningen.

- Behandlingen sker mot bakgrund av en **intresseavvägning**; eller
- Behandlingen sker mot bakgrund av ett **samtycke**

Vid en intresseavvägning ska ditt s.k. *berättigade intresse* av att utföra behandlingen, t.ex. dokumentera ett chefsstöd du ger till företaget X, väga tyngre än de registrerades intresse av att behandlingen inte sker. Ett sätt att försäkra sig om att ett sådant berättigat intresse föreligger är att inhämta den/de registrerades godkännande till behandlingen. Observera att detta inte innebär att grunden för behandlingen är samtycke utan visar bara på att även den person som ger sitt godkännande har ett intresse av att behandlingen sker. Ett godkännande är heller ingen förutsättning för att använda intresseavvägning som grund. Du måste således inte ha ett godkännande, men det är ett bra sätt att tydliggöra den

[2] Exempel på ändamål finns i bilagan ”Exempel på förteckning och register över personuppgifter”

rättsliga grunden intresseavvägning. Om däremot en registrerad person uttryckligen motsätter sig behandlingen, och invändningen som Datainspektionen uttryckt det ”är sakligt motiverad”, är det bara i undantagsfall som behandlingen kan fortsätta, eftersom intresseavvägningen då normalt anses väga över åt andra hållet.

Ett samtycke i GDPR:s mening kan alltid återkallas och ska vara entydigt och tydligt. Om samtycket inte ges, eller återkallas, måste för att behandlingen ska få ske en annan rättslig grund kunna tillämpas. Är inte det möjligt så får inte uppgifterna behandlas. Den personuppgiftsansvariga ska kunna visa att samtycke getts. Det bör alltså dokumenteras[3].

Någon av de rättsliga grunderna intresseavvägning eller samtycke kan användas när personuppgiftsbehandlingen avser klienter, men inte sker enligt PDL:s regler, t.ex. inom organisationsområdet eller vid handledning och inte någon annan rättslig grund är användbar.

4. Behandling av s.k. känsliga personuppgifter enligt GDPR

Enligt GDPR är uppgifter om bl.a. hälsa, sexualliv och sexuell läggning känsliga personuppgifter. Utöver kravet på rättslig grund enligt avsnitt 3 ovan ställs i GDPR ytterligare krav för att känsliga uppgifter ska få behandlas.

Utanför hälso- och sjukvårdens område är huvudregeln att samtycke krävs för att känsliga uppgifter ska få behandlas, det kan t.ex. gälla inom organisationsområdet. Ett samtycke utgör i de fallen både rättslig grund och ett giltigt skäl för att få behandla de personuppgifter som i GDPR klassificeras som känsliga.

När det däremot handlar om uppgifter i patientjournaler behövs inte något samtycke för att behandla känsliga uppgifter, eftersom man måste följa reglerna i PDL och föreskrifterna.

5. Tänk igenom de nya krav som ställs vid journalföring och annan behandling

GDPR innehåller de grundläggande reglerna för all personuppgiftsbehandling, även patientuppgifter. När det gäller behandling av andra personuppgifter än patientuppgifter, t.ex. uppgifter om anställda, är det GDPR i sin helhet som gäller.

Patientdatalagen (PDL) och Socialstyrelsens föreskrifter om journalföring är komplement till GDPR:s regler och för journaluppgifter gäller därför de reglerna istället för många delar av GDPR. De flesta regler som rör journalföringen kommer inte att förändras genom GDPR. Det handlar om bl.a. innehållet i journalerna och när journalföring ska ske, hur rättelser av uppgifter ska gå till samt den minsta lagringstiden för journaluppgifter.

Rättigheten för patienter att få **information** om personuppgiftsbehandlingen regleras särskilt i PDL från den 25 maj 2018. För andra registrerade än patienter, exempelvis

[3] Ang. utformningen av en samtyckestext se ”Exempel på samtyckestext”

anställda eller klienter i handledning, är det däremot reglerna i GDPR som ska tillämpas när det gäller rätten att få information. (Se p 6 nedan).

De viktigaste delarna av GDPR som ska tillämpas för såväl patienter som andra registrerade, eftersom motsvarande regler saknas i PDL och Socialstyrelsens föreskrifter är följande.

- **Övriga rättigheter** som registrerade har förstärks och tydliggörs (se p 7 nedan).
- Kravet på att underrätta tillsynsmyndigheten (f.n. Datainspektionen) om en s.k. **personuppgiftsincident** inträffar (se p 8 nedan).
- Kravet på att i vissa fall ha ett **dataskyddsombud** (se p 9 nedan).
- Kravet på att upprätta **personuppgiftsbiträdesavtal** med utomstående personuppgiftsbiträden som behandlar personuppgifter för din verksamhets räkning (se p 10 nedan).

6. Ge information om personuppgiftsbehandlingen

Både GDPR och PDL anger att de registrerade ska ges viss individuell skriftlig information om hur deras uppgifter kommer att behandlas redan i samband med att uppgifterna första gången samlas in. När det gäller patienter är det vanligen i samband med patientens första kontakt eller besök.

Informationen ska bl.a. innehålla vilken typ av uppgifter du behandlar, ändamålet med behandlingen och hur du behandlar uppgifterna. Informationen kan du till exempel ge i en kortfattad text på papper som ges till patienten. Bifogade exempel på informationstext innehåller alla de delar som GDPR i förekommande fall kräver.

Utöver det som GDPR innehåller om information anges i den kompletterande regeln i PDL den ytterligare information som ska ges till patienter. Det gäller bl.a.
vilken uppgiftsskyldighet som kan finnas, exempelvis orosanmälningsskyldigheten,
de sekretess- och säkerhetsbestämmelser som gäller för uppgifterna samt rätten till skadestånd om personuppgifter behandlas i strid med PDL.

Informationen kan också, men måste inte, kompletteras med en mer allmänt hållen text på en hemsida om du har en sådan i form av en personuppgiftspolicy. I den kan du i allmänna termer beskriva din verksamhet med fokus på behandlingen av patientuppgifter. En sådan text kan ha ett tydligt ”goodwillvärde” på det sättet att här kan tydliggöras att du i din verksamhet tar integritetsfrågorna på största allvar och hur du därför hanterar uppgifterna. Det kan konkret gälla både ändamålet med journalföringen (patientsäkerhetsskälen), hur uppgifterna förvaras, hur och när de raderas samt att du följer lagstiftningen om journalföring.

Tips!

- Skriv en informationstext som du ger till patienterna i inledningen av kontakten, se bilaga med exempel på en sådan information.
- Även ”gamla” patienter ska få informationen med anledning av de nya reglerna.
- Om du har en webbsida kan där läggas en allmän information, en s.k. ”personuppgiftspolicy”.

7. Tänk igenom hur registrerades övriga rättigheter ska hanteras

Bland övriga rättigheter som den registrerade har bör du särskilt tänka igenom dessa. Tillämpningen skiljer sig åt beroende på om det är fråga om journaluppgifter eller personuppgifter i andra sammanhang.

Rätten att få personuppgifter rättade

GDPR ger alla registrerade en grundläggande rätt att få felaktiga uppgifter rättade. En rättelse av en journaluppgift måste dock följa de kompletterande regler om rättelse av journaluppgifter som finns i PDL. Rätten till rättelse leder inte till att patienten kan bestämma om t.ex. en diagnos ska få stå i journalen. Innehållet i journalen styrs av PDL:s regler.

Rätten till radering

Rätten för den registrerade att få sina uppgifter raderade kallas i GDPR för ”rätten att bli glömd”. När det gäller journaluppgifter gäller istället PDL:s bestämmelser. Se om radering under p 11 nedan.

Rätten att på begäran få information om personuppgiftsbehandlingen

Den här rätten kan delvis jämföras med information som den beskrivits ovan under p 6. Skillnaden är här att den registrerade själv begär att få ut information om vilka behandlingar som sker. Om en sådan begäran kommer från t.ex. en patient, ska du ”utan onödigt dröjsmål” och senast inom en månad ge information om:

- Ändamålet med behandlingen
- Vilka kategorier av personuppgifter som behandlas, t.ex. namn och kontaktuppgifter, uppgifter om hälsa och personliga förhållanden.
- Hur länge uppgifterna är tänkta att lagras. För journaluppgifter är grundregeln 10 år efter sista anteckningen.

Sekretessbestämmelser, som i vissa fall gäller även gentemot patienten, kommer inte att förändras. Om en sekretessbestämmelse förhindrar att information lämnas ut så gäller

sekretessen före GDPR.

Tips!

- Mer information om de registrerades rättigheter hittar du på tillsynsmyndighetens hemsida.
- Skapa gärna en rutin för hur information ska ges om en registrerad själv begär det med tanke på skyndsamhetskravet.

8. Ha beredskap för om en personuppgiftsincident skulle inträffa

Enligt GDPR är en personuppgiftsincident en händelse som leder till en oavsiktlig eller olaglig förstöring, förlust eller ändring eller ett obehörigt röjande eller åtkomst till uppgifter. Det kan t.ex. gälla om din dator där du har journaluppgifter stjäls vid ett inbrott i dina lokaler, eller att du tappar bort ett USB-minne med uppgifter på. Det kan också vara att datorn går sönder så att uppgifter försvinner. Virus eller hackare är också incidentorsaker.

Sådana här händelser ska enligt GDPR anmälas till tillsynsmyndigheten inom 72-timmar efter det att händelsen upptäckts. Tillsynsmyndigheten har aviserat att man under våren 2018 kommer att lansera en webbtjänst för anmälningar.[4]

I undantagsfall behöver händelser inte anmälas, som t.ex. att det är fråga om en tillfällig förlust av uppgifter p.g.a ett strömavbrott eller att uppgifter snabbt kan återskapas via en backup. Eftersom man så snabbt kan behöva rapportera incidenter, rekommenderas att man förbereder sig genom att skapa tydliga rutiner för att enkelt kunna upptäcka personuppgiftsincidenter och för hur en incident ska hanteras om den skulle inträffa..

Exempel på enkla rutiner kan vara att:

- Kontrollera en backup regelbundet så att den fungerar.

- Ha ett uppdaterat antivirussystem installerat på datorn.

[4] Mer information om personuppgiftsincidenter finns på tillsynsmyndighetens hemsida.

Tips!

- Upprätta en handlingsplan att ha till hands om en personuppgiftsincident skulle inträffa.
- Om du är osäker på om en incident ska rapporteras – kontakta tillsynsmyndigheten

9. Tänk efter om du behöver ett dataskyddsombud

I vissa fall krävs att ett dataskyddsombud utses, det gäller bl.a. om en verksamhet i stor omfattning behandlar känsliga personuppgifter. Journaluppgifter är känsliga personuppgifter. Tillsynsmyndigheten anser f.n. inte att verksamheten hos en yrkesutövare som är egenföretagare i ett vårdyrke, t.ex. en psykolog som är egenföretagare, är av sådan stor omfattning att ett dataskyddsombud måste utses. Om du är osäker på om din verksamhet ska anses ha en stor omfattning rekommenderas att du kontaktar tillsynsmyndigheten för att få närmare besked hur de ser på den frågan.

Även om ett dataskyddsombud inte krävs, är det möjligt att ändå utse en sådan. Dataskyddsombudet har till uppgift att se till att GDPR:s regler följs och kan också vara ett stöd för en verksamhet i dess arbete med dataskydd och integritetsfrågor.

Enligt GDPR kan dataskyddsombudet vara en anställd i verksamheten med god kunskap om personuppgiftsfrågor, eller en extern konsult. Dataskyddsombudet får inte ha en position som ger rätt att bestämma hur personuppgifter hanteras i organisationen. Ett dataskyddsombud ska involveras i god tid, i alla frågor som rör personuppgiftsskydd, och ska rapportera till den högsta ledningen.

10. Se till att ha personuppgiftsbiträdesavtal om du anlitar externa konsulter av olika slag[5]

Att träffa ett avtal med personuppgiftsbiträde kan vara aktuellt om du har en utomstående leverantör av IT-stöd, och om den leverantören hanterar personuppgifter för din verksamhets räkning, exempelvis om du använder en molnlösning för ditt journalsystem. Ett annat exempel är om du anlitar ett redovisningsföretag att sköta din bokföring och personuppgifter finns med på de underlag som redovisningsföretaget hanterar för din

[5] Exempel på personuppgiftsbiträdesavtal, se ”Mall biträdesavtal.docx”

räkning. Leverantören av tjänsten är då personuppgiftsbiträde med vilken ett avtal ska tecknas.

Ett första steg här är att ta kontakt med den tjänsteleverantören och begära att få veta hur den avser att uppfylla GDPR:s bestämmelser. Många leverantörer är medvetna om reglerna och tar fram egna avtalsförslag att tillställa sina kunder. Om du själv väljer att ta fram ett eget avtal finns som en bilaga till denna vägledning en mall för avtalsinnehåll.

Observera att avtalet måste kompletteras utifrån dina egna förhållanden (rödmarkerade avsnitt i mallen).

Tips!

- Ta kontakt med just dina leverantörer och begär att få besked om hur de uppfyller GDPR. Tydliggör att ett biträdesavtal behöver upprättas.
- Användande av molntjänster innebär att ett personuppgiftsbiträde anlitas. Även Microsoft är personuppgiftsbiträde om du t.ex. använder deras Office 365-system.
- Om du anlitar biträden är det viktigt att försäkra sig om att uppgifter inte förs utanför EU (”till tredje land”) vilket kan inträffa om de servrar företaget använder är placerade utanför EU.

11. Spara inte personuppgifter längre än nödvändigt

En viktig regel i dataskyddsförordningen är att du inte får spara personuppgifter för länge. Grundregeln i GDPR är att när uppgifterna inte längre behövs för det ändamål som de en gång samlades in för, så ska de tas bort.

Den regeln kompletteras när det gäller journaluppgifter av reglerna i PDL och föreskrifterna om journalföring. Enligt dem får journaluppgifter raderas tidigast 10 år efter den senaste journalanteckningen. Det innebär normalt att när 10 år har gått sedan den senaste journalanteckningen, uppgifterna ska raderas om det inte finns något särskilt skäl för att behålla dem.

Enligt GDPR har den registrerade rätt att få sina uppgifter raderade. Om en patient skulle begära att uppgifter raderas ur journalen innan 10 års perioden gått, gäller istället PDL:s regel om förstörande av patientjournal. Enligt den regeln måste patienten i så fall ansöka hos Inspektionen för vård och omsorg om förstörande av journaluppgifter.

Tips!

- Om du inte redan har det bör du skapa rutiner för radering av journalanteckningar och andra personuppgifter.
- I din förteckning över de personuppgifter som hanteras i verksamheten kan du även ange hur länge olika typer av uppgifter ska sparas.
- Det gäller även att ha rutiner på plats som säkerställer att uppgifterna verkligen tas bort efter utsatt tid.

12. Tänk på säkerheten för personuppgifterna

Antivirusprogram, trådlöst nätverk med kryptering, backupsystem och datorer med uppdaterad programvara är några allmänna exempel på hur man höjer säkerheten inom verksamheten. GDPR ställer krav på att göra en konsekvensbedömning, d.v.s. tänka igenom säkerheten för de uppgifter som behandlas. Det handlar om att göra en riskbedömning: hur stor är risken att någon obehörig kommer åt uppgifterna, att de försvinner eller förvanskas, och hur stor kan skadan i så fall bli? Anpassa sedan skyddet därefter.[6] På tillsynsmyndighetens hemsida finns mer information om konsekvensbedömningar – när, var och hur.

Glöm inte bort organisatoriska säkerhetsåtgärder, som att begränsa vilka anställda som får komma åt olika typer av personuppgifter. Informera anställda om de rutiner som finns i verksamheten, t.ex. om hur e-post ska hanteras.

I både PDL och föreskrifterna finns dessutom särskilda regler som tar sikte på vilka säkerhetsåtgärder som krävs kring journaluppgifter. Dessa regler har funnits även tidigare och ändras inte när GDPR börjar gälla. I Socialstyrelsens handbok om journalföring, som kan laddas ner från myndighetens hemsida, finns mer information om säkerheten kring journaluppgifter, bl.a. riskanalys, säkerhetskopiering och skydd mot obehörig åtkomst.[7]

Även om du i din verksamhet inte behandlar journaluppgifter enligt PDL kan de vara mycket integritetskänsliga. Ju känsligare uppgifter, desto mer omfattande skyddsåtgärder kan behövas. Av säkerhetsskäl kan det finnas anledning att behandla sådana uppgifter på det sätt som anges i Socialstyrelsens regler om Öppna nät, även om reglerna inte är formellt tillämpliga.

13. Tänk igenom hur du hanterar din e-post

GDPR gäller personuppgifter som förekommer i e-post, t.ex. e-postadresser. Samtidigt finns även särskilda regler om e-posthantering i Patientdatalagen och Socialstyrelsens föreskrifter. Man kan därför dela in e-posthanteringen i två huvuddelar, dels allmän e-post i

[6] Ett exempel på en dokumenterad riskbedömning, se ”Exempel Risk och åtgärdsanalys”
[7] http://www.socialstyrelsen.se/publikationer2017/2017-3-2

verksamheten som inte innehåller patientuppgifter och dels e-post som innehåller patientuppgifter.

Exakt hur GDPR kommer att påverka e-posthantering är inte klart i nuläget. tillsynsmyndigheten ger löpande information om bl.a. det här på sin hemsida. Följande är dock värt att påpeka om e-posthantering. När det gäller patientuppgifter i fakturor och andra redovisningsunderlag, se avsnitt 14 nedan.

Allmänt om e-post

Det här bör du tänka på när det gäller verksamhetens e-post i allmänhet.

- Du måste göra samma bedömningar för behandlingen av personuppgifter i e-post som för behandlingen av personuppgifter i andra system. Det innebär bland annat att du måste ha en rättslig grund[8] som tillåter behandling av personuppgifterna
- Undvik att skicka integritetskänsliga uppgifter som exempelvis lönebesked via e-post. För journaluppgifter gäller särskilda regler, se nedan.
- Det som skiljer e-post från annan uppgiftshantering är att innehållet oftast är okänt när e-posten kommer in till verksamheten. Utgångspunkten är att en verksamhet behöver ta hand om inkommande post. Företag och privata organisationer kan därför som regel *initialt* behandla personuppgifter i inkommande e-post med stöd av en intresseavvägning. När e-posten väl är mottagen beror det på innehållet om och hur länge det får sparas. När e-posten har lästs måste du därför bedöma hur personuppgifterna ska behandlas i fortsättningen och vilket rättsligt stöd samt skäl för att behandla eventuellt känsliga uppgifter som finns för den fortsatta behandlingen.
- E-postsystem är ur GDPR-synpunkt mycket osäkra att använda som lagringsplats för personuppgifter. Flytta därför så snart som möjligt över personuppgifter som behöver sparas till andra system och radera e-postmeddelandet. Exempel: Kommer e-post från en patient så ska meddelandet raderas i e-postsystemet så snart relevanta uppgifter införts i journalen. E-postar en anställd in och sjukanmäler sig, registrera det i lönesystemet och radera därefter meddelandet.
- Om du ändå behöver spara e-posten, bestäm i förväg hur länge du behöver spara den och radera den därefter – dock aldrig längre än 1 år. Spara överhuvudtaget inte e-post med personuppgifter ”för att det kan vara bra att ha”.
- Informera dina anställda om ovanstående punkter.

Att hantera uppgifter om patienter i e-post

Enligt PDL och Socialstyrelsens föreskrifter gäller särskilda regler för överföring av patientuppgifter via s.k. öppna nät, till vilka e-postmeddelanden (och för övrigt även SMS) hör.[9]

[8] Se avsnitt 3 ovan.
[9] Se bilaga ”Hantering av journaluppgifter i öppna nät”

Tips!

- Undvik att använda e-postsystemet som en lagringsplats. Flytta istället uppgifter som behöver lagras till andra system, t.ex. journalsystem eller lönesystem och radera e-post snarast möjligt.
- E-post som innehåller uppgifter om patienter kan bara användas i samband med tidbokning och under de förutsättningar som anges i Socialstyrelsens föreskrifter.
- Om patienter skickar e-post till verksamheten, radera meddelandena så snart som möjligt. Om patientuppgifter i ett e-postmeddelande behöver sparas ska det göras i journalsystemet.
- Ovanstående gäller även SMS.
- OBS! Din e-post leverantör är personuppgiftsbiträde, vilket innebär att ett biträdesavtal måste finnas, se ovan avsnitt 10.

14. Tänk på andra personuppgifter än de som finns i journaler

I en egenföretagares verksamhet behandlas personuppgifter i många olika sammanhang. Ett syfte med kartläggningen[10] är att få kontroll över alla de processer där personuppgifter förekommer. Här följer några exempel på vanliga processer innehållande personuppgifter, men fler kan förekomma.

Bokförings- och ekonomisystem

För uppgifter i olika ekonomisystem gäller bokföringslagens bestämmelser, bl.a. om hur länge uppgifterna ska sparas.

Hanterar du uppgifter i patientjournal omfattas de som ovan angivits av Patientdatalagen och Socialstyrelsens föreskrifter. De krav som finns vad gäller innehållet i fakturor gör att de normalt sett innehåller personuppgifter om patienterna och därmed att reglerna om Öppna nät i föreskrifterna är tillämpliga om du hanterar fakturor via e-post.

Detta innebär i sin tur att man får skicka fakturor per e-post om man skickar det på ett sådant sätt att obehöriga inte kan ta del av dem och att man använder sig av stark autentisering. Man kan inte göra undantag från denna bestämmelse genom samtycke från patienten.

Om du inte hanterar patientuppgifter i din verksamhet gäller istället GDPR:s regler som anger att du ska informera om hur du hanterar fakturor. Du måste också ha en rättslig grund för fakturahanteringen och ha lämpliga skyddsåtgärder efter att ha gjort en riskbedömning. En rättslig grund för att skicka en faktura är i regel att fullgöra avtal med

[10] Se avsnitt 1.

den registrerade. Vilka skyddsåtgärder som krävs beror till stor del på innehållet i materialet som skickas

Leverantörsregister, avtal m.m.

Många företag köper in produkter eller tjänster, men inte alla. Även om ditt företag inte registrerar några uppgifter om leverantörer så kan det vara bra att känna till att uppgifter om juridiska personer inte omfattas av reglerna i dataskyddsförordningen.

Ett leverantörsregister innehåller normalt endast uppgifter om juridiska personer. Sådana uppgifter är inte personuppgifter.

Uppgifter om enskilda näringsidkare och uppgifter om kontaktpersoner på företagen är dock personuppgifter, och sådana personuppgifter är tillåtna att hantera för att hantera avtalet med leverantörerna. Det kan exempelvis gälla hyresavtal där namn på kontaktpersoner hos hyresvärden finns angivna. Att sådana uppgifter behandlas ska noteras i förteckningen (p 1 ovan).

Anställda

För anställdas personuppgifter gäller samma grundregler som för övriga uppgifter. Det är inte patientdatalagens regler som gäller. Det kan här vara fråga om anställningsavtal, om uppgifter i lönesystem eller personliga uppgifter kring enskilda anställda.

Vill du ha ytterligare information?

Tillsynsmyndighetens hemsida

https://www.datainspektionen.se/dataskyddsreformen/ .

Information från Bolagsverket m.fl myndigheter

https://www.verksamt.se/

Psykologföretagarnas medlemsrådgivning

Öppettider: mån, ons-fre kl 9-11 samt tis kl 13-15
Tel: 08 56706420
E-post: medlemsradgivningen@psykologforbundet.se

Förteckning över bilagor

1. **Hantering av journaluppgifter i öppna nät**
2. **Exempel på förteckning och register över personuppgifter**
3. **Mall biträdesavtal**
4. **Exempel på risk och åtgärdsanalys**
5. **Exempel på informationstext**
6. **Exempel på samtyckestext**

Bilaga 1. **Hantering av journaluppgifter i öppna nät**

Utdrag ur Socialstyrelsens Handbok vid tillämpningen av Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården, sid 25 ff.

Ur Socialstyrelsens föreskrifter HSLF-FS 2016:40

> ***3 kap. 15 §***
>
> *Om vårdgivaren använder öppna nät vid behandling av personuppgifter, ska denne ansvara för att*
>
> *1. överföring av uppgifterna görs på ett sådant sätt att inte obehöriga kan ta del av dem, och*
>
> *2. elektronisk åtkomst eller direktåtkomst till uppgifterna föregås av stark autentisering.*

Vad innebär öppna nät?

Öppna nät kan beskrivas som datornätverk som en enskild användare har tillgång till, exempelvis Internet. Genom att utnyttja Internet är det möjligt att enkelt och effektivt kommunicera text, ljud och bild. Om inte vårdgivaren vidtar särskilda sk0yddsåtgärder kommer dock informationen att överföras oskyddad. Därför är det nödvändigt med specifika säkerhetslösningar för att minska risken för att obehöriga personer får tillgång till informationen.

Skydd mot obehörig åtkomst

Om en vårdgivare gör uppgifter om patienter tillgängliga över öppna nät, exempelvis för att hälso- och sjukvårdspersonalen ska kunna utföra arbetsuppgifter på distans, måste det göras på ett sådant sätt att ingen obehörig kan nå uppgifterna. I praktiken innebär det bland annat att uppgifter om patienter måste överföras genom en krypterad förbindelse eller genom att kryptera uppgifterna. Teknikutvecklingen medför att krypteringsmetoderna hela tiden kan behöva förbättras för att minimera risken för obehörig åtkomst.

Vad innebär skydd med starkt autentisering?

För att en behörig användare ska få tillgång till personuppgifter via öppna nät måste vårdgivaren se till att åtkomsten föregås av en så kallad stark autentisering. Det innebär att vårdgivaren använder inloggningslösningar som ställer krav på att identiteten kontrolleras på minst två olika sätt, exempelvis:

• med någonting användaren kan − till exempel lösenord eller pinkod

• med någonting användaren har − till exempel kodbox, certifikat, smart-kort, engångskoder eller mobiltelefon

• med hjälp av användaren själv – till exempel fingeravtryck eller avläsning av iris.

En etablerad metod för stark autentisering är att använda en e-legitimation. Det är en identitetshandling i elektronisk form som vid elektronisk kommunikation används för legitimering och underskrift. E-legitimationen kan lagras på en dator (certifikat på fil), på ett smartkort eller i en mobiltelefon.

Med hjälp av e-legitimationen och det tillhörande lösenordet (exempelvis en pinkod) skapas förutsättningar för en stark autentisering. Denna metod används bland annat av Skatteverket och Försäkringskassan för att låta kunderna identifiera sig och signera sina handlingar när de använder e-tjänster, till exempel vid deklaration och begäran om föräldraledighet.

Överföra uppgifter om patienter via fax

Telenätet räknas som ett öppet nät. Faxar använder telenätet för sin kommunikation. Därför gäller bestämmelserna om öppna nät också överföring av uppgifter om patienter med hjälp av fax. Detta innebär att det kan vara svårt att överföra uppgifter via fax på ett sätt som uppfyller föreskrifternas krav på säkerhet. Den vårdgivare som använder fax för sådana överföringar måste förvissa sig om att ingen obehörig kan nå uppgifter om patienter. Detta innebär att uppgifter om patienter som faxas ska vara krypterade och att åtkomsten till innehållet i faxet ska föregås av stark autentisering.

Behandling av personuppgifter i öppna nät – undantag

Undantag för påminnelser och kallelser

Undantag från kraven om skyddad överföring i 3 kap. 15 § 1 får göras då uppgifter om patienter ingår i påminnelser och kallelser. Det innebär att uppgifter om patienter i elektroniska påminnelser och kallelser som kommuniceras över öppna nätverk, exempelvis via sms eller e-post, inte behöver krypteras. Däremot behöver åtkomsten fortfarande föregås av stark autentisering. Det är inte fråga om ett beslut i varje enskilt fall då en påminnelse eller kallelse ska skickas ut med exempelvis e-post eller sms.

Undantaget från kraven i 3 kap. 15 § 1 har tillkommit eftersom det anses praktiskt och smidigt både för vårdgivare och patienter med kallelser och påminnelser om besök i vården per sms eller e-post.

En överföring av en påminnelse eller en kallelse får inte avslöja detaljer om en patients hälsotillstånd eller andra personliga förhållanden. En överföring av en påminnelse eller en kallelse får endast göras efter att patienten har gett sitt medgivande. Vårdgivaren bör ha rutiner som säkerställer att patientens kontaktuppgifter är riktiga och aktuella. Ett av de grundläggande kraven vid behandling av personuppgifter är att personuppgifter som behandlas ska vara riktiga, och om nödvändigt, aktuella (prop. 2007/08:126 s. 63

Bilaga 2. **Exempel på förteckning och register över personuppgifter**

Förteckning och register över personuppgifter (exempel) Röda rutor = Obligatoriska uppgifter enligt GDPR										
GDPR:		**Artikel 30 p.1c**	**Artikel 30 p.1c**	**Artikel 30 p.1g**	**Artikel 30**	**Artikel 30 p.1b**	**Artikel 30 p.1d**	**Artikel 30 p.1e**	**Artikel 30 p.1f**	**Artikel 30 p.1e**
Alternativ 1: System (Var behandlas uppgiften)?	**Alternativ 2: Process**	**De kategorier (grupper) av personer som berörs av behandlingen**	**Beskrivning av kategorier av personuppgifter**	**Allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder enligt artikel 32 p.1**	**Behandling hur?**	**Ändamålet med behandlingen**	**Kategorier av mottagare som uppgifter har eller ska lämnas ut till**	**Ev. överföring av uppgifter till tredje land eller internationella organisationer**	**Radering enligt interna raderingsrutiner.**	**Dokumentation av lämpliga skyddsåtgärder vid sådan överföring som avses i artikel 49 p.1 st2.**
Patientjournal system	**Exempel: Förande av löpande journalanteckningar i patientjournalsystemet**	Exempel: Patienter	Ex på innehåll: Namn, Personnummer, Adress, E-post, Telefon, Hälsouppgifter, andra uppgifter om personliga förhållanden	Ex på innehåll: Beskrivning av säkerhetssystem såsom Brandvägg, Behörighetstilldelning, lösenordsskydd, Kryptering av filer, backupsystem, Integritetspolicys är kändaoch tillämpas i organisationen. Biträdesavtal i förekommande fall som reglerar säkerhetsfrågor.	Exempel: Insamling, registrering, lagring, ändring, läsning, utlämning, radering.	Exempel: Dokumentation vid vård av patienter och administration som föranleds av vård av patienter såsom hantering av patientavgifter. Dokumentation för att hantera det systematiska och fortlöpande patientsäkerhetsarbetet.Uppföljning, planering och utvärdering av verksamheten, samt myndighetstillsyn.	Ex: System- och Driftleverantör av Patientjournalsystemet samt e-postsystemet Myndigheter	Exempel: Molntjänster, Bärbar utrustning (telefoner, datorer, surfplattor) som används i tredje land d.v.s. utanför EU/EES.	Exempel: Radering sker i enlighet med reglerna i Patientdatalagen SFS 2008:355	
Patientjournal system	**Exempel: Utlämnande av journaluppgifter till andra vårdgivare eller myndigheter, patienter, m.fl**	Exempel: Patienter	Ex på innehåll: Namn, Personnummer, Adress, E-post, Telefon, Hälsouppgifter, andra uppgifter om personliga förhållanden	Ex på innehåll: Överföring av journaluppgift sker endast i krypterad form, samt med säker autentisering. Alternativt sker överföring postalt.	Exempel: utlämning, registrering	Exempel: Följa tvingande lagstiftning, t.ex. vid uppgiftsskyldighet till socialnämnd, eller då patienten begär att få ut sina journalhandlingar. Vid remittering till andra vårdgivare.	Ex: Andra vårdgivare, Patienten själv, Vårdnadshavare, andra vårdgivare, Myndigheter	Ex: Inte aktuellt		
Klient/kundsystem	**Exempel: Registrering och dokumentering av handledning till chefer inom respektive uppdrag**	Exempel: Klienter, kontaktpersoner hos kundföretag	Ex på innehåll: Namn, Personnummer, Adress, E-post, Telefon, andra uppgifter om yrkesmässiga och personliga förhållanden	Ex på innehåll: Beskrivning av säkerhetssystem såsom Brandvägg, Behörighetstilldelning, lösenordsskydd, Kryptering av filer, backupsystem. Biträdesavtal i förekommande fall som reglerar säkerhetsfrågor.	Exempel: Insamling, registrering, lagring, ändring, läsning, utlämning, radering.	Exempel: Dokumentation vidutförande av handledningsuppdrag hos kunder och övrig administration som föranleds av kundens uppdrag. Även underlag för ekonomisk redovisning.	Exempel: Kundföretagen, de enskilda chefer som erhållit handledning.	Ex: Inte aktuellt	Ex: När kunduppdraget avslutats. Redovisningsunderlag raderas enligt bokföringslagens bestämmelser.	
Personalsystem		Anställda	Ex på innehåll: Namn, Personnummer, Adress, E-post, Telefon, Anställningsuppgifter, Lön, Uppdrag, befattning,	Se exempel ovan	Exempel: Insamling, registrering, lagring, ändring, läsning, utlämning, radering.	Administration av anställningsrelaterade frågor	Exempel: A-kassa, Försäkringsbolag, Tjänstepensionsbolag, Företagshälsovård, Skattemyndighet, Försäkringskassa		Exempel: Radering sker när anställningen har upphört.	
Extern webb "AB.se", Intranät		Anställda	Ex på innehåll: Namn, Personnummer, Adress, E-post, Telefon, Befattning, utbildning, titel, tidigare anställningar, yrkeserfarenheter, Uppdrag, Foto	Se exempel ovan	Exempel: Insamling, registrering, lagring, ändring, läsning, utlämning, radering.	Administration av webbsida	Leverantör IT-drift och Webb-leverantör			
Lönesystem		Anställda, uppdragstagare	Ex på innehåll: Namn, Personnummer, Adress, E-post, Telefon, Löner och arvoden, Bankkonto, frånvaro, personalstatistik, preliminärskatt, traktamenten	Se exempel ovan	Exempel: Insamling, registrering, lagring, ändring, läsning, utlämning, radering.	Fullgöra kontrolluppgiftsskyldighet, Behandling av lön, frånvaro och personalstatistik	Skatteverket, Leverantör löneadm, leverantör IT-drift, VISMA/AGDA			

Bilaga 3. **Mall biträdesavtal**

PERSONUPPGIFTSBITRÄDESAVTAL

MELLAN

[NAMNET PÅ DIN VERKSAMHET]

OCH

[NAMNET PÅ BITRÄDETS VERKSAMHET]

INNEHÅLL

PSYKOLOG FÖRETAGARNA

PERSONUPPGIFTSBITRÄDESAVTAL

mellan

(1) [*namn*], [*org. nr.*], [*adress*] ("**Personuppgiftsbiträdet**"),

och

(2) [*namn*], [*org. nr*], [*adress*] ("**den Personuppgiftsansvariga**")

1. BAKGRUND OCH SYFTE

1.1 *[Mer om bakgrund. Ange behandlingens föremål, art och ändamål.]* I uppdraget innefattas att Personuppgiftsbiträdet kommer att behandla personuppgifter för den Personuppgiftsansvarigas räkning.

EU:s nya dataskyddsförordning (Europaparlamentets och rådets förordning 2016/679 av den 27 april 2016) uppställer krav på att skriftligt avtal ingås när ett personuppgiftsbiträde ska behandla personuppgifter för en personuppgiftsansvarigs räkning. Detta avtal har till syfte att uppfylla nämnda krav i dataskyddsförordningen. Skyddet för patienternas personliga integritet är av största vikt för den Personuppgiftsansvariga och syftet med detta avtal är vidare att tillse att Personuppgiftsbiträdet behandlar personuppgifterna i enlighet med den Personuppgiftsansvarigas anvisningar och i enlighet med dataskyddsförordningen, tillämpliga lagar, föreskrifter och branschnormer.

2. DEFINITIONER

2.1 Detta avtal har motsvarande definitioner som återfinns i dataskyddsförordningen, vilket bland annat innebär följande.

Med "**personuppgifter**" avses varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Med **"registrerad'** avses i detta avtal den som en personuppgift avser.

Med **"behandling"** avses en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

3. TYP AV PERSONUPPGIFTER OCH KATEGORIER AV REGISTRERADE

3.1 Personuppgiftsbiträdet ska inom ramen för detta avtal behandla följande typer av personuppgifter beträffande nedan angivna kategorier av registrerade: [*Anpassa listan i enskilda fall.*]

Typer av personuppgifter

a) Namn, personnummer, adress, e-postadress, telefonnummer
b) Uppgifter om personliga förhållanden, hälsa, etc
c) [ ]

Kategorier av registrerade

a) Patienter
b) Anställda
c) [ ]

Den Personuppgiftsansvariga har rätt att från tid till annan meddela tillägg eller ändringar i de uppgifter som framgår av punkterna 3.1.1. och 3.1.2 ovan.

4. PERSONUPPGIFTSBITRÄDETS ÅTAGANDEN

4.1 Personuppgiftsbiträdet förbinder sig att säkerställa att all behandling av personuppgifter sker enligt dataskyddsförordningen, tillämpliga lagar, föreskrifter och branschnormer. Personuppgiftsbiträdet förbinder sig att hålla sig informerad om regelverket avseende dataskydd samt förändringar däri.

4.2 Personuppgiftsbiträdet, och den eller de personer som arbetar under dennes ledning, får bara behandla personuppgifter, inklusive överföringar av personuppgifter till ett

tredjeland eller en internationell organisation, i enlighet med de skriftliga instruktioner som från tid till annan lämnas av den Personuppgiftsansvariga, såvida inte en behandling krävs enligt unionsrätten eller tillämplig nationell rätt som gäller för Personuppgiftsbiträdet. I det sistnämnda fallet ska Personuppgiftsbiträdet informera den Personuppgiftsansvariga om det rättsliga kravet innan uppgifterna behandlas, såvida sådan information inte är förbjuden med hänvisning till ett viktigt allmänintresse enligt tillämplig rätt.

4.3 Instruktion för Personuppgiftsbiträdets behandling av personuppgifterna framgår av Bilaga 1 till detta avtal.

4.4 Om registrerad, Tillsynsmyndigheten eller annan tredje man begär information från Personuppgiftsbiträdet som rör behandling av personuppgifter enligt detta avtal, ska Personuppgiftsbiträdet hänvisa till den Personuppgiftsansvariga. Personuppgiftsbiträdet får inte lämna ut personuppgifter eller annan information om behandlingen av personuppgifter utan uttrycklig instruktion från den Personuppgiftsansvariga. Personuppgiftsbiträdet ska bistå den Personuppgiftsansvariga med att ta fram information som begärts av Tillsynsmyndigheten eller av registrerad så att den Personuppgiftsansvariga kan fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter i enlighet med kapitel III i dataskyddsförordningen.

4.5 Personuppgiftsbiträdet ska utan dröjsmål informera den Personuppgiftsansvariga om eventuella kontakter från Tillsynsmyndigheten som rör eller kan vara av betydelse för behandlingen av personuppgifter. Personuppgiftsbiträdet har inte rätt att företräda den Personuppgiftsansvariga eller agera för den Personuppgiftsansvarigas räkning gentemot Tillsynsmyndigheten eller annan tredje man.

4.6 Personuppgiftsbiträdet ska bistå den personuppgiftsansvarige med att se till att skyldigheterna enligt artiklarna 32–36 (säkerhet för personuppgifter, konsekvensbedömning avseende dataskydd och förhandssamråd) i dataskyddsförordningen fullgörs, med beaktande av typen av behandling och den information som Personuppgiftsbiträdet har att tillgå. I detta ingår skyldighet att utan onödigt dröjsmål underrätta den personuppgiftsansvariga vid personuppgiftsincidenter.

4.7 Personuppgiftsbiträdet ska ge den Personuppgiftsansvariga tillgång till all information som krävs för att visa att de skyldigheter som fastställs i detta avtal har fullgjorts samt möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den Personuppgiftsansvariga eller av en annan revisor som bemyndigats av den

Personuppgiftsansvariga. Personuppgiftsbiträdet ska omedelbart informera den Personuppgiftsansvariga om Personuppgiftsbiträdet anser att en instruktion strider mot detta avtal, dataskyddsförordningen eller mot andra unionsrättsliga eller nationella dataskyddsbestämmelser.

4.8 Personuppgiftsbiträdet ska, när detta avtal upphör att gälla, återlämna samtliga personuppgifter på av den Personuppgiftsansvariga angivet medium och se till att det inte finns några personuppgifter kvar hos Personuppgiftsbiträdet eller, enligt skriftlig överenskommelse mellan parterna radera alla data som innehåller personuppgifter, samt skriftligen bekräfta att personuppgifterna har utplånats på samtliga media som har använts för behandlingen på ett sådant sätt att de inte kan återskapas.

5. SÄKERHET

5.1 Personuppgiftsbiträdet ska i enlighet med artikel 32 (säkerhet i samband med behandlingen) i dataskyddsförordningen vidta de tekniska och organisatoriska åtgärder som krävs för att skydda personuppgifterna.

5.2 Personuppgiftsbiträdet ska på begäran av den Personuppgiftsansvariga förse denna med en sammanställning av de tekniska och organisatoriska åtgärderna som har vidtagits.

5.3 Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med hänsyn till den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter. Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

5.4 Åtgärderna omfattar, bl.a.,

5.4.1 pseudonymisering och kryptering av personuppgifter,

5.4.2 förmågan att fortlöpande säkerställa sekretess, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,

5.4.3 förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,

5.4.4 ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

5.5 Personuppgiftsbiträdet ska under hela avtalstiden upprätthålla en god säkerhet för personuppgifterna. Personuppgifterna ska av Personuppgiftsbiträdet skyddas mot förstöring, förlust, ändring, obehörigt röjande och otillåten tillgång.

5.6 Personuppgiftsbiträdet ska bl.a. säkerställa att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta sekretess enligt punkten 6 nedan eller omfattas av en lämplig lagstadgad tystnadsplikt samt säkerställa att dessa personer endast behandlar personuppgifterna i enlighet med instruktion från den Personuppgiftsansvariga, om inte unionsrätten eller tillämplig nationell rätt ålägger denne att göra det.

5.7 den Personuppgiftsansvariga har rätt att vidta nödvändiga åtgärder för att förvissa sig om att Personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som ska vidtas enligt ovan, samt för att förvissa sig om att Personuppgiftsbiträdet verkligen vidtar dessa åtgärder. Personuppgiftsbiträdet åtar sig att se till att den Personuppgiftsansvariga får den assistans som skäligen kan krävas för att på ett enkelt sätt ska kunna förvissa sig om detta.

6. SEKRETESS

6.1 Personuppgiftsbiträdet förbinder sig att inte till tredje man lämna ut eller eljest röja information om behandling av personuppgifter som omfattas av detta avtal eller annan information som Personuppgiftsbiträdet erhållit till följd av detta avtal eller annan information som Personuppgiftsbiträdet erhållit i sin roll som personuppgiftsbiträde. Personuppgiftsbiträdet åtar sig att inte utnyttja personuppgifterna för egna ändamål.

6.2 Åtagandet i punkten 5.1 första meningen gäller inte

(a) information som part kan visa var allmänt känd vid tidpunkten för mottagandet, eller

(b) information som part föreläggs att utge till myndighet.

6.3 Sekretessåtagandet gäller även efter det att detta avtal i övrigt har upphört att gälla.

7. UNDERBITRÄDE

7.1 Personuppgiftsbiträdet får endast anlita ett annat personuppgiftsbiträde (underbiträde) efter att ha erhållit skriftligt samtycke från den Personuppgiftsansvariga. I sådant fall ska underbiträdet i skriftligt avtal åläggas samma skyldigheter i fråga om dataskydd som de som anges i detta avtal. Personuppgiftsbiträdet ska ge tillräckliga garantier för att lämpliga tekniska och organisatoriska åtgärder vidtas så att behandlingen uppfyller kraven i detta avtal samt i dataskyddsförordningen. Om underbiträdet inte fullgör sina skyldigheter är Personuppgiftsbiträdet fullt ansvarigt gentemot den Personuppgiftsansvariga för utförandet av underbiträdets skyldigheter.

8. IMMATERIELLA RÄTTIGHETER M.M

8.1 Samtliga immateriella rättigheter till samlingen av personuppgifter tillkommer den Personuppgiftsansvariga och den Personuppgiftsansvariga upplåter endast en icke-exklusiv rätt för Personuppgiftsbiträdet att nyttja personuppgifterna för utförandet av uppdrag enligt detta avtal.

9. ERSÄTTNING

9.1 Personuppgiftsbiträdet har inte rätt till särskild ersättning för behandling av personuppgifter enligt detta avtal.

10. ANSVAR GENTEMOT TREDJE MAN

10.1 För det fall registrerad, eller annan tredje man riktar anspråk mot den Personuppgiftsansvariga på grund av Personuppgiftsbiträdets behandling av personuppgifter ska Personuppgiftsbiträdet hålla den Personuppgiftsansvariga skadeslös för sådana krav som följer av att Personuppgiftsbiträdet inte har behandlat personuppgifterna i enlighet med regelverket avseende dataskydd. Denna punkt gäller även efter det att detta avtal i övrigt har upphört att gälla.

11. AVTALSTID

11.1 Avtalet gäller från dess undertecknande och så länge Personuppgiftsbiträdet behandlar personuppgifter för den Personuppgiftsansvariga räkning. ALTERNATIVT: … så länge som Huvudavtalet gäller.

12. TVIST

12.1 Tvist angående tolkning eller tillämpning av detta avtal ska avgöras av allmän domstol.

Detta avtal har upprättats i två (2) exemplar, varav parterna har tagit var sitt.

Ort:
Datum:

[ ]

_____

Ort:
Datum:

[ ]

_____

Bilaga 1

Instruktion avseende Personuppgiftsbiträdets behandling av personuppgifter

Här kan man ge särskilda instruktioner om behandlingen av personuppgifter, t.ex. genom tydliga hänvisningar till valda delar av Socialstyrelsens handbok för journalföring. Det kan exempelvis gälla hur journaluppgifter ska lagras/förvaras.
Om man väljer att inte ha med den här bilagan kan p 4.3 ovan strykas.

Bilaga 4. **Exempel på risk och åtgärdsanalys**

Risk och åtgärdsanalys

Beskrivning av de analyserade personuppgifterna

Ändamål med behandlingen

Kategorier/grupper av personer som berörs av behandlingen

Personuppgifter eller kategorier/grupper av personuppgifter som skall behandlas

Känsliga personuppgifter eller kategorier/grupper av personuppgifter som skall behandlas

Åtgärder som har vidtagits för att trygga säkerheten i behandlingen

Kommer uppgifterna att överföras till tredje land?

Riskanalysens steg

1. Hotbeskrivning: Identifiera och beskriv hot mot uppgifterna som behandlas.
2. Händelseförlopp: Vad kan inträffa som negativt påverkar uppgifternas
   Riktighet?
   Konfidentialitet?
   Tillgänglighet?
   Spårbarhet?
3. Konsekvenser: Beskriv konsekvensen om det inträffar. Vilken påverkan skulle det få?
4. Gör en sammanvägd riskbedömning av Konsekvens/Sannolikhet.

Riskanalys

Hotbild nr					
Hotbeskrivning:					
Beskrivning av händelseförlopp:					
Beskrivning av konsekvenser:					
	Bedömning av sannolikhet och konsekvens av hotet. Placeringen ger en fingervisning om vilken prioritet åtgärderna bör ges i åtgärdsplanen				
Konsekvens	Allvarlig				
	Betydande				
	Måttlig				
	Försumbar				
Sannolikhet		Mycket sällan	Sällan	Regelbundet	Ofta

Riskanalys

Hotbild nr					
Hotbeskrivning:					
Beskrivning av händelseförlopp:					
Beskrivning av konsekvenser:					
	Bedömning av sannolikhet och konsekvens av hotet. Placeringen ger en indikation om vilken prioritet åtgärderna bör ges i åtgärdsplanen				
Konsekvens	Allvarlig				
	Betydande				
	Måttlig				
	Försumbar				
Sannolikhet		Mycket sällan	Sällan	Regelbundet	Ofta

Åtgärdsanalys

Hotbild	Riskbedömning	Åtgärd:	Prioritet:	Ansvarig:
Exempel: Nr 1: Integritetskänslig information finns och läcker ut	Konsekvens: Betydande --- Sannolikhet: mycket sällan	Se till att ha krypterad information, uppdaterad antivirus och brandvägg.	Mellan	

Bilaga 5. **Exempel på informationstext**

Nedan följer ett exempel på informationstext utformad i enlighet med kraven i GDPR och Patientdatalagen (PDL), framförallt att använda vid information till patienter, men kan även vara en utgångspunkt för hur information till andra registrerade och hur en allmän personuppgiftspolicy kan se ut. Enligt en ny informationsregel i PDL (8kap 6§) ska utöver den information som ska ges enligt GDPR, information ges

- om den uppgiftsskyldighet som kan följa av lag eller förordning, samt
- om de sekretess- och säkerhetsbestämmelser som gäller för uppgifterna och behandlingen.

Det innebär att vid journalföring enligt PDL särskilda rubriker bör användas för dessa två punkter (se nedan).

Tanken är att mallen ska kunna användas när du utformar din egen informationstext. Rubrikerna utgår från de krav som ställs i GDPR på vilken information som ska ges. Brödtexten är endast exempel. Du själv behöver ansvara för den slutgiltiga utformningen av texten under respektive rubrik och anpassa den utifrån dina förutsättningar och de personuppgiftsbehandlingar som är aktuella för just din verksamhet. Det är här särskilt viktigt att tänka på att GDPR är tydlig med att informationen ska vara lättillgänglig och tydlig. Både ordningsföljd på rubrikerna och layout kan naturligtvis förändras utan att det strider mot GDPR. Använd ett så enkelt och tydligt språk som möjligt och försök också att skriva kort och koncist.

Kommentarerna som är inlagda med kursiv stil syftar till att underlätta förståelsen av innehållet i mallen och är inte avsedda att ingå i en slutlig officiell text.

Information om behandling av personuppgifter

GDPR, eller dataskyddsförordningen, är en lag som gäller i hela EU från den 25 maj 2018. Den syftar till att vi alla ska få större kontroll över hur uppgifter om oss hanteras och öka säkerheten för hur våra personuppgifter behandlas. Personuppgifter är alla uppgifter som direkt eller indirekt kan kopplas till en enskild person. Dataskyddsförordningen kompletteras med andra regler, som gäller till exempel de krav som ställs på patientjournaler (Patientdatalagen) och de lagar som handlar om sekretess och tystnadsplikt.

Den här informationen syftar till att förklara hur [verksamhetens namn] hanterar dina personuppgifter. Om du har några frågor kring vår personuppgiftsbehandling kan du vända dig till /namn/.

> *Kommentar: En inledande text av ”goodwillkaraktär” om varför informationen lämnas och om integritetsfrågorna kan ges här, men är inte obligatorisk.*

Personuppgiftsansvarig

[verksamhetens namn] är ansvarig för de personuppgifter som behandlas i samband med vårdkontakterna mellan dig och oss. Kontaktuppgifter till [verksamhetens namn] är följande:
Adress
Tel
E-post

Dataskyddsombud

Den övergripande och viktigaste uppgiften för dataskyddsombudet är att övervaka att den personuppgiftsansvariga följer dataskyddsförordningen. Dataskyddsombudet ska bl.a. vara kontaktperson för de registrerade och personalen inom organisationen samt samarbeta med Datainspektionen, till exempel vid inspektioner.

[verksamhetens namn] dataskyddsombud har följande kontaktuppgifter:
Namn
Adress
Tel
E-post

> *Kommentar: Endast aktuell om du har ett dataskyddsombud. En förklaring av dataskyddsombudets roll är inte obligatorisk enligt GDPR, men kan ändå vara lämplig av tydlighetsskäl.*

Ändamål och rättslig grund för behandling

[verksamhetens namn] använder de uppgifter du lämnar till oss för att jag/vi/verksamheten ska kunna ge dig en god och säker vård. De används också i det systematiska och fortlöpande patientsäkerhetsarbetet. Uppgifterna förs under vårdtiden löpande in i journalsystemet. Uppgifterna är också till för att vara en informationskälla för dig som patient.

Den rättsliga grund som vi/jag/verksamhetens namn har för att behandla dina personuppgifter är att hälso- och sjukvård är en uppgift av s.k. allmänt intresse, det vill säga en verksamhet som är grundläggande för att vårt samhälle ska fungera. Legitimerade psykologer är också skyldiga enligt lag att dokumentera vården genom att föra journal (bland annat enligt Patientdatalagen). Vår/min verksamhet precis som alla vårdgivare står under tillsyn av Inspektionen för vård och omsorg och i händelse av deras tillsyn fyller patientuppgifterna en viktig funktion.

Lagringstid

[verksamhetens namn] kommer att radera dina personuppgifter i enlighet med reglerna i Patientdatalagen, dvs tidigast tio år efter den senast gjorda journalanteckningen.

Dina rättigheter

Du har rätt att få information om den personuppgiftsbehandling som sker. Du har även, med de begränsningar som följer av Patientdatalagen, rätt att få dina personuppgifter

rättade, att få uppgifterna raderade, att kräva att behandlingen av uppgifter i vissa fall begränsas, samt att i vissa fall invända mot behandling.

Mottagare av uppgifter

Uppgifter lämnas till utomstående endast om du i enskilda fall samtycker till det. I särskilda fall kan vi dock ha skyldighet enligt lag att lämna ut uppgifter, exempelvis när barn far illa, eller XXX /fyll i de som gäller i din verksamhet/.

Kommentar: Den sista meningen kan användas om man inte tillämpar PDL i verksamheten och därför inte använder nästkommande rubrik. Informationen här syftar till att den registrerade ska veta vad denna kan förvänta sig när det gäller vem eller vilka som skulle kunna få uppgifterna.

Uppgiftsskyldighet enligt lag

I särskilda fall kan jag/vi/verksamhetens namn ha skyldighet enligt lag att lämna ut uppgifter. En sådan uppgiftsskyldighet gäller enligt reglerna i:

- Socialtjänstlagen, om ett barn far illa
- Socialförsäkringsbalken, när det gäller uppgifter som behövs för beslut i socialförsäkringsärende.

Kommentar: Använd den här rubriken om behandlingen av personuppgifter sker i patientjournaler, det är ett krav enligt PDL. Här behöver man tänka igenom vilka skyldigheter man kan ha i verksamheten och ange de lagar eller andra bestämmelser som ger uppgiftsskyldighet.

Regler om sekretess och säkerhet för uppgifterna

För alla patientuppgifter, både sådana du lämnar och sådana vi använder exempelvis i journalen, gäller de regler om tystnadsplikt som följer av Patientsäkerhetslagens bestämmelser.

Kommentar: Använd den här rubriken om behandlingen av personuppgifter sker i patientjournaler, det är ett krav enligt PDL. Inom organisationsområdet finns inte något krav på att ge den här informationen eftersom enbart GDPR:s regler om information gäller där.

Rätten att lämna klagomål

Du har rätt att lämna klagomål till Datainspektionen rörande min/vår/verksamhetens behandling av dina personuppgifter.

Uppgifter som krävs enligt lag

Enligt Patientdatalagen och Socialstyrelsens föreskrifter ställs krav på ett visst innehåll i patientjournalen. De krav som ställs är att vi ska föra in uppgifter om din identitet, väsentliga uppgifter om bakgrunden till vården, de bedömningar som vi/jag/verksamheten gör, de planeringar som görs, och de åtgärder som genomförs. Vidare ställs krav på att vi anger vilken information som vi har lämnat till dig som patient, om val av behandlingsalternativ, utfärdade intyg och remisser samt ingående och utgående handlingar.

Överföring av uppgifter till tredje land

Kommentar: Om uppgifter överförs till tredje land (utanför EU) måste det anges. Det kan vara aktuellt när ett personuppgiftsbiträde anlitas.

Bilaga 6. Exempel på samtyckestext

Samtycke till behandling av personuppgifter

För att [namn på verksamheten] ska behandla dina personuppgifter genom att …(beskrivning av behandlingen) behöver du ge ditt samtycke genom att markera nedanstående kryssruta. Du har alltid rätt att ta tillbaka samtycket utan att återtagandet påverkar lagligheten av den behandling som skett dessförinnan. Om du inte samtycker kommer [namn på verksamheten] inte att utföra denna behandling.

☐ Jag samtycker till att mina personuppgifter behandlas av [namn på verksamheten] genom att… (beskrivning av behandlingen)

Kommentar: Om behandling av personuppgifter grundar sig på samtycke ska det vara frivilligt och dessutom ska följande villkor vara uppfyllda:
Den personuppgiftsansvariga ska kunna visa att den registrerade har samtyckt till behandlingen.
Om samtycke lämnas i en skriftlig förklaring som också rör andra frågor, ska begäran om samtycke läggas fram på ett sätt som klart och tydligt kan särskiljas från de andra frågorna. Det ska förklaras enkelt och begripligt, på ett klart och tydligt språk.
Den registrerade ska ha rätt att när som helst återkalla sitt samtycke. Återkallandet påverkar inte lagligheten av behandling som grundar sig på samtycket innan detta återkallas. Innan samtycke lämnas ska den registrerade informeras om detta. Det ska vara lika lätt att återkalla som att ge sitt samtycke.
Samtycket kan vara antingen muntligt eller skriftligt, och det kan endast ske efter det att den som samtycker har fått information om den aktuella behandlingen.
Samtycket ska innebära att den registrerade entydigt godkänner behandlingen. Tystnad, på förhand ikryssade rutor eller inaktivitet godtas därför inte som samtycke.