Hvem må få adgang til personoplysninger

Hvad må medarbejdere ved AAU give af personoplysninger til andre hhv. kolleger og eksterne parter i henhold til databeskyttelsesreglerne?

Introduktion

I rigtig mange af de arbejdsopgaver, vi hver især sidder med, er der behov for, at andre bliver involveret og dermed får adgang til personoplysninger. Her kan både være tale om kolleger enten i samme afdeling eller fra andre dele af organisationen, og så kan der være tale om eksterne parter fra f.eks. en IT-leverandør, et konsulentfirma, en offentlig myndighed eller en samarbejdspartner fra et forskningsprojekt.

Hvad?

Før man kan definere, *'hvad'* der må gives videre, bør man kigge på *'til hvad'* (formålet).

Formål

Vores anvendelse af personoplysninger er helt grundlæggende bundet sammen med det formål, oplysningerne skal anvendes til. Det betyder, at al anvendelse af personoplysninger skal ske til et formål, og dette formål skal være udtrykkeligt og legitimt. Kravet om udtrykkelighed betyder, det skal være klart for andre, og især de personer, oplysningerne handler om, hvad det er, de konkrete oplysninger, skal bruges til. Kravet til legitimitet betyder, at formålet, personoplysningerne skal bruges til, skal være lovligt (ikke at forveksle med hjemmelskravet, der bliver beskrevet nedenunder). Det betyder, at vi ikke må behandle eller videregive personoplysninger til formål som skatteunddragelse, hvidvaskning eller andre kriminelle formål.

Hjemmel

Ud over det specifikke formål skal vi have en hjemmel til at behandle personoplysningerne, hvilket betyder, at vi skal kunne leve op til kravene for behandlingsgrundlag som beskrevet i databeskyttelsesreglerne. Hjemmel er et juridisk begreb, der betyder retlig bemyndigelse eller behandlingsgrundlag. Så for at der kan behandles personoplysningerne til formålet, skal vi have hjemmel (ikke at forveksle med at formålet skal være lovligt, som nævnt ovenfor). F.eks. er der hjemmel at behandle personoplysninger, hvis det er som led i en kontrakt mellem AAU og den person oplysningerne vedrører, hvilket også gælder for handlinger, der går forud for kontraktindgåelsen. Yderligere må AAU behandle personoplysninger, hvis det er for at overholde en retlig forpligtigelse, eller hvis vi har samtykke fra de personer, hvis oplysninger vi behandler.

Hvilke data må gives videre?

Kravene til formål og hjemmel gør sig også gældende, når vi giver personoplysninger videre til andre. Dem, vi giver oplysningerne til, skal have et formål med at få oplysningerne, og de er underlagt de samme krav: formålet skal være udtrykkeligt og legitimt.

Mængden eller kategorierne af personoplysninger, vi må give videre, er defineret af formålet. I databeskyttelsesforordningen er det beskrevet, at ved behandling af personoplysninger skal disse være *tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles.* Det betyder, at vi skal have tilstrækkelige personoplysninger, men ikke flere end hvad der er nødvendigt, for at vi kan løse den opgave, som er formålet med at behandle personoplysningerne. Dette gør sig også gældende, når vi giver personoplysninger videre: personoplysningerne skal være nødvendige, for at modtageren kan løse sin opgave.

Formålet og hjemlen definerer dermed, hvad vi må give videre af personoplysninger. Det betyder, at vi i nogle situationer kan give alt videre, i andre situationer kan vi intet give videre, og nogle gange kan vi give dele af et datasæt med personoplysninger videre.

Eksempler:

1: SU-Styrelsen

Der må foretages en delvis videregivelse af relevante personoplysninger til SU-styrelsen om den studerendes optagelse på et studie. Dette sker i forbindelse med, at en studerende optages på et studie, og der skal søges om SU. AAU videregiver f.eks. oplysninger til SU-styrelsen, der bekræfter, at den studerende er optaget på et studie og dermed er kvalificeret til at modtage SU. Til dette skal SU-styrelsen modtage de relevante oplysninger til formålet bl.a. den studerendes identitet og bekræftelse på optagelse, men de behøver ikke vide, at den studerende sidder som lægmand i National Videnskabsetisk Komité, eller om den studerende har anmodet om adgang til et bederum på universitetet pga. vedkommendes religiøse overbevisning.

2: Censor

Der må delvist videregives relevante personoplysninger til censorer om den studerende i forbindelse med eksamen. Censorernes formål med at behandle personoplysninger knytter sig til den eksamen, de er inde for at bedømme. Det betyder, at de udelukkende skal have udleveret personoplysninger, som knytter sig til den enkelte studerende til den respektive eksamen og dermed ikke behøver vide noget om hele holdet, om andre eksamener eller øvrige personoplysninger om den studerende, som ikke er relevante for den respektive eksamen, f.eks. at et familiemedlem umiddelbart forinden er død af kræft

3: Studerende

Der må delvist gives oplysninger videre til studerende om andre studerende i forbindelse med holdlister og studiegrupper. De studerendes formål med at kende disse oplysninger er for at kunne kontakte deres hold for at koordinere gruppe-opgaver eller lignende. Det betyder, at der kan udleveres oplysninger, der er relevante for at kunne koordinere disse opgaver, og der må f.eks. ikke gives oplysninger videre om CPR numre, sygdomsforløb eller dispensationer.

Hvem?

Når man skal kigge på *'hvem',* der må gives personoplysninger til, så kigges der på, hvem der er *autoriseret* til at udføre den opgave (formål), som personoplysningerne gives videre til.

Autoriserede personer kan både være kolleger, eksterne enkeltpersoner eller virksomheder/organisationer, der handler i regi af en opgave, de skal udføre for eller i samarbejde med AAU eller på selvstændig vis, hvor de skal udføre en opgave for dem selv.

Typisk for virksomheder og organisationer, især af en vis størrelse, så har de et antal af medarbejdere, som er autoriseret til at udføre en række opgaver til et bestemt formål, og derfor må hele denne gruppe af medarbejdere få adgang til personoplysningerne.

Interne modtagere (medarbejdere på AAU)

Når der er tale om medarbejdere, så skal det sikres, at det kun er de medarbejdere, der er beskæftiget med de opgaver, som er formålet med behandlingen af personoplysningerne, der modtager oplysningerne. I databeskyttelsesreglerne hedder dette, at en medarbejder er *autoriseret* til at have adgang til personoplysningerne. Det betyder også, at andre ansatte, for hvem oplysningerne er uvedkommende, ikke må have adgang til disse. Af samme grund må personoplysninger heller ikke opbevares ukritisk i diverse systemer.

Autorisationen for, om den enkelte medarbejder må have adgang til og arbejde med et sæt af personoplysninger, afhænger af de arbejdsopgaver, vedkommendes stillingsbetegnelse medfører. Så for at du må give en kollega adgang til et datasæt med personoplysninger, så skal denne kollega være autoriseret til at behandle netop dette datasæt med personoplysninger, hvilket vil sige, at denne kollega skal have arbejdsopgaver, der nødvendiggør adgang til bestemte personoplysningerne om en specifik person eller persongruppe Alle andre medarbejdere er i forbindelse med den omhandlede behandling uvedkommende og må ikke have adgang til personoplysningerne.

Eksterne modtagere

Når der er tale om eksterne parter, der skal have adgang til personoplysninger, så kaldes det overordnet for en *overførsel* af personoplysninger.

En overførsel af personoplysninger er, når eksterne parter får adgang til de personoplysninger, AAU har. En *overførsel* dækker både over, når AAU videregiver personoplysninger til en anden dataansvarlig, og når AAU overlader behandlingen af personoplysninger til en databehandler.

Videregivelse

AAU videregiver f.eks. personoplysninger til SU-Styrelsen, som behandler personoplysninger til egne formål: de skal bl.a. bruge personoplysninger om studerende ved AAU for at kunne tildele dem SU

Ved en videregivelse skal AAU forinden sikre sig, at der videregives til et legitimt formål.

Overladelse

AAU *overlader* en behandling af personoplysninger til f.eks. KMD, der behandler personoplysninger til AAU's formål: KMD er leverandør af WorkZone og står bl.a. for lagring af de personoplysninger, AAU har i WorkZone.

Når AAU overlader behandling af personoplysninger til en databehandler, så skal dette forhold reguleres med en databehandleraftale.

Hvornår?

For at du må overlade personoplysninger til en Databehandler, skal der forinden indgås en databehandleraftale. Du kan finde flere oplysninger her

For at du må give personoplysninger videre til en kollega, skal det sikres, at denne kollega har en saglig begrundelse for at skulle have adgang til personoplysningerne.

For at der kan ske videregivelse til en anden Dataansvarlig, skal det sikres, at der sker videregivelse til et legalt formål, og AAU skal kunne dokumentere dette.

Er du i tvivl om, hvorvidt du må give personoplysninger videre til en kollega eller ekstern part, kan du kontakte din nærmeste leder eller sende en mail til AAU's DPO på dpo@aau.dk