ASKOV HØJSKOLE
& EFTERSKOLE

Datasikkerhedshåndbog for Askov Højskole og Efterskole

Indholdsfortegnelse

Reglerne i denne datasikkerhedshåndbog er fastsat på baggrund af databeskyttelsespolitikken Databeskyttelsespolitik I-3.

Organisering og ansvar

Planlægning, implementering og kontrol af databeskyttelsespolitikken er defineret af Askov Højskole og Efterskoles ledelse, der også er ansvarlig for implementering og vedligeholdelse af datasikkerhedssystemet og er ansvarlig for opfølgning på sikkerhedshændelser.

Askov Højskole og Efterskoles ledelse har i vedlagte bilag 1 fastsat, hvem der har ansvaret for forskellige del af databehandlingssikkerheden på følgende områder:

- ***Automatiske (IT) databehandlingssystemer***, de data, der opbevares i systemerne samt de forretningsgange, der har tilknytning til systemerne (***systemejer***)
- ***Manuelle systemer med persondata (arkiv)***, de data, der opbevares i systemerne samt de forretningsgange, der har tilknytning til systemerne (***systemejer***)
- ***System- og netværksadgang***, styring, tildeling af rettigheder og adgangskoder
- ***IT-kontrakter og andre kontrakter***, der indebærer behandling af persondata – indgåelse og opfølgning
- ***Indkøb af hardware og installation af software***
- ***Henvendelser fra de registrerede*** om indsigt i sine personoplysninger eller udøvelse af retten til berigtigelse, sletning eller begrænsning af behandling og ret til dataportabilitet.
- ***Meddelelser til den registrerede*** om registreringer, herunder oplysninger på institutionens hjemmeside
- ***Sikkerhedshændelser,*** opsamling og styring ***og pligtig anmeldelse af brud på persondatasikkerheden*** til Datatilsynet og de registrerede, der er berørt af bruddet
- ***I forbindelse med ansættelsen*** modtager medarbejderen særskilt instruktion i databehandlingssikkerhed og anvendelse af databehandlersystemerne

1. Retningslinjer for sikkerhed, der især berører medarbejderne.

Ledere og medarbejdere er ansvarlige for at efterleve retningslinjer og procedurer for databehandlingssikkerhed i det daglige arbejde.

Askov Højskole og Efterskole behandler som led i sit arbejde følsomme oplysninger om elever og kursister på såvel højskole som efterskole som grundlag for arbejdet, og det er derfor vigtigt at medarbejderne har fokus på, at ***personoplysninger altid skal behandles fortroligt*** og kun ***videregives eksternt***, hvis der foreligger et samtykke fra den registrerede, eller hvis det sker som følge af lovgivningen.

I det ***interne samarbejde*** hos Askov Højskole og Efterskole gives eller udveksles kun personoplysninger, der er nødvendige for udførelse af arbejdet med elever, kursister og ansatte eller som er nødvendige for udførelse af personaleadministration.

2.1 Instruktion og undervisning om databehandlingssikkerhed

Ledelsen sørger for, at den nødvendige viden og kompetence om databehandlingssikkerhed kommunikeres til alle medarbejdere, og at der løbende bliver arbejdet med holdninger og viden omkring databehandlingssikkerhed, herunder især i forbindelse med indførelse af nye automatiske databehandlingssystemer eller ændring af eksisterende systemer eller retningslinjer.

I forbindelse med ansættelsen modtager medarbejderne særskilt instruktion i databehandlingssikkerhed og anvendelse af databehandlersystemerne og medarbejderne underskriver i forbindelse med ansættelsen en erklæring om, at have gjort sig bekendt med institutionens databehandlingssikkerhedspolitik og at være forpligtet til at overholde den.

De ansvarlige for de forskellige automatiske databehandlersystemer modtager den fornødne instruktion, oplæring og kurser om anvendelsen af disse systemer herunder også om persondatasikkerhed, som giver den nødvendige kompetence til at kunne varetage ansvaret.

ASKOV HØJSKOLE
& EFTERSKOLE

2.2 Retningslinjer for adgangsstyring

Styringen og daglig administration af adgangsrettigheder tilrettelægges således, at hver medarbejder kun adgang til de persondata, der er nødvendige for at kunne udføre arbejdet med Askov Højskole og Efterskoles elever, kursister og ansatte i overensstemmelse med den besluttede arbejdsfordeling.

Ledere og mellemledere har adgang til sine egne medarbejderes oplysninger i løn- og HR-systemet.

Medarbejdere, der arbejder med løn og HR har adgang til alle personaleoplysninger.

Askov Højskole og Efterskoles forstandere har adgang til alle oplysninger i alle systemer.

2.3 Brugeroprettelse og nedlæggelse

Ved oprettelse som bruger i et databehandlingssystem, skal hver medarbejder tildeles et unikt brugernavn og adgangskode.

Brugernavnet er personligt og må ikke overdrages til andre.

Ved oprettelse eller nulstilling af adgangskode skal medarbejderen tildeles en midlertidig adgangskode, som skal ændres ved første anvendelse.

Udlevering af den midlertidige adgangskode skal ske på en sikker måde.

Midlertidige adgangskoder skal opfylde de gældende krav til adgangskoder, som er beskrevet nedenfor.

Standardadgangskoder fra systemleverandører skal ændres i forbindelse med installation af nye databehandlingssystem.

Ved omplaceringer og omorganiseringer, skal den nye leder sikre, at medarbejderen kun har de autorisationer, der er et arbejdsmæssigt behov for og at eventuelle ændringer af adgangsrettigheder registreres i systemerne af den ansvarlige for styring af adgangsstyringen.

Ved ansættelsesforholdets ophør skal medarbejderen aflevere IT-udstyr og lignende som tilhører Askov Højskole og Efterskole, og den ansvarlige for adgangsstyringen inddrager medarbejderens adgangsrettigheder senest ved den pågældendes fratræden.

2.4 Regler for login og password

Adgangen til alle IT-systemer og netværk sker via et personligt tildelt brugernavn og adgangskode.

Adgangskode skal opfylde følgende krav:

- minimum 12 karakterer langt
- indeholde både store og små bogstaver samt mindst et tal eller tegn
- ikke tidligere være anvendt af brugeren
- blokeres i 30 minutter efter 5 mislykkede loginforsøg
- Alle arbejdsstationer skal have en skærmlås, der aktiveres automatisk efter højest 15 minutters inaktivitet med krav om indtastning af password

Adgangskoder til ***administratoradgang*** opbevares i en forseglet kuvert i et aflåst pengeskab i boksen på kontoret. Den ansvarlige for adgangsstyringen kan vælge at ***forny en brugers adgangskode*** og tildele brugeren en ny, hvis dette skønnes at være nødvendigt.

For at sikre overholdelse af retningslinjerne om databehandlingssikkerhed, samt med henblik på at forebygge eller udbedre systemnedbrud, kan den ***ansvarlige for systemadgang logge på enhver brugerkonto*** for at arbejde der.

ASKOV HØJSKOLE
& EFTERSKOLE

2.5 Medarbejdernes brug af password

Adgangskoder er personlige og må under ingen omstændigheder udleveres til andre eller skrives ned.

Anvendelse af fælles adgangskode er ikke tilladt.

Hvis flere medarbejdere benytter den samme PC-arbejdsstation, skal den enkelte medarbejder logge på med sin personlige adgangskode, før der udføres arbejdsopgaver på PC-arbejdsstationen, og logge af, inden den næste medarbejder overtager PC-arbejdsstationen.

Når en medarbejder forlader en tændt arbejdsstation, skal den adgangskodebeskyttede skærmlås være aktiveret.

Brug af programmer og behandling af data, hvor en anden medarbejder er logget på, kan undtagelsesvis benyttes og efter konkret godkendelse af ledelsen, f.eks. i vikartilfælde.

Anvendelse af en ***password-keeper*** på f.eks. egen mobiltelefon, skal godkendes af den ansvarlige for adgangsstyring.

Såfremt ***adgangskoden kompromitteres***, eller der opstår mistanke herom, er det medarbejderens ansvar straks at ændre sin adgangskode og underrette den ansvarlige for adgangsstyring.

2.6 Anvendelse af mails og opbevaring af mails i mailboks

E-mailsystemer er beregnet til arbejdsmæssige forhold, men i det omfang det ikke generer den arbejdsrelaterede anvendelse, må e-mailsystemet anvendes til private formål.

Medarbejderne skal overholde følgende regler vedr. brug af mail:

- Askov Højskole og Efterskoles regler om databeskyttelse skal overholdes ved brug af e-mailsystemer.
- Man må ikke åbne filer i e-mails fra en afsender, der er ukendt eller som man ikke har tillid til.
- E-mails der indeholder fortrolige eller personfølsomme oplysninger skal altid sendes med sikker e-mail hvis de sendes udenfor institutionens interne netværk. Se instruktion om sikker e-mail GDPR-doc Y-1
- Såfremt en modtager ikke kan modtage sikker e-mail, kan der ikke anvendes e-mails til denne modtager som indeholder fortrolige eller personfølsomme oplysninger, herunder f.eks. cpr-nummer.
- Det er ikke tilladt at sætte e-mailsystemet op til automatisk at videresende modtagne e-mail til en privat eller anden ekstern e-mailadresse.
- E-mails kan sendes uden kryptering inden for institutionens interne netværk
- ***Private e-mails*** skal markeres med teksten **"PRIVAT"** i emnefeltet og arkiveres i en ***undermappe navngivet med "PRIVAT"***, hvis medarbejderen ønsker, at institutionen i videst muligt omfang ikke gør sig bekendt med indholdet. Ved sikkerhedsbrud, systemfejl eller mistanke om brud på databehandlingssikkerheden vil administrationen og systemleverandøren i nødvendigt omfang kunne tilgå de private e-mails.

Personoplysninger om elever, kursister eller medarbejdere ***må ikke opbevares eller gemmes i mailsystemet*** i den enkelte medarbejders mail-mapper.
Askov Højskole og Efterskoles forstandere kan af arbejdsmæssige og forretningsmæssige årsager vælge at lade en tidligere medarbejders e-mailkonto forblive åben i kortere eller længere tid efter medarbejderens ophør. Forstanderne kan udpege andre ansatte til at administrere den fratrådte medarbejders arbejdsmail.

2.7 Regler for anvendelse af institutionens mobile udstyr

2.7.1 Oplysninger og programmer

Medarbejderne må ikke downloade eller gemme følsomme personoplysninger, herunder cpr-nummer om elever, forældre, kursister eller andre medarbejdere på institutionens mobile udstyr som PCér, USB-nøgler, mobiltelefoner mv.

Ledelsen kan i konkrete tilfælde tillade download af personoplysninger på Askov Højskole og Efterskoles mobile udstyr, hvis arbejdet nødvendiggør dette. Det anvendte mobile udstyr skal i disse tilfælde være beskyttet med password – dette gælder også USB-nøgler. Personoplysningerne skal slettes på det mobile udstyr umiddelbart efter brugen.

2.7.2 Beskyttelse af udstyr mod bortkomst og tyveri

Medarbejderne skal håndtere mobilt udstyr på en måde, så risikoen for tyveri minimeres.

Mobilt udstyr bør ikke efterlades i biler uanset om det er placeret i kabine, handskerum eller bagagerum.

Mobilt udstyr, der efterlades på kontoret efter arbejdstid skal lægges væk i aflåst skab eller aflåst skuffe. Hvis de efterlades på kontorer eller i lokaler skal det være aflåst med tilkoblet alarm.

2.8 Anvendelse af <u>private</u> PC'er, datamedier og telefoner til behandling af personoplysninger

Oplysninger vedrørende Askov Højskole og Efterskoles elever, forældre og kursister samt HR-oplysninger om medarbejdere må ikke downloades på private PC'er, private mobiltelefoner eller andet privat udstyr, uanset hvilken sikkerhedsbeskyttelse disse enheder har.

2.9 Regler for anvendelse af internettet og netværkstjenester

Privat brug af internetadgang må finde sted i det omfang, det er foreneligt med medarbejderens varetagelse af sit daglige arbejde og i øvrigt ikke strider mod lovgivningen, Askov Højskole og Efterskoles regler om databehandlingssikkerhed og værdigrundlag.

Medarbejdere må ikke anvende Askov Højskole og Efterskoles IT-udstyr til bevidst at opsøge anstødelige eller ulovlige hjemmesider, som f.eks. racistiske eller børnepornografiske hjemmesider.

Det er tilladt at downloade IT-programmer, spil, billeder og lignende på Askov Højskole og Efterskoles IT-udstyr, i det omgang det er nødvendigt i arbejdsmæssig sammenhæng.

Det er tilladt at bruge ***sociale netværkstjenester*** i arbejdsmæssig sammenhæng.

Der må ikke via de godkendte sociale netværkstjenester udveksles fortrolige oplysninger, herunder personoplysninger vedrørende Askov Højskole og Efterskoles forhold eller sager.

2. Generelle sikkerhedsbestemmelser

3.1 Beskyttelse af udstyr

IT-udstyr skal være placeret så skader og uautoriseret adgang minimeres og driftskritisk IT-udstyr skal beskyttes mod tyveri.

IT-udstyr, der benyttes til behandling af personoplysninger eller værdioplysninger, skal placeres på en sådan måde, at det er beskyttet mod adgang fra uvedkommende.

Printere, der benyttes til udskrivning af personoplysninger bør være konfigureret således, at det er muligt at udskrive dokumenter fortroligt under medarbejderens tilstedeværelse ved printeren. Ligeledes bør der være mulighed for at printe til printerens mailboks, der er beskyttet med personlig kode.

I forbindelse med indkøb af IT-udstyr besluttes det, om IT-udstyret, skal tyverisikres gennem mærkning.

Bortskaffelse af IT-udstyr, som indeholder personoplysninger skal i det omfang det er muligt ske ved fysisk destruktion.

ASKOV HØJSKOLE
& EFTERSKOLE

Ved salg, genbrug eller bortskaffelse af IT-udstyr herunder PC'ere og eksterne harddiske skal alle data lagrede på udstyret slettes på en sådan måde, at data ikke kan gendannes.

3.2 Logning og overvågning

Der foretages logning af brugeraktiviteter i de IT-systemer, hvor der behandles følsomme personoplysninger om Askov Højskole og Efterskoles elever og kursister samt ansatte.

Logningen omfatter:

- medarbejderidentifikation
- dato for systemanvendelse, specificering af systemer, log-on og log-off.
- fejlede og succesfulde adgangsforsøg

Logdata opbevares i 6 måneder, hvorefter de skal slettes hvis der ikke er særlige grunde til at opbevare dem længere

3.3 Backup

Der skal tages backup af data, der ikke hostes hos en ekstern databehandler.

Backup tages en gang i døgnet. Backuppen opbevares både lokalt på virksomhedens egen server og hos server hos ekstern IT-support.

For data, der hostes hos en ekstern databehandler, aftales det i IT-kontrakten og/eller i databehandleraftalen, hvilken metode og hyppighed for backup der anvendes. Backup af hostede data hos ekstern databehandler, skal minimum foretages en gang i døgnet.

3.4 Retningslinjer for netværkssikkerhed

Netværksudstyr med gæsteadgang for Askov Højskole og Efterskoles elever, gæster, kursister, besøgende skal afvikles på et særskilt netværk, der er fysisk og logisk adskilt fra det administrative netværk.

Al adgang til det administrative netværk skal ske med brugernavn og adgangskode.

Netværksudstyr skal konfigureres efter bedste praksis for sikkerhedskonfigurationer.

3.5 Beskyttelse mod skadevoldende programmer og kode

Alle servere, arbejdsstationer, bærbare PC'ere og andet mobilt IT-udstyr, netværksenheder og andre relevante enheder, skal være beskyttet mod ondsindet kode, såsom virus, malware, mm.

Netværksindgange og e-mail trafik til og fra institutionen skal være beskyttet mod ondsindet kode.

Det skal være muligt at blokere ondsindede websider eller e-mails, således at disse ikke kan tilgås.

Der skal som minimum skannes for følgende typer af data:

- Kritiske systemfiler
- Master boot records
- Specifikke filer såsom PDF, eksekverbare filer, makroer, scripts, ondsindede links i e-mails, mm.
- Indgående/udgående netværkstrafik
- Alle vedhæftede filer i e-mail systemer skal scannes inden de åbnes. Mobile medier såsom USB-enheder, eksterne drev og CD/Dvd'er
- Java applets og browser-relaterede trusler

ASKOV HØJSKOLE
& EFTERSKOLE

3.6 Retningslinjer for styring af sikkerhedshændelser

Ved konstatering af brud eller formodning om brud på reglerne om databehandlingssikkerhed **s**kal den ansvarlige leder og den ansvarlige for indberetning til Datatilsynet underrettes herom. For højskolen er det højskoleforstanderen, for efterskolen er det efterskoleforstanderen. I deres fravær underrettes nærmeste leder.

Hvis hændelsen har relation til et bestemt IT-system skal systemejeren også underrettes.

Medarbejdere der konstaterer IT-sikkerhedshændelser eller har en formodning herom, skal øjeblikkeligt notere alle vigtige detaljer såsom typen af brud, den opståede fejl, beskeder på skærmen og usædvanlige hændelser.

Den ansvarlige for indberetning til Datatilsynet skal sikre:

- at databehandlere, der hoster de pågældende data og/eller IT-systemer anmodes om at bistå med at sikre overholdelse af forpligtelserne om behandlingssikkerhed og anmeldelse af brud på sikkerheden til Datatilsynet og den registrerede
- at der, sker anmeldelse af sikkerhedsbruddet til Datatilsynet inden for fristen på 72 timer, med mindre det er usandsynligt at bruddet indebærer en risiko
- at der sker underretning til de registrerede, hvis bruddet er en risiko for den registreredes rettigheder
- at der straks iværksættes de foranstaltninger, der er nødvendige for at korrigere de konstaterede fejl eller svagheder
- at der udarbejdes en redegørelse fra involverede parter ved større it-sikkerhedshændelser
- at der sker opsamling og bearbejdning af oplysninger om it-sikkerhedshændelser.

3.7 Retningslinjer for styring af leverandører og databehandlere

Askov Højskole og Efterskole anvender man i videst muligt omfang hostede løsninger hos eksterne leverandører og databehandlere.

I alle tilfælde, hvor persondata hostes og/eller behandles hos en ekstern databehandler, skal der indgås en ***databehandleraftale*** enten som en del af IT-kontrakten eller som en særlig aftale, der evt. kan dække flere IT-kontrakter.

IT-kontrakten og/eller databehandleraftalen skal også altid indeholde en beskrivelse af de ***fysiske og logiske sikkerhedsforanstaltninger*** som databehandleren er forpligtet til at overholde.

3.7.1 Databehandleraftaler

Ved indgåelse af databehandleraftaler skal Askov Højskole og Efterskole som minimum sikre sig, at databehandleraftalen er i overensstemmelse med Databeskyttelsesforordningens artikel 28.

Databehandlerens behandling af persondata skal således være reguleret af en ***bindende kontrakt***, der skal foreligge skriftligt, herunder elektronisk. Ifølge forordningen skal denne kontrakt, der kaldes en ***databehandleraftale*** mindst indeholde følgende bestemmelser:

- Fastsættelse af genstanden for og varigheden af behandlingen, behandlingens karakter og formål, typen af personoplysninger og kategorierne af registrerede
- Beskrivelse af den dataansvarliges Askov Højskole og Efterskoles forpligtelser og rettigheder
- At databehandleren kun må behandle personoplysninger efter ***dokumenteret instruks*** fra den dataansvarlige
- At databehandleren sikrer, at de personer, der behandler personoplysninger, har ***tavshedspligt***
- At databehandleren iværksætter alle de ***tekniske og organisatoriske sikkerhedsforanstaltninger***, som kræves i henhold til forordningens artikel 32 (se nedenfor i næste afsnit)
- At databehandleren så vidt muligt bistår den dataansvarlige teknisk og organisatorisk med forpligtelsen til at besvare ***henvendelser fra de registrerede*** om deres rettigheder
- At databehandleren bistår den dataansvarlige med at sikre overholdelse af forpligtelserne om behandlingssikkerhed samt anmeldelse af brud på sikkerheden til Datatilsynet og den registrerede
- At databehandleren efter den dataansvarliges valg sletter eller tilbageleverer alle personoplysninger til den dataansvarlige
- At databehandleren stiller alle oplysninger, der er nødvendige, til rådighed for den dataansvarlige

- At databehandleren ikke gør brug af en anden databehandler (***underleverandør***) uden skriftligt godkendelse fra den dataansvarlig

Hvis den eksterne databehandler ønsker at anvende ***underleverandører*** skal databehandleraftalen med databehandleren indeholde følgende bestemmelser:

- at databehandleren skal opfylder de betingelser, der er fastsat, for at gøre ***brug af en anden databehandler*** (underleverandør) – fx at behandling af personoplysninger kun må ske inden for EU
- at databehandleren har pligt til at indgå en ***databehandleraftale med sin underleverandør***, der sikrer, at denne har de samme forpligtelser, som databehandleren har over for den dataansvarlige, herunder de passende tekniske og organisatoriske sikkerhedsforanstaltninger.

3.7.2 Leverandørens/databehandlerens sikkerhedsniveau, håndtering af sikkerhed og kontrol med leverandøren

Det skal fremgå af databehandleraftalen og/eller IT-kontrakten, at databehandleren forpligter sig til at gennemføre passende tekniske og organisatoriske foranstaltninger, der sikrer et sikkerhedsniveau, der opfylder kravene i Databeskyttelsesforordningens artikel 32.

Af IT-kontrakterne og/eller databehandleraftalerne bør ***fremgå bestemmelser om at leverandøren/databehandleren***:

- er bekendt med og garanterer, at ydelserne opfylder alle krav i Askov Højskole og Efterskoles databehandlingssikkerhedspolitik, herunder datasikkerhedshåndbogen.
- behandler Askov Højskole og Efterskoles data fortroligt i overensstemmelse med god it-skik
- opretholder en rimelig og opdateret beskyttelse af driftsmiljøet i overensstemmelse med god it-skik og praksis
- har et beredskab, der begrænser driftsafbrydelser, herunder backup
- foretager en årlig katastrofe- og reetableringstest
- kan reetablere systemer og data efter et nedbrud
- får foretaget en årlig IT-revision af driften efter en international anerkendt revisionsstandard
- tillader, at kunden er berettiget til at gennemføre inspektion af driftsmiljøet
- skal opretholde relevante forsikringer, herunder for datatab
- er ansvarlig for, at hans ydelser overholder lovgivningen
- skal udforme og kontinuerlig ajourføre dokumentation, herunder driftshåndbog
- efter anmodning udlever oplysninger og dokumentation

4 Principper, regler og forretningsgange for behandling af persondata

Ledelsen fastsætter principper og forretningsgange for Askov Højskole og Efterskoles behandling af persondata, der sikrer overholdelse af Databeskyttelsesforordningen og Databeskyttelsesloven.

Forretningsgangene, omfatter de nedenfor fastsatte principper og regler.

4.1 Principper for behandling af personoplysninger

Ledelsen har besluttet at det – ud over det øvrige fastsatte sikkerhedsniveau – skal sikres at persondata:

- Behandles ***lovligt, rimeligt og på en gennemsigtig*** måde (***hjemmel)***
- indsamles og viderebehandles til udtrykkeligt angivne og legitime formål (***formålsbegrænsning***)
- begrænses til, hvad der er nødvendigt til formålet (***dataminimering***)
- er korrekte og ajourførte (***rigtighed***)
- ikke opbevares i et længere tidsrum end hvad der er nødvendigt (***opbevaringsbegrænsning***)

Beslutning vedrørende principper for behandling

I forbindelse med instruktionerne for de enkelte databehandlingssystemer fastlægges behandlingen af persondata så det sikres, at behandlingen har hjemmel, at den er formålsbegrænset, nødvendig og rigtig.

Opbevaringsbegrænsning

Der er fastsat regler for opbevaringsbegrænsning i form af, hvornår persondata skal slettes i alle databehandlingssystemer, såvel elektroniske som manuelle. Slettepolitik C-10

4.2 Anvendelse af samtykke som grundlag for behandling af personoplysninger

Det skal sikres:

- at samtykket er givet ***frivilligt***
- at samtykket er ***specifikt***, så det klart og tydeligt fremgår, hvad det er givet til
- at det ***tydeligt kan påvises***, at den registrerede har givet samtykke
- at samtykket er gives ***skriftligt*** på en måde, hvor det klart kan skelnes fra andre forhold
- at det gives i et ***klart og enkelt sprog*** og
- at den registrerede er oplyst om, at samtykket nemt kan ***trækkes tilbage***

Beslutning vedrørende samtykke

Ledelsen har udarbejdet retningslinjer for brug af samtykke i følgende tilfælde:

- Samtykke fra ansøgere til ledige stillinger GDPR-doc G-2-5
- Samtykke til personaleadministration under ansættelsen GDPR-doc G-3-1 og GDPR-doc G-3-2 og GDPR-doc G-3-4
- Samtykke til honorarudbetaling GDPR-doc G-3-3
- Samtykke til medlemmer af Styrelsen og Repræsentantskabet GDPR-doc G-3-5
- Samtykke til indmeldelse fra elever på efterskolen Samtykkesæt efterskoleelever G-5-1
- Samtykke til indmeldelse fra elever på højskolen Samtykkesæt højskoleelever G-5-2
- Samtykke til tilmelding fra korte kursister via WebTilmeld Persondatapolitik korte kurser D-7-B

Der henvises til de udarbejdede samtykker

4.3 Procedurer for udøvelse af den registreredes rettigheder, der sikrer

- at den registrerede i en let tilgængelig form i et kortfattet, gennemsigtigt, letforståeligt, klart og enkelt sprog kan få oplysning om det registrerede
- at den registrerede modtager de lovpligtige oplysninger ved indsamling af personoplysninger hos den registrerede eller hos andre
- at der er en klar placering af hvem, der har ansvaret for at behandle anmodninger fra den registrerede om indsigt i sine personoplysninger eller udøvelse af retten til berigtigelse, sletning eller begrænsning af behandling og ret til dataportabillitet

Beslutning vedr. den registreredes rettigheder

Ledelsen har udarbejdet retningslinjer om sikring af de registreredes rettigheder i h.h.t. Databeskyttelsesforordningen. I retningslinjerne er angivet, hvem der har ansvaret i de forskellige tilfælde for, at den registreredes behandles i overensstemmelse med reglerne, og der er udarbejdet skabeloner for oplysning om behandling af personoplysninger om den registrerede.

Der henvises til de udarbejdede skabeloner i bilag 4 GDPR-doc D-2

4.4 Fortegnelser udarbejdet over behandlingsaktiviteter med personoplysninger, der beskriver

- Navn på og ***kontaktoplysninger*** om den dataansvarlige
- ***Formålene*** med behandlingen af personoplysningerne
- ***Kategorier*** af de registrerede og kategorier af personoplysninger
- Kategorier af modtagere, som personoplysningerne ***videregives*** til
- ***Tidsfrister for sletning*** af de forskellige kategorier af oplysninger
- Generel beskrivelse af de ***tekniske og organisatoriske sikkerhedsforanstaltninger*** vedrørende behandling af persondata (ved henvisning til Databehandlingssikkerhedspolitikken).

Beslutning vedr. fortegnelser

Der udarbejdes fortegnelser over behandling af personoplysninger på følgende områder:

- Persondata vedr. elever på efterskolen GDPR-doc C-8

- Persondata vedr. elever/kursister på højskolen GDPR-doc C-8
- Persondata vedr. medarbejdere til personaleadministration og HR-virksomhed GDPR-doc C-9

Der henvises til de udarbejdede fortegnelser.

Godkendt af Styrelsen for Askov Højskole og Efterskole 24. februar 2020

ASKOV HØJSKOLE
& EFTERSKOLE

Bilag 1 Organisation og ansvar

Askov Højskole og Efterskoles ledelse har fastsat, hvem der har ***ansvaret for forskellige del af databehandlingssikkerheden*** på følgende områder.

Databehandlingssikkerhedsområde	**Ansvarlig leder/medarbejder**
Styring af ***systemadgang og netværksadgang*** samt ***tildeling af rettigheder***	Forstandere (én eller i forening)
Indgåelse af ***IT-kontrakter og andre kontrakter***, der indebærer behandling af persondata	Forstandere (én eller i forening)
Indkøb af hardware og installation af software	Forstandere (én eller i forening)
Behandling af ***henvendelser fra de registrerede*** om indsigt i sine personoplysninger eller udøvelse af retten til berigtigelse, sletning eller begrænsning af behandling	Forstandere afhængig af om den registrerede var på højskole eller efterskole
Meddelelser til den registrerede om registrering, herunder oplysninger på hjemmesiden	Forstandere
Opsamling og styring af sikkerhedshændelser og Anmeldelse af brud på persondata-sikkerheden til Datatilsynet og de registrerede, der er berørt af bruddet - når dette er påkrævet	Forstandere eller stedfortræder
I forbindelse med ansættelsen modtager medarbejderen særskilt instruktion i databehandlingssikkerhed og anvendelse af databehandlersystemerne	Forstandere Kontorleder

For hver af institutionens, ***automatiske og manuelle databehandlingssystemer***, de data, der opbevares i systemerne samt de forretningsgange, der har tilknytning til systemerne er udpeget en ansvarlig ***(systemejer)***

Automatisk databehandlingssystem	***Systemejer (ansvarlig)***
KomIt	Forstandere
SkolePlan	Forstandere
Hosting-aftaler	Forstandere
Bærbare PC 'er og telefoner	Forstandere
Netadgang og opkoblinger	Forstandere og ekstern IT-support
Administrativ løsning på PC' ere	Forstandere og ekstern IT-support
Viggo	Forstandere

Manuelt databehandlingssystem (arkiv)	***Systemejer (ansvarlig)***
Arkiv med personalemapper i kontorleders kontor	Kontorleder
Arkiv med Indmeldelser/prøvebeviser efterskolen	Sekretær efterskolen
Arkiv med tilmeldinger korte kurser højskolen	Kursus- og udlejningskoordinator
Arkiv med tilmeldinger lange kurser højskolen	Kursus- og udlejningskoordinator