GDPR och patientdatalagen

IT i hälso- och sjukvården

Anders Avdic

(16 bilder)

1

Dataskyddsförordningen GDPR (The General Data Protection Regulation) ersätter PUL (Personuppgiftslagen)

- **GDPR** ersatte PUL 25 maj 2018
- **gäller i hela EU** och har till syfte att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter så att det fria flödet av uppgifter inom Europa inte hindras.
- liknar de regler som fanns i personuppgiftslagen

- Tillsyn: Datainspektionen.
- https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/grundlaggande-principer/

2

2

EU:s dataskyddsförordning (The General Data Protection Regulation) ökat fokus på integritetsskydd

- **Uppgiftsminimering**
- ”privacy by design” eller ”**inbyggt dataskydd**” innebär hänsyn vid utformningen av systemen (T.ex. att de förvalda inställningarna i en tjänst för sociala media är satta så att inte mer information än nödvändigt samlas in, delas ut eller visas)
- en **tjänst inte får göras villkorad** av att personen lämnar sitt *samtycke** till behandling av uppgifter som inte är nödvändiga
- rätt att när som helst begära att få sina **uppgifter raderade**
- rätten att kunna **få sina uppgifter flyttade** från en aktör till en annan,
- Tillsynsmyndigheten (Datainspektionen) kommer genom dataskyddsförordningen ges möjlighet att i vissa fall döma ut en administrativ sanktionsavgift på upp till ***20 miljoner euro*** eller fyra procent av organisationens globala omsättning.

* Personuppgifter får bara behandlas om det har ett tydligt redovisat syfte enligt någon av sex rättsliga grunder: samtycke, avtal, rättslig förpliktelse, intresseavvägning, uppgift av allmänt intresse eller myndighetsutövning samt grundläggande intresse.[6] I de fall individens samtycke behövs ska samtycket dokumenteras, specificera ett tydligt ändamål, vara frivilligt, tidsbegränsat, lätt att förstå och kunna tas tillbaka.

3

3

Skillnader GDPR - PUL

- **Hårdare straff.** Upp till 20 miljoner euro eller fyra procent av företagets årsomsättning.
- **Ökad kontroll.** Kontrollmyndigheter – som Integritetsskyddsmyndigheten (tidigare Datainspektionen) – får utökat ansvar och större resurser.
  Anmälan om säkerhetsproblem inom 72 timmar.
- **En helt ny roll införs.** Dataskyddsombud
- **Strängare regler om samtycke.** Du måste till exempel i efterhand kunna bevisa att samtycke har getts, och samtycke ska när som helst kunna dra tillbaka.
- **”Missbruksregeln” försvinner.** Den så kallade ”missbruksregeln” som gör att e-post vanligtvis undantas från PuL försvinner helt. Organisationer behöver ta ett mycket starkare grepp om hur e-post och bilder används.
- **Dataportabilitet.** Data skall tillhandahållas i ett format som möjliggör överföring. Förhindra inlåsning.

https://assently.com/sv/5-skillnader/

4

4

GDPR – principer I

- **Laglighet, korrekthet och öppenhet**
  All personuppgiftsbehandling måste vara laglig, korrekt och präglas av öppenhet.

- Personuppgiftsbehandlingen ska stå **i rimlig proportion till den nytta** som personuppgiftsbehandlingen innebär.
- Det ska vara klart och tydligt för de registrerade hur ni behandlar deras personuppgifter.

5

5

GDPR – principer II

- **Ändamålsbegränsning**
  Ni får bara samla in personuppgifter för särskilda, uttryckligt angivna och berättigade ändamål.

- Ändamålen måste vara specifika och konkreta, inte luddiga eller otydliga.
- Ändamålet måste också vara berättigat.

6

6

GDPR – principer III

- **Uppgiftsminimering**
  Personuppgifter som behandlas ska vara adekvata, relevanta och inte för omfattande i förhållande till ändamålet.

- Det är med andra ord inte tillåtet att samla in personuppgifter för obestämda framtida behov, för att de kan vara "bra att ha".

7

7

GDPR – principer IV

- **Riktighet**
  Personuppgifter som behandlas ska vara riktiga och, om nödvändigt, uppdaterade.

- Om personuppgifterna inte stämmer ska ni rätta eller radera dem. Det är därför viktigt att det finns rutiner på plats för att kunna **korrigera och ta bort** oriktiga personuppgifter, till exempel om en registrerad begär det.

8

8

GDPR – principer V

- **Lagringsminimering**
  Ni får bara spara personuppgifter så länge som de behövs för ändamålet.

- När personuppgifterna inte längre behövs för ändamålet ska ni radera eller avidentifiera dem. Ni bör därför införa rutiner för gallring av personuppgifter.
- Det kan också vara tillåtet att lagra personuppgifter, tex för vetenskapliga eller historiska forskningsändamål eller statistiska ändamål

9

9

GDPR – principer VI

- **Integritet och konfidentialitet**
  Personuppgifterna måste skyddas på ett bra sätt genom att vidta lämpliga säkerhetsåtgärder.

- Ni måste skydda alla personuppgifter som ni behandlar, så att ingen obehörig kommer åt dem och så att de inte används på ett otillåtet sätt.
- Ni måste därför införa lämpliga tekniska och organisatoriska säkerhetsåtgärder, tex brandväggar kryptering etc.

10

10

GDPR – principer VII

- **Ansvarsskyldighet**
  Ni ansvarar för att följa de grundläggande principerna om personuppgiftsbehandling. Ni måste också kunna visa att ni följer dem och på vilket sätt ni gör det.

- T.ex.: lämna tydlig information till de registrerade, föra register över och dokumentera, upprätta interna riktlinjer för dataskydd, bygga in integritetsvänliga lösningar, göra en konsekvensbedömning innan, utse ett dataskyddsombud, ansluta er till en godkänd uppförandekod eller certifieringsmekanism.

11

Brott mot GDPR

- Sedan GDPR trädde i kraft i maj 2018 har flera företag fällts för brott mot förordningen. De största fallen har handlat om hantering av kunders och användares personuppgifter.
- Till exempel dömdes **Google** i januari till en halv miljard kronor i böter av den franska tillsynsmyndigheten. I september dömdes **British Airways** till cirka 2 miljarder kronor i böter av den brittiska tillsynsmyndigheten, vilket motsvarar 1,5 procent av företagets omsättning.
- Men hur ser det ut när det gäller arbetsgivares behandling av anställdas personuppgifter? Här har det också varit några fall, även om bötes-beloppen inte varit i närheten av Googles och British Airways.

Sjukhus får betala miljonbelopp för övertramp mot GDPR

- Capio St Görans sjukhus, 10 miljoner
- Karolinska universitetssjukhuset, 4 miljoner
- Sahlgrenska universitetssjukhuset, 3,5 miljoner
- Region Östergötland, 2,5 miljoner
- Region Västerbotten
- Totalt 22 miljoner.

- Stora mängder känsliga uppgifter har varit tillgängliga för många anställda.

https://lakartidningen.se/aktuellt/nyheter/2021/05/sjukhus-far-betala-miljonbelopp-for-overtramp-mot-gdpr/

13

Patientdatalagen

För journalföring är patientdatalagen överordnad och styr hur behandlingen får och ska göras. I frågor som inte täcks in av patientdatalagen eller andra överordnade regleringar (som till exempel vid arkivering) så gäller GDPR.

2 § **Lagens syfte är att skydda din integritet och att öka patientsäkerheten.**

Informationshantering inom hälso- och sjukvården ska vara organiserad så att den tillgodoser **patientsäkerhet och god kvalitet samt främjar kostnadseffektivitet**.

Personuppgifter ska utformas och i övrigt behandlas så att patienters och övriga registrerades **integritet respekteras**.

Dokumenterade personuppgifter ska **hanteras och förvaras** så att obehöriga inte får tillgång till dem.

http://www.notisum.se/rnp/document/?id=20080355

14

14

Patientdatalagen

- Syftet med att föra en patientjournal är i första hand att bidra till en god och säker vård av patienten.
- **Målet** med patientdatalagen (PDL 2008:355) är att det ska bli **enklare att samarbeta** mellan olika vårdinrättningar och mellan patienter och vårdgivare med en sammanhållen journalföring.
- Lagen ska göra det möjligt för vårdgivare och patient att **få en samlad bild av patientens vårdhistorik**, oavsett hur många eller vilka vårdgivare patienten har.
- **Patientens insyn** i journalen förbättras kraftigt vilket ökar delaktigheten och självbestämmandet . Enligt patientdatalagen har varje vårdgivare möjlighet att ge patienten tillgång till sin journal elektroniskt, t ex genom att patienten loggar in på nätet med hjälp av e-legitimation.
- **Patienten kan bestämma över vilka vårdenheter som får ta del av journalen** och kan även se vilka vårdenheter som läst journalen.
- Kravet på **samtycke** och **möjligheten att spärra känslig information** är viktiga delar.

15

15

Hälso- och sjukvårdslagen

- **3 kap. Allmänt**
- **1 §** Målet med hälso- och sjukvården är en god hälsa och en vård på lika villkor för hela befolkningen.
- Vården ska ges med respekt för alla människors lika värde och för den enskilda människans värdighet. Den som har det största behovet av hälso- och sjukvård ska ges företräde till vården.

https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/halso--och-sjukvardslag_sfs-2017-30#K3

16