Fortegnelse over behandling af personoplysninger

Skabelon til brug ved fortegnelser over administrative processer, hvor AAU er **Databehandler**

## Overordnet vejledning:

AAU har pligt til at udarbejde og løbende opdatere fortegnelser over alle organisationens behandlingsaktiviteter, hvor AAU udfører databehandlinger for dataansvarlige. Det er et krav at fortegnelsen foreligger skriftligt og elektronisk, så den på anmodning kan udleveres til Datatilsynet.

**Manglende udarbejdelse af fortegnelsen kan medføre bøde.**

For at anvende denne skabelon, skal den ansvarlige leder eller vedkommendes ansvarlige medarbejder udfylde samtlige punkter i fortegnelsen.

|  |  |
| --- | --- |
| **1 Stamoplysninger** | |
| **Fortegnelse over behandlingsaktivitet(er) vedrørende** | [INDSÆT enhed]behandling af personoplysninger i forbindelse med |
| **Databehandlende enhed**  Den databehandlende organisation, virksomhed eller privatperson | [INDSÆT navn]  [INDSÆT adresse]  [INDSÆT kontaktoplysninger] |
| **Dataansvarlig enhed**  Her oplyses den afdeling eller forretningsområde, der er ansvarlig for behandlingsaktiviteten og som fremadrettet skal drifte fortegnelsen | [INDSÆT den ansvarlige afdeling]  Eksempel:  Fakultetskontoret EST |
| **Ansvarlig leder**  Det er den leder, der har det ledelsesmæssige ansvar for processen i praksis, som skal angives her, eksempelvis sekretariatetslederen eller en områdeleder. Det vil være denne person, der rettes henvendelse til i tilfælde af en sikekrhedshændelse mv. | [INDSÆT oplysninger]  Navn:  Titel:  Mail:  Tlf. nr.: |
| **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 en sikkerhedshændelse mv. | [INDSÆT oplysninger]  Navn:  Funktionsområde:  Mail:  Tlf. nr.: |
| **Databeskyttelsesrådgiveren (DPO)** | Navn: Teia Melvej Stennevad  Kontaktoplysninger: [dpo@aau.dk](mailto:dpo@aau.dk) |

|  |  |
| --- | --- |
| **2 Kategorier af behandlinger** | |
| **Kategorier af behandlinger, der foretages på vegne af den dataansvarlige:**  Afkryds alle de typer af behandlinger, der foretages under | Indsamling  Registrering  Organisering  Systematisering  Opbevaring  Tilpasning  Ændring  Genfinding  Søgning  Brug  Videregivelse ved transmission  Formidling  Sammenstilling  Samkøring  Sletning  Tilintetgørelse  Andet  Ved andet angiv: |

|  |  |  |
| --- | --- | --- |
| **3 Overførsel af personoplysninger til et tredjeland eller en international organisation** | | |
| **Der overføres oplysninger til tredjelande:** | Nej  Ja  Ved ’Nej’ gå videre til pkt. 4  Ved ’Ja’ skal man angive grundlaget for overførslen nedenunder. | |
| **Kategorier af tredjelande eller internationale organisationer:**  Personoplysninger, som er angivet ovenfor i punkt 3, 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)  Felterne udfyldes ved at afkrydse de relevante bokse  Hvis der er flere end 3 kategorier tilføjes et ekstra angivelsesfelt ved at kopiere ’kategoriangivelsen’ og indsæt angivelser for alle typer af kategorier af tredjelande eller internationale organisationer  Se Vejledning om ’sikre tredjelande’ | **Angivelse af land eller organisation:** | **Overførselsgrundlag:** |
| [INDSÆT tredjeland, f.eks. USA, Kina m.m. eller international organisation, f.eks. FN, UNICEF og WHO]  Felterne udfyldes ved at afkrydse den relevante boks | Overførsel til sikkert tredjeland  Retligt bindende aftaler mellem offentlige myndigheder og organer  Bindende Virksomhedsregler (Binding Corporate Rules)  Adfærdskodeks og Certificering  Standardbestemmelser om databeskyttelse  Ad hoc kontrakt godkendt af tilsynsmyndighed  Samtykke |
| [INDSÆT tredjeland eller international organisation] | Overførsel til sikkert tredjeland  Retligt bindende aftaler mellem offentlige myndigheder og organer  Bindende Virksomhedsregler (Binding Corporate Rules)  Adfærdskodeks og Certificering  Standardbestemmelser om databeskyttelse  Ad hoc kontrakt godkendt af tilsynsmyndighed  Samtykke |

|  |  |  |
| --- | --- | --- |
| **4 Hvilke aktiver anvendes i behandlingsaktiviteten** | | |
| Angiv hvilke aktiver (tekniske løsninger, software, hardware, systemer mm.) der anvendes til at behandle data med i behandlingsaktiviteten.  Inkluder eventuelle behandlingsløsninger så som statistik-programmer, hvis der lagres lokalt i dette.  Angiv både de løsninger I anvender som stilles til rådighed af AAU eller databehandleren samt eventuelle eksterne løsninger eller løsninger der er truffet tilvalg om at anvende, f.eks. Dropbox, Google Onedrive, P-drev, USB-nøgler m.fl. |  | **Software**  Outlook – mail  Fællesdrev  Angiv drev:  Facebook  Intranet  Instagram  Twitter  Snapchat  Linkedin  Dropbox  Google drev  Onedrive  DropZone  Online Studieguide  Minuba  Webbetalingsmodul  ØSS  Andet:  **Studieadministrative systemer**  iStads  STADS  DANS  Digital eksamen  Uddannelsesbasen  Modulbasen  Studieordningsbasen  Andet:  **ESDH**  KMD WorkZone  Scanjour Captia  STADS-Captia integration  Registrering af budget til forskningsansøgning  Historisk journaldatabase 2000-2005  Historisk journaldatabase 2005-2010  Historisk journaldatabase 2010-2016  Historisk journaldatabase SBi 2008-2014  QlikView  Andet:    **AAU Egenudvikling**  Jira supportsystem  Mossad web Modul  AAUCARD  PhD manager  INDB  RUS  VBN  AAU Webbook  Timesheet -digitale timesedler  RES  Andet:    **HR systemer**  PeopleXS  Rekruttering  APV handleplanmodul  Sygefraværssystem  AAU fraværsstatistik  ScanTid  Scanpas  Andet:  **Elektroniskformidling**  AAU-Håndbog  Infoglue  Moodle  Andet:  **Hardware**  PC  Mobiltelefon  Diktafon  Tablet  Telefon  Almindelig post  USB stik  Papirarkiver  Andet: |

|  |  |
| --- | --- |
| **5 Tekniske og organisatoriske sikkerhedsforanstaltninger** | |
| 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 IT-services.  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:*** *Det 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]* |