

Vejledning om behandling af personoplysninger til forskning

1. Hvad er personoplysninger?

Personoplysninger defineres som oplysninger, der direkte eller indirekte kan identificere en fysisk person. Det kan være et navn, registreringsnummer på en bil eller oplysninger om et sygdomsforløb. Det kan også være erfaringer, oplevelser eller andre ting, som kan henføres til en bestemt person. Det betyder, at flere oplysninger, som i sammenhæng kan knyttes til en person, vil også være personoplysninger - selvom de enkelte oplysninger i sig selv, ikke ville være personoplysninger.

Man skelner således mellem direkte identifikation og indirekte identifikation. En direkte identifikation er f.eks. et navn eller personnummer. Indirekte identifikation er alder, køn, uddannelse og andre oplysninger, som ikke direkte giver mulighed for at identificere en person – men som kan anvendes, i sammenhæng med andre oplysninger, til identifikation.

Der er ingen grænser for, hvilke oplysninger, der kan være personhenførbare, og det vil derfor være en konkret vurdering i hvert tilfælde. Skal man f.eks. lave en spørgeskemaundersøgelse, kan hvert svar godt være anonymt, men koblingen af svarerne vil i nogle tilfælde give mulighed for at identificere en person. Det kan være der bliver stillet spørgsmål omkring klassetrin, skole, køn, fritidsinteresser og om forældrene er skilt. De enkelte svar vil ikke være personoplysninger, men når resultaterne af det enkelte skema samles i en helhed, vil man kunne identificere deltageren – i nogle tilfælde.

Selvom der muligvis kan være flere elever, der har svaret det samme, og der dermed f.eks. vil være to, som kan identificeres, vil det fortsat være personoplysninger, da det er så snæver en gruppe, at man ikke er i tvivl. Man skal derfor se oplysningerne i en større sammenhæng, og ikke se på hvert spørgsmål isoleret. Direkte identifikatorer er dem, som umiddelbart kan identificere personen uden at have behov for yderligere informationer. Det er f.eks. det fulde navn eller CPR.nr. på en person – hvor den ene oplysning alene, kan identificere personen.

Indirekte identifikatorer er dem, som ikke kan stå alene, hvis de skal knyttes til en person. Postnr. er f.eks. ikke en personoplysning i sig selv, men kan være det, hvis det knyttes til andre oplysninger og dermed, i sammenhæng, gør det muligt at identificere personen.

2. Hvad er behandling af personoplysninger?

Al brug af personoplysninger er behandling i juridisk forstand. Det er således enhver aktivitet eller række af aktiviteter som personoplysninger gøres til genstand for.

Det kan være indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfindning, søgning, brug, videregivelse, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse. Også en kiggeadgang er omfattet af begrebet behandling.

Eksempel:

En forsker ønsker at undersøge fremtiden inden for droneindustrien. Der udsendes et spørgeskema til en række virksomheder, inden for dette felt. De skal svare på deres tanker om udviklingen og hvordan de ser deres virksomhed udvikle sig.

Der vil være forskel i størrelsen på de enkelte virksomheder og deres indtjening, hvilket vil kunne identificere dem. Da der er enkeltmandsvirksomheder blandt de adspurgte vil der være tale om indsamling af personoplysninger.

Det er således enhver håndtering af data – i bred forstand.

2.1 Databehandler vs. dataansvarlig

Det er afgørende at få klarlagt dataansvaret, når der sker behandling af personoplysninger. Den dataansvarlige er den organisation, person eller virksomhed, der har det overordnede ansvar for behandlingen af data. Det er således den dataansvarlige, der tager initiativ til behandlingen og beslutter hvilket formål og med hvilke hjælpemidler, der skal ske behandling. Den enkelte forsker er ikke dataansvarlig i ovennævnte forstand, det er derimod SDU.

Databehandleren er en ekstern person eller virksomhed (i forhold til den dataansvarlige), som behandler

personoplysninger for den dataansvarlige. Det er således efter instruks, og normalt også på opfordring af den dataansvarlige.

Databehandleren har ansvaret for at opbevare og behandle data i overensstemmelse med den aftale, der sætter rammer for behandlingen. Aftalen kaldes en databehandlertale, og skal indgås mellem den dataansvarlige og databehandleren. Det er vigtigt at have rollerne på plads forud for opstarten af behandlingerne.

Eksempel:

En forsker skal bruge spytprøver fra patienter på OUH med en særlig sygdom. Lægen på OUH indsamler prøven, men ikke som led i behandlingen. Lægen (OUH) er derfor databehandler for forskeren (SDU).

Overvejelser:

- Ville samarbejdsparten selv have indsamlet oplysningerne, hvis SDU ikke havde bedt dem om det?
 - Hvis ikke, så er der tale om databehandling.

I forbindelse med udarbejdelsen af en databehandlertale, er det juristerne ved RIO, der står for forhandlingene. Vi har en standardaftale, som der tages udgangspunkt i. Det er ligeledes hos RIO, alle databehandlertaler skal registreres og underskrives. Vi vil derfor bede dig om at sende en mail til sdu.persondata@sdu.dk, hvis der er brug for hjælp med en databehandlertale.

Når SDU er dataansvarlig i forbindelse med indsamling af data til forskningsprojekter, skal projekterne anmeldes til SDU RIO. Læs mere om anmeldelse her: <http://sdu.dk/anmeldelse>

3. Anonymisering vs. pseudonymisering

Det er væsentligt at gøre sig klart, om der er tale om anonyme data eller personoplysninger. Hvis data er tilstrækkeligt anonymiserede, finder reglerne i databeskyttelsesforordningen ikke anvendelse, og derfor kan man behandle data inden for en langt friere ramme. Det er imidlertid meget svært at anonymisere oplysningerne således, at de ikke længere er identificerbare. Anonymiseringen skal være uigenkaldelig, hvilket betyder, at man ikke må kunne føre oplysningerne tilbage til deres oprindelige form. Indsamler man anonyme data eller anonymiserer personoplysningerne efter endt brug, er de ikke længere omfattet af GDPR og man kan derfor frit bruge dem.

3.1 Pseudonymisering

Pseudonyme data er også personoplysninger. Pseudonymisering er den handling, som gør at oplysningerne ikke er direkte personhenførbare, men som heller ikke sikrer total anonymitet. Den typiske situation er, når man udskifter navnet med et andet navn eller CPR.nr. med en kode. Så længe, der findes en nøgle, som kan tilbageføre data til direkte personhenførbare oplysninger (til den oprindelige form), er oplysningerne ikke anonyme – men pseudonyme. En sletning af nøglen er ikke ensbetydende med at data bliver anonyme. Det afgørende for, om der er tale om pseudonyme data er, om der findes en nøgle til at decode (afkode) oplysninger.

Pseudonymisering sikrer at en evt. uvedkommende ikke umiddelbart kan identificere personerne ud fra datasættet. En identificering vil kræve supplerende oplysninger. Pseudonymisering er således betegnelsen for udskiftningen af den direkte identifikation med nogle pseudonymer eller koder. Koderne skal opbevares separat, og skal ligeledes beskyttet teknisk, således at det ikke er muligt for en udefrakommende at sammenstille koder og data og derved identificere personerne i datasættet. Så længe nøglen til pseudonymiseringen findes, er der tale om pseudonyme data.

Hvor det er muligt at pseudonymisere personoplysningerne, bør man gøre det så hurtigt som muligt, efter at oplysningerne er indsamlet. Som nævnt ovenfor er pseudonyme data stadig omfattet af regler i GDPR, men det er en effektiv sikkerhedsforanstaltning. Skulle oplysningerne komme til uvedkommendes kendskab er skaden ikke så stor som tilfældet vil være, hvis direkte personhenførbare oplysninger kommer til uvedkommendes kendskab.

Eksempel:

*En blodprøve påføres et ID.nr. i stedet for CPR.nr.
Det er kun den dataansvarlige, der kender
identiteterne bag hvert ID.nr.
Der er tale om pseudonyme data.*

3.2 Anonymisering

Anonyme oplysninger er ikke personhenførbare, og betyder at det ikke er muligt at identificere en person ud fra oplysninger i datasættet. Der findes nogle forskellige værktøjer til at anonymisere og sikre, at der reelt bliver tale om anonyme data. Hvis oplysningerne, med en rimelig indsats, kan anvendes til at identificere en fysisk person, er der ikke tale om anonyme oplysninger.

Hvad der nærmere ligger i begrebet *en rimelig indsats*, er svært at klarlægge. Det er en vurdering af de tekniske muligheder, der er for at identificere personen. Man skal tage højde for alle de hjælpemidler der, med rimelighed, kan tænkes anvendt i forsøget på at identificere en person.

Når det handler om andre muligheder for at identificere personer ud fra information i åbne spørgsmål og risikoen for at oplysningerne bliver tilgængelig, skal denne risiko vurderes i hvert tilfælde ud fra forskningsprojektets emne og de bagvedlæggende omstændigheder.

Det vil formentligt være svært at lave en fuldstændig anonymisering, men data anses for at være anonyme, hvis det ikke er muligt, med en rimelig indsats, at identificere en given person. Når det skal vurderes om det er muligt at identificere en person, skal man tage alle hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse for at identificere den pågældende person, i betragtning. Man skal også have for øje, om andre er i besiddelse af oplysninger, der gør det muligt at identificere den enkelte.

4. Valg af behandlingshjemmel

Når man skal behandle personoplysninger til forskningsbrug, er der flere valgmuligheder i forhold til lovhjemmel. For det første, skal man gøre sig klart om der er tale om personoplysninger. Herefter skal det vurderes hvilken hjemmel, der passer bedst til projektet og giver deltagerne de bedste rettigheder. Der er forskel på rettighederne og kravene i forhold til de forskellige lovhjemler.

Uanset hvilken hjemmel man vælger, skal oplysningspligten opfyldes, så deltageren ved, hvad vedkommendes personoplysninger anvendes til. Hvis man bruger SDU's skabeloner, er man dækket ind i forhold til kravene til oplysningspligt.

Generelt skal man tænke på, at man ikke må behandle flere oplysninger, end det er relevant for projektet. Man skal derfor minimere databehandlingen og de data man anvender mest muligt, så man alene beder om de oplysninger, der er nødvendige. Dernæst kan man minimere behandlingerne ved at slette/anonymisere unødvendige oplysninger

i takt med, man ikke længere har behov for dem. Dette er naturligvis alene en mulighed i forhold til de oplysninger, man ikke har brug for i forhold til verificering af forskningsresultater.

Hvis man skal indsamle, bruge osv. personoplysninger til et forskningsprojekt og man ved, at oplysningerne ikke senere skal bruges til andet end forskning, vil det ofte være en mulighed at bruge databeskyttelseslovens § 10 (og/eller databeskyttelsesforordningens artikel 6, stk. 1. e) som hjemmelsgrundlag. Derved undgås de risici der kan være forbundet med at benytte samtykke som hjemmelsgrundlag, som angivet nedenfor.

En anden hjemmel er samtykket, som giver deltageren en række rettigheder, men som også giver mulighed for at lave aftaler omkring offentliggørelse og deling af data. Det vigtigt, man vælger den korrekte hjemmel før man starter indsamlingen af personoplysninger. SDU RIO har skrevet en vejledning om valg af behandlingshjemmel, som beskriver mere indgående hvad man skal være opmærksom på.

5. Anonymiseringsmetoder

Der findes nogle forskellige teknikker til at anonymisere. Man kan gøre sig nogle tanker forud for indsamlingen, så man tilpasser sin indsamling af data, på en måde, så det alene er de relevante oplysninger, der indsamles og i en form, som er så lidt personhenførbare som muligt. Det kan f.eks. være ved at lave lukkede spørgsmål, hvor deltageren ikke har mulighed for at tilføje egne oplysninger. På den måde får man ikke flere detaljer end dem, der er behov for. Man skal derfor være påpasselig med at indsætte spørgsmål, hvor det er muligt at skrive fritext, men afgrænse til afkrydsning af forudbestemte muligheder.

Det er også muligt at ændre oprindelseskommune til at opdele i kategorier som urban, semi-urban, landlig osv. Dette vil minimere risikoen for identifikation – men kan stå ikke alene. Det vil være en del af en større anonymiseringsproces.

Man kan også tilføje *noise* eller støj, så oplysningerne tilføjes nogle ekstra oplysninger eller detaljer. Det kan f.eks. være ved at ændre alderen på deltageren med +/- 2 år. Så vil data, til en vis grad være nøjagtige men ikke umiddelbare tilgængelig for uvedkommende – hvis støjen er en del af den fulde anonymisering. Det kan også være en teknik at fjerne eller ændre oplysninger, så f.eks. personer med AIDS bliver kategoriseret som personer med svær, langvarig sygdom og andre personer er blot kategoriserede som raske eller syge. På den måde skelnes der ikke mellem de forskellige sygdomme, men deltagerne deles op i grupper, som fortsat er relevante for forskningsprojektet.

Man kan også kategorisere de øvrige oplysninger i grupper, så der ikke fremgår så mange personhenførbare detaljer. Ved at dele deltagerne op i kategorier f.eks. i forhold til alder, uddannelsessted, arbejdsplads, bosted og husholdning. Det kan kategoriseres som 41-45 år, længevarende uddannelse, butik, by i Jylland og kone og to børn. På den måde er oplysningerne så generelle, at det er svært at identificere personen, da beskrivelsen kan passe på flere forskellige personer.

Eksempel:

I marts 2019 udtalte Datatilsynet alvorlig kritik vedr. et taxaselskabs behandling af personoplysninger. Selskabet havde 'anonymiseret' kundernes oplysninger ved at slette kundernes navne men ikke deres telefonnr. Dermed er der fortsat mulighed for at identificere den enkelte kunde – ud fra oplysninger om dato for kørslen, kørselens begyndelses- og sluttidspunkt, antal kørte kilometer, betalingen, GPS-koordinater. Dermed medfører at oplysningerne alene er pseudonyme og derfor stadig personhenførbare.

Nedenfor findes en overordnet oversigt over typen af oplysninger og hvad der kan gøres for at anonymisere dem. De **følsomme** oplysninger er markeret med fed.

6. Anmeldelse af forskningsprojekt

Forskningsprojekter skal anmeldes til SDU's fortegnelse, hvis der behandles personoplysninger i projektet. Anmeldelsen skal ske via universitetets fortegnelse, som SDU RIO forvalter. SDU RIO skal, på forespørgsel fra Datatilsynet, kunne fremvise en fortegnelse over igangværende projekter på universitetet, hvor der behandles personoplysninger, til brug for Datatilsynets inspektion. For at anmelde projektet skal der udfyldes et anmeldelsesskema i den elektroniske fortegnelse. Det sker ved at tilgå SDU's fortegnelsesside her: <https://www.sdu.dk/da/anmeldelse>.

Herefter kommer en række spørgsmål, som alle relaterer sig til projektet – herunder om der behandles almindelige eller følsomme oplysninger, hvor længe det forventes, at projektet vil vare osv. Når man har udfyldt skemaet, trykker man indsend. SDU RIO gennemgår herefter det anmeldte materiale med henblik på at sikre, at de databeskyttelsesretlige krav er opfyldt. En udtalelse fremsendes herefter til anmelderen.

7. Godkendelse fra andre myndigheder

Nogle projekter kræver yderligere godkendelse, end den, man får hos RIO. Sundhedsvidenskabelige projekter, hvor der indgår biologisk materiale fra mennesker, skal godkendes af Den Nationale Videnskabsetiske Komité. Hvis der skal anvendes udtræk af oplysninger i patientjournaler, uden samtykke fra patienterne, kræver det en godkendelse fra Regionsrådet.

Derudover kan der være tilfælde, hvor man ønsker at modtage oplysninger fra andre myndigheder, virksomheder eller registre mv., og her kræver det den afgivende parts godkendelse eller accept, før man kan modtage oplysningerne.

De fleste har et videregivelsessystem, hvor man kan søge om at modtage oplysninger. Andre ønsker at udarbejde en videregivelseserklæring, som man kan sende forbi SDU RIO til gennemlæsning. Når man modtager oplysningerne fra modparten, bliver SDU dataansvarlig for oplysningerne og det skal anmeldes til fortegnelsen.

8. Videregivelse eller overladelse af forskningsdata

Juristerne i SDU RIO skal inddrages, når forskningsdata ønskes videregivet/overladt til andre med henblik på at sikre, at de databeskyttelsesretlige regler bliver overholdt.

Videregivelse er den situation, hvor man videregiver personoplysninger til eksterne parter uden for SDU. Det er altså personer, virksomheder, kommuner eller andre, som ikke er knyttet til eller ansat ved SDU.

Videregivelse kan også ske til parter uden for EU.

Overladelse er den situation, hvor der overlades data til en anden SDU-kollega og dermed forbliver data internt på SDU. Det vil typisk være en forsker, som skal bruge data til et nyt projekt.

Du kan finde overlades- og videregivelsesblanketter her:

https://www.sdu.dk/da/forskning/service_til_forskere/juridiske_spoergsmaal/anmeldelse_til_datatilsynet/videregivelse.

9. Har du spørgsmål?

Spørgsmål vedr. behandling af persondata stiles til sdu.persondata@sdu.dk.

Dette skema kan være en rettesnor til at vurdere, hvilken teknik der er anvendelige i forhold til at anonymisere personoplysninger. Forskellige metoder kan anvendes – afhængig af oplysningens type.

Identifikations type	Direkte identifikator	Stærk indirekte identifikator	Indirekte identifikator	Anonymiseringsmetode
CPR.nr.	X			Sletning
Fulde navn	X			Sletning/ændring
Emailadresse	X	X		Sletning
Telefonnr.		X		Sletning
Postnummer			X	Sletning/Kategorisering
Landsdel			X	Kategorisering
Kommune			X	Kategorisering
Region			X	Sletning
Lydfil (af stemme)	X			Sletning/sløring
Video (af person)	X			Sletning/sløring
Foto (af person)	X			Sletning/sløring
Fødselsår			X	Kategorisering
Alder			X	Kategorisering
Køn			X	Sletning
Ægteskabelig status			X	Sletning
Husholdnings- sammensætning			X	Kategorisering
Erhverv			X	Kategorisering
Uddannelse			X	Kategorisering
Arbejdssituation		(X)	X	Sletning
Modersprog			X	Kategorisering
Nationalitet			X	Kategorisering
Arbejdsplads		(X)	X	Kategorisering
Registreringsnummer på bil		X		Sletning
Hjemmeside		(X)	X	Sletning
Studenternr.		X		Sletning
Kontonr.		X		Sletning
Helbredsoplysninger		(X)		Kategorisering/sletning
IP-adresse		X		Sletning
Etnicitet		(X)		Kategorisering/sletning
<i>Strafbare forhold</i>			X	Kategorisering/sletning
Politiske forhold			X	Kategorisering
Religiøse forhold			X	Kategorisering
Sociale forhold			X	Kategorisering/sletning
Seksuel orientering			X	Sletning
Biometriske data		X		Sletning

