ESDH

Hvorfor og hvordan?

Gymnasiefællesskabet den 6. februar 2017

Hvorfor?

- I behandler personoplysninger – derfor har I behov for EDSH
- ESDH systemets primære opgave er hjælpe jer til at passe på personoplysninger
- Derudover effektivisering af administrationen

Hvorfor?

- Fordi samfundet generelt bliver mere og mere digitalt – teknologien tillader det
- Fordi staten har en digitaliseringsstrategi => langt hovedparten af al kommunikation med det offentlige skal kunne ske digitalt.
- Mængden af registreret data stiger markant
- Dette udløser større offentlig bevågenhed
- Og skærpede krav til datasikkerhed – både fra de registrerede, politikerne og de myndigheder og virksomheder
- Øget bevidsthed om, at der er forskel på, hvilken databehandling, der er "teknologisk mulig" og hvilken databehandling, der er "lovlig"

- Den 26. maj 2018: ny EU-databeskyttelsesforordning træder i kraft.
- Dette kaster nyt lys på de regler om databeskyttelse, **der allerede gælder nu**
- Det nye bliver store bøder + vi skal kunne dokumentere lovligheden af en databehandling før den sættes igang

Hvilke myndighedskrav er der til behandlingen af personoplysninger – og øvrige data?
Et kludetæppe af krav!

PERSONDATALOVEN → Hvornår skolen må behandle data

STX-LOVGIVNINGEN:
- Se senere slide

FORVALTNINGSLOVEN:
- Aktindsigt: parterne kan forlange at få indsigt i sagens dokumenter
- Tavshedspligt om enkeltpersoners private forhold og virksomheders væsentlige forretningsforhold

OFFENTLIGHEDSLOVEN:
- Loven har til formål "at støtte borgernes adgang til offentlige myndigheders oplysninger" (åbenhed, indsigt, kontrol, tillid, demokrati, indflydelse)
- Midlet hertil er aktindsigt

ARKIVLOVEN:
- adgangen til offentlige institutioners arkivalier
- aflevering på anmodning fra Statens Arkiver
- Herefter sletning (effektivt)

BOGFØRINGSLOVEN:
- Opbevaring i 5 år

LOV OM DIGITAL POST:
- Fra 1. november 2014 er det obligatorisk for alle > 15 år at kunne modtage post digitalt fra det offentlige
- Digital Post har samme retsvirkninger som – og erstatter – fysiske breve
- Kun undtagelse herfra, hvis borgeren har bedt sig fritaget

} Hvornår skolen skal behandle data

Hvad er persondata?

”*Enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede)*.”

Persondata kategoriseres i forskellige typer:

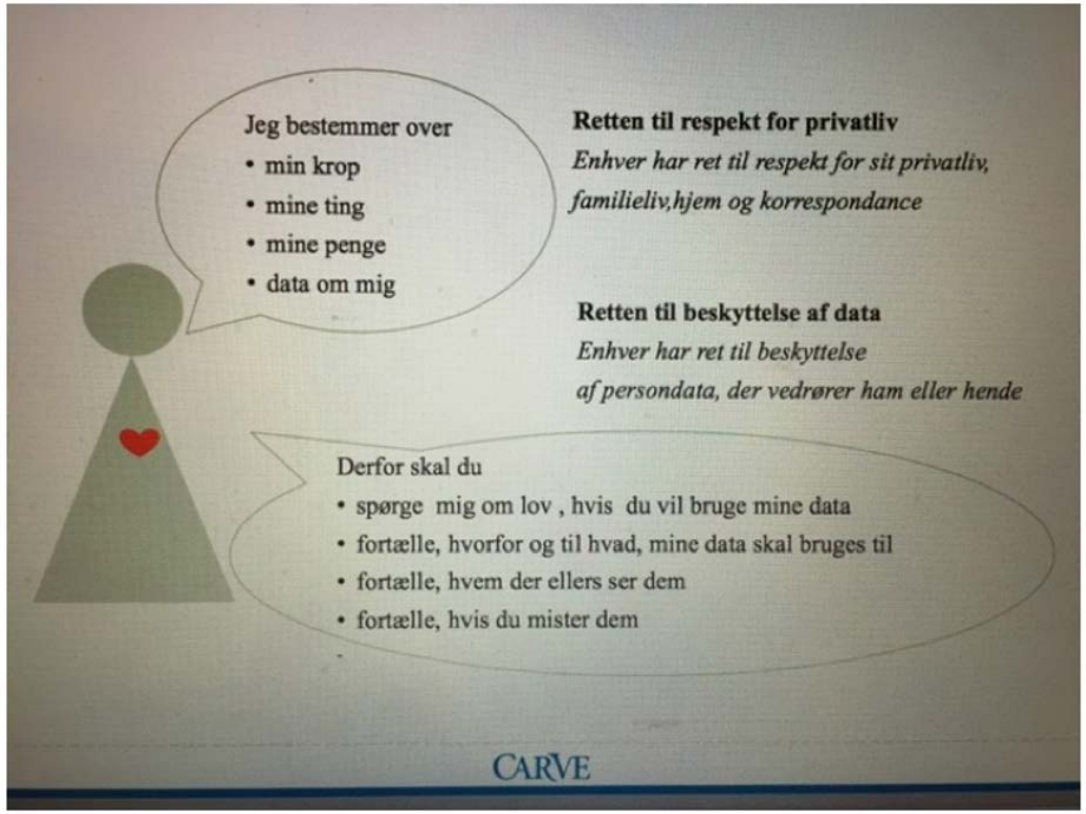
1) ”Almindelige”,
2) ”semifølsomme”
3) ”følsomme” personoplysninger

Kategoriseringen anvendes, fordi der gælder forskellige betingelser og procedurer for behandling af personoplysninger afhængig af oplysningernes følsomhed.

PERSONOPLYSNINGER, SOM SKOLER TYPISK KOMMER I KONTAKT MED					FORTROLIGE OPLYSNINGER I ØVRIGT
	Elev	**Forældre**	**Medarbejdere**	**Bestyrelsesmedlemmer**	
Almindelige personoplysninger	Ansøgning, stamdata/kontaktdata, optagelse, indskrivning, udlån af bøger/Ipad, valg af studieretning, hold/fag, skema, lektiegivning, situationsbilleder fra skolens hverdag, logning af internettrafik/korrespondance på Lectio, deltagelse i arrangementer, rejser, fremmøde/fravær, udskrivning, jubilæer,	Stamdata/kontaktdata, civilstand, forældremyndighed	Stamdata/kontaktdata, rekruttering, cv, ansættelse, løn, kontooplysninger, beskatning, fri telefon og pc, hjemmeopkobling, arbejdsopgaver, kurser, meritter, fremmøde og fravær, referat af MUS-samtaler, sletning af oplysninger,	Stamdata/kontaktdata, honorering, mandat (udpegningsgrundlag)	
(Fortrolige oplysninger) *hører til de "almindelige personoplysninger, men er omfattet af tavshedspligt*	CPR, portrætbillede (offentliggørelse på internet kræver samtykke), karakterer, studievejledning, oplysninger om væsentlige sociale problemer, sanktioner, eksamensbeviser, karakterer, økonomiske oplysninger og andre private forhold,	CPR, oplysninger om væsentlige sociale problemer, økonomiske oplysninger og andre private forhold,	CPR, foto (både portræt og situationsbilleder - offentliggørelse på internettet kræver samtykke), karakterer, oplysninger om væsentlige sociale problemer, økonomiske oplysninger og andre private forhold, personlighedstest, logning af internettrafik og kontrol med e-mails, disciplinære foranstaltninger, afskedigelse, fratrådte medarbejders e-mails,	CPR	Oplysninger om skolens drift: Vedtægter, strategiske forhold, mødereferater, årsrapporter, indberetninger, optælling, indberetning, prognoser, søgetal, tilskud, revision, instrukser Oplysninger om leverandører: Kontrakter, udbud, priser, forretningshemmeligheder (særligt know how)
Semifølsomme personoplysninger	Straffedomme og lovovertrædelser	do	do	do	
Følsomme personoplysninger	helbredsoplysninger, (fag)foreningsmæssig tilknytning, politisk, religigøs eller filosofisk overbevisning, oplysninger om race, etnicitet, oplysninger om seksuel orientering	do	do	do	

Generelle principper for behandling af persondata

Persondatalovgivningen fastlægger, hvornår vi har RET til at behandle persondata (spørgsmålet om, hvornår vi har PLIGT til at behandle persondata følger af anden lovgivning).



Generelle principper for behandling af persondata

Følgende skal altid være opfyldt for at en behandling af personoplysninger er lovlig:

a) Personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede

b) Personoplysninger skal indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål

c) Personoplysninger skal være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles

d) Personoplysningerne skal være korrekte og ajourførte. Urigtige personoplysninger slettes eller berigtiges straks

e) Personoplysninger skal opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt ifht formålet

f) Personoplysninger skal behandles på sikker vis og beskyttes imod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse

g) Der skal foreligge en ”behandlingsbetingelse” – enten i form af samtykke til databehandlingen fra eleven (der skal altid foreligge samtykke hvis der er tale om helbredsoplysninger/diagnoser) eller fordi databehandlingen er ”nødvendig” for 1) udførelse af den offentlige myndighedsopgave, som skolen er pålagt eller for at skolen kan overholde en retlig forpligtelse, som påhviler den overfor eleven

Skolen er ansvarlige for at principperne a)-g) overholdes og skal kunne dokumentere dette (dette sikres via bl.a. retningslinjer og arbejdsgange for behandling af personoplysninger)

Hvad vil det sige at ”behandle” persondata?

”Behandling” er et meget bredt begreb. Nærmest alt, jf. lovteksten:

”Ved behandling forstås enhver aktivitet med eller uden brug af elektronisk databehandling, som oplysninger gøres til genstand for, fx indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse”

Sletning - elevdata

Sletning efter hhv. 5, 10 og 30 år, jf. stx-lovgivningen:

- Identifikationsoplysninger, oplysninger om studieretning og indskrivningsperioder slettes ved meddelelse om den studerendes død.
  - Dette har fx betydning ifht. at kunne indkalde til jubilæer mv.

- Øvrige oplysninger, der er nødvendige for at udstede et prøve- eller eksamensbevis, opbevares i 30 år, jf. § 38, stk. 1, i den almene eksamensbekendtgørelse.
  - Bemærk, at indberetning til UVM's centrale systemer ikke fritager for jeres opbevaringspligten.

- Oplysninger, der er nødvendige for at udstede attestationer for gennemført undervisning, opbevares i 10 år, jf. § 142, stk. 4, i stx-bekendtgørelsen.

- Alle øvrige oplysninger om elever slettes efter 5 år.

- Evt. logningsdata (herved forstås logning af elevers internettrafik på skolens netværk) slettes efter senest 6 måneder

Når retten til at slette oplysninger i henhold til stx-lovgivningen aktualiseres, skal sletning kunne ske effektivt, jf. persondatalovgivningen.

Medarbejderdata

- Personoplysninger om ansøgere, der ikke kom i betragtning til jobbet, skal slettes senest efter 6 måneder. U: hvis samtykke til længere opbevaring.

- Personoplysninger om medarbejdere kan opbevares indtil denne er fratrådt.
  - Dvs. at der kan være situationer, hvor medarbejderens anmodning om sletning af visse oplysninger skal efterkommes

- Når en medarbejder er fratrådt, kan personoplysninger som tommelfingerregel opbevares i yderligere en periode, hvis skolen konkret har behov for det:
  - Dette gælder for ansatte, der er født den 1. i måneden og chefer. Her er der opbevaringspligt ifølge reglerne om Statens Arkiver, og oplysningerne må ikke slettes, men skal afleveres til Statens Arkiver, når de beder om det.
  - Dette gælder også for ansatte, hvor der er verserende arbejdsskadesager, uafsluttede retssager eller arbejdsretlige tvister mellem medarbejderen og arbejdsgiver. Eller det kan gælde oplysninger om pensionsforpligtelser, dagpengerefusion og udbetaling af tilgodehavender.
  - I disse tilfælde bør oplysningerne overføres til et arkiv efter 5 år – herfra kan de så hentes frem, hvis det bliver nødvendigt.

IT-sikkerhed – en del af betingelserne for at persondata kan behandles lovligt

Persondatalovens § 41:

Stk. 1. Personer der udfører arbejde for den dataansvarlige (skolen) og som får adgang til oplysninger, må kun behandle disse efter instruks fra den dataansvarlige (skolen) […].

[…]

Stk. 3. Den dataansvarlige (skolen) skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. […]

I praksis betyder det, at IT-sikkerheden skal være til stede

- fysisk (lokalemæssigt, den menneskelige faktor),
- teknisk (brug af de rette it-systemer)
- organisatorisk (brugeradgange, roller, rettigheder)

Krav til system og organisation

Det betyder, at det it-system, som skolen benytter til behandling af personoplysninger, skal kunne:

- Understøtte lovgivers hensigt om digitalisering (aktindsigt via e-mail, opbevare sikker digital kopi af originalen, alle digitalt udsendte breve skal være sendt og gemt i uredigérbar version, alle digitalt udsendte breve skal være underskrevet)
- Sikre at oplysninger og fortilfælde (egen praksis) kan findes frem via søgning på metadata (emner, stikord, sagstyper, cpr.nr., dato, organ)
- Sikre at udvalgte oplysninger, dokumenter og sager kan findes og slettes effektivt (når der ikke længere er et sagligt behandlingsgrundlag)
- Sikre en fast struktur – dvs. hvor mapper ikke kan flyttes eller slettes (fx ved en fejl eller et uheldigt træk med musen – som man måske ikke selv opdager).

Det betyder også, at skolen skal have politikker/arbejdsgange/instrukser for medarbejdernes:

- Brug af ESDH til arkivering af oplysninger, dokumenter, sager
- Styring af brugerroller og –rettigheder
- Kontrol med saglig behandling af personoplysninger
- Brug af ensartede metadata til oprettelse og arkivering af sager i ESDH
- Sletning af data

Uddrag af bud på retningslinjer:

Retningslinjer for behandling af personoplysninger via ESDH og andre godkendte systemer

Når man som [administrativ] medarbejder på [*] Gymnasium behandler oplysninger om personer (medarbejdere, elever, ansøgere, pårørende, bestyrelsesmedlemmer eller andre personer), skal oplysningerne lagres i og behandles via de administrative systemer, som [*] Gymnasium stiller til rådighed.

Disse systemer er for personoplysninger: [DocuNote ESDH, Statens lønsystem, Navision stat, Indfak2, HRdatabasen, Gymbetaling og CPR-Registeret (der kan alene foretages opslag til CPR-Registeret)].

I alle systemer som indeholder personfølsomme/fortrolige oplysninger bliver opslag/handlinger logget.

Der må ikke formidles og/eller gemmes personoplysninger i andre systemer.

Systemer og platforme som [fx eget drev, skrivebordet på computeren, Outlook, Meebook, EduLife, GoogleApps, Skydrive, Dropbox], må ikke bruges til personhenførbare oplysninger. Dette skyldes blandt andet, ***at*** systemerne ikke er sikre, ***at*** vi ikke kan sikre den nødvendig logning som kræves, ***at*** vi ikke med sikkerhed kan kontrollere, hvilken server oplysningerne befinder sig og ***at*** vi evt. ikke kan tilgå oplysningerne i tilfælde af en administrativ medarbejders længerevarende fravær.

Reglerne om logning gælder ikke den behandling af personoplysninger, som sker, når oplysningerne indgår i tekstbehandlingsdokumenter, regneark og lign. så længe disse dokumenter er under udarbejdelse eller fungerer som arbejdsdokumenter, hvori der løbende tilføjes nye oplysninger i forbindelse med behandlingen af den enkelte sag. https://www.retsinformation.dk/Forms/R0710.aspx?id=1002

Hvis man er i tvivl om et konkret system må benyttes til at formidle og/eller gemme et konkret dokument eller konkrete oplysninger skal nærmeste leder kontaktes.

De angivne systemer er sikre, fordi der tages back up, benyttes firewall og antivirus, anvendes login, sker systemlogning af al aktivitet i systemet og fordi systemerne kun kan tilgås af de medarbejdere, der har arbejdsmæssigt behov for det.

Krav til system og organisation

PERSONDATALOVEN

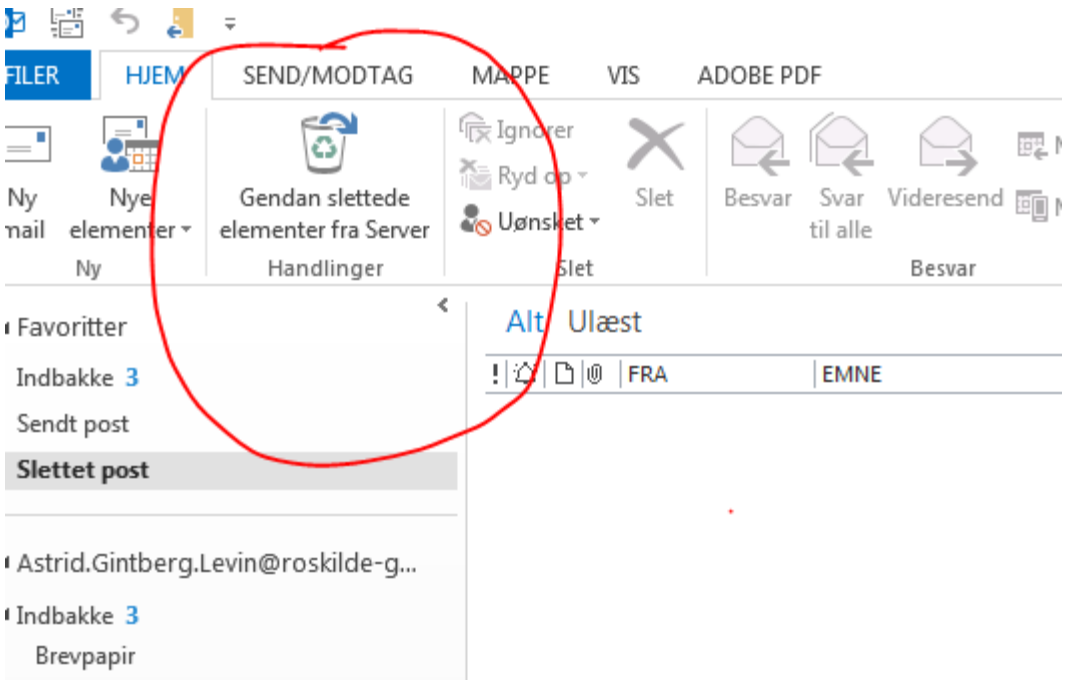
- god databehandlingsskik = skolen må kun behandle personoplysninger, hvis der er et sagligt behov for det. Og kun de medarbejdere, der har relevante arbejdsopgaver (fx elevadministration) må behandle elevoplysninger (”autoriseres hertil”).
- ”De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for”, jf. sikk.bkg. § 11.
- Autorisationer skal angive, i hvilket omfang brugeren må forespørge, inddatere eller slette personoplysninger.
- Kortlægning af behandlingsbehov
- Hver bruger skal tildeles en unik profil, som ikke arves af ny medarbejder
- Ledelsen skal mindst en gang hvert halve år kontrollere, at autorisationerne svarer til det saglige behov. Overflødiggjorte autorisationer inddrages.
- Der må ikke udstedes autorisationer “just in case”
- Instrukser om behandling af persondata (saglighed, fortrolighed, makulering af ind- og uddata, låseskærm når man forlader sin pc)
- Brug af passwords samt begrænset antal chancer til at indtaste korrekt password (Datatilsynet anbefaler, at ”password har en længde på mindst 8 tegn. Passwords bør opbygges af en blanding af tal og store og små bogstaver. Password bør skiftes mindst en gang om året”.)
- Systemlogning alle anvendelser af personoplysninger (oplysning om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium. Lovgivningskrav. Med henblik på kontrol af, at kun autoriserede personer søger på og behandler persondata

Logning

Formål med logning, jf. Datatilsynets afgørelse af 4/7-2014 i sag om Danmarks Statistiks manglende opfyldelse af logningskravet :

> *"Formålet med logning er at sikre et spor efter en autoriseret brugers behandling af fortrolige eller følsomme personoplysninger. Dette spor vil i en konkret sag eller ved en stikprøvekontrol skulle holdes op mod brugerens forklaring om den givne behandling. Logning har således – udover efterforskning – et præventivt formål, idet logningen kan bevirke, at en bruger undlader at foretage behandling af personoplysninger, som han eller hun er autoriseret til, hvis det ikke sker i en arbejdsmæssig sammenhæng."*

Sletning af mails i indbakken:



Slettede mails gemmes i 180 dage og
kan i den periode gendannes.
Evt. slette (effektivt og for bestandigt) ved at holde
”shift-tasten” neden, mens der slettes i ”slettet post”

Hvordan skal vi bruge ESDH for at overholde kravene?

- Mål kunne være:
  - ESDH = platform for daglig administration
  - Alle aktive P-sager overføres - og føres kun her
  - Der ryddes samtidig op i aktive P-sager (”hvad skal der ligge på personalesag?”)
  - Arbejdsflow for en ansættelse i ESDH beskrives.
  - Øvrige relevante dokumenttyper (elevsager, studievejledning, best.materiale, tilskudssager, økonomi, indkøb)
  - Implementeringen – tovholder
  - Instruks til medarbejdere om ikke at gemme andre steder
    - Folder de overordnede sikkerhedskrav ud
    - Gør dem operationelle
    - Skal give mening – og rejser derfor nye spørgsmål

Hvad er risikoen?

- Datatilsynet
- Folketingets Ombudsmand
- Medierne
- Tab af data
- Erstatning/godtgørelse
- EU-lovgivning på vej (2018) om beskyttelse af persondata