Modtager(e): Alle ansatte inden for økonomiområdet på AU
Alle ansatte i AU Økonomi og Bygninger

Instruks om behandling af personoplysninger

Som ansat inden for økonomiområdet arbejder du med personoplysninger i forskellige sammenhænge f.eks. økonomiadministration af eksterne projekter og udarbejdelse af budgetter.

Formålet med denne instruks er at vejlede dig om, hvordan du korrekt anvender, registrerer, behandler og opbevarer disse oplysninger i overensstemmelse med forvaltningsloven, straffeloven og persondataretten.
Hver gang du behandler en personoplysning, skal du have et sagligt formål. Du må kun hente personoplysninger fra fagsystemer (f.eks. Navision, promark mv), kuber eller andre datakilder, hvis oplysningerne er direkte relevante for dit arbejde. Persondataretten giver den nødvendige hjemmel til at registrere og behandle de oplysninger, der er nødvendige i sagsbehandlingen.

Hvad er personoplysninger i henhold til lovgivningen?
Persondataretten inddeler personoplysninger i:

1. Særlige personoplysninger (følsomme)
2. Cpr. nummer
3. Almindelige personoplysninger

1) De særlige personoplysninger er: Racemæssig eller etnisk baggrund, politisk religiøs eller filosofisk overbevisning, fagforening, seksuel orientering og helbredsmæssige forhold. Derudover er genetiske og biometriske data omfattet.

   De særlige personoplysninger, må du som udgangspunkt ikke indhente, registrere og behandle uden udtrykkeligt samtykke. For så vidt angår helbredsoplysninger, må disse behandles uden udtrykkeligt samtykke, hvis det er nødvendigt, for at universitetet overholder sine forpligtelser f.eks. i forhold til forskelsbehandlingsloven og sygedagpengeloven.

AU Økonomi og Bygninger
Aarhus Universitet
Trøjborgvej 82-84
8000 Aarhus C

Tlf.: +45 8715 0000
E-mail: au@au.dk
Web: www.au.dk

2) Cpr. nummer er en almindelig oplysning, der f.eks. kan anvendes som journalnummer. Cpr. nummer må ikke offentliggøres (jf. lov om behandling af personoplysninger §11, stk. 3).

3) De almindelige oplysninger er alle andre oplysninger, f.eks. navn, adresse, telefon, fødselsdato, titel, bolig, bil, familieforhold, statsborgerskab m.v.

Tavshedspligt
Du har tavshedspligt (jf. forvaltningsloven og straffeloven) med hensyn til de fortrolige oplysninger, du som et led i dit arbejde har adgang til. Du må gerne udtale dig generelt om, hvilke arbejdsopgaver du løser, men du må ikke udtale dig om enkeltpersoners oplysninger til uvedkommende. Ifølge forvaltningsloven er oplysninger om enkeltpersoners private, herunder økonomiske forhold fortrolige. Tavshedspligt inden for økonomiområdet gælder f.eks.:

- Oplysninger om løn
- En række oplysninger i forbindelse med udbud – herunder timepriser mv.
- Ansættelsesforhold – herunder viden om kommende ændringer eks. ansættelsesophør eller pension.
- En række oplysninger i forbindelse med ansøgninger om eksterne midler

Du må ikke hverken mundtligt eller skriftligt videregive oplysninger til udenforstående, kolleger eller ledere, der ikke har en tjenstlig anledning til at modtage disse oplysninger.

Hvis du er i tvivl, om du i konkrete tilfælde er berettiget til at videregive oplysninger, bør du søge tvivlen afklaret ved dialog med din nærmeste leder.

Tavshedspligten ophører ikke, når din ansættelse på AU ophører, jvf. straffelovens bestemmelser.

Særligt om cpr. nummer
Universitetet må som offentlig myndighed gerne anvende cpr. nummer til identificering af medarbejdere, også i korrespondance med andre offentlige myndigheder. Det afgørende er, at udveksling af oplysninger om cpr. nummer sker på en sikker måde.

Det anses for sikkert at sende cpr. nummer inden for eget netværk, via en mailadresse der ender på au.dk. Hvis du sender uden for AU's netværk, skal det sendes sikkert f.eks. krypteret eller i e-boks.

Du bør altid overveje, om det er nødvendigt at anvende cpr. nummer. Ofte er AU ID tilstrækkeligt.

Lønoplysninger
Lønoplysninger – som kostpris, ressourcenummer og lignende – skal håndteres på samme vis som cpr. nummer.

Sletning af unødvendig data
Udtræk af data fra IT-systemer indeholder ofte en række data, der ikke skal anvendes i den efterfølgende sagsbehandling. Disse data skal du som udgangspunkt slette før du påbegynder databehandlingen og evt. videresender oplysningerne/data.
Unødvendige data, er data, hvor der ikke er et lovligt og sagligt formål til anvendelse heraf – eks. cpr. nummer i et dataudtræk, hvor cpr. nummeret ikke skal anvendes i den efterfølgende databehandling.

E-mails indeholdende personoplysninger
Sender du e-mails, der indeholder personoplysninger, skal du gøre modtager opmærksom på dette ved at indsætte nedenstående tekst i mailsignaturen før "Venlig hilsen/Med venlig hilsen":

> *" Vær opmærksom på, at denne mail indeholder personoplysninger. Det betyder, at du dels skal sikre, at personoplysningerne ikke unødigt tilgår andre samt, at oplysningerne straks slettes, når oplysningerne ikke længere er nødvendige i forhold til det formål, de er fremsendt" – jf. Håndtering af mail*

Engelsk version:

> *"Please note that this email contains personal data. You must ensure that this data cannot be accessed by anyone else without good reason, and that it is deleted immediately when it is no longer required in relation to the purpose for which it was sent."*

Ovenstående orientering må kun fremgå af mailsignaturen, hvis en mail indeholder personoplysninger. Endvidere må der ikke anvendes en KAN-version af orienteringen, altså at mailen kan indeholde personoplysninger. Det er dig som afsender, der skal træffe afgørelsen, hver gang du sender en mail.

Skal du sende personoplysninger til modtagere uden for AU, skal du anvende en sikker kommunikationsform jf. Håndtering af mail.
Du må ikke sende personoplysninger, som ikke er nødvendige i forhold til sagen.

Modtager du e-mails indeholdende unødvendige personoplysninger for sagsbehandlingen, bør du gøre afsender opmærksom herpå.

Husk e-mails indeholdende personoplysninger skal slettes efter senest 30 dage i indbakke, udbakke og papirkurv. Workzone anvendes til journalisering, hvis oplysningerne skal opbevares for eftertiden.

Anvendelse af sikre fællesdrev
Et sikkert fællesdrev kan anvendes til deling af data i tværgående samarbejde (f.eks. mellem økonomifunktionen på fakulteterne og institutterne).

Fordelen ved anvendelse af sikre drev er muligheden for yderligere sikkerhedsmekanismer såsom udvidet logning og kryptering. Endvidere ligger data kun ét sted, modsat mail hvor data ligger mange steder (indbakke/slettet post/sendt post + diverse PC'ere, telefoner m.v.)

Data må ikke opbevares længere end det er nødvendigt i forhold til sagsbehandlingen. Såfremt der er behov for/krav til at data opbevares efter endt sagsbehandling, skal disse journaliseres i Workzone.

Anvendelse af sikre drev er ikke en erstatning til journalisering i Workzone, hvis oplysningerne i øvrigt er omfattet af journaliseringspligt. Inden for økonomiområdet er der udarbejdet journaliseringsvejledning for eksterne projekter, som kan tilgås på økonomiportalen.

Anvendelse af systemer
Er vi på sikker grund vedr. persondata i systemerne?
Der skal være en hjemmel til den pågældende databehandlingsaktivitet:

- Kreditoradministration og Købsfakturahåndtering
- Debitoradministration og Salgsfakturering
- Rejseafregning
- Betalingsoverførsler
- Ressourceallokering og Tidsregistrering
- Lønbudgettering
- Budget- og budgetopfølgning
- Regnskabsrapportering

Er det forbudt at anvende cpr numre i Navision?

- Nej, AU må gerne registrere oplysninger om kreditors, debitors, medarbejders og ressources CPR-nummer i Navision Stat
- Brug altid det felt, der for hvert af de nævnte kartoteker er beregnet til CPR-nummer. Typisk vil dette felt være navngivet enten 'CPR-nr.' eller 'CPR nummer'.
- Hvis AU angiver CPR-numre i andre felter, end de dertil beregnede, gælder det imidlertid, at du ikke kan stole 100 % på den nye Navision Stat rapport, der kan anvendes i tilfælde af, at borgere gør deres indsigelsesret gældende jf. den nye EU persondataforordning.

Anvendelsen af 'fritekstfelter' i Økonomisystemerne:

- Der må som udgangspunkt IKKE angives følsomme persondata eller personhenførbare data i fritekstfelter beregnet til andre formål, f.eks. beskrivelses- og bemærkningslinjefelter.
- Det betyder, at der ikke må skrives CPR nummer, AU ID mv. i beskrivelsen for en postering i Navision, IndFak, RejsUd mv.
  Undtagelsesvis, indtil andet fremgår af nærværende instruks, kan Ressourcenummer skrives i fritekstfeltet, men kun hvis det er absolut nødvendigt.

Retten til at blive glemt

- Retten til at blive glemt, og dermed til at få slettet sine data, skal kunne efterkommes medmindre, at kravet er i strid med regnskabsbekendtgørelsens § 44 om opbevaring af regnskabsmateriale og borgerens egen interesse.
- Derfor vil det være meget atypisk, at en borger, medarbejder eller anden samarbejdspartner, hvorom der findes data i f. eks Navision Stat, kan kræve sine data slettet.
- Gyldigt regnskabsmateriale skal gemmes i minimum 5 år regnet fra regnskabsårets afslutning
- Det vil være teknisk og datakonsistensmæssigt uforsvarligt at slette udvalgte transaktionsdata
- Det gælder omvendt, at hvis data er ældre end 5 år og der ikke længere kan findes argumenter for opretholdelse af data, at borgerens krav om retten til at blive glemt skal imødekommes.

Pligt til videregivelse af oplysninger til andre

I en lang række tilfælde er universitetet som myndighed både berettiget og forpligtet til at videregive oplysninger om enkeltpersoner. Det drejer sig f.eks. om lønudgifter i projekter med ekstern finansiering.

Ved videregivelse af oplysningerne skal der ikke indhentes samtykke fra medarbejderen, da AU har direkte hjemmel i forordningens artikel 6 og 9 og Databeskyttelseslovens § 12 til behandling af oplysninger i ansættelsesforhold og videregivelse, hvor AU er retligt/overenskomstmæssigt forpligtet f.eks. videregivelse til revisionen, SKAT m.fl.

Det betyder, at du må sende oplysninger til bevillingsgiver eller andre organisationer, som AU samarbejder med omkring en bevilling, men det skal ske på en sikker måde f.eks. krypteret eller i e-boks.

Anvendelse af IT-systemerne

Alle data skal gemmes i sikre IT-systemer, hvor man kun kan få adgang efter tildeling af password.

IT-systemer, hvor AU profilen og et password anvendes til at logge ind, betragtes som sikre IT-systemer.

Du må kun slå op i og arbejde med de personoplysninger, der er relevante i forhold til de arbejdsopgaver, du skal løse. Det betyder, at du ikke må skaffe dig oplysninger om enkeltpersoner, som du ikke i kraft af dine arbejdsopgaver har behov for at få oplysninger om. Det betyder også, at du ikke må slå dine egne oplysninger op i f.eks. Workzone.

Inden for økonomi arbejdes der med en række forskellige systemer, der indeholder persondata. Du skal ud over tavshedspligten være opmærksom på overholdelse af AU's informationssikkerhedspolitik, herunder at:

- aktivere kodeordsbeskyttet skærmlås på din computer, når du forlader din arbejdsstation, og når den er uden for din synsvidde
- sørge for at din computer og mobile enheder automatisk aktiverer skærmlås efter 5-10 min. inaktivitet
- aldrig at overdrage dine kodeord til andre personer, heller ikke til kolleger.

Opbevaring og transport af personoplysninger
Du skal jf. AU`s informationssikkerhedspolitik påse, at personoplysninger opbevares, fragtes og beskyttes sikkert, så risikoen for at oplysningerne kommer til uvedkommendes kendskab mindskes mest muligt. Det gælder uanset om oplysningerne findes i papirform eller på elektroniske medier. Du skal påse, at data ikke opbevares i længere tid, end det er nødvendigt for behandling af den konkrete sag. Anonymiserede dokumenter må gerne opbevares.

Papirdokumenter
Personoplysninger på papir skal opbevares aflåst, når de ikke er i brug (dvs. aflåst skab eller kontor). Dokumenter med personoplysninger må ikke unødigt tilgå andre. Dokumenterne skal straks makuleres, når oplysningerne ikke længere er nødvendige i forhold til det formål, de er indsamlet; eller journaliseres i et aflåst skab/lokale.

De relevante oplysninger på papirdokumenter journaliseres inden de slettes ved afslutning af den konkrete sagsbehandling.
Der opfordres til at begrænse brugen af papirdokumenter.

Hvad betragtes som personoplysninger?
Personoplysninger er enhver form for information, der kan henføres til bestemte personer, også selv om dette forudsætter kendskab til et personnummer, registreringsnummer eller lignende. Også oplysninger i form af f.eks. et billede eller et fingeraftryk er personoplysninger.
Selv om oplysninger som et navn eller en adresse er erstattet af en kode, er det stadig en personoplysning, hvis koden kan føres tilbage til den oprindelige personoplysning. F.eks. er oplysninger, der er krypteret, fortsat personoplysninger, så længe der er nogen, der kan gøre oplysningerne læsbare og identificere de personer, det drejer sig om.

Reglerne for, under hvilke betingelser offentlige myndigheder og private virksomheder, foreninger m.v. må behandle personoplysninger, er i vidt omfang skønsmæssige. Det vil derfor ofte afhænge af en konkret vurdering i den enkelte situation, om betingelserne for at behandle personoplysninger er opfyldt.

Hvis du (ud fra andre love såsom offentlighedsloven) har ret til at foretage en behandling af persondata, skal følgende desuden altid være opfyldt:

- Lovlighed, rimelighed og gennemsigtighed
- Formålsbegrænsning

- Dataminimering
- Rigtighed
- Opbevaringsbegrænsning
- Integritet og fortrolighed

Læs mere herom i Databeskyttelsesforordningen.