**Vejledning til udfyldelse af fortegnelse over behandlingsaktiviteter**

1. **Introduktion**

AAU har i henhold til databeskyttelsesforordningens § 30 pligt til at udarbejde og løbende opdatere fortegnelser over alle organisationens behandlingsaktiviteter. Det er et krav, at fortegnelsen foreligger skriftligt og elektronisk, så den på anmodning kan udleveres til Datatilsynet.

AAU har 8 fortegnelsesskabeloner.

De 7 af dem afspejler de hovedområder, som AAU opererer indenfor, når AAU er dataansvarlig:

1. Diverse administrative opgaver
2. Kommunikation og markedsføring
3. Personaleadministration
4. Ph.d. og forskning
5. Rekruttering
6. Studieadministration
7. Økonomi og budget

Den 8. skal anvendes, når AAU er databehandler.

Skabelonerne, samt denne vejledning kan findes her: <https://www.informationssikkerhed.aau.dk/persondata/administrativt/>

Det er de enkelte organisatoriske enheder, der skal udfylde og vedligeholde fortegnelserne. Der skal kun udfyldes det antal fortegnelser, som er relevante for den enkelte enhed.

Hver fortegnelse indeholder 7 underpunkter, som i de næste afsnit vil blive gennemgået med henblik på, hvordan fortegnelserne skal udfyldes under hvert punkt. I denne vejledning tages udgangspunkt i skabelonen for ***Diverse administrative opgaver.***

**Vejledningen er opbygget således, at forklaring fremgår af yderste højre kolonne, og eksempler er indsat i skemaet med forklaring ligeledes i højre kolonne.**

**Generel vejledning til udfyldelse af fortegnelsen**

Det er en god ide, for ikke at miste overblikket, at tage ét underformål ad gangen og gøre fortegnelsen færdig for det underformål.

Der kan være tilfælde, hvor I modtager flere oplysninger om en person, end I har bedt om, det kan f.eks. være følsomme oplysninger, oplysninger vedr. straffedomme, oplysninger om familiemedlemmer, deres beskæftigelse m.v. Hvis det er noget I oplever hele tiden, så skal disse oplysninger angives i fortegnelsen.

I de tilfælde, hvor det kun sker en gang imellem, vil det være nok at gøre opmærksom på det i [Bilag 1](#Bilag). I bilaget kan der kort redegøres for, hvordan disse ikke nødvendige personoplysninger modtages og håndteres.

Det er ligeledes vigtigt, at I i forbindelse med udfyldelsen af fortegnelserne er ærlige i forhold til, hvordan i behandler personoplysninger – så hvis I f.eks. ikke ved, hvad hjemmelsgrundlaget er, så angiv med et kryds i ”ved ikke” .

De eksempler, der er anvendt i denne vejledning er illustrative og kan ikke bruges ved udfyldelsen af jeres fortegnelser.

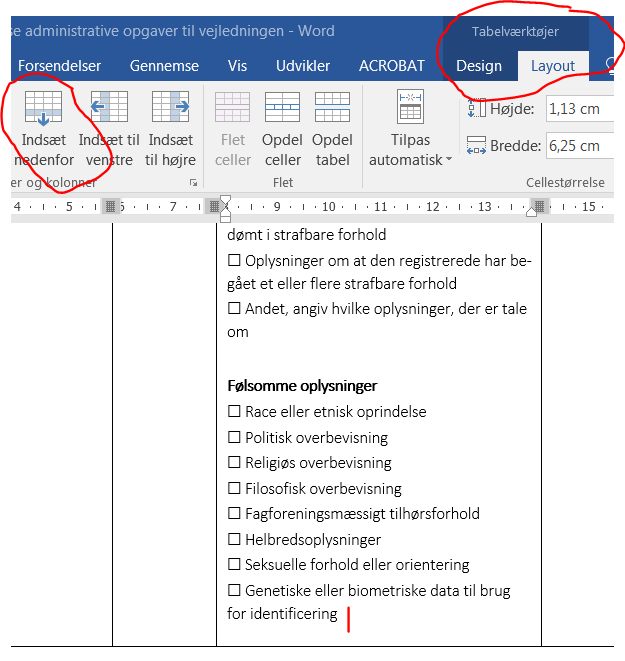
**For overskuelighedens skyld er de underformål m.m., der ikke indgår i de illustrative eksempler, slettet. I må ikke slette i de fortegnelser, I udfylder.**

1. **Gennemgang af underpunkterne 1-7**

|  |  |  |
| --- | --- | --- |
| **1 Stamoplysninger** | | **Vejledende tekst** |
| **Fortegnelse over behandlingsaktivitet(er) vedrørende** | [INDSÆT enhed]behandling af personoplysninger i forbindelse med diverse administrative opgaver | Her angives, hvilken enhed behandlingsaktiviteten vedrører f.eks. et institut, ph.d.-skole eller en fællesserviceenhed. |
| **Dataansvarlig enhed**  Her oplyses den afdeling eller det forretningsområde, der er ansvarlig for behandlingsaktiviteten og som fremadrettet skal drifte fortegnelsen | [INDSÆT den ansvarlige afdeling]  Eksempel:  Fakultetskontoret EST | Her angives, hvem der er den dataansvarlige enhed, som håndterer personoplysningerne til daglig, og som fremadrettet skal drifte fortegnelsen, f.eks. instituttet, dekansekretariatet, ØA etc. |
| **Ansvarlig leder**  Det er den leder, der har det ledelsesmæssige ansvar for processen i praksis, som skal angives her, eksempelvis en sekretariatsleder eller en områdeleder. Det vil være denne person, der rettes henvendelse til i tilfælde af sikkerhedsbrud mv. | [INDSÆT oplysninger]  Navn:  Titel:  Mail:  Tlf.nr.: | Som ansvarlig leder skal angives den leder, der har det ledelsesmæssige ansvar for processen i praksis. Det kan f.eks. være en sekretariatsleder eller en områdeleder. Det er samtidig den ledelsesperson, der skal rettes henvendelse til i tilfælde af sikkerhedsbrud mv. |
| **Ansvarlig medarbejder/nøglemedarbejder**  Skal kun udfyldes, hvis det ikke er den ansvarlige leder, der selv står for at varetage opgaven med fortegnelsen. Der skal kun angives én ansvarlig medarbejder, således at det er klart, hvem der skal rettes henvendelse til i tilfælde af sikkerhedsbrud mv. | [INDSÆT oplysninger]  Navn:  Funktionsområde:  Mail:  Tlf.nr.: | Hvis den ansvarlige leder ikke selv er ansvarlig for at få beskrevet og løbende opdateret/kvalitetssikret fortegnelsen, skal der angives en ansvarlig medarbejder/nøglemedarbejder, der har denne opgave. |
| **Databeskyttelsesrådgiveren (DPO)** | Navn: Teia Melvej Stennevad  Kontaktoplysninger: [dpo@aau.dk](mailto:dpo@aau.dk) |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **2 Behandlingsaktiviteten, kategorier af registrerede personer og kategorier af personoplysninger** | | | | | **Vejledende tekst** |
| **Formål med behandlingsaktiviteten**  Samt eventuelle underformål/afledte formål  Der skal krydses af i de relevante underformål. De underpunkter, der er under hvert underformål (kursiveret skrift) er hjælp til at finde ud af hvilke underformål, der er med behandlingen af personoplysninger. | **Formål:** Diverse administrative opgaver  **Underformål:**  **Kontordrift**  *Flexskema*  *Fordeling af e-mails fra funktionspostkasse*  **Kurser og konferencer**  Lokalebooking  Receptioner (forberedelse, afvikling og efterbehandling) | | | | Her angives ved afkrydsning hvilken behandlingsaktivitet, der finder sted – altså til hvilket formål/underformål personoplysninger behandles.  Der kan angives flere underformål. |
| **Kategorier og antal af registrerede personer**  En ’registreret person’ er alle de personer, AAU har oplysninger omkring. I dette felt skal du/I krydse af hvilke kategorier af ’registrerede personer’, der behandles oplysninger om.  Kryds alle kategorier af og vær opmærksom på, at f.eks. enkeltmandsvirksom-heder også tæller som en kategori af ’registrerede personer’.  ’Antal af registrerede personer’. Indsæt ca. antal pr. år, i parentes efter, hver afkrydset kategori. | Gæster ***(40)***  Samarbejdspartnere **(30)**  TAP-medarbejdere **(10)**  Kursusdeltagere **(300)**  VIP’er **(5)**  Kommende studerende **(500)** | | | | Her angives, hvilke kategorier af registrerede personer, der er i forbindelse med det/de valgte underformål.  I parentes ud for hver kategori af registrerede angives ca. antal personer. |
| **Kategori af personoplysninger og behandlingshjemmel**  Angiv hjemlen til at AAU behandler person-oplysningerne.  Der kan opdeles i underformål, hvis der gælder en forskellig behandlingshjemmel for de enkelte underformål. Hvis samme behandlingshjemmel gælder for det overordnede formål, angives der ikke noget i ”underformål”. | **Underformål** | **Kategori af**  **registrerede** | **Kategori af person-oplysninger** | **Behandlingshjemmel**  [(Udybning af hjemmelsgrundlaget)](#hjemmelsgrundlag) | **Vejledende tekst** |
|  | Kontordrift,  \*Flexskema  Kurser og konferencer \*lokalebooking  \*receptioner (forberedelse, afvikling og efterbehandling) | TAP  Kursusdeltagere  Samarbejds-partnere  Gæster | **Almindelige person-oplysninger**  Navn  Adresse  Tlf.nr.  E-mailadr. | **Almindelige personoplysninger**  Myndighedsudøvelse | Her angives underformål, kategori af registrerede personer, hvilke personoplysninger, der behandles for hvilke kategorier af registrerede under det valgte underformål og med hvilken hjemmel.  **Eksempel:** *I fortegnelsen ”Diverse administrative opgaver” angives ”Kontordrift” som et underformål og ”flexskema” som underkategori. Efter at have krydset af i boksen for ”Kontordrift”, ”Flexskema” fortsætter man ned til næste boks, hvor der skal angives, hvilke kategorier af registrerede personer, der registreres oplysninger om. Der har man valgt ”TAP”. Der er tale om ca. 40 TAP’er. De oplysninger, man registrerer i forbindelse med ”Kontordrift”, ”Flexskema” vil typisk være TAP’ens navn, det vil sige en almindelig personoplysning. Hjemmelsgrundlaget vil i dette tilfælde være myndighedsudøvelsei form af faktisk forvaltningsvirksomhed, da der er tale om en administrativ beslutning om, at medarbejderne kan flexe og hvordan, det skal registreres.*  Man **skal** samle flere underformål og tilhørende underkategorier i én boks, når kategorien af personoplysninger og hjemmelsgrundlaget er det samme.  **Eksempel:** *Det erfares, at iI forbindelse med kurser og konferencer, lokalebooking, receptioner (forberedelse, afvikling og efterbehandling) indhentes der også kun almindelige oplysninger i form af navn, adresse, telefonnummer og e-mailadresse, der er tale om VIP’er, samarbejdspartnere og gæster, og at hjemlen er myndighedsudøvelse.*  Det betyder, at dette underformål skal stå i samme boks som ”Kontordrift”, ”Flexskema”.  Hvis et underformål og et eller flere af dets underkategorier har en anden kategori af personoplysninger eller et andet hjemmelsgrundlag, skal der udfyldes en ny boks.  ***Eksempel****: I forbindelse med fordeling af e-mails fra funktionspostkassen behandles der både almindelige personoplysninger, CPR- numre og følsomme personoplysninger i form af helbredsoplysninger i forbindelse med sygemeldinger m.m.* |

Har man brug for flere bokse, så kan man oprette nye ved at stille sig i bunden på den foregående side i den kolonne, hvor der er tekst (rød lodret streg I, i nedenstående billede) og derefter gå op under Layout i Tabelværktøjer og trykke på ”Indsæt nedenfor.”



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **3 Eksterne modtagere af personoplysninger** | | | | | | **Vejledende tekst** |
| **Kategorier af modtagere:**  Personoplysninger som er angivet ovenfor i punkt 2, vil blive overladt eller videregivet til følgende kategorier af eksterne modtagere.  Der skal alene angives kategori af personoplysninger, såfremt der kun er tale om, at alene udvalgte kategorier for den pågældende registrerede videregives til tredjemand.  Med eksterne modtagere menes der alle, der får adgang til personoplysningerne, som ikke er ansat ved AAU.  Der skal angives både selvstændige dataansvarlige og databehandlere:  *andre organisationer, offentlige myndigheder: angiv de enkelte offentlige myndigheder med navne f.eks. SU-styrelsen, Skat, Aalborg Kommune, Region Nordjylland, domstole, faglige organisationer, pensionsselskaber, banker, inkassobureauer, eksterne leverandører, samarbejdspartnere, revisorer, software og hosting-udbydere, m.v.* | **Under-formål** | **Kategori af registrerede** | **Kategori af eksterne modtagere** | **Kategori af person-oplysning** | **Overførsels-/videregivel-sesgrundlag** |  |
| Kontordrift, \*Flexskema  Kurser og konferencer -\*lokalebooking  \*receptioner (forberedelse, afvikling og efter-behandling) | TAP  Kursus-deltagere  Samarbejds-partnere  Gæster | SKAT | Almindelige person-oplysninger | Myndighedsudøvelse | Dette underpunkt i fortegnelsen skal udfyldes, såfremt de personoplysninger, der behandles, overlades eller videregives til en ekstern modtager. Igen følges logikken fra underpunkt 2, således at der, hvor der er sammenfald mellem personoplysninger og overførsels-/videregivelsesgrundlaget, kan flere underformål samles i en boks.  Når personoplysninger **overlades** til en ekstern part, vil den eksterne part ofte være databehandler, og overførsels-/videregivelsesgrundlaget vil derfor oftest være en databehandleraftale.  Når personoplysninger **videregives** til en ekstern part, vil det ofte være til en anden dataansvarlig, og overførsels-/videregivelsesgrundlaget vil oftest være en videregivelsesaftale.  Et overførsels-/videregivelsesgrundlag kan også være i kraft af myndighedsudøvelse eller anden lovhjemmel.  Såfremt man ikke er sikker på, hvad overførsels-/videregivelsesgrundlaget er, er det vigtigt, at der krydses af i ”Ved det Ikke”.  Med eksterne modtagere menes der alle, der får adgang til personoplysningerne registreret i regi af AAU, og som ikke er ansat ved AAU.  Der skal angives både selvstændige dataansvarlige og databehandlere:  Det kan være andre organisationer eller offentlige myndigheder. Angiv med navn f.eks. SU-styrelsen, Skat, Aalborg Kommune, Region Nordjylland, domstole, faglige organisationer, pensionsselskaber, banker, inkassobureauer, eksterne leverandører, samarbejdspartnere, revisorer, software og hosting-udbydere, m.v.  Såfremt der ikke sker en overførsels-/videregivelse til en ekstern part, skal underpunktet ikke udfyldes. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **4 Overførsel af personoplysninger til et tredjeland eller en international organisation** | | | | | | | **Vejledende tekst** |
| **Kategorier af tredjelande eller internationale organisationer:**  Personoplysninger, som er angivet ovenfor i punkt 2, vil blive overladt eller videregivet til følgende modtager(e) i et tredjeland (et tredje land er et land uden for EU/EØS) og/eller international organisation (både selvstændige dataansvarlige og databehandlere), f.eks. USA, Kina m.m. eller international organisation, f.eks. FN, UNICEF og WHO.  Hvis der er flere end 3 kategorier tilføjes et ekstra angivelsesfelt ved at kopiere ’kategoriangivelsen’ og indsætte angivelser for alle typer af kategorier af tredjelande eller internationale organisationer.  . | **Under-formål** | **Kategori af registrerede** | **Kategori af person-oplysning** | **Overføres oplysninger til tredjelande** | **Angivelse af land eller organisation** | **Overførselsgrundlag** | I dette underpunkt, skal det angives, om der sker en overførsel af personoplysninger til et tredje land eller en international organisation.  Sker der ikke overførsel til et tredjeland eller en international organisation, skal underformålet angives, og der skal krydses af i nej. Det skal i disse tilfælde ikke oplyses, hvilke kategorier af registrerede eller personoplysninger, der er tale om. Også her kan der samles flere underformål i en boks, så længe der er tale om de samme personoplysninger og det samme overførselsgrundlag.  Sker der overførsel til et tredjeland, så skal samtlige oplysninger angives.  Et tredjeland er et land uden for EU/EØS f.eks. USA, Kina m.m. og/eller en international organisation (både selvstændige dataansvarlige og databehandlere) f.eks. FN, UNICEF og WHO.  Af vejledning om ’sikre tredjelande’ fremgår det, at følgende ikke er tredje lande:  Lande, der er medlem af EU eller EØS, sidstnævnte betyder at f.eks. Norge og Island ikke er at betragte som tredjelande.  Vejledningen kan findes her: <http://www.informationssikkerhed.aau.dk/persondata/administrativt/>  **Tredjelande**  Tredjelande opdeles i to kategorier:   1. **Sikre tredjelande**  * Andorra * Argentina * Australien (angår kun overførsel af personoplysninger vedrørende flypassagerer - se Kommissionens hjemmeside for yderligere oplysninger) * Canada (begrænset anvendelsesområde - se Kommissionens hjemmeside for yderligere oplysninger) * Færøerne * Guernsey * Isle of Man * Israel * Jersey * New Zealand * Schweiz * Uruguay * USA (overførsel af personoplysninger vedrørende flypassagerer - se Kommissionens hjemmeside for yderligere oplysninger) * USA (overførsel af personoplysninger til organisationer (typisk virksomheder), der har tilsluttet sig EU - U.S. Privacy shield - se [her](https://www.datatilsynet.dk/erhverv/tredjelande/eu-us-privacy-shield/) for yderligere oplysninger)  1. **Ikke sikre tredje lande**   Resten |
| Kontordrift, \*Flexskema  Kurser og konfe-rencer  \*lokale-booking  \*receptioner (forberedelse, afvikling og efter-  behandling) | TAP  Kursus-deltagere  Samarbejdspartnere  Gæster | Almin-delige person-oplysninger  Fortrolige person-oplysninger  CPR-numre  Straffe-domme og lovover-trædelser  Følsomme oplysninger | Nej  Ja |  | Overførsel til sikkert tredjeland  Retligt bindende aftaler mellem offentlige myndig-heder og organer  Bindende Virksom-hedsregler (Binding Corporate Rules)  Ad-færdskodeks og Certificering  Standardbestemmelser om databeskyttelse  Ad hoc kontrakt godkendt af tilsynsmyndighed  Samtykke  Ved det ikke |
| Kontordrift, -Flexskema | TAP | Almindelige personoplysninger  Fortrolige personoplysninger  CPR-numre  Straffedomme og lovovertrædelser  Følsomme oplysninger | Ja | Kina | Bindende Virksomhedsregler (Binding Corporate Rules) |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **5 Sletning af kategorier af personoplysninger** | | | | | **Vejledende tekst** |
| Om muligt skal der angives de forventede tidsfrister for sletning af de personop-lysninger, der er angivet i punkt 2. Hvis der ikke kan afkrydses i de tre første valgmuligheder, skal der som minimum under ”andre overvejelser” angives, hvilke tanker der er gjort omkring, hvor lang tid oplysningerne opbevares.  Hvis samme slette-/opbevaringspolitik gør sig gældende for flere kategorier af registrerede og kategorier af personoplysninger, samles disse under et. | **Underformål** | **Kategori af registrerede** | **Kategori af personoplysninger** | **Slettefrister / overvejelser ift. opbevaring** |  |
| Kontordrift, -Flexskema  Kurser og konferencer -lokalebooking  -receptioner (forberedelse, afvikling og efterbehandling) | TAP  Kursusdeltagere  Samarbejdspartnere  Gæster | Almindelige personoplysninger | Andre overvejelser ift. opbevaring, angiv:  Vi sletter aldrig, vi har | Her skal for hvert underformål angives Kategori af registrerede, Kategori af personoplysninger og hvornår, der arkiveres til statens arkiver, sker en total anonymisering, eller hvornår oplysninger slettes uden mulighed for at genskabe dem.  Såfremt man ikke sletter efter nogle af de nævnte muligheder, skal man under ” Andre overvejelser” skrive, hvad man så gør eller ikke gør med de konkrete personoplysninger. |
| Kontordrift, - *Fordeling af e-mails fra funktionspostkasse* | VIP  Kommende studerende | Almindelige personoplysninger  Følsomme oplysninger | Sletning efter 5 år ved arkivering til Statens Arkiver: Man laver en aflevering til Statens Arkiver og sletter sin egen version af datasættet. |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **6 Hvilke aktiver anvendes i behandlingsaktiviteten** | | | | | **Vejledende tekst** |
| Angiv hvilke aktiver (tekniske løsninger, software, hardware, systemer m.m.), der anvendes til at behandle data med i behandlingsaktiviteten.  Inkluder eventuelle behandlingsløsninger så som statistik-programmer, hvis der lagres lokalt i dette.  Hvis samme aktiver anvendes for flere kategorier af registrerede og kategorier af personoplysninger, samles disse under et.  Angiv både de løsninger I anvender, som stilles til rådighed af AAU samt eventuelle eksterne løsninger eller løsninger, der er truffet tilvalg om at anvende, f.eks. Dropbox, Google Onedrive, P-drev, USB-nøgler m.fl. | **Underformål** | **Kategori af registrerede** | **Kategori af personoplysninger** | **Aktiver der anvendes i behandlingen** |  |
| Kontordrift, -Flexskema  Kurser og konferencer -lokalebooking  -receptioner (forberedelse, afvikling og efterbehandling) | TAP  Kursusdeltagere  Samarbejdspartnere  Gæster | Almindelige personoplysninger | **Software**  Outlook – mail  Fællesdrev  Angiv drev: O | Under dette punkt skal angives hvilke aktiver, der anvendes til at håndtere personoplysninger. Med aktiver menes alle de elektroniske og fysiske steder personlysninger opbevares.  Igen følges systematikken fra tidligere, således at der, hvor der er tale om de samme kategorier af personoplysninger og de samme aktiver, kan flere underformål samles i en boks.  Såfremt de aktiver, man bruger, ikke fremgår af listen, kan der tilføjes yderligere aktiver under boksene ”Andet”. |
|  | Kontordrift, - *Fordeling af e-mails fra funktionspostkasse* | VIP  Kommende studerende | Almindelige personoplysninger  CPR-numre  Følsomme oplysninger | **Software**  Outlook – mail |  |

|  |  |  |
| --- | --- | --- |
| **7 Tekniske og organisatoriske sikkerhedsforanstaltninger** | | **Vejledende tekst** |
| Oplysninger om sikkerhedsforanstaltningerne findes i jeres aftalegrundlag med leverandører af løsninger mm. og kan, hvis I ikke selv har adgang til kontrakter og serviceaftaler, indhentes ved at kontakte ITS.  Viden om de fysiske sikkerhedsforanstaltninger kan indhentes ved henvendelse til Campus Service. | [INDSÆT en generel/overordnet beskrivelse af AAU’s tekniske og organisatoriske sikkerhedsforanstaltninger]  *Eksempel*  *Virksomheden har både truffet fysiske, tekniske og organisatoriske sikkerhedsforanstaltninger:*   * ***Fysisk:*** *Virksomheden har alarmer på alle udvendige døre. Serverrum er aflåst og kan alene tilgås med kode.* * ***Teknisk:*** *Virksomhedens it-systemer kan alene tilgås med brug af brugernavn og password. Personoplysninger opbevares i krypteret form. Virksomhedens systemer er beskyttet af firewall og antivirusprogrammer.* * ***Organisatorisk:*** *Der er fastsat interne regler for autorisation og adgangskontrol. Der foretages logning af adgangsforsøg både til it-systemer og serverrum.*   *AAU’s behandling sker i øvrigt under iagttagelse af sikkerhedsstandard [f.eks. ISO 27xxx eller 291xx]* | Der er indsat et eksempel på en beskrivelse af, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der anvendes. Under dette punkt skal I skrive, hvad I gør eller ikke gør for at sikre de personoplysninger, I har i jeres varetægt. |

**Bilag 1: Bilag til uddybende bemærkninger og observationer i forhold til behandlingsaktiviteter**

*Angiv her problematikker, som I oplever i dagligdagen og som fortegnelserne ikke giver mulighed for at få belyst.*

**Uddybning af hjemmelsgrundlag i fortegnelserne**

**Almindelige personoplysninger**

**Samtykke** Skal være frivillig, specifik og informeret viljestilkendegivelse, hvorved den registrerede indvilger i, at oplysninger, der vedrører den pågældende selv, gøres til genstand for behandling. (bør kun finde anvendeles når, der ikke findes et andet hjemmelsgrundlag)

**Kontraktgrundlag** Som den registrerede er part i eller påtænker, at blive part i

**Retlig forpligtelse** En retlig forpligtelse foreligger, når AAU som følge af aftale, lovgivning eller retspraksis skal indfri en forpligtelse). F.eks. igennem en kollektiv overenskomst, en retssag m.v.)

**Nødvendig for at beskytte den registreredes eller anden fysisk person vitale interesser** F.eks. hvis det ikke er muligt for et hospital at komme i kontakt med en patient, som venter på et nyt organ på det tidspunkt, hvor hospitalet kommer i besiddelse af organet, hvorfor hospitalet er nødt til at behandle personoplysninger om patientens kæreste for at komme i kontakt med patienten. Bør kun finde sted, hvis der ikke findes et andet hjemmelsgrundlag.

**Udførelse af en opgave i samfundets interesse.** Forordning indebærer ikke, at der kræves en specifik lov til hver enkelt behandling. Det kan være tilstrækkeligt med en lov som grundlag for adskillige databehandlingsaktiviteter, hvis behandling er nødvendig for at udføre en opgave i samfundets interesse. Forordningen kræver heller ikke nødvendigvis, at opgaven, som kræver behandling af personoplysninger, udtrykkeligt i lovgivningen er pålagt myndigheden.

Eksempel 1: Undervisningsministeriet, som den centrale myndighed på området, løser en opgave vedrørende digital tilmelding til og ansøgning om optagelse på uddannelser, selvom der ikke er en udtrykkelig lovhjemmel, der pålægger ministeriet opgaven.

**Myndighedsudøvelse** Det kan være tilstrækkeligt med en lov som grundlag for adskillige databehandlingsaktiviteter, som henhører under offentlig myndighedsudøvelse. Kræver heller ikke nødvendigvis, at opgaven, som kræver behandling af personoplysninger, udtrykkeligt i lovgivningen er pålagt myndigheden. Myndighedsudøvelse opdeles:

1. Udstedelse af forvaltningsakter i form af egentlige afgørelser. F.eks. tilbagekaldelse og annullering af en eksamens karakter (afgørelse) eller beslutning om, at gå til eksamen på særlige vilkår som følge af højt fravær (afgørelse)
2. Faktisk forvaltningsvirksomhed. F.eks. karaktergivning (ikke en afgørelse), vejledning til borgere (vejledningspligt), kontraktforhold og andre privatretlige dispositioner.

**Følsomme personoplysninger**

**Udtrykkeligt samtykke** Det er endnu ikke helt klart hvad der ligger i ”Udtrykkeligt”. Der er ikke beskrevet forskel fra kravene til almindeligt samtykke, men med brugen af ”udtrykkeligt”, er det ønsket at sende et signal fra lovgivers side, om der ikke må være tvivl om, at der er givet et samtykke.

**Nødvendig for at opretholde den registreredes arbejds-, sundheds-, og socialretlige forpligtigelse.** Man må behandle følsomme oplysninger, når der er hjemmel i EU-retten eller medlemsstaternes nationale ret og er omfattet af de fornødne garantier, således at personoplysninger og andre grundlæggende rettigheder beskyttes, hvis dette er i samfundets interesse. Dette gælder, navnlig behandling af personoplysninger inden for ansættelsesret, socialret, herunder pensioner og med henblik på sundhedssikkerhed, overvågning og varsling, forebyggelse eller kontrol af overførbare sygdomme og andre alvorlige trusler mod sundheden.

Det samme gør sig gældende, hvis behandlingen sker til sundhedsformål, herunder folkesundhed og forvaltning af sundhedsydelser, især for at sikre kvaliteten og omkostningseffektiviteten af de procedurer, der anvendes til afregning i forbindelse med ydelser og tjenester inden for sygesikringsordninger, eller til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål.

**Nødvendig for at beskytte den registreredes eller anden fysisk person vitale interesser, hvor den registrerede ikke er i stand til at give samtykke.** F.eks. hvis det ikke er muligt for et hospital at komme i kontakt med en patient, som venter på et nyt organ på det tidspunkt, hvor hospitalet kommer i besiddelse af organet, hvorfor hospitalet er nødt til at behandle personoplysninger om patientens kæreste for at komme i kontakt med patienten. Bør kun finde sted, hvis der ikke findes et andet hjemmelsgrundlag.

**Tydeligvis er offentliggjort af den registrerede.** Hvor det er åbentlyst, at den registrerede selv offentliggjort følsomme oplysninger om sig selv.