

Behandling af personoplysninger i digitale medier ifm. undervisning i faget Digitale Metoder

Om kurset: Faget Digitale Metoder, som beskrevet i Studieordning for Bacheloruddannelsen i Medievidenskab (2021). Kurset starter 1. februar 2026 og slutter ved semesterslut samme år.

Hjemmelsgrundlag: I forbindelse med undervisningen i ovennævnte kursus behandles almindelige personoplysninger med hjemmel i Persondataforordningens art. 6, litra e, og følsomme personoplysninger behandles med hjemmel i Persondataforordningens art. 9, stk. 2, litra e og litra g.

Formål med behandlingen: Formålet med behandlingen er, at de studerende i ovennævnte undervisningsforløb lærer at indsamle, rense/klargøre og analysere digitalt materiale med henblik på at kunne gennemføre det pågældende undervisningsforløb i overensstemmelse med kravene i studieordningen. Nedenstående behandlingsaktiviteter er således nødvendige for at kunne indfri undervisningens formål.

Beskrivelse af behandlingsaktiviteterne samt af det digitale materiale: De studerende skal indsamle materiale i forskellige typer digitale medier, som er offentligt tilgængelige, dvs. som alle kan få adgang til (ikke bag password). Der er konkret tale om følgende typer digitalt materiale:

- digitaliserede aviser (fx fra Det Kongelige Bibliotek),
- digitaliseret radio og tv (fx fra Det Kongelige Bibliotek),
- websider (fx fra det online web samt fra det amerikanske online webarkiv the Internet Archive),
- sociale medier (fra online såvel som arkiverede udgaver), hvor den pågældende platforms Terms of Service tillader indsamling til undervisningsformål.

Materialet skal efter indsamling renses og klargøres til analyse. Analyserne vil blive foretaget med en række forskellige digitale metoder og analyseværktøjer, som fx netværksanalyse af hyperlinks, ordfrekvensanalyser, sentiment analysis, topic modelling og lyd- og billedanalyse (ikke udtømmende liste).

Tekniske og organisatoriske foranstaltninger: Behandlingen af data sker i overensstemmelse med følgende tekniske og organisatoriske foranstaltninger:

- de studerende instrueres og undervises i, hvordan ovennævnte behandlingsaktiviteter kan foregå, og herefter skal de selv eftergøre dem, så de skaber deres egen datasamling,
- de studerendes egen datasamling skal straks efter indsamling overføres til og opbevares på de studerendes egen krypterede computer eller i AUs sikre computermiljø; data må ikke opbevares andre steder (fx på ukrypterede USB-drev, løse harddiske, eller lignende),
- den efterfølgende behandling kan foregå på de studerendes egen krypterede computer eller i AUs sikre computermiljø,
- data må ikke deles med personer, som ikke er studerende på undervisningsforløbet,
- data slettes efter behandlingen er afsluttet, senest ved undervisningssemestrets afsluttende eksamen; ved sletning skal det sikres, at materialet ikke misbruges eller kommer til uvedkommendes kendskab,

- kontrol af sletning følger følgende proces, som de studerende orienteres om ved semesterstart: (a) ved semesterstart orienteres de studerende om, at hvis de opbevarer personoplysninger relateret til undervisningen på deres egen krypterede computer, så skal de oprette en mappe 'Data', og personoplysninger må herefter kun ligge i den nævnte mappe, (b) umiddelbart efter afslutning af den mundtlige eksamen flytter den studerende de personoplysninger, som måtte ligge på egen krypterede computer, til det sikre server-miljø, som AU stiller til rådighed (dvs. UCloud) og sletter herefter data på egen krypterede computer, (c) underviserne kontrollerer umiddelbart efter afslutning af den mundtlige eksamen, at personoplysninger i ovennævnte mappe er slettet på egen computer, (d) umiddelbart efter afslutning af den mundtlige eksamen lukker underviserne for de studerendes adgang til det sikre server-miljø, som AU stiller til rådighed, men data forbliver liggende der, indtil klagefristen efter eksamen er udløbet, herefter slettes de af underviserne.

Konkret risikovurdering af risiciene for krænkelse af den registreredes rettigheder og frihedsrettigheder

Fortrolighed

Hvor sandsynligt er det, at andre får utilsigtet adgang til personoplysninger? *Dette gælder også personoplysninger, der behandles af en databehandler (sæt kryds)*

- ☒ Usandsynligt (1)
☐ Mindre sandsynligt (2)
☐ Sandsynligt (3)
☐ Forventet (imminent) (4)

Fritekst: Det vurderes som usandsynligt, at andre får utilsigtet adgang til personoplysninger, fordi disse opbevares på krypteret computer eller på sikker server.

Hvad vil konsekvensen være af en utilsigtet adgang til personoplysninger for de personer, hvis data behandles i projektet? *(sæt kryds)*

- ☒ Ingen eller ubetydelige konsekvenser (1)
☐ Generende konsekvenser (2)
☐ Kritiske konsekvenser (3)
☐ Uacceptable konsekvenser (4)

Fritekst: Konsekvensen af en utilsigtet adgang til personoplysninger for de personer, hvis data behandles i projektet vurderes som ubetydelige, idet der er tale om offentligt tilgængelige oplysninger, som de registrerede tydeligvis selv har offentliggjort

Sandsynlighed gange konsekvens (Fx usandsynligt x generende konsekvenser $= 1x2 = 2$) *(afkryds i risikobilledet)*

Konsekvens X Sandsynlighed	Ingen eller ubetydelige konsekvenser	Generende konsekvenser	Kritiske konsekvenser	Uacceptable konsekvenser
Usandsynligt	1 ☒	2 ☐	3 ☐	4 ☐
Mindre sandsynligt	2 ☐	4 ☐	6 ☐	8 ☐
Sandsynligt	3 ☐	6 ☐	9 ☐	12 ☐
Forventet Imminent	4 ☐	8 ☐	12 ☐	16 ☐

Hvad er der gjort for at begrænse sandsynligheden og konsekvenserne?

Beskriv: Sandsynligheden og konsekvenserne begrænses ved, at oplysningerne opbevares på krypteret computer eller sikker server, og samtidig ved at der er tale om oplysninger, som de registrerede tydeligvis selv har offentliggjort.

Integritet

Hvor sandsynligt er det, at personoplysninger utilsigtet bliver ændret? *Dette gælder også data, der behandles af en databehandler (sæt kryds)*

- ☒ Usandsynligt (1)
☐ Mindre sandsynligt (2)
☐ Sandsynligt (3)
☐ Forventet (imminent) (4)

Fritekst: Det er usandsynligt at personoplysninger utilsigtet bliver ændret, idet de digitale analytiske værktøjer arbejder på en kopi af data, hvorfor de ikke ændrer på rådata.

Hvad vil konsekvensen være af en utilsigtet ændring af data for de personer, hvis data behandles i projektet? (sæt kryds)

- ☒ Ingen eller ubetydelige konsekvenser (1)
☐ Generende konsekvenser (2)
☐ Kritiske konsekvenser (3)
☐ Uacceptable konsekvenser (4)

Fritekst: En utilsigtet ændring af data for de personer, hvis data behandles i projektet, vurderes at have ubetydelige konsekvenser, fordi det oprindelige data allerede findes offentligt tilgængelige.

Sandsynlighed gange konsekvens (Fx usandsynligt $\times$ generende konsekvenser = $1 \times 2 = 2$) (afkryds i risikobilledet)

Konsekvens X Sandsynlighed	Ingen eller ubetydelige konsekvenser	Generende konsekvenser	Kritiske konsekvenser	Uacceptable konsekvenser
Usandsynligt	1 ☒	2 ☐	3 ☐	4 ☐
Mindre sandsynligt	2 ☐	4 ☐	6 ☐	8 ☐
Sandsynligt	3 ☐	6 ☐	9 ☐	12 ☐
Forventet Imminent	4 ☐	8 ☐	12 ☐	16 ☐

Hvad er der gjort for at begrænse sandsynligheden og konsekvenserne?

Beskriv: Sandsynligheden og konsekvenserne begrænses, i og med der kun arbejdes på kopier af rådata, og i og med oplysningerne allerede findes offentligt tilgængelige

Tilgængelighed

Hvor sandsynligt er det, at personoplysninger ikke er tilgængelige, fx på grund af IT-svigt eller databehandlers konkurs? *Dette gælder også personoplysninger, der behandles af en databehandler (sæt kryds)*

- ☒ Usandsynligt (1)
☐ Mindre sandsynligt (2)

- ☐ Sandsynligt (3)
- ☐ Forventet (imminent) (4)

Fritekst: Det vurderes som usandsynligt, at personoplysninger ikke er tilgængelige, idet de opbevares både på krypteret computer og på en sikker server.

Hvad vil konsekvensen være af en manglende tilgængelighed til personoplysninger for de personer, hvis oplysninger behandles i projektet? (sæt kryds)

- ☒ Ingen eller ubetydelige konsekvenser (1)
- ☐ Generende konsekvenser (2)
- ☐ Kritiske konsekvenser (3)
- ☐ Uacceptable konsekvenser (4)

Fritekst: Konsekvensen af en manglende tilgængelighed til personoplysninger for de personer, hvis oplysninger behandles, vurderes ikke at have nogen konsekvenser, fordi der er tale om allerede offentliggjorte oplysninger.

Sandsynlighed gange konsekvens (Fx usandsynligt x generende konsekvenser = $1 \times 2 = 2$) (afkryds i risikobilledet)

Konsekvens X Sandsynlighed	Ingen eller ubetydelige konsekvenser	Generende konsekvenser	Kritiske konsekvenser	Uacceptable konsekvenser
Usandsynligt	1 ☒	2 ☐	3 ☐	4 ☐
Mindre sandsynligt	2 ☐	4 ☐	6 ☐	8 ☐
Sandsynligt	3 ☐	6 ☐	9 ☐	12 ☐
Forventet Imminent	4 ☐	8 ☐	12 ☐	16 ☐

Hvad er der gjort for at begrænse sandsynligheden og konsekvenserne?

Beskriv: Sandsynligheden og konsekvenserne begrænses derved, at oplysningerne opbevares mere end ét sted, og de har allerede været offentliggjort.

Samlet set vurderes de registrerede at eksponeres for lav risiko.

Ovenstående er udfyldt ud fra retningslinjerne på websiden 'Hvordan laver jeg en skriftlig risikovurdering?', <https://medarbejdere.au.dk/informationssikkerhed/databeskyttelse/saerligt-om-forskning/risikovurdering-og-konsekvensanalyse/>

Dato, navn, underskrift: _____