Sikker behandling af persondata ifbm. personale- og elevadministration

- *Hvad, hvorfor og hvordan?*

Februar 2017

Gymnasiefællesskabet

Hvorfor det store fokus på databeskyttelse?

- Fordi samfundet generelt bliver mere og mere digitalt
- Fordi staten har en digitaliseringsstrategi
- Mængden af registreret data stiger markant
- Dette udløser større offentlig bevågenhed og skærpede krav til datasikkerhed – både fra de registrerede, politikerne, myndigheder og virksomheder
- Øget bevidsthed om, at der er forskel på, hvilken databehandling, der er ”teknologisk mulig” og hvilken databehandling, der er ”lovlig”

Hvor for det store fokus på databeskyttelse?

- 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

Teaser

De vigtigste grunde til, at man skal kende og bruge de nye regler:

- man får kortlagt data i organisationen og bygget bro mellem forskellige funktioner (brugere – IT – jura)
- Det kan gøre den daglige administration lettere
- Man kan svare på stående fod
- Man kan overholde den eksterne rapporteringsfrist på 72 timer i tilfælde af læk
- Man kan ”tåle” at blive kigget efter i sømmene af brugerne, revisor, medierne, Datatilsynet og Folketingets Ombudsmand
- Man risikerer fremover store bøder, hvis man ikke overholder reglerne
- Man kan få vejledning hos sin databeskyttelsesrådgiver i tvivlspørgsmål
- Man kan lettere identificere sikkerhedsbrud, læk og datatab
- Man kan på sigt spare penge

Kurset har 2 dele

I. Hvad & hvorfor?

- Få det nødvendige kendskab til reglerne og hvorfor de påvirker den daglige administration

- Hvornår må/skal en skole behandle data?

<u>Persondataloven</u>

- Definitioner
- Generelle principper og betingelser for behandling af personoplysninger
- Kravet om IT-sikkerhed
- De registrerede personers rettigheder
- Indførelse af en ny aktør – Databeskyttelsesrådgiveren
- Sletning – ret og pligt

II. Hvordan?

- Få anvist praktiske veje til at løse de udfordringer, som reglerne giver

- Hvordan flyder persondata igennem vores organisation?
- Hvilke it-systemer egner sig til behandling af personoplysninger?
- ”Beredskab” ifht. den registrerede persons rettigheder (dokumentation)
- Hvordan arbejder vi med datasikkerhed i praksis? (vaner, retningslinjer, arbejdsgange)

Dagens emne I

Hvad & hvorfor?

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

PERSONDATALOVEN

Hvornår en skole må behandle data

STX-LOVGIVNINGEN:
- Se slide 23

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

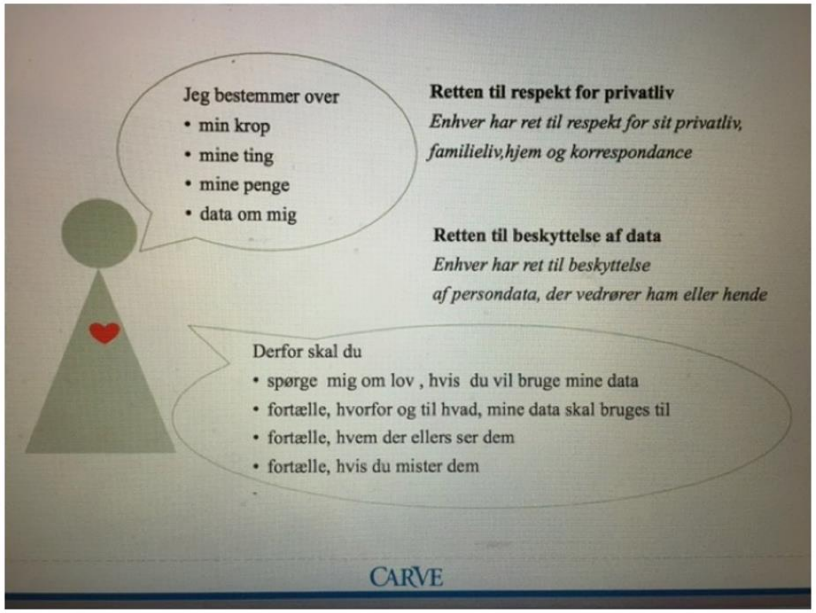
LOV OM DIGITAL POST:
- Fra 1. november 2014 er det obligatorisk for alle > 15 år at kunne modtage post digitalt fra det offentlige
- Digital Post har samme retsvirkninger som – og erstatter – fysiske breve
- Kun undtagelse herfra, hvis borgeren har bedt sig fritaget

Hvornår skolen skal behandle data

Den overordnede forståelse af, hvad behandling af persondata er og kræver

Generelle principper for behandling af persondata

Beskyttelse af mine data er en grundlæggende frihedsrettighed, jf. EU's Charter om grundlæggende rettigheder, art. 7 og 8.



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				
	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
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

Hvornår behandler I 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”

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

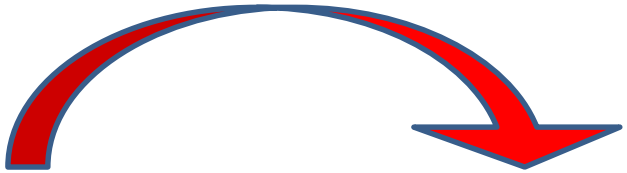
f) Personoplysninger skal behandles på sikker vis og beskyttes imod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse

g) Der skal foreligge en ”behandlingsbetingelse” – enten i form af samtykke til databehandlingen fra den pågældende person (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 vi/skolen er pålagt eller for at vi/skolen kan overholde en retlig forpligtelse, som påhviler os overfor den registrerede person

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)

Den registrerede persons rettigheder

Persondataloven – den registrerede persons rettigheder



På elevens initiativ:

- Medarbejderen/eleven har ret til **indsigt** i, hvilke personoplysninger, der konkret behandles om ham/hende
- Medarbejderen/eleven har ret til at få **berigtiget** urigtige personoplysninger om ham/hende
- Medarbejderen/eleven har – i visse tilfælde – ret til at få sine personoplysninger **slettet**

På skolens initiativ:

oplysningspligt: skolen har pligt til at informere medarbejderen/eleven om, at hans/hendes personoplysninger behandles

Persondataloven - Den registrerede persons rettigheder

Ad **orienteringspligten**:

Orienteringen skal bl.a. indeholde:

- Gymnasiets kontaktoplysninger
- kontaktoplysninger for gymnasiets databeskyttelsesrådgiver
- Formålene med behandlingen og retsgrundlaget (behandlingsbetingelsen) herfor
- Kategorier af personoplysninger
- Eventuelle modtagere eller kategorier af modtagere af personoplysningerne
- Det tidsrum, hvor personoplysningerne vil blive opbevaret
- Information om, hvordan den registrerede kan varetage sine interesser (øvrige rettigheder), jf. næste slide

Persondataloven - Den registrerede persons rettigheder

Ad retten til **indsigt** i, hvilke personoplysninger der behandles:

- Intet krav til specifikation
- Forælder og barnet selv kan fremsætte begæringen
- Måske er der oplysninger, der er så private og personlige, at forældremyndighedsindehaver ikke bør have indsigt. Ex fra tidligere praksis i Datatilsynet: fuld fortrolighed om legalt provokeret abort.

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)

Databeskyttelsesrådgiveren

- En ny aktør

Databeskyttelsesrådgiveren (DPO'en)

Nyskabelse i EU-datasikkerhedsforordningen:

Pr. 26. maj 2018 skal alle offentlige myndigheder have en databeskyttelsesrådgiver (i daglig tale "DPO" (Data Protection Officer). , som skal sikre at behandlingen af persondata er i orden.

DPO'ens opgave er at

- oplyse og vejlede skolerne og de ansatte, der behandler personoplysninger, om deres forpligtelser i henhold til EU-datasikkerhedsforordningen og lovgivning om databeskyttelse (armslængdeprincip)
- at overvåge overholdelsen af databeskyttelseslovgivningen samt skolens lokale politikker om beskyttelse af personoplysninger, herunder fordeling af ansvar, oplysningskampagner og uddannelse af det personale, der medvirker ved behandlingsaktiviteter, og de tilhørende revisioner
- at rådgive skolen og de registrerede personer om databeskyttelse
- at samarbejde med Datatilsynet
- at være kontaktperson for Datatilsynet i spørgsmål om databehandling

DPO'en kan være en medarbejder eller en ekstern konsulent

DPO´en får formentlig en slags TR-beskyttelse mod afsked

Skoler i adm. fællesskaber må godt dele om en DPO fremfor at ansætte en egen DPO

Sletning

Sletning - personoplysninger

RET til at opbevare eller PLIGT til at slette oplysninger?

Skolen har ret til at opbevare data, når lovgivningen pålægger os det:

- STX-lovgivningen
- Forvaltningsloven
- Offentlighedsloven
- Arkivloven
- Lov om digital post
- Bogføringsloven
- Slide nr. 7

Pligt til at slette persondata ifølge persondataloven: på medarbejderens anmodning, HVIS behandlingen rækker ud over det nødvendige og KUN HVIS den øvrige lovgivning tillader det

Slettefrister – elevoplysninger:

NB. Ingen aflevering af elevoplysninger til Statens Arkiver

1. **Identifikationsoplysninger, oplysninger om studieretning og indskrivningsperioder** studieretning og indskrivningsperiode kan opbevares tidsubegrænset
2. Grundlaget for udstedelse af **eksamensbeviser** opbevares i 30 år
   - Dette er elevoplysninger, fag, karakterer, oplysninger om den konkrete eksamen- eller prøveafholdelse
   - Opbevaringskravet er uafhængigt af indberetningen af karakteren til Eksamensdatabasen

3. Oplysninger om **forsømmelser og sanktioner** efter studie- og ordensreglerne opbevares i 10 år, jf. stx-bkg. § 142, stk. 4, med henblik på at sætte rektor i stand til at afgive merit-erklæring
   - Fraværsregistrering, lægelige eller sociale oplysninger som dokumentation for fravær, forseelser, SU, SPS,
   - Advarsel, udelukkelse fra arrangementer eller aktiviteter, aflæggelse af prøve i alle fag, udelukkelse fra eksamen, bortvisning (midlertidigt eller permanent)

4. Alle **andre oplysninger** slettes efter 5 år – eller før.
   - Fx adresse og telefonnummer, oplysninger om nær familie, oplysning om status vedr. hemmelig adresse, foto id, oplysninger om tilknytning til en eller flere institutioner, kopi af pas, kørekort, udlån af bøger, ipad, adgangskort, nationalitet, systembrugeroplysninger, betalingsoplysninger, helbredsoplysninger, misbrug, oplysninger om strafbare forhold, oplysninger væsentlige sociale problemer, interne familieforhold, referat af samtaler, møder mv.

5. **Studievejledning** slettes v/ udskrivning – forudsat at de nødvendige oplysninger til sager under pkt. 3. er gemt dér

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

Sletning - elevdata

Anbefaling fra Danske Gymnasier sommeren 2016:

”*Skolerne skal være opmærksomme på at sikre deres data. Det kan blandt andet ske ved regelmæssigt at indhente backup af data placeret i eksternt hostede systemer. Skolerne skal særligt være opmærksomme på lovpligtige og kritisk data, som skolen har ansvar for at opbevare ifølge gældende lovgivning. Det drejer sig blandt andet (men ikke udelukkende) om: Karakterer og protokollinjer; elev-data; studieplaner, undervisningsbeskrivelser, hold-data, eksamensdata og aktivitetsindberetningstal. Uanset hvilket studieadministrativt system skolen anvender, anbefaler Danske Gymnasier, at de eksisterende backup-planer gennemgås, og at der hurtigt etableres en plan for datasikring, såfremt den ikke allerede findes og er dækkende*.”

Danske Gymnasiers vejledning om sikring af data:

http://www.danskegymnasier.dk/wp-content/uploads/2014/10/Sikring-af-data.pdf

Sletning - 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.

Risici ved ikke at overholde reglerne

- Datatab – og besvær med at komme op og køre igen
- Kritik fra revisor, folketingets ombudsmand,
- Klagesager fra de registrerede personer
- Mediesag, shitstorm
- Og så de meget omtalte forhøjede bødeniveauer – som dog pt. kun ser ud til at få virkning for private virksomheder. Dette kan dog ændre sig, hvis et flertal i folketinget beslutter det. Der er hjemmel til bødeniveauer på op til 10-20.000.000 euro, eller 2-4 % af den globale omsætning – alt afhængigt af, hvad der er højest.

Dagens emne II

Hvordan?

Hvor ”bor” persondata i skolens system?

- Kortlægning ”fra vugge til grav”. ESDH, N-drev, Lectio, cloud, mv.
- Fx i form af svømmebanediagram, der viser handlinger og ansvarsområder
- Hvor er knudepunkterne og hvor skal der træffes de rette valg?
- Instruks og arbejdsgange udarbejdes

Svømmebanediagram – slette aht. datasikkerhed. Kontakt evt. Astrid, hvis I ønsker hjælp til at udarbejde jeres eget.

Excelbeskrivelse af dataflow – slettet aht. datasikkerhed.

Hvordan opfylder skolen sin oplysningspligt angående databehandlingen overfor den registrerede person?

Skolen opfylder sin forpligtelse ved på eget initiativ at orientere eleven/forælderen/medarbejderen om behandlingen og personens rettigheder i den sammenhæng

- i en kortfattet, gennemsigtig, letforståelig og lettilgængelig form
- i et klart og enkelt sprog
- skriftlig (evt. digitalt)

Orienteringen gives senest 1 måned efter indsamlingen, hvis indsamlingen sker hos 3.mand.

Orienteringen gives samtidig med indsamlingen, hvis indsamlingen sker hos den registrerede person selv

Skolen skal føre en oversigt over meddelte og tilbagekaldte samtykker.

Skabelon A
(elev)

Hvordan opfylder skolen sin oplysningspligt overfor den registrerede person?

Formulering i ansættelsesbrev (medarbejder):

”<u>Offentliggørelse</u>

Dit navn og billede vil blive offentliggjort på [*] Gymnasiums hjemmeside og i det studieadministrative system Lectio i forbindelse med din ansættelse. I Lectio fremgår dit undervisningsskema også.

<u>Persondata</u>

Som et nødvendigt led i din ansættelse foretager [*] Gymnasium elektronisk behandling af dine personoplysninger. Behandlingen sker som led i gymnasiets løn- og personaleadministration.

[…]

Jeg ønsker at tiltræde stillingen på ovennævnte vilkår:

Dato:_____ Navn:_____”

Hvordan opfylder skolen sin oplysningspligt overfor den registrerede person? (medarbejder)

Pr. maj 2018 skal orienteringen endvidere indeholde oplysninger om:

- kontaktoplysninger for arbejdsgivers databeskyttelsesrådgiver
- Retsgrundlaget for behandlingen (”EU-forordningens art. 6, stk. 1, litra c”)
- Kategorier af personoplysninger
- Eventuelle modtagere eller kategorier af modtagere af personoplysningerne
- Det tidsrum, hvor personoplysningerne vil blive opbevaret
- Information om, hvordan den registrerede kan varetage sine interesser (øvrige rettigheder)
- Klageadgang til Datatilsynet

Hvordan håndterer skolen en persons anmodning om indsigt i egne persondatabehandling?

- Anmodningen kan være formløs og uspecifik
- Forinden anmodningen efterkommes, skal skolen træffe alle rimelige foranstaltninger for at bekræfte identiteten af en den person, som anmoder om indsigt.
- Oplysninger om andre personer end ham/hende, der anmoder om at se sine egne oplysninger, skal slettes effektivt (blændes eller streges ud) inden kopien udleveres.
  - U: hvis det er forælderen, der anmoder om at se sit barns oplysninger
- Hvis den registrerede indgiver anmodningen elektronisk, udleveres oplysningerne også i elektronisk form.
- Indsigt i egne personoplysninger er gratis.

Skabelon B og C

IT – hvad er do og don’t, når vi behandler persondata? Brugeradgange, passwords, digitale enheder, distancearbejde, forskellige netværk

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)

Lovens formulering af sikkerhedskravene er uspecifikke – dvs. fremtidssikrede.
Stiller krav om en risikobaseret tilgang til valg af sikkerhed.

Konkretisering af datasikkerhed

Skolen skal formulere og anvende information til medarbejderne om, hvordan persondata behandles sikkert. Følgende emner bør beskrives:

1. Hvilke systemer skolen stiller til rådighed for behandling af personoplysninger, fx ESDH og hvilke systemer der ikke er godkendt til – især de følsomme – personoplysninger. Det bør beskrives, at brug af fritekstfelter til noter mv. indebærer stor risiko for, at for mange brugere kan se fortrolige og følsomme persondata + fritekstfelter systemlogges ikke
   - *Skabelon D_Retningslinjer for brug af ESDH mv.*

2. Adgang til oplysningerne skal begrænses til personer, der har et sagligt behov for adgang til oplysningerne. Det skal være så få personer som muligt
   - *Skabelon D_Retningslinjer for brug af ESDH mv.*

3. Medarbejdere, der håndterer personaleoplysninger, skal have instruktion og oplæring i, hvad de må gøre med oplysningerne, og hvordan de skal beskytte oplysningerne.
   - *Skabelon D_Retningslinjer for brug af ESDH mv.*

4. Personaleoplysninger på papir – f.eks. i kartoteker og ringbind – skal opbevares aflåst, når de ikke er i brug. Når dokumenter (papirer, kartotekskort mv.) med personaleoplysninger skal smides ud, skal der anvendes makulering eller anden foranstaltning, der forhindrer, at uvedkommende kan få adgang til oplysningerne.
   - *Skabelon G_Retningslinjer for god databehandlerskik*

5. Der skal anvendes adgangskode for at få adgang til pc'er og andet elektronisk udstyr med personoplysninger. Kun de personer, der skal have adgang, må få en kode. De personer, der har adgangskode, må ikke overlade koden til andre eller lade den ligge, så andre kan se den. Kontrol af tildelte koder skal foretages mindst en gang hvert halve år.
   - *Bør fremgå af skolens it-sikkerhedspolitik*

6. Det skal registreres, hvis der er forgæves forsøg på at få adgang til it-systemer med følsomme personaleoplysninger. Hvis der registreres et nærmere fastsat antal på hinanden følgende afviste adgangsforsøg, skal der blokeres for yderligere forsøg.
   - *Bør fremgå af skolens it-sikkerhedspolitik*

7. Hvis personaleoplysninger lagres på en USB-nøgle, skal oplysningerne beskyttes. Der kan f.eks. bruges en USB-nøgle med adgangskode og kryptering. Ellers skal USB-nøglen opbevares i aflåst skuffe eller skab. Tilsvarende gælder ved opbevaring af personaleoplysninger på andre bærbare datamedier.
   - *Retningslinjer bør udarbejdes*

8. PC'er koblet til internettet skal have en opdateret firewall og viruskontrol installeret.
   - *Skabelon J_Retningslinjer ang. forebyggelse af ransomeware*

9. Hvis følsomme personaleoplysninger og personnummer sendes med e-mail via internettet, anbefaler Datatilsynet kryptering.
   - *Skabelon E_*Retningslinjer for behandling af personoplysninger i postsystemer (Microsoft Outlook, G-Mail, mv.)
   - *Skabelon F_Retningslinjer for brug af Sikker Mail*

10. Hvis der anvendes hjemmearbejdsplads skal følgende overvejes og adresseres i skriftlige retningslinjer: sker der lokal lagring eller arbejdes der via terminal? Bringes der fysiske kopier af materiale med hjem? Har andre end medarbejderen adgang til hjemme-pc'en derhjemme?

11. Der bør der være formuleret retningslinjer i tilfælde af tyveri af pc'er, tablets, smartphones mv., der indeholder personoplysninger. Hvem kontakter man, hvad er adgangen til sletning af (privat) indhold mv.?

12. I forbindelse med reparation og service af dataudstyr, der indeholder personoplysninger, og når datamedier skal sælges eller kasseres, skal der træffes de fornødne foranstaltninger, så oplysninger ikke kan komme til uvedkommendes kendskab.
   - *Skabelon H_Retningslinjer for sletning af datamedier*

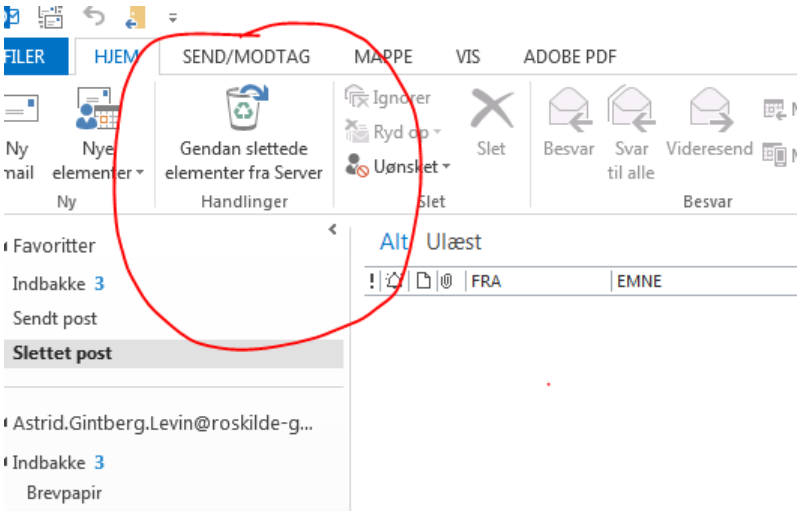
Kilde: http://www.datatilsynet.dk/erhverv/personaleadministration/krav-om-datasikkerhed-i-forbindelse-med-personaleadministration/

Følsomme personoplysninger skal opbevare i et system, der foretager systemlogning – fx ESDH

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 håndterer vi datalæk eller –tab?

Forebyggelse sker i kraft af sikkerhedsorganisation, retningslinjer, uddannelse og overvågning af systemer.

- Komplicér (forebyggelse af hacking mv.)
- Reagér (hav beredskab på forhånd)
- Håndtér (overvej kommunikationen omkring et læk på forhånd, så man er forberedt)

Skolerne skal have procedurer til at opdage, rapportere og undersøge brud på datasikkerhed, der der fremover er

- pligt til at rapportere brud til Datatilsynet inden 3 døgn (kræver styr på databehandlere)
- pligt til at underrette den registrerede, hvis bruddet indebærer risici for misbrug af personoplysninger

Skabelon K og L til rapportering

Hvordan formidles viden og god adfærd ud i organisationen?

- Formulering af retningslinjer, kommunikation, uddannelse, opfølgning (kontrol), ajourføring mindst 1 x årligt

Skabeloner:

a) Underretning og indhentning af samtykke fra elev og forældre ifbm. optagelse
b) Behandling af anmodning om indsigt fra elev
c) Behandling om anmodning om indsigt fra medarbejder
d) Retningslinjer for brug af ESDH, mv.
e) Retningslinjer for behandling af personoplysninger i postsystemer
f) Retningslinjer for Sikker Mail
g) Retningslinjer for god databehandlerskik
h) Retningslinjer for sletning af datamedier
i) Retningslinjer for brug af hjemmearbejdspladser
j) Retningslinjer for beskyttelse mod ransomeware
k) Skabelon – anmeldelse af brud på datasikkerhed til Datatilsynet
l) Skabelon – underretning af registreret person om læk af personoplysninger

Bud på leveregler vedr. datasikkerhed

1. Alle dokumenter oprettes, behandles og gemmes i ESDH (med mindre andet konkret er aftalt)
2. Aktivér din pauseskærm, når du forlader dit skrivebord
3. Læg fysiske personoplysninger i aflåst skab eller skuffe, når du forlader dit skrivebord i længere tid og altid før du forlader arbejdspladsen
4. Undlad at gemme personoplysninger på USB-nøgle el.lign
5. Personoplysninger, der elektronisk sendes til eksterne uden for vores egen mailserver skal sendes til en sikker mailpostkasse, fx E-boks
6. Papir eller andet fysisk materiale med personoplysninger skal altid bortskaffes ved makulering
7. Print der indeholder personoplysninger hentes i printeren straks
8. Vær bevidst om kun at behandle persondata, hvor der er et sagligt og konkret formål til behandlingen, undgå at personoplysninger senere bruges til et andet formål og slet oplysningerne, når du ikke længere skal bruge dem
9. Videregiv ikke personoplysninger uden at være sikker på, at oplysningerne må videregives
10. Åben ikke mails der ser mistænkelige ud eller som kommer fra afsendere, du ikke kender
11. Kontakt IT hvis du bliver opmærksom på noget, du mener kan udgøre en risiko for sikkerheden for behandling af persondata

Tak for i dag

Spørgsmål kan rettes til Astrid i Gymnasiefællesskabet

Mobil 23815081

gfagl@gfadm.dk