Anteckningar från GDPR-seminarium med ASCRO/LIF 15Maj2018

Peter Asplund, ordförande i ASCRO hälsade välkomna och introducerade GDPR:
Individens rättigheter stärks och databehandlares skyldigheter har förtydligats.

Lotta Wikman Öman, Ahlford Advokatbyrå – GDPR ur ett juridiskt perspektiv.
Nya lagen är delvis motsägelsefull och otydlig tyvärr.
Om man har följt PUL tidigare så är man i en bra sits inför GDPR. Tidigare EU lagstiftning ledde till nationella anpassningar och olika regler i länderna - svårt för internationella verksamheter. Syftet med GDPR är att skydda individerna i det nya informationssamhället med ”big data” och internet. GDPR är en förordning och nya svenska dataskyddslagstiftningen i Sverige (kommer också 25Maj18) är underordnad GDPR.

Personuppgiftsansvarig = fysisk eller juridisk person som bestämmer ändamålen och medlen för behandlingen av personuppgifter.
Personuppgiftsbiträde: fysisk eller jurisdisk person som behandlar personuppgifter åt en personuppgiftsansvarig. T.ex. IT-leverantörer, rädgivare, revisorer, advokater, underleverantörer, CRO.
Underbiträden = personuppgiftsbiträden i andra/tredje/fjärde led, dvs kontrakterad av ett personuppgiftsbiträde. Stora företag som google, Microsoft etc kommer inte skriva avtal specifikt för GDPR, men har bekräftat att de följar GDPR i sin verksamhet.

Personuppgifter gäller endast för levande människor. Gäller även om man har kryptering, denynomiserat, kodat etc. Gäller allt som är sökbart, både pappersform och IT-baserade system. Privatpersoner får ha i princip vilka register vi vill, men inte företag/organisationer/föreningar.

Behandling av personuppgifter får endast ske med rättslig grund (avtal, samtycke, rättslig förpliktelse, skydda grundläggande intressen, allmänt intresse (ffa myndigheter/studieförbund), myndighetsutövning, intresseavvägning, nödvändig behandling. De första två är tydligast (avtal och samtycke) och enklast att bevisa vid tvist. Man får bara hantera/lagra **nödvändiga** uppgifter och inte också ”nice to have”.

Alla som har personuppgifter registrerade (även om uppgifter inte lämnats frivilligt) har rätt att vet hur uppgifter hanteras och vad som hanteras. **Info om detta ska finnas offentligt, på hemsida och i företagspolicy mm. Vilken rättslig grund behandlingen vilar på ska vara definierat. Denna information/policy MÅSTE finnas på plats 25Maj18. Mailsignaturer bör innehålla information om databehandling man gör inom verksamheten.**

Dataskyddsombud behöver utses. Ska finnas på varje företag inom EU (GDPR-området), men måste inte finnas i varje land. Denna person ska vara fristående från företagsledning/styrelse ffa vad gäller hantering av HR-uppgifter mm.

Personuppgiftsbiträden har fått förtydligade skyldigheter, tidigare vilade ansvaret på personuppgiftsansvarig. Viten kan ges även till myndigheter och inte bara till företag och organisationer.

Sk känsligar personuppgifter får **ENDAST** hanteras/lagras vid samtycke eller nödvändigt för social trygghet och skydd. Krav på IT-systemens säkerhets och dokumentation av hur systemen används och vad som görs med data i systemen. Ska finnas procedurbeskrivningar (SOPar osv) för detta. Mycket viktigt att dokumentera händelser/intrång mm och följa upp med förbättringar av rutiner.

Undantaget för sk ostrukturerad information tas bort (sk missbruksregeln). T.ex. all mail som sparas gäller under GDPR. 2 år på sig att bli helt compliant och rensa upp i tidigare register/mail/databaser. Nya uppgifter ska hanteras korrekt från 25Maj2018.

Rätten att bli glömd är svår att hantera. Gäller bara om det finns samtycke eller den rättsliga grunden tillåter det, dvs om uppgifterna lämnats frivilligt. Gäller inte t.ex. information hos skattemyndigheten osv.

Maria Fagerquist – GDPR och forskning

LIF arbetar koordinerat med EFPIA kring GDPR. Huvudfrågorna reflekteras i bifogad presentation.

Forskningsdatautredningen:

- För delar av det utredningen omfattar har utkast till lagrådsremiss varit ute på remiss. Förslag på införande av lag 01Jan2019. Slutbetänkande kommer 25Maj18.
- En av huvudfrågorna för vår bransch är hur personuppgifter får hanteras för forskning, och att forskning initierad av privata aktörer behöver beredas samma möjligheter som forskning initierad av offentliga aktörer. Svensk lagstiftning behöver harmoniseras med den europeiska och tillåta verksamhet/forskning som sker internationellt och i samverkan mellan olika aktörer.

Mall för **Personuppgiftsbiträdesavtal** är under uppdatering och kommer reflektera de nya krav som kommer med GDPR.

Existerande patientsamtycken: Behöver något göras? Globala företag har olika riktlinjer och texter. **De flesta företag kommer att gå ut med skriftlig information till patienter i pågående studier via prövare/sites.**

Patientinformationer efter 25Maj18: Kommer det finnas/komma en malltext? Finns önskemål om detta och om att texten bör komma från den nya Etikprövningsmyndigheten.

Det bör förberedas standardiserade svar/uppföljning med site/leverantörer vad gäller GDPR.