Dataskydd och forskning i Europa och Sverige

Magnus Stenbeck, Karolinska Institutet
Institutionen för neurovetenskap
och
Forskningsdatautredningen (U 2016:04)

Dataskyddsregleringen i EU

Gamla systemet

- 1995 års Dataskyddsdirektiv
  - → Föreskriver att medlemsstaterna ska implementera lagar och förordningar i överensstämmelse med direktivet
- Personuppgiftslagen
  - → svensk implementering
  - → upphör 25 maj 2018

Nya systemet

- 2016 års Allmän Dataskyddsförordning
  - → tillämpas fr.o.m. 25 maj 2018
  - → direkt gällande i alla medlemsländer och associerade länder (t.ex. Norge)
  - → Needs additional union or MS legislation
- All nationell reglering av samma sak(er) är ogiltig/måste upphöra
  - → Svensk tilläggslagstiftning behövs
  - → Många modifikationer av existerande regler behövs

General Data Protection Regulation (”GDPR”)
Allmän dataskyddsförordning

- Ersätter personuppgiftslagen (PUL)
- Ersätter inte tryckfrihetsförordningen (TF) eller yttrandefrihetsgrundlagen (YGL)
  → GDPR lämnar utrymme för dessa
- Ersätter inte lagen om offentlighet och sekretess (OSL)
  → GDPR lämnar utrymme för den
- Behandlar inte etikprövning för forskning
- Är överordnad svensk lagstiftning
  → PUL var subsidiär (annan lagstiftning tar över om den finns)
  → GDPR lämnar inget utrymme för avvikande nationell rätt
- Men tilläggslagstiftning behövs på icke reglerade eller undantagna områden
  → Många artiklar hänvisar till kompletterande unions eller nationell rätt

Gällande lagstiftning som fortsätter att gälla

- Lagen om offentlighet och sekretess
  - → Kapitel 24, 8 § Statistiksekretess
  - → Kapitel 25, 1 § Sekretess i hälso och sjukvården
  - → Vissa skillnader, men båda har ”omvänt skaderekvisit”
    - Den personuppgiftsansvarige måste visa att behandling inte riskerar att medföra men (eller skada) för den registrerade
  - → Kapitel 11, 3 § Sekretessen medföljer uppgifterna om de ska användas för forskningsändamål
- Etikprövningslagen
  - → Etikprövning är obligatorisk bland annat för behandling av känsliga personuppgifter, uppgifter om lagöverträdelser, eller behandling av biologiska prover från levande personer i forskning
  - → Godkännande kan lämnas för forskning i Sverige

Sverige:
Föreslagen ny lagstiftning

- Dataskyddslagen
  → SOU 2017:39 Ny dataskyddslag
- Forskningsdatalagen
  → SOU 2017:50 Personuppgifter för forskningsändamål
- Flertalet lagar och författningar gällande register behålls, men måste anpassas
  → Ds 2017:40 Ändringar i vissa författningar inom Finansdepartementets ansvarsområde med anledning av EU:s dataskyddsreform
  → SOU 2017:66 Dataskydd inom socialdepartementets verksamhetsområde
  → S 2016:04 Biobanksutredningen (slutbetänkande 2017-12-31)

Viktiga frågor för Sverige i Bryssel 2012-2016

- Försvara tryck/yttrandefriheten och offentlighetsprincipen
  - → Resultat: Artiklarna 85 och 86
- Undantag för arkiv-, statistik- och forskningsändamål
  - → Försvara populationbaserade register och fortsatt registerbaserad forskning!
  - → Resultat: tillägg till Artikel 5 b och Artikel 89
    - Undantag från finalitetsprincipen
- Extra stränga restriktioner gällande användning av uppgifter om hälsa utanför direkt användning i vård och behandling
  - → Resultat: borttagna, hälsouppgifter jämställs med andra känsliga personuppgifter
- GDPR tillåter därmed fortsatt registerbaserad forskning om den har stöd i nationell lagstiftning

Centrala begrepp

- Personuppgift
- Känslig personuppgift (”special categories of personal data”)
- Samtycke
- Pseudonymisering
- Forskningsändamål
- Skyddsåtgärd

Personuppgifter

- Personuppgift
  → varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad *en registrerad*), 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 onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet
- Pseudonymisering
  → behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person

Grundläggande principer för personuppgiftsbehandling Artikel 5

- Ska behandlas lagligt, korrekt och öppet
- Ändamålsbegränsning
  → Undantag för arkivering, statistik, forskning
- Uppgiftsminimering
- Korrekthet
  → Undantag föreslaget för arkiveringsändamål
- Lagringsminimering
  → Undantag för arkivering, statistik, forskning
- Integritet (avseende data) och konfidentialitet (=datasäkerhet)
- Ansvarsskyldighet

Personuppgiftsbehandling är laglig enbart om minst en av dessa rättsliga grunder gäller
Artikel 6

a) *Samtycke*
eller personuppgifstbehandling är **nödvändig** för att:

b) Fullgöra ett avtal

c) Fullgöra en rättslig förpliktelse

d) Skydda den registrerades eller någon annans grundläggande intressen

e) *Utföra en uppgift av allmänt intresse*

f) Den personuppgiftansvarige berättigade intresse väger tyngre än den registrerades intresse av att uppgifterna ej behandlas

→ f kan ej användas av myndigheter, men av privata forskningsutövare

→ c och e måste grundas på unionsrätt eller nationell rätt (nytt krav!)

Känsliga personuppgifter (”särskilda kategorier”)
Artikel 9

- Ras, etniskt ursprung
- Politiska åsikter, religiös eller filosofisk övertygelse
- Medlemskap i fackförening
- *Genetiska uppgifter*
- *Biometriska uppgifter för identifikationsändamål*
- Hälsa
- Sexualliv (*sexuell läggning)*

Behandling av känsliga personuppgifter

- är förbjuden
  - → såsom idag
- Undantag om
  - → … uttryckligt samtycke från den registerade
  - → … utom då unionsrätten eller den nationella rätten föreskriver att förbudet inte kan hävas av den registrerade
    - Sverige: den nationella rätten föreskriver obligatorisk etikprövning i vissa fall
  - → Behandlingen är nödvändig för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål
    - I enlighet med artikel 89.1
    - Måste vara grundad på unions-eller nationell rätt
      - → som är proportionell
      - → och innehåller lagstadgade skyddsåtgärder

Samtycke

- Frivilligt
- Specifikt
- Informerat
- Otvetydigt
- Ett uttalande eller en entydig bekräftande handling
- och för känsliga personuppgifter: Uttryckligt

- Den personuppgiftsanvarige ska kunna visa att den registrerade har samtyckt (enligt ovanstående definition)
- Samtycke kan återkallas när som helst
  → och gäller då för fortsatt behandling

Rättslig grund för myndigheter

- Intressavvägning? Nej!
  → Nyhet!
- Samtycke?
  → Tveksamt

Skäl 43:

” För att säkerställa att samtycket lämnas frivilligt bör det inte utgöra giltig rättslig grund för behandling av personuppgifter i ett särskilt fall där det råder betydande ojämlikhet mellan den registrerade och den personuppgiftsansvarige, särskilt om den personuppgiftsansvarige är en offentlig myndighet och det därför är osannolikt att samtycket har lämnats frivilligt när det gäller alla förhållanden som denna särskilda situation omfattar. ”

→ Om en myndighet vill använda samtycke måste man kunna visa (=dokumentera) att det lämnades frivilligt

- *Utföra en uppgift av allmänt intresse blir den huvudsakliga rättsliga grunden*

Skyddsåtgärder

- Obligatoriska i forskning
- Föreslagna i forskningsdatalagen
  - → Etisk prövning
  - → Pseudonymisering
  - → Rätt att motsätta sig deltagande i forskningen (opt out)
- Andra möjligheter
  - → Organisationslösningar
    - Organisatoriskt separerad behandling av direkt identifierbara personuppgifter
  - → Tekniska lösningar
    - Federerade data, remote access, andra distribuerade lösningar, kryptering, loggning, säker auktorisering, etc.

Den registrerades rättigheter

- I princip liknande dagen regler men betydligt mer detaljerade och med högre krav på dokumentation
- Art 12: Klar och tydlig information och kommunikation samt klara och tydliga villkor för utövandet av den registrerades rättigheter
- Art 13:Information som ska tillhandahållas om personuppgifterna samlas in från den registrerade
- Art 14: Information som ska tillhandahållas om personuppgifterna inte har erhållits från den registrerade
- Art 15: rätt till tillgång (” registerutdrag”)
- Art 16: Rätt till rättelse
- Art 17: Rätt till radering (”rätt att bli bortglömd”)
- Art 18: Rätt till begränsning av behandling
- Art 21: Rätt att invända mot behandling
- I de flesta fall finns undantag, t ex
  - → om nödvändigt för forskning, eller
  - → omöjligt att tillgodose

Några viktiga roller i personuppgiftsbehandlingen

- Personuppgiftsansvarig (PuA)
- Personuppgiftsbiträde (PuB)
- Dataskyddsombud

Ansvarsskyldighet

- PuA ansvarar för att tekniska och organisatoriska åtgärder genomförs för att garantera att personuppgiftsbehandlingen följer GDPR
- Detta kan exempelvis innefatta
  - → godkända uppförandekoder (Artikel 40)
  - → certifieringprocedurer (Artikel 42)
  - → Konsekvensbedömning av behandling med avseende på dataskydd (Artikel 35)
- Möjliga administrativa sanktioner:
  - → Upp till 20 000 000 EUR eller 4 % av omsättningen (om högre)
  - → Dataskyddsutredningen har föreslagit en övre gräns på 20 000 000 SEK för myndigheter

Vad behöver göras innan 25 maj 2018?

- Analysera om och hur personuppgiftsbehandlingen i din organisation (fortfarande) är laglig
  → Måste göras genom ordentlig dokumentation
  - Dokumentera existerande behandling
  - Dvs: 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
  - Bygg upp ett dokumentationssystem baserat på GDPR
  - KI kommer att lämna vägledning vad gäller detta - ett pilotprojekt pågår