# 10 STEG SOM HJÄLPER DIG ATT KLARA GDPR-ANPASSNINGEN

**1. KARTLÄGG**

Undersök hur ni lagrar och behandlar personuppgifter i dag.  Frågor att ställa sig är:

- Var lagras och behandlas personuppgifter? På interna servrar, i mobila enheter, i molnet, i e-post eller i appar?
- Vilken datasäkerhet finns i dag?
- Vilka har access till personuppgifterna?
- Hur skyddas personuppgifterna?

Tänk på att företag i fortsättningen riskerar att få betala betydligt högre böter än tidigare vid bristande efterlevnad av GDPR. I Sverige har de böter som företag hittills har betalat varit blygsamma.

**2. UNDERSÖK BEFINTLIGA IT-SYSTEM**

IT-systemen behöver vara utformade så att de kan ge det integritetsskydd som GDPR kräver. Ni ska till exempel kunna,

- Korrigera, ändra eller radera personuppgifter i enlighet med de rättigheter som de registrerade har enligt GDPR.
- Upptäcka och rapportera dataintrång, läckage eller andra incidenter som berör personuppgiftshanteringen.
- Visa att ni behandlar personuppgifter i enlighet med GDPR.

**3. PERSONUPPGIFTSANSVARIG**

GDPR gäller för både den som är personuppgiftsansvarig (ditt företag) och så kallade personuppgiftsbiträden som anlitas för att på olika sätt hantera personuppgifter (till exempel en leverantör av molntjänster). I dessa fall ska ett så kallat personuppgiftsbiträdesavtal tecknas. Både den personuppgiftsansvarige och personuppgiftsbiträdet ansvarar för att reglerna inom GDPR följs.

Om ditt företag är Vårdgivare så är företaget personuppgiftsansvarig och ansvarig för GDPR-frågorna, inklusive avtal.

Om det förhåller sig så att varje person på en klinik har en egen etablering ska dessa ”etableringar” som huvudregel ha egna personuppgiftsbiträdesavtal. Var och en av näringsidkarna har ett journalsystem och det måste finnas ett bolagsspecifikt personuppgiftsbiträdesavtal för dessa.

**4. JOURNALSYSTEM**

En vårdgivare (nytt moment) ska ha testat sina journalsystem innan de använder systemen i verksamheten och detta bör även framgå i deras patientberättelse som skall vara uppdaterade den 1 mars varje år i enlighet med PDL samt SOSFS 2009:11. Vårdgivaren ska använda sig av ett

personbiträdesavtal mellan leverantören och vårdgivaren, se bifogat exempel. Syftet med detta är att se till att leverantören omhändertar känsliga personuppgifter.

**5. INCIDENTER**

Om incidenter av allvarligare slag sker ska detta rapporteras till tillsynsmyndigheten, Datainspektionen, redan inom 72 timmar. Det är en fördel om ni har bestämt i förväg vem som i så fall ska göra anmälan så att ni hinner göra den i tid.

Om ni inte redan har gjort det – bestäm vem eller vilka som ska ansvara för säkerhet.

**6. UTVECKLA RUTINER**

Undersök om det finns tydliga policys, regler och instruktioner i ditt företag om vad som gäller när man behandlar personuppgifter. Tänk på att skapa rutiner för hur ni ska dokumentera, rapportera och hantera dataintrång och incidenter.

En mycket viktig, del är att stödja medarbetarna att agera på ett säkert sätt beträffande hanteringen av personuppgifter. Det handlar om att medvetandegöra medarbetarna. Detta är en stor utmaning för speciellt mindre företag. Det blir det extra viktigt med användarvänliga IT-system som underlättar en säker behandling av personuppgifter.

**7. RÄTTSLIG GRUND FÖR BEHANDLINGEN**

I Undersök, och dokumentera, att ni har rättslig grund för behandlingen av personuppgifter, så att ni kan visa att ni följer reglerna enligt GDPR. Tänk på att detta gäller all personuppgiftsbehandling.

Inom hälso-och sjukvård finns grund för behandling av personuppgifter. Uppgifter får föras till om det behövs för,

1. att journalföra enligt PDL och att upprätta annan dokumentation som behövs för vården av patienter.

2. administration som rör patienter och syftar till att ge vård i enskilda fall eller som annars föranleds av vård i enskilda fall.

När uppgifter väl finns får det också användas för,

- Att upprätta annan dokumentation som behövs på grund av föreskrift i lag, förordning eller författning.
- Att systematiskt utveckla och förbättra kvaliteten i verksamheten.
- Administration, uppföljning, utvärdering och tillsyn av verksamheten.
- Eller för att framställa statistik för hälso- och sjukvården.

**8. RUTINER FÖR ATT RADERA**

Personuppgifter får som huvudregel sparas så längre de behövs för att uppfylla det ändamål som ni angav när ni samlade in dem. Undantagsvis får personuppgifter behandlas för andra syften än för det som de har samlats in förutsatt att det nya syftet inte är oförenligt med det ursprungliga.

Därför måste det finnas rutiner för att regelbundet radera uppgifter som ni inte längre får behandla. Det gäller även personuppgifter i backuper, vilket kan bli en utmaning rent praktiskt.

OBS. Rättigheten att få sina uppgifter raderade stärks av GDPR men begränsas av PDL. Patienter som vill få sina uppgifter utplånade måste fortfarande ansöka om detta hos IVO enligt 8:4 PDL.

**9. KÄNSLIGA UPPGIFTER**

Känsliga uppgifter såsom etniskt ursprung, politiska åsikter, religiös tro, medlemskap i fackföreningar, sekretessbelagda uppgifter eller uppgifter om sexualitet och hälsa är som huvudregel förbjudet att behandla men förbudet gäller inte inom hälso- och sjukvård. Känsliga uppgifter får dock inte användas som sökbegrepp (2:8 PDL).

Särskilda regler gäller även för behandling av barns personuppgifter.

**10. OM NI KÖPER NYTT**

Säkerhetsaspekter som IT-systemet bör tillgodose är:

- Inställningar som kan anpassas så att av mängden personuppgifter som samlas in eller behandlas minimeras.
- Funktioner för att radera uppgifter som inte längre får behandlas.
- Behörighetsstyrning så att enbart de som behöver uppgifterna för att utföra sitt arbete har åtkomst.
- Stark autentisering vid inloggning när personuppgifter ska behandlas.
- Skydd av personuppgifter när de skickas eller lagras, till exempel på olika enheter eller i molnet, exempelvis genom kryptering.
- Distansradering av uppgifter eller spärrning av enheter som tappas bort eller blir stulna.
- begränsning av vilka appar som kan användas vid behandling av personuppgifter.