Arbejdsnotat fra workshop: "Persondata i forskning" afholdt den 24. april 2017

Indhold i notatet:

Formål med workshop og arbejdsnotat

Det Nationale Forum for Forskningsdata Management (https://www.deic.dk/da/datamanagement) etablerede i efteråret 2016 et samarbejde med netværket for "Jura – eScience, forskning og etik" (https://vidensportal.deic.dk/netvaerket-for-jura) om afholdelse af en aktivitet indenfor konceptet "Train-the-trainers" med henblik på at styrke og udbygge juridiske kompetencer hos jurister og andre, der arbejder i forskningsstøttende enheder på universiteter, nationale dataarkiver og forskningsbiblioteker.

I alt blev der afholdt tre workshops i foråret 2017:

- Adgang til og råderet over data
- Juridiske udfordringer ved reproducerbar forskning
- Persondata i forskning

Fra hver workshop publiceres et arbejdsnotat, som indeholder en opsamling og perspektivering på dagenes faglige tema. Arbejdsnotatet skal ses som en første "indhegning" af de juridiske problemstillinger.

Arbejdsgruppen bag de tre afholdte workshops:

Jurist Hanne Johansen, Det Kgl. Bibliotek, Aarhus (*skiftede i foråret 2017 arbejdsplads*)
Jurist Line Slemming, Det Kgl. Bibliotek Aarhus, lihs@kb.dk
Jurist Kathrine Tvorup Pajkes, AAU, ktp@adm.aau.dk
Prof. Morten Rosenmeier, KU, morten.rosenmeier@jur.ku.dk
Lektor Clement Salung Petersen, KU, clement.petersen@jur.ku.dk
Jurist Lars Engelstoft, SDU, lae@sdu.dk
Områdedirektør Ellen Knudsen, Det Kgl. Bibliotek, Aarhus, evk@kb.dk
Projektleder Helle Meldgaard, DeIC, helle.meldgaard@deic.dk

Dagens program "Persondata i forskning":

9.00 **Ankomst,** kaffe/te og netværk

10.00 **Velkommen** v/Lars Engelstoft, SDU og Kathrine Tvorup Pajkes, AAU

10.10 **Deltagerpræsentation**

10.25 **Den gældende persondatalovs regulering af forskning** – se arbejdsnotat 1 s. 3 – 9.
v/Fuldmægtig Signe V. Abildskov, Datatilsynet

- Personoplysninger – anonymisering og pseudoanonymisering
- Dataansvarlig og databehandler problematikken i relation til forskningsprojekter med flere parter, hvor flere projektledere er sammen om at bestemme over projektet, og dermed behandlingen af personoplysninger.
- § 10 Hjemmel og videregivelse
- § 27 Overførsel til tredjeland
- Den registreredes rettigheder i relation til forskning
- Håndtering af data efter projektets afslutning

12.00 **Frokost**

12.45 **Den fremtidige persondatabeskyttelsesforordnings regulering af forskning**
v/Professor Peter Blume, KU – se arbejdsnotat 2 s. 10 - 14

- Hvilke bestemmelser i forordningen er relevant at tage i betragtning allerede nu ift. vejledning af forskere.
- Tager forordningen højde for forskning? Er der f.eks. en bestemmelse, der ligner § 10 (hjemmel til forskning og videregivelse)?

14.30 **Pause** (Kaffe/te og kage)

14.45 **Konklusioner og opsamling** med henblik på input til notat
v/Kathrine Tvorup Pajkes, Lars Engelstrup og Clement Salung Pedersen.

15.30 **Tak for i dag**

Arbejdsnotat 1: Den gældende persondatalovs regulering af forskning

Notatet er udarbejdet på baggrund af oplæg v/Signe V. Abildskov, Datatilsynet fra den 24. april 2017.

Introduktion til persondataloven – relevante bestemmelser

Persondatalovens anvendelsesområde

Persondataloven er baseret på et EU direktiv. Da det er et EU direktiv er følgen, at direktivet er implementeret forskelligt i alle EU lande.

Persondataloven finder anvendelse når der sker elektronisk behandling af personoplysninger eller manuel behandling, hvor personoplysningerne indgår i et register.

Personoplysninger defineres som enhver form for information om en identificeret eller identificerbar fysisk person jf. § 3, nr. 1. Persondataloven omfatter således både almindelige, følsomme og fortrolige personoplysninger.

Behandling defineres som enhver form for håndtering af personoplysninger. F.eks. indsamling, opbevaring, sletning osv.

Anonymisering

Personoplysning**:** ”Enhver form for information om en identificeret eller identificerbar *fysisk person*.”

Anonymisering inebærer, at enhver rimelig mulighed for at identificere personen er fjernet. Vigtigt at alle muligheder for at finde personen er udvisket. Hvis der findes en ”nøgle”, der kan bruges til at identificere en person, så er oplysningen ikke anonymiseret.

Man skal i vurderingen tage alle mulige hjælpemidler, der med rimelighed kan tages i betragtning med – altså, kan man på nogen måde komme frem til hvem personen er på baggrund af disse oplysninger. Det er først når dette ikke er muligt, at det er at kategorisere som anonymiseret.

Er f.eks. navn, adresse eller personnummer erstattet af en kode, et løbenummer el.lign., der kan føres tilbage til den oprindelige individuelle personoplysning, vil der stadigvæk være tale om en personoplysning.

Krypterede og pseudonymiserede oplysninger

- Skal leve op til kravene i persondataloven, da der stadig er tale om personoplysninger. Kryptering og pseudonymisering er sikkerhedsforanstaltninger

Biologisk materiale

Biologisk materiale er kun en personoplysning, når oplysningerne, der er bundet i det biologiske materiale, kan henføres til enkeltpersoner.

Efter databeskyttelsesforordningen er blod altid en personoplysning.

En biobank er:

- En struktureret samling af menneskeligt biologiske materiale
- Der er tilgængeligt efter bestemte kriterier
- og som indeholder oplysninger der er bundet i det biologiske materiale, som kan henføres til enkeltpersoner

Modsat er en samling af biologisk materiale, der ikke skal anvendes til fremtidig brug, (altså biologisk materiale, der kun skal bruges til ét projekt) ikke en biobank.

En biobank er et manuelt register, hvorefter at persondataloven finder anvendelse, herunder bl.a. anmeldelsespligten.

Geografisk område

Hvis man er indenfor EUs grænser, så finder enten den danske persondatalov eller en af de øvrige EU landes persondatalov anvendelse.

Hvis den dataansvarlige er etableret i Danmark, så finder den danske Persondatalov anvendelse

Hvis den dataansvarlige er etableret i et andet EU land, så finder vedkommendes lands lov anvendelse.

Hvis den dataansvarlige er etableret i et tredjeland, så finder den danske persondatalov anvendelse i følgende situationer:

a. behandlingen af oplysninger sker under benyttelse af hjælpemidler, der befinder sig i Danmark, medmindre hjælpemidlerne kun benyttes med henblik på forsendelse af oplysninger gennem Det Europæiske Fællesskabs område eller
b. Indsamling af oplysninger sker i Danmark med henblik på behandling i et tredjeland.

Dataansvarlig / Databehandler

Dataansvarlige:

- afgør til hvilke formål og med hvilke hjælpemidler oplysningerne behandles
- f.eks. den myndighed/virksomhed, der har taget initiativ til projektet
- f.eks. den myndighed/virksomhed, der finansierer projektet

Databehandleren:

- behandler oplysningerne efter instruktion.
- behandler ikke oplysningerne til egne formål
- behandlingen af oplysninger sker på vegne af den dataansvarlige

Delt dataansvar:

- parterne er begge dataansvarlige
- parterne er solidarisk ansvarlige

Delt dataansvar er ikke omfattet af universiteternes fællesanmeldelse, og vil derfor skulle anmeldes særskilt til Datatilsynet. Datatilsynet vil stille spørgsmål til, hvordan man vil overhole reglerne, herunder f.eks. reglen om indsigtsret.

Deltager spørgsmål: Det gør, at vi får det svært, når vi i fælleskab laver en database hver med oplysninger, og forsætte med at lave databehandleraftaler, så bliver vi til dataansvarlige dermed laver videregivelse, når de to i samme projekt henter oplysninger til analysen fra begge databaser.

Signe: Ja, det er noget rod, men vi anerkender hos os, at I arbejder således.

Persondatalovens bestemmelser

Bestemmelserne:

- Behandlingsregler
  - Hjemmelsregler (særligt §§ 6-11)
  - Grundlæggende principper (§ 5)
  - Overførsel af oplysninger til tredjelande (§ 27)
- De registreredes rettigheder
  - bl.a. oplysningspligt, indsigtsret, indsigelsesret
- Datasikkerhed (§§ 41-42)
- Anmeldelse

Hjemmel

§ 10 kan bruges som hjemmel til at behandle semifølsomme (§ 8) og følsomme (§ 7) personoplysninger i videnskabeligt øjemed (forskning) uden samtykke.

Betingelserne er følgende:

- Forskning eller statistik
- Nødvendig for udførelsen af undersøgelsen
- Væsentlig samfundsmæssig interesse
- Ej senere behandles til andet end statistisk eller videnskabelig øjemed
- Videregivelse kræver tilladelse fra Datatilsynet

Hjemlen til at behandle almindelige personoplysninger (§ 6) i forskning er § 6, stk. 1, nr. 5

Samtykke:

- Skal leve op til § 3, nr. 8. (specifikt og informeret)
- Samtykke kan tilbagekaldes

Samtykke kan bruges som hjemmel i stedet for § 10, og samtykke kan bruges til videregivelse.

Deltager spørgsmål: I specialeopgaver, kan man forsat bruge § 10?

Signe: Vi mener, at både speciale og bachelor opgaver falder under bestemmelsen. Uagtet af det, så er det vigtigt, at den dataansvarlige tager stilling til, hvad denne anmelder.

Grundlæggende betingelser § 5

- **God databehandlingsskik** jf. § 5, stk. 1
- **Formålsbestemthed** jf. § 5, stk. 2.
  - Udtrykkeligt angivne og saglige formmål
  - Senere behandling må ikke være uforeneligt med formålet. Senere behandling i historisk, statistisk eller videnskabeligt øjemed er ikke uforenligt med det oprindelige formål.
- **Proportionalitetprincippet** jf. § 5, stk. 3
  - Oplysningerne skal være relevante og tilstrækkelige.
- **Datakvalitet** jf. § 5, stk. 4

- **Tidsbegrænsning** jf. § 5, stk. 5.
  - Personoplysninger må ikke opbevares længere tid end nødvendigt af hensyn til formålet med indsamlingen.

Anmeldelse

	Offentlige dataansvarlige	Private dataansvarlige
Anmeldelse	Pligt til at anmelde behandling af følsomme (§§ 7 og 8) og fortrolige oplysninger. Anmeldelsen skal ske inden behandlingen påbegyndes.	Private dataansvarlige skal anmelde behandling af følsomme oplysninger (§§ 7 og 8). Anmeldelsen skal ske inden behandlingen påbegyndes.
Datatilsynets behandling	Datatilsynet registrerer anmeldelsen i Fortegnelsen og sender en udtalelse. Offentlige dataansvarlige skal overholde sikkerhedsbekendtgørelsen.	Datatilsynet registrerer anmeldelsen i Fortegnelsen og sender en godkendelse med en række vilkår.
Undtagelser til anmeldelses-pligt		- Studenterprojekter og opgaver, hvor den studerende indhenter samtykke. - Forskningsprojekter, der er god-kendt af en Videnskabsetisk Komité. - kliniske forsøg med lægemidler - kliniske afprøvninger af medicinsk udstyr - pligtmæssig sikkerhedsovervågning af lægemidler/medicinsk udstyr
Fælles/paraply anmeldelse	Alle universiteter har en fællesanmeld-else, der dækker forskning bredt. Alle regioner har en paraplyanmeldelse, der dækker sundhedsvidenskabeligt forskning og godkendte kliniske kvalitetsdatabaser.	

Der opstår ofte et spørgsmål om, hvorvidt det er forskeren eller universitetet, der er dataansvarlig. Retsvirkningen af at det er forskeren personligt er, at reglerne om private dataansvarlige finder anvendelse, og retsvirkningen af at universitetet er dataansvarlig er, at reglerne om offentlige dataansvarlige finder anvendelse.

Spørgsmål til vurdering:

- Hvem initierer projektet?
- Finansiering?
- Varighed?
- Hvem deltager?
- Aflønnes af myndigheden?
- Hvilket it-udstyr og hvem ejer udstyret?
- Instruktionsbeføjelse?
- Hvad sker der, hvis forskeren finder nyt job?
- Hvem kan tage skridt til sletning?

→ Universitetet og forskeren må afgøre det.

Deltager spørgsmål: Så leder det lidt til spørgsmålet: er den studerende dataansvarlig eller er universitetet?

Signe: Det kommer meget an på, i hvor stor grad deres projekt er selvstændigt. Om de laver det på vegne af universitetet. Fx i mit eget speciale, var det meget selvstændigt udenom universitet, foruden om enkelte samtaler med min vejleder. Her ville jeg være dataansvarlig, hvis jeg havde brugt personoplysninger. Omvendt er der situationer, hvor nogle har meget tæt tilknytning til universitetet i deres projekt.

Overladelse, videregivelse og/eller overførsel af personoplysninger

Databehandler

En databehandler behandler oplysninger efter instruks fra den dataansvarlige og på den dataansvarliges vegne.

Når en dataansvarlig bruger en databehandler, har den dataansvarlige pligt til:

- At sikre, at der indgås en skriftlig databehandleraftale med databehandleren.
- Såfremt databehandleren bruger en underdatabehandler, så skal den dataansvarlige
  - enten indgå en underdatabehandleraftale direkte med underdatabehandleren
  - eller give databehandleren fuldmagt til at indgå en underdatabehandleraftale med underdatabehandleren.
- Aktivt sikre/påse at sikkerhedsforanstaltninger overholdes hos databehandler.
- Husk at anføre databehandlere i anmeldelsen til datatilsynet.

Videregivelse jf. § 10, stk. 3

Retsvirkningen af videregivelse er, at giveren og modtageren hver i sær er dataansvarlig for egen kopi af personoplysningerne. (Det er ikke solidarisk ansvar).

Hovedregel: Man må ikke videregive oplysninger til tredjemand.
Undtagelse: Kan ske med forudgående tilladelse fra Datatilsynet på nærmere vilkår, og kun til videnskabelig eller statistisk brug.

Reglen om videregivelse omfatter både følsomme og almindelige personoplysninger.

Særligt vedrørende fælles- og paraplyanmeldelserne:
Offentlige myndigheder, der har en fælles- eller paraplyanmeldelse har en general tilladelse til at videregive fortrolige personoplysninger, forudsat at de af Datatilsynet fastsatte vilkår overholdes.

Vilkårene er bl.a. at:

- der alene kan ske videregivelse indenfor Danmarks grænser
- til konkrete forskningsprojekter, der er anmeldt

Overførsel til tredjelande

Overførsel kan både være databehandling og videregivelse.
Tredjelande er lande uden for EU/EØS

Overførsel kræver hjemmel i persondatalovens § 27

- Kommissioners standardkontrakter
- Samtykke
- Tredjemand
- Privacy Shield

De registreredes rettigheder

Oplysningspligt (§§ 28 og 29)

- Begrænset oplysningspligt i forskningsprojekter
- Afhænger af det konkrete projekt (antal registrerede)

Indsigt (§§ 31 og 32)

- Den registrerede har ikke indsigtsret, hvis vedkommendes oplysninger bliver behandlet i videnskabeligt øjemed, jf. § 32, stk. 4.

Indsigelse (persondatalovens § 35)

- Den registrerede har ret til, at gøre indsigelse mod at den dataansvarlige behandler vedkommendes oplysninger.
- Hvis indsigelse er berettiget, må behandlingen ikke længere omfatte de pågældende oplysninger, jf. § 35, stk. 2.

Hvis behandling i videnskabeligt eller statistisk øjemed → indsigelsen skal som altovervejende hovedregel ikke tages til følge.

Sikkerhed

Almindelige sikkerhedsregler (§ 41, stk. 3)

Den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger:

- Hændeligt eller ulovligt tilintetgøres
- Fortabes eller forringes
- Oplysningerne kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven

Sikkerhed for offentlige myndigheder

Sikkerhedsbekendtgørelsen:

- Interne bestemmelser om sikkerhedsforanstaltninger (organisation, autorisationer, kontrol, fysisk sikkerhed mv.)
- Fornøden instruktion af medarbejdere (f.eks. forskere) i behandling af personoplysninger
- Autorisation og adgangskontrol
- Logning: maskinel registrering af alle anvendelser af personoplysninger - bruger og tidspunkt for behandlingen (Særlige logningskrav for forskningsprojekter, jf. § 19, stk. 4)

Sikkerhed for private

Vilkår i tilladelser fra Datatilsynet:

- Manuelt materiale, herunder udskrifter, fejl- og kontrollister mv. med oplysninger, der direkte eller indirekte kan henføres til bestemte personer, skal opbevares forsvarligt aflåst og på en sådan måde, at uvedkommende ikke kan gøre sig bekendt med indholdet.

- Identifikationsoplysninger skal krypteres eller erstattes af et kodenummer eller lignende. Alternativt kan alle oplysninger lagres krypteret. Krypteringsnøgle, kodenøgle mv. skal opbevares forsvarligt og adskilt fra personoplysningerne.
- Adgangen til personoplysninger må kun finde sted ved benyttelse af et fortroligt password. Password skal udskiftes mindst én gang om året.
- Ved overførsel af personoplysninger via internettet eller andet eksternt netværk → Som minimum kryptering, hvis følsomme personoplysninger overføres via internettet (eller andre åbne net).
- USB, sikkerhedskopier af data mv. skal opbevares forsvarligt aflåst og således, at uvedkommende ikke kan få adgang til oplysningerne.
    - Datatilsynets krav til undtagne behandlinger (se tilsynets hjemmeside)

Sikkerhed for biobanker

- Skal opbevares forsvarligt aflåst, så uvedkommende ikke kan få adgang
- Skal sikres, at materialet ikke fortabes, forringes eller hændeligt eller ulovligt tilintetgøres
- Materiale med personnummer eller navn skal opbevares under iagttagelse af særlige sikkerhedshensyn
- Der skal være interne retningslinjer for opbevaringen
- Materiale skal destrueres eller anonymiseres, når projektet er afsluttet

Ved projektets afslutning

Personoplysninger (herunder biologisk materiale) skal slettes, anonymiseres eller tilintetgøres senest ved projektets afslutning, medmindre en fortsat opbevaring kræves efter anden gældende lovgivning/regulering. Det må efterfølgende ikke være muligt at identificere enkeltpersoner i projektet.

Alternativt kan oplysningerne overføres til arkiv efter arkivlovens regler.

Sletning af oplysninger fra elektroniske medier skal ske på en sådan måde, at oplysningerne ikke kan genetableres.

Nærværende notat 1 er udarbejdet af
Kathrine T. Pajkes, Specialkonsulent, AAU

Notatet er udarbejdet på baggrund af:
Signe V. Abildskovs præsentations materiale
og studentermedhjælp Christian Kroghs referat.

Arbejdsnotat 2: Den fremtidige persondatabeskyttelsesforordnings regulering af forskning

Notatet er udarbejdet på baggrund af oplæg v/ Professor Peter Blume, KU fra den 24. april 2017.

Ret til databeskyttelse

Forordningen får først virkning den 25/5/2018 og forordningens udgangspunkt er, at enhver har ret til databeskyttelse i henhold til det europæiske charter.

Charterets artikel 8 er det grundlæggende udgangspunkt for forordningen.

At gøre retten til databeskyttelse til en grundlæggende værdi betyder også, at domstolene vil anlægge en borgervendt fortolkning, dvs. til fordel for borgeren over for den dataansvarlige.

Før forordning

Retsgrundlaget er ganske gammelt og siden persondataloven i 2000, er der ikke ændret, og det er det, man nu laver om.

Det grundlæggende i reguleringen er ***business as usual***.

Behandling omfatter stadig enhver aktivitet i forbindelse med personoplysninger (jf. også GOOGLE-dommen: https://www.datatilsynet.dk/nyheder/nyhed/artikel/personoplysninger-paa-soegemaskiner/) og enhver oplysning, som kan *relateres til en identificeret eller identificerbar fysisk person, er en personoplysning.*

Omfattet er også IP-adresser, både statiske og dynamiske IP-adresser.

Personoplysningsbegrebet er derfor ret bredt – det bliver samtidigt kun større og større.

For at undgå misbrug af personoplysninger skal forskere så vidt muligt *pseudonymisere* personoplysningerne.

Døde personer

Der vil forekomme ændringer i opfattelsen af de dødes stilling i forhold til databeskyttelse. Oplysninger om døde er efter Persondataloven omfattet så længe, det giver mening.

Som udgangspunkt gælder forordningen ikke for døde personer, men forordningen giver medlemsstaterne muligheden for at bestemme andet.

Hvorfor nye regler?

Der er flere grunde til at lave nye regler:

1. Den teknologisk udvikling

Det er lang tid siden sidste direktiv, og dermed er der fulgt en enorm udvikling.

2. Øget transparens

Det skal være overskueligt for borgerne end det er i dag. Det viser sig ved at man har styrket retten for borgerne.

3. Den ansvarlige

Nye princip for den ansvarlige som sanktioneres.

4. Bedre rettigheder for borgerne

Det er en af kommissionens hovedargumenter, at det er det, forordningen skal medføre.

5. Bedre sikkerhed

Der skal være mere fokus på at sikkerheden skal være i top. Sikkerheden skal være et meget prioriteret felt. Der er så mange farer i den elektroniske verden, at man må sikre sig at oplysningerne ikke bliver misbrugt.

6. Større grad af harmonisering

Kræver derfor større ensartede regler i alle EU-lande. Overholdes reglerne i Danmark, kan vi frit overføre til andre EU-lande, uden at spørge om tilladelse.

7. Alvor

Nu skal man sætte fokus på persondatabeskyttelse, hvor sanktionsordningen får sin ret.

Databeskyttelse er ikke det eneste

Retten til databeskyttelse er ingen absolut ret, men er en ret blandt flere, jf. præambel nr. 4.

Forskning

- Forskning er et legitimt formål, når man skal behandle personoplysninger.
- Ofte behandles der følsomme oplysninger i forskningsmæssig sammenhæng. Ses specielt på sundhedsområdet.
- Når det kommer til forskning rejser spørgsmålet sig, om det er privat forskning eller offentlig forskning. Forordningen gælder både privat forskning og offentlig forskning. Men selvom det er udgangspunktet, er der mange regler i forordningen, som kun gælder i den ene sektor.
    - Forskning har traditionelt været forbundet med den private sektor.

Dataforordningens struktur

Når man ser på, hvordan forordningen er opbygget, så baseres den på følgende:

1. Principper
2. Betingelser
3. Rettigheder
4. Sikkerhed
5. Overførsel
6. Kontrol og sanktioner

Principper i forordningen

- Der findes de ”lette” principper, som ikke giver nogen problemer:
    - God databehandlingsskik

  - Sagligt formål
  - Proportionalitet
  - Der skal være kvalitet og sikkerhed
- Der findes de "Svære" principper, som siger, at man ikke må behandle oplysninger uden for formålet, de skulle bruges til. *F.eks. hos lægen med en blodprøve, hvor den skal bruges til andet end formålet, den var beregnet til.*
- Minimalitet.
  Er det nødvendigt at behandle personoplysningerne? Oplysninger må ej hellere opbevares længere end nødvendigt. Tidsbegrænsningen gælder dog ikke forskning, jf. art. 5, 1 e)
- Almindelige personoplysninger og følsomme personoplysninger.
  - Sondringen mellem hvornår noget er en almindelig oplysning og en følsom oplysning. Alle de oplysninger, som er følsomme i dag, er også følsomme efter forordningen. Persondatalovens § 8 oplysninger bliver dog stort set almindelige oplysninger efter forordningen. De følsomme oplysninger omfatter dog også biometriske oplysninger.
  - Personnummer? Overlades til de enkelte lande. Persondatalovens § 11 opretholdes.
- Persondatalovens § 6, stk. 1, nr. 7 (interesseafvejningsreglen) gælder efter forordningen ikke for det offentlige.

Rettigheder

- Den første rettighed man har som borger, er **underretnings-sikringen** for de oplysninger, der behandles om én.
- Man har ydermere **ret til indsigt og korrektion** i oplysningerne, og ret til at gøre indsigelse, hvis den dataansvarlige bryder reglerne.
- Man har også ret til at få **slettet oplysninger** om én i kraft af retten til at blive glemt. Retten til at blive glemt er dog udtyndet i den endelige udgave af forordningen.
- **Portabilitet** – Det vil sige, at en person har ret til at **få udleveret de oplysninger** som personen selv har overgivet til den dataansvarlige.
  Portabilitet er en ny ret, og der er **ikke nogen undtagelse for forskning**.

Sikkerhed

- **Ansvarlig brug af persondata** - krav om dokumentation. Der er ingen krav om anvendelse, som det er i dag.
- **Sikkerhed** – der er ingen konkrete sikkerhedskrav. Ingen Sikkerhedsbekendtgørelse.
  Det er op til den dataansvarlige at sørge for at kun personer, der skal have adgang til data, får adgang til data.
- **Meddelelsespligt** indebærer at senest 72 timer efter fundet sikkerhedsbrist skal Datatilsynet orienteres. Er der tale om meget følsomme oplysninger, skal de relevante personer kontaktes.
- **Konsekvensanalyse** (DPIA) indebærer, at man nøje skal vurdere, om disse risici kunne blive til virkelighed.

Overførsler

- Forordningen er nogenlunde uændret i forhold til i dag. Man sondrer ikke mellem, om det er i EU og til godkendte tredjelande. Men her slår man fast i forordningen, at de lande der i dag er godkendte, at

de også skal godkendes fra 25 maj. Man fastslår samtidigt principper om, at man hvert fjerde år, skal revurdere de lande, som har opnået godkendelse.

- Dernæst er der alle de andre, som skal godkendes i forhold til de kommende målestokke.
- Man giver samtidigt muligheden for at kunne overføre til de internationale organisationer (f.eks. FN institutioner).
    - Der er der ikke grundlag for i dag, eftersom det jo ikke er et land.

Hjælp til dataanvendelse

- Databeskyttelsesrådgiveren, et system brugt i Norge og Tyskland, som er en person, der passer på og har ekspertise i persondataret. DPO er obligatorisk i det offentlige.

Internationalt forskningssamarbejde = dataoverførsler

- I EU
- Godkendte tredjelande – hver fjerde år skal de efterses – inden 2022.
- Øvrige tredjelande
- Ny mulighed for at overføre informationer til Internationale organisationer – områder – sektorer

Særlig regulering af forskning

Der er to typer regler om forskning. Den generelle regel i art. 89, men også nogle specielle regler, som fastslår at :

Behandling af følsomme persondata

Art 9(2j) indeholder en række undtagelser til reglen om forbud for at behandle følsomme person-oplysninger.

Indholdet i bestemmelsen:

- **Rimeligt** forhold til målet
- Det skal være **fornuftigt**, at man skal bruge de personoplysninger for at løfte forskningsopgaven. Saglige grunde
- Man skal huske at **respekterer databeskyttelsen**
- **Passende og specifikke foranstaltninger**

Art. 89(1) – Indhold i bestemmelsen

- **Fornødne garantier** – Man må behandle oplysningerne, hvis man har levet op til de fornødne garantier. Garantier som skal sikre databeskyttelse
- **Sikkerhed** – man skal leve op til reglerne om sikkerhed
- **Minimering** – det skal være således at man skal tage hensyn til om det er nødvendigt at behandle personoplysninger. Kan man klare sig med oplysninger som ikke er personhenførebare.
- Brugen af **pseudonymer**.

Art. 89(2) - Rettigheder kan udelukkes eller begrænses:

- Indsigt – den pågældende person har derfor ikke ret til at vide hvordan oplysningerne (blodet) bliver behandlet
- Korrektion – Som ovenstående ikke ret til korrektion af data
- Begrænsning – Man har ikke ret til begrænsning
- Indsigelse – Man har ikke nogen ret til indsigelse hellere
- Underretningspligt (14(5b)) – Ingen underretningspligt
- Sletning/Glemt (17(3d)) – Derfor heller ikke ret til at blive glemt

Art. 89(4)

Skal man bruge det til andre formål, kan man gøre det hvis man opfylder forordningens almindelige regler. Fraviger Persondatalovens § 10, stk. 2 (nydannelse).

Business as usual:

- Persondatalovens § 10
- Anmeldelse/Tilladelse (artikel 36(5): Tryghed over for bureaukrati
- Sanktion Artikel 83
    - Art. 83 drejer sig om de bøder de pålægges brud. Bøder om er omfattet af det øverste system for bøder.

Selvdisciplin

- Forskningen må vogte forskningen
- Forskningsetik

Deltager spørgsmål: Har du nogen fornemmelse af, om der er en mulighed for om den enkelte medlemsstat kan tage stilling til, hvorvidt offentlige myndigheder kan ifalde bøder og i hvilket omfang?

Peter Blume: Umiddelbart skulle man tro, at pilen drejede, så det ikke blev tilfældet. Men min fornemmelse er, at man godt ved, at det vil medrøre stor ballade. Justitsministeriet er i gang med at udarbejde en betænkning. Den kommer her sidst i maj.

Deltager spørgsmål: Kunne man forestille sig en regel kyndig IT ansat?

Peter Blume: Man skal sikre sig mod inhabilitet.

Nærværende notat 1 er udarbejdet af
Lars Engelstoft, Legal Advisor, SDU

Notatet er udarbejdet på baggrund af:
Peter Blumes præsentations materiale
og studentermedhjælp Christian Kroghs referat.

Referenceliste se bl.a.:

- "**Den nye Persondataret – Persondataforordningen**" af Peter Blume, 2016
- "**Persondataforordningen – en håndbog for praktikere**" af Nis Peter Dall, Jesper Lange mark og Amalie Langebæk, 2016
- Link til **Datatilsynet**: https://www.datatilsynet.dk/forside/
  - **Ny betænkning om Databeskyttelsesforordningen**: https://www.datatilsynet.dk/nyheder/nyhed/artikel/ny-betaenkning-om-databeskyttelsesforordningen/
  - **Husk de 12 spørgsmål vedrørende databeskyttelsesforordningen**: https://www.datatilsynet.dk/nyheder/nyhed/artikel/husk-de-12-spoergsmaal-vedroerende-databeskyttelsesforordningen/
- Link til "**Forskerportalen**" - http://forskerportalen.dk/da/ Forskerportalen er udviklet af Udvalget til Beskyttelse af Videnskabeligt Arbejde (UBVA), som er et stående udvalg under Akademikerne, der varetager akademikernes interesser i ophavsretlige og patentretlige spørgsmål.
  - **Forskningsdata**: http://forskerportalen.dk/da/category/forskningsdata/