EPINION

SKOLERS OG INSTITUTIONERS HÅNDTERING AF ELEVERNES PERSONDATA OG ANVENDELSE AF GRATIS DIGITALE PRODUKTER

STYRELSEN FOR IT OG LÆRING

JANUAR 2019

INDHOLDSFORTEGNELSE

1. INDLEDNING

Med ikrafttrædelse af den europæiske General Data Protection Regulation (GDPR) d. 25. maj 2018 skal det danske uddannelsessystem, herunder institutioner og deres ansatte, håndtere data under en række både nye og skærpede juridiske betingelser.

Overordnet set betyder det sikring af udstyr, inventar, arbejdsgange og en ny kulturel tilgang til, hvad der egentlig udgør persondata om elever. Forandringer, som denne undersøgelse peger på, er i fuld gang ude på institutionerne, men hvor visse spørgsmål stadig kræver afklaring eller konsensus mellem flere interessenter.

Når flere spørgsmål omkring persondatahåndtering og datasikkerhed kræver afklaring, så er det dog ikke nødvendigvis let eller ligetil. For de sikreste valg kan også til tider være kostelige, og opleves som besværlige for ledelse, begrænse administrationens arbejdsmuligheder og undervisernes metodefrihed.

Undersøgelsens overordnede formål er derfor at danne et empirisk grundlag for at kunne pege på sektorens nuværende praksis og de dilemmaer og tvivlsspørgsmål, der opstår, når GDPR implementeres i det daglige arbejde.

God læsning.

1.1 ANALYSENS FORMÅL

Som led i Regeringens nationale cyber- og informationssikkerhedsstrategi (2018-2021[1]) sættes der i initiativ 2.1 fokus på digital dømmekraft og kompetencer via uddannelsessystemet. I forlængelse af initiativ 2.1 har Undervisningsministeriet bedt Epinion udarbejde en konsulentanalyse med henblik på at give et billede af grundskoler og ungdomsuddannelsesinstitutioners håndtering af elevernes persondata, deres anvendelse af digitale produkter samt institutionernes indgåede databehandleraftaler. Analysen skal anvendes til at afklare og styrke Undervisningsministeriets fremadrettede indsatser i arbejdet med rådgivning og vejledning om institutionernes håndtering af elevernes persondata. Rapporten afdækker her, jf. Undervisningsministeriets udbud, følgende:

1. En afdækning og analyse af institutionernes håndtering af elevernes persondata.
2. En afdækning af institutionernes anvendelse af gratis digitale materialer (eksempelvis cloudløsninger og forskellige sociale medier), samt en afdækning af i hvilket omfang institutionerne har indgået databehandleraftaler med leverandørerne af gratis materialer.
3. En afdækning af databehandleraftalerne med leverandørerne af kommercielle digitale læringsmidler. Analysen skal endvidere indeholde en afdækning af hvilke typer af persondata, der i disse tilfælde behandles af/afleveres til leverandørerne.
4. En afdækning af uddannelsessektorens udfordringer og behov på området. F.eks. hvilke udfordringer møder skolelæreren og skolelederen i arbejdet med persondata, og hvilke behov opstår deraf. Undersøgelsen skal omfatte lærerne, det administrative personale, ressourcepersoner, skolelederen og skolebestyrelsen/forældre.
5. En afdækning af udvalgte landes praksis omkring governance vedr. persondata lokalt på institutionerne.

Analysens pointer har til formål at kvalificere vidensgrundlaget for ministeriets fremtidige indsatser.

[1] Regeringens nationale cyber- og informationssikkerhedsstrategi: https://www.fm.dk/publikationer/2018/national-strategi-for-cyber-og-informationssikkerhed

2. DATAGRUNDLAG

2.1 SPØRGESKEMAER

Undersøgelsen bygger på spørgeskemaer sendt ud til undervisere, administration og elever på:

4 erhvervsskoler	**13** folkeskoler	**5** frie grundskoler	**13** gymnasier

Derudover er der spørgeskemabesvarelser fra kommunale it-ansvarlige og skolebestyrelsesformænd. Nedenfor fremgår svarprocenter for de enkelte respondentgrupper.[2]

Tabel 1: Oversigt over svarprocenter i spørgeskemaundersøgelserne blandt undersøgelsens målgrupper

Målgruppe	Population	Antal besvarelser	Svarprocent
Ledere	**1.022**	**468**	**46%**
Folkeskoler	413	188	46%
Frie grundskoler	187	90	48%
Erhvervsskoler m.v.	289	95	33%
Gymnasier og HF-kurser	133	95	71%
Kommunalt it-ansvarlige	**60**	**35**	**58%**
Elever	**36.421**	**7.048**	**19%**
Folkeskoler	2.035	481	24%
Frie grundskoler	413	175	42%
Erhvervsskoler m.v.	23.671	1.417	6%
Gymnasier og HF-kurser	10.302	4.975	48%
Lærere	**2.148**	**708**	**33%**
Folkeskoler	432	136	31%
Frie grundskoler	152	28	18%
Erhvervsskoler m.v.	484	193	40%
Gymnasier og HF-kurser	1.080	351	33%
Administration	**392**	**167**	**43%**
Folkeskoler	51	12	24%
Frie grundskoler	20	6	30%
Erhvervsskoler m.v.	174	71	41%
Gymnasier og HF-kurser	147	78	53%
Forældrebestyrelser	**86**	**30**	**35%**

[2] Se uddybning i rapportens afsluttende metodeafsnit.

Kolonnen 'population' angiver antallet af respondenter, som er blevet inviteret til undersøgelsen.

2.2 CASEBESØG

I alt har projektteamet været ude på 9 caseinstitutioner, fordelt på hhv. 3 grundskoler, 3 erhvervsskoler og 3 gymnasier. Metodisk har været anvendt dybdeinterview, typisk med ledere og fokusgruppeinterviews med administration og undervisere. I alt blev 62 personer interviewet. Alle interviews er blevet optaget på lydfiler og senere transskriberet og kodet.

Tabel 2: Fordeling af interviews på institutions- og medarbejdertyper på afholdte interviews

Dybde og fokusgruppeinterviews	Ledere	Undervisere	Administration
Grundskoler	8	6	6
Erhvervsskoler	4	11	7
Gymnasier	4	9	7
I alt:	**16**	**26**	**20**

2.3 MOBILETNOGRAFI

Derudover har også været anvendt et mobiletnografisk studie. Her har administrative medarbejdere og undervisere fra caseinstitutionerne henover en arbejdsuge modtaget forskellige opgaver og spørgsmål, som de skulle løse omkring datahåndtering og datadilemmaer i dagligdagen. Nogle deltagere i dette studie deltog også i interviews, imens andre udelukkende deltog her. Alle svar og billeder fra det mobiletnografiske studie er blevet transskriberet og kodet. 15 personer deltog i mobiletnografien, og der blev opnået en besvarelsesprocent på 83 pct. af de stillede opgaverne.

Tabel 3: Fordeling af deltagere på institutions- og medarbejdertyper i det mobiletnografiske studie

Mobiletnografi	Lærere	Administration
Grundskoler	2	2
Erhvervsskoler	3	3
Gymnasier	2	3
I alt:	**7**	**8**

2.4 INTERVIEWS MED INTERESSENTER I DESK RESEARCH

Som et led i undersøgelsens desk research er der desuden interviewet 8 aktører fra relevante brancheforeninger, interessenter, forlag og teknologivirksomheder. Disse interviews har indgået som baggrundsmateriale for analyser og casebesøg.

3. BEGREBER OG AFGRÆNSNINGER

3.1 INDLEDNING

Gennem rapporten bruges der en række begreber. Disse knytter dels an til juridiske, dels til tekniske aspekter ved datasikkerhed. Nedenfor følger en kort begrebsgennemgang.

3.2 DIGITALE PRODUKTER

I analysen arbejdes der med begrebet om *digitale produkter*. Der findes en lang række af betegnelser (fx platforme, læremidler, teknologier, materialer, værktøjer eller ressourcer), der refererer til forskellige pædagogiske og tekniske traditioner og brugsaspekter. Når der i denne analyse bruges begrebet digitale *produkter,* er det fordi betoningen i analysen ligger på det aspekt af teknologierne, der handler om, at den er udviklet med henblik på at imødekomme en forbrugers (fx institution, elev eller underviser) behov. Dette behov tilfredsstiller produktet på baggrund af en udveksling, fx af penge eller data. I rapporten arbejdes der med en inddeling af produkter i forskellige kategorier: Digitale forlagsprodukter, cloudløsninger, sociale medier, læringsplatforme og øvrige produkter. Inddelingen er nærmere beskrevet i kapitel 7.

Med betoning af det *digitale* understreges, at analysen fokuserer på de produkter, som er "uhåndgribelige" (engelsk: *intangible*), altså noget som ikke er fysisk, og hvor kopier kan deles som data uden originalen forsvinder[3]. I praksis er det hjemmesider, software og apps som bruges i undervisningen. Der kigges altså i mindre grad på de fysiske enheder, såsom computere, tablets og telefoner.

3.3 PERSONDATA OM ELEVER (ELEVDATA)

Omdrejningspunktet for denne undersøgelse er institutionernes håndtering af persondata om elever. I rapporten bliver dette sammentrukket til elevdata. Elevdata refererer til den type data om elever, der i Databeskyttelsesforordningen kaldes personoplysninger. Personoplysninger inddeles i hhv. almindelige og følsomme. Jf. Datatilsynet defineres almindelige personoplysninger således:

> "Almindelige personoplysninger omfatter alle oplysninger, der ikke er klassificeret som særlige kategorier af oplysninger (følsomme personoplysninger). Det kan for eksempel være identifikationsoplysninger som navn og adresse eller oplysninger om økonomi, skat, gæld, væsentlige sociale problemer, andre rent private forhold, sygedage, tjenstlige forhold, familieforhold, bolig, bil, eksamen, ansøgning, CV, ansættelsesdato og -stilling, arbejdsområde og arbejdstelefon."[4]

Følsomme oplysninger vedrører specifikke oplysningstyper, og adgangen til at behandle disse er snævrere end almindelige personoplysninger. Følsomme oplysninger er oplysninger om:

- Race og etnisk oprindelse
- Politisk overbevisning

[3] https://en.wikipedia.org/wiki/Intangible_good
[4] https://www.datatilsynet.dk/generelt-om-databeskyttelse/hvad-er-personoplysninger/

- Religiøs eller filosofisk overbevisning
- Fagforeningsmæssige tilhørsforhold
- Genetiske data
- Biometriske data med henblik på entydig identifikation
- Helbredsoplysninger
- Seksuelle forhold eller seksuel orientering.

Det er vigtigt at have in mente, at spørgsmålet om, hvornår der er tale om personoplysninger kræver en juridisk og kontekstuel fortolkning. Det afgørende er, om oplysningen er personhenførbar, dvs. om det i praksis er muligt at identificere en person ud fra oplysningerne eller i kombination med andre. Som forskning også har peget på, er spørgsmålet om, hvad der er persondata dog ikke altid helt ligetil i praksis: "personal data must be understood as a much larger and even more invasive class of information than the straightforward items we might think."[5]

I denne analyse beror identifikationen af personoplysninger på den måde, informanter og institutioner selv gengiver disse. Hvor der er anledning til tvivl om fortolkningen af juridiske forhold i de empiriske eksempler, er der knyttet en kommentar til.

3.4 GDPR, DATABESKYTTELSESLOVEN OG DATABEHANDLERAFTALER

Databeskyttelsesforordningen, persondataforordningen eller General Data Protection Regulation (GDPR) refererer alle til den EU-lovgivning, der trådte i kraft i medlemslandene fra 25. maj 2018[6]. GDPR indeholder en række krav til, hvordan myndigheder og virksomheder skal behandle og omgås personoplysninger. En forordning virker som en lov for medlemslandene og er bindende.

Databeskyttelsesloven er den danske forvaltning af de bestemmelser, der gør sig gældende i GDPR[7]. Et af kapitlerne i denne lov vedrører relationen mellem dataansvarlig og databehandler. Når en virksomhed eller myndighed vælger at benytte en anden myndighed eller virksomhed til at behandle personoplysninger på sine vegne, skal der indgås en databehandleraftale, hvor betingelser for arbejdet med persondata udspecificeres.

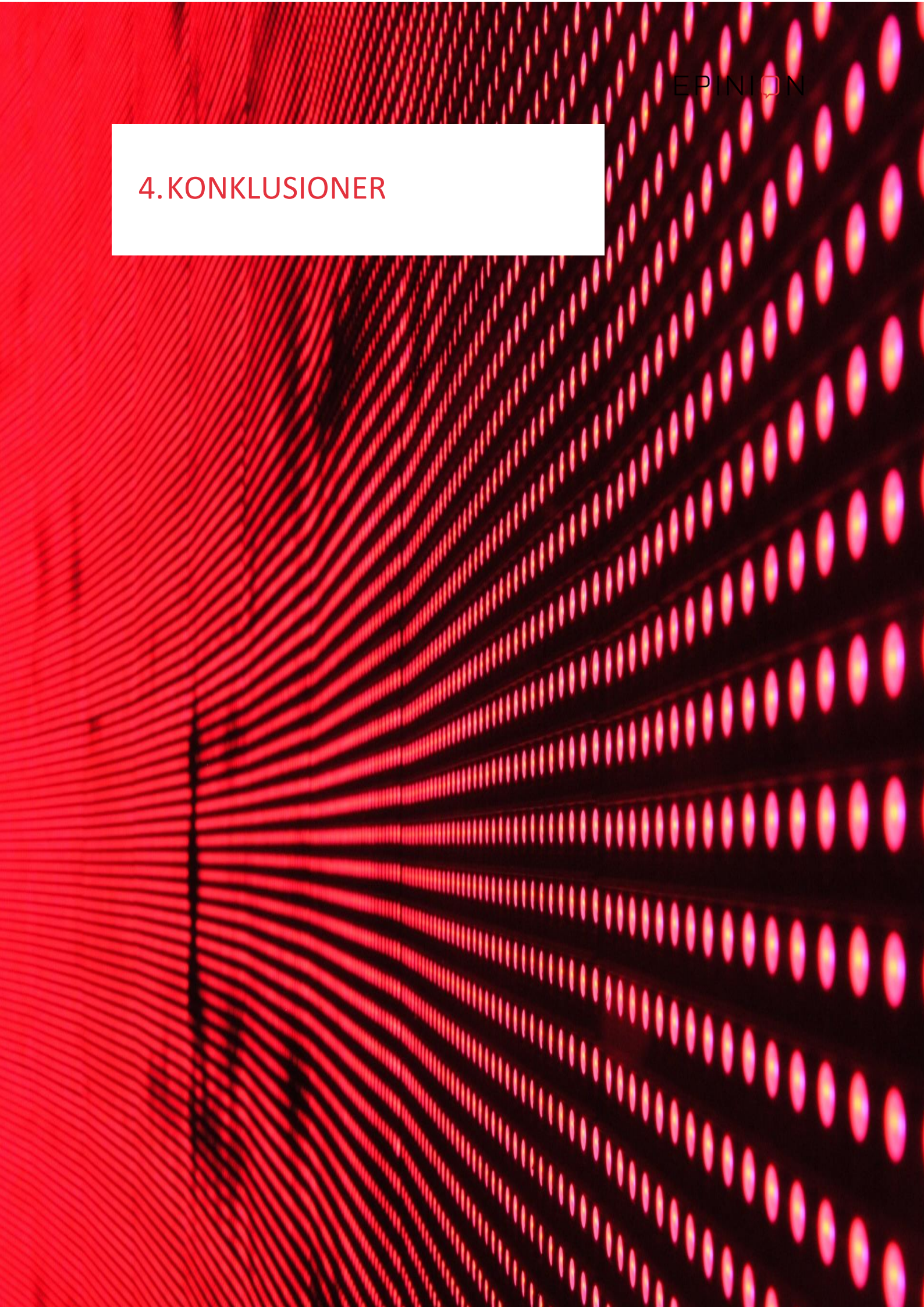
3.5 KOMMUNALE FOLKESKOLER OG SELVEJENDE INSTITUTIONER

I rapporten refereres til forskellige typer af positioner og institutioner. Når der i rapporten skrives skoler, inkluderer det frie grundskoler og folkeskoler. Når der udelukkende er tale om folkeskoler, er dette angivet. Når der i rapporten omtales institutioner indbefatter det samtlige typer, der er adspurgt i spørgeskemaerne: Gymnasier, erhvervsskoler, folkeskoler og frie grundskoler. Givet at folkeskolerne drives af kommunerne, ser den ledelsesmæssige organisering for disse også anderledes ud end den gør for gymnasier, erhvervsskoler og frie grundskoler. Derfor er der i rapporten også en

[5] Golumbia citeret i Pangrazio, L., & Selwyn, N. (2018). 'Personal data literacies': A critical literacies approach to enhancing understandings of personal digital data. *New Media & Society*, 1461444818799523. Side 3.
[6] https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016R0679&from=DA
[7] https://www.datatilsynet.dk/generelt-om-databeskyttelse/lovgivning/

sondring mellem folkeskoler og selvejende institutioner. De relevante respondenter på ledelsesniveau for folkeskoleområdet er folkeskoleledere og kommunalt it-ansvarlige. Kommunalt it-ansvarlige dækker over den eller de ansatte, som kommunernes skolechefer har udpeget som ansvarlige for it og sikkerhed på folkeskoleområdet i den enkelte kommune. For selvejende institutioner er det lederne, rektorer, direktører og skoleledere. Det fremgår løbende i rapportens analyse og figurer, hvilke respondenter og institutioner, der tales om.

4. KONKLUSIONER



4.1 INDLEDNING

Nedenfor følger rapportens overordnede konklusioner, der er delt ind efter digitale produkter i undervisningen og personalegruppernes håndtering og organisatoriske forandringer i forbindelse med sikker datahåndtering. Selvom konklusionerne drages på baggrund af et omfattende kvantitativt og kvalitativt datagrundlag, peger data også på, at der er stor lokal variation i måden at arbejde med datahåndtering. Det betyder også, at der for de skoler og institutioner, der ikke har deltaget i undersøgelsen muligvis gør sig andre forhold gældende, end denne rapport peger på. Data er indsamlet i efteråret 2018, på et tidspunkt umiddelbart efter Databeskyttelseslovens ikrafttræden. Det må derfor også antages, at der siden dataindsamlingen er sket meget på feltet, da det som udgangspunkt er et højt prioriteret anliggende både for ledelse og kommuner.

4.1.1 Datasikkerhed og digitale produkter i undervisningen

På baggrund af analysen kan de anvendte digitale produkter i undervisningen overordnet deles ind i to grupper: De mere og mindre kontrollerede. De *mere kontrollerede* produkter er karakteriseret ved at de i højere grad opleves af brugerne, som mere mulige at kontrollere datasikkerhedsmæssigt. De *mindre kontrollerede* er de produkter, der overvejende opleves som mere ukontrollerbare af brugerne datasikkerhedsmæssigt. De respektive grupper deler en række karakteristika, som fremgår af tabellen nedenfor.

	De mere kontrollerede produkter	De mindre kontrollerede produkter
Kategorier	Læringsplatforme, cloudløsninger*, digitale forlagsprodukter, sagshåndteringssystemer	Sociale medier og øvrige produkter
Karakteristiske brugsformål	Kommunikation med elever, journalisering, dokumentopbevaring, træne elevers faglighed, motiverende og varierende undervisning	Skabe motiverende og varierende undervisning, afprøve elevernes viden, kreative elevproduktioner
Overvejende niveau for beslutning om brug	Institutionsledelse eller kommune	Undervisere og elever
Tillid til datasikkerheden blandt undervisere	Højere	Lavere
Produktvariation	Lille	Stor
Oprindelse	Overvejende danske	Overvejende udenlandske
Licensformer	Overvejende betaling	Overvejende gratis
Databehandleraftaler	I overvejende grad indgået eller påbegyndt	I lavere grad indgået eller påbegyndt

Relevante datatyper (der potentielt kan være personlige)	Resultater, diagnoser, navn, adresse, mail, CPR, billeder, fravær, intern kommunikation m.v.	Billeder, video, lydoptagelse, geolokation, ip-adresse, tekniske indstillinger, e-mail, telefon nr., søgehistorik.
Initiativ til deling af data	Brugeren er i højere grad intiativtager til at dele data	Produktet deler i højere grad data uden initiativ fra brugeren

4.1.1.1 Stor variation i digitale produkter brugt i undervisningen

Der tegner sig et mønster når det kommer til, hvordan underviserne på tværs af institutionerne bruger digitale produkter. Den gennemsnitlige underviser har en produktprofil der ser ud således, at de først og fremmest bruger de produkter, der er stillet til rådighed af institutionen. Det drejer sig især om digitale forlagsprodukter, cloudløsninger og læringsplatforme (disse udgør samlet 20 pct. af de benyttede produkter). Disse produkter er ofte betalte og i højere grad danske, og bruges til kommunikation, dataopbevaring og at tilgå og dele undervisningsindhold.

Derudover bruger de fleste undervisere en række øvrige produkter (69 pct. af de benyttede produkter), der oftere er udenlandske og gratis. Underviserne finder enten selv disse produkter eller får dem vist af kollegaer. De bidrager oftest til at skabe variation og motivation i undervisningen samt at give eleverne mulighed for at lave kreative produkter såsom film og lyd. Sociale medier er også en integreret del af undervisningen (11 pct. af de benyttede produkter), men adskiller sig fra de andre produkter ved oftest at blive taget i brug på elevernes initiativ.

4.1.1.2 Lav tillid til produkterne og behov for kompetencer til at vurdere datasikkerhed

Det er et gennemgående træk, at datasikkerhed sjældent er et hensyn, når undervisere og elever vælger og prioriterer digitale produkter til brug i undervisningssammenhæng. De hensyn, der vejer tungest, er pædagogiske og læringsmæssige. Dette kan være med til at forklare hvorfor, at **størstedelen af underviserne bruger øvrige produkter i undervisningen, selvom de ofte har lavest tillid til datasikkerheden ved disse** (39 pct. har tillid til, at gratis, udenlandske produkter lever op til lovkrav om datasikkerhed). Underviserne angiver også, at de ofte ikke har de fornødne kompetencer til at vurdere datasikkerheden (69 pct. mener, de mangler viden om datadeling med tredjeparter) eller fortælle eleverne, hvilke risici og faldgruber der sikkerhedsmæssigt kan være forbundet med brugen af digitale produkter i undervisningen (30 pct. angiver at have være helt eller delvist enige i at kunne dette).

Det varierer i høj grad, hvordan underviserne kunne tænke sig, at der blev taget hånd om datasikkerhedsmæssige aspekter ved digitale produkter undervisningen. Dette kommer til udtryk ved, at 19 pct. ønsker, at ledelsen eller andre afgør, hvilke produkter de må bruge. 36 pct. ønsker selv at vælge digitale produkter og derefter få dem sikkerhedsgodkendt af en it-kompetent og 33 pct. ønsker selv at bestemme, hvornår og på hvilke betingelser, de bruger digitale produkter i undervisningen. Kun 6 pct. ser ikke noget behov for at blive klædt yderligere på ift. at vurdere datasikkerheden ved digitale produkter.

4.1.1.3 Databehandleraftaler indgås

Institutionerne er meget opmærksomme på at indgå databehandleraftaler med leverandører af de digitale produkter som anvendes hyppigst og er mest udbredte på tværs af institutionerne. **Det betyder også, at langt størstedelen enten har eller er i gang med at indgå aftaler med de leverandører af forlagsprodukter, cloudløsninger og læringsplatforme, hvis produkter bliver anvendt.** Gennem interviews og casebesøg er det vist, hvordan der lokalt også bliver gjort opmærksom på på hvilke betingelser (fx deling eller tidsfrister) forskellige datatyper kan håndteres, fx hvad der må lægges på cloud.

Flere ledere og administrationschefer fremhæver, at de ikke har et fuldt overblik over, hvilke produkter der bruges i undervisningen, og at de godt ved, at der potentielt anvendes en lang række af produkter. For de selvejende institutioner[8] angiver kun 27 pct. af lederne, at de i nogen eller høj grad har overblik over de brugte produkter. For de kommunalt it-ansvarlige er tallet 60 pct.

De produkter, ledere og kommuner ikke kender til, er oftest ikke omfattet af databehandleraftaler og heller ikke reguleret gennem lokale restriktioner eller retningslinjer for, hvordan de må bruges. De produktkategorier der bruges på disse betingelser, er de øvrige produkter og sociale medier. Nogle af institutionerne har dog taget en række initiativer for at skærpe kapaciteten til at beskytte elevdata. Det er fx monitorering af netværksaktivitet eller restriktioner på hvilke apps, der kan installeres på institutionens enheder.

4.1.1.4 Håndtering af data er sjældent et dominerende hensyn for undervisere

Det varierer i høj grad, hvordan undervisere tænker om datasikkerhed. Det kvalitative materiale peger på, at vægtningen af datasikkerhed kan være bestemt af underviserens private holdninger. En undervise fortalte, at kollegaer, der ikke lægger ting på sociale medier privat, vil heller ikke tilskynde elever til det i undervisningen.

Relativt få har overvejet at delagtiggøre eleverne i risici ved handlinger, hvor data om eleverne deles. Det er således kun 9 pct. af underviserne, der har vist eleverne, hvad et givet produkts brugerbetingelser går ud på, selvom 67 pct. af eleverne i undersøgelsen angiver, at de i undervisningen har oprettet en profil, hvor de afgiver e-mail eller navn i forbindelse med profiloprettelse på en hjemmeside. **Samtidig varierer det, hvornår underviserne skønner, at det ligger inden for institutionens opgave at tage sikkerhedsmæssige forholdsregler.** Der er forskellige variable, der er med til at forme holdningen. I det kvalitative materiale har det fx betydning, på hvis initiativ brugen finder sted, hvad formålet er (fx undervisning overfor frikvarter), hvilken enhed (fx privat overfor institutionens) der bruges eller hvilket netværk det foregår på (fx institutionens eller privat netværksdækning). Andre angiver, at de fravælger digitale produkter, fordi de ikke vil eksponere eleverne for reklamer.

Overordnet er billedet dog, at datasikkerhed sjældent spiller en rolle i undervisernes overvejelser ift. brugen af digitale produkter. I den udstrækning det gør, er normen ofte at pædagogiske eller bekvemmelighedshensyn vejer tungest i sidste ende.

[8] Jf. begrebsafklaringen i kapitel 3, er 'selvejende institutioner' erhvervsskoler, gymnasier og frie grundskoler.

4.1.1.5 Eleverne har høj tillid til institutionernes datasikkerhed

De fleste elever har relativt stor tiltro til, at institutionen håndterer og opbevarer deres persondata sikkert, men omvendt mindre tiltro til, at institutionen vælger de mest sikre it-programmer og digitale produkter. Undersøgelsen viser, at eleverne overordnet set har tillid til, at deres institution og undervisere håndterer deres data sikkert. Tilliden er højest, når det gælder spørgsmålet om, hvorvidt institutionerne opbevarer elevernes prøveresultater og karakterer samt personlige oplysninger sikkert (72 pct.). Omvendt er tilliden mindst, når det gælder spørgsmålet om, hvorvidt eleven oplever, at institutionerne vælger de mest sikre it-programmer (55 pct.).

4.1.1.6 Eleverne mest bekymrede for deling af data om deres adfærd og humør

Eleverne bryder sig ikke om, at der bliver indsamlet "usynlig" data om dem gennem diverse applikationer – særligt ikke, hvis de bliver brugt til at vurdere humør eller adfærd. Undersøgelsen viser, at det i høj grad er den "usynlige" datadeling, der spiller en vigtig rolle for eleverne. 77 pct. af eleverne er helt eller delvist enige i, at det er vigtigt for dem, at hjemmesider der anvendes i undervisning ikke deler oplysninger, som de afgiver. Det er særligt risikoen for, at data kan bruges til at vurdere elevens humør/psykiske tilstand.

Der er en svag, men signifikant, sammenhæng mellem elevernes viden om datasikkerhed og bekymringsgrad. Undersøgelsen viser, at elever med størst viden om datasikkerhed generelt set også er mest bekymrede mht. deling af deres digitale data via digitale produkter (apps og hjemmesider). Ligeledes indikerer undersøgelsen, at de elever, der ved relativt lidt om datasikkerhed kun skal højne deres vidensniveau relativt lidt for at blive bekymrede i samme grad, som dem der ved meget om datasikkerhed.

4.1.1.7 Usynlig datatrafik og risici ved digitale produkter

Når det er uvant for underviserne at tænke i datasikkerhed ved nogle typer af digitale produkter hænger det sammen med, at måden produkterne deler data på, ofte er uigennemskuelig. Inspireret af aktuel forskning i datatrafik og deling gennem apps og hjemmesider, er de mest udbredte produkter blevet testet ift. datadeling. **Konklusionen er, at de mest udbredte digitale produkter ofte deler typer af data, som undervisere og elever ikke er klar over. Det er især fordi data ikke er direkte forbundet med noget, undervisere eller elever selv producerer** (modsat filer man gemmer i en cloud eller en besked man skriver på en læringsplatform). Det er fx oplysninger om geografisk placering, ip-adresse eller enheden (fx tablettens) tekniske opsætning. Denne 'usynlige' datadeling finder ofte sted gennem øvrige produkter, der er udenlandske og gratis.

4.1.2 Personalegruppernes håndtering af persondata

4.1.2.1 Databeskyttelsesloven er en god anledning til at rydde op – men volder også ledelserne problemer

Databeskyttelsesloven er for ca. halvdelen af lederne en god anledning og et ledelsesværktøj til at øge sikkerhedsdagsordenen. Lederne beskriver deres modtagelse af databeskyttelsesloven som et pres, men et pres som i manges øjne har været nødvendigt. Til dette viser spørgeskemaundersøgelsen, at mere end 6 ud af 10 ledere på selvejende institutioner samt 5 ud af 10 folkeskoleledere er enige i, at databeskyttelsesloven har givet anledning til at kvalificere institutionernes brug af digitale produkter.

Implementering er udfordret af uklare og manglende retningslinjer omkring, hvad man skal, bør og kan. En overordnet pointe fra dataindsamlingen er, at der stadig er flere elementer, som institutionerne oplever som uklare. Det er ikke alle ledere, der synes, at rammerne for fortolkning er sat tydelige nok op af de relevante myndigheder. Denne uklarhed kan føre til overimplementering, en bekymring som halvdelen af lederne for de selvejende institutioner er enige i, de har, og over halvdelen af folkeskolelederen mener, der er fare for.

4.1.2.2 Forskellige strategier – dog med et gennemgående fokus på administration

Der arbejdes i et vist omfang med intern kompetenceoprustning og inddragelse af eksterne input. Institutionerne har både brugt interne ressourcer (fx arbejdsgruppe og opgavefordelinger) og indgået i samarbejder og fællesskaber på tværs af institutioner samt tilkøbt konsulenthjælp udefra. Der er en tendens til, at særligt de selvejende institutioner søger viden udenfor organisationen. Over halvdelen af de selvejende institutioner deltager i it-fællesskaber og foreninger. 45 pct. tilkøber konsulenthjælp udefra.

Ledelsen fokuserer indledningsvist mere på at sikre administrative arbejdsgange end arbejdsgange knyttet til undervisning. Undersøgelsen viser, at der er blevet gjort en del forskellige tiltag fra ledelsens side mht. håndteringen af elevernes persondata. Der har været særligt fokus på de administrative arbejdsgange og i mindre grad arbejdsgange knyttet til undervisningen og brugen af digitale produkter i undervisningen. På tværs af institutionstyperne er der dog forskel på, i hvilket omfang arbejdsgange i det hele taget er blevet gennemgået. 73 pct. af lederne på de selvejende institutioner svarer således i spørgeskemaundersøgelsen, at de har lavet systematiske beskrivelser og risikovurderinger af administrationens håndtering af forskellige datatyper, mens det samme kun gør sig gældende for 47 pct. af folkeskolelederne.

4.1.2.3 For administrationen er udfordringerne af praktisk karakter

Undersøgelsen viser, at de fleste administrative medarbejdere ikke oplever, at det aktuelle fokus på datasikkerhed har medført radikale ændringer i deres kerneopgave. Primært fordi de traditionelt set har haft for vane at tænke i sikker håndtering af data. Nogle angiver endda, at nye procedurer har haft en optimerende effekt på deres kerneopgave, idet 58 pct. af de administrative medarbejdere er helt enige eller enige i at have fået et bedre overblik over de elevdata, som de sidder med, og 51 pct. er helt enige eller enige i, at de har fået større ansvarsfølelse. Der er tilbøjelighed til, at **administrative medarbejdere oplever hensigten med databeskyttelsesloven som meningsfuld.**

Udfordringerne for det administrative personales (sikre) håndtering af data knytter sig primært til praktiske og ressourcemæssige forhold. 55 pct. af det administrative personale svarer, at de er helt enige eller enige i, at tiltagene også har besværliggjort deres arbejde. Udfordringen knytter sig dog først og fremmest til praktiske eller ressourcemæssige forhold (fx at det kan tage ekstra tid at sende noget via e-Boks, eller at der på tværs af institutioner anvendes forskellige it-løsninger, der ikke kan kommunikere sammen). De administrative medarbejdere er således ikke i tvivl om, hvad persondata er eller, at persondatadata skal håndteres korrekt og sikkert. De udfordringer, de oplever knytter sig i stedet til spørgsmålet om, *hvordan* de skal gøre det.

4.1.2.4 Administrative udfordringer på tværs: Sikker post, elevbilleder og systemsikring

En central udfordring er sikker kommunikation med eksterne aktører

En central udfordring for det administrative personale er kommunikation med eksterne aktører (andre myndigheder, institutioner, praktiksteder, forældre o.l.). Problemstillingen handler om, at institutionerne langt hen ad vejen er i stand til at sikre sig sine egne interne kommunikationsløsninger, men at sikkerheden i mange tilfælde også er afhængig af, at de eksterne parter, som man udveksler data med, vælger tilsvarende løsninger. Blandt det adspurgte administrative personale svarer 62 pct. af dem, det er relevant for, at de er helt enige eller enige i, at det i deres daglige arbejde er udfordrende at dele elevdata med andre institutioner eller myndigheder.

En anden udfordring er, at procedurer for behandling af elevbilleder og samtykke er uklare
Undersøgelsen viser, at administration på de fleste institutioner er blevet opmærksomme på, at billedmateriale af eleverne kan udgøre en datasikkerhedsmæssig udfordring. Derfor er der flere steder indført nye rutiner og procedurer for, hvordan denne type elevdata håndteres teknisk og praktisk.

Men institutionernes sikkerhedsstrategier i den henseende er forskelligartede, hvilket formentlig kan forklares med, at de ikke oplever, at der findes tilstrækkeligt klare kriterier for, hvornår et billede må bruges til hvad (bl.a. peges der på en vanskelig gråzone mellem definitionerne af hhv. portræt- og situationsbilleder som en årsag hertil). 32 pct. af det administrative personale svarer således, at de er helt enige eller enige i, at de mangler juridisk viden om de betingelser, hvorunder man skal håndtere elevbilleder.

Administrationen angiver stærkt behov for at der træffes afgørelser om sikkerhedsniveauet på de systemer, som de har brugt tid og penge på at flytte alle deres kommunikationsaktiviteter over på
En overordnet udfordring som synes at være gennemgående ift. at øge datasikkerheden på institutionerne, handler om, at institutionerne i de senere år har flyttet en lang række af deres aktiviteter over på få, samlende platforme og datasdelingsløsninger. Dette gør institutionerne sårbare, såfremt disse løsninger ikke imødekommer de nye sikkerhedskrav, jf. databeskyttelsesloven. Der er blevet investeret tid og ressourcer i licensaftaler, implementering og kompetenceoprustning i disse løsninger, og det ville være en besværlig og dyr proces at finde nye alternativer.

4.1.2.5 Datasikkerhed er et nyt og uvant hensyn for underviserne

Underviserne oplever ikke i samme omfang som administrationen hensigten med databeskyttelsesloven som meningsfuld. Mange undervisere har været igennem en proces (eller er ved at tage tilløb dertil), der har til formål at rydde op i undervisningsrelateret elevdata – fx makulere dokumenter eller slette gamle opgaver. I de kvalitative interview kommer det også til udtryk, at der – sammenlignet med det administrative personale – er tale om en anden fagkultur. Undervisernes kernefokus er ikke på registrering og arkivering, men på undervisning, læring og udvikling. Så hvor det administrative personales udfordringer primært knytter sig til spørgsmålet om, *hvordan* de skal håndtere elevernes persondata korrekt, spørger det pædagogiske personale i højere grad, *hvorfor* de skal bruge ekstra tid på udvalgte elementer.

Underviserne oplever en risiko for overimplementering, når sikkerhedskrav møder deres pædagogiske praksis. Undersøgelsen viser, at det i flere tilfælde opleves som uklart, hvilke typer af *faglige data* (opgaver o.l.), underviserne skal håndtere med blik for databeskyttelsesloven. 39 pct. af de adspurgte undervisere svarer i spørgeskemaundersøgelsen, at der på deres institution er procedurer for, hvordan elevernes faglige produktioner skal opbevares. Dette indikerer, at der på den ene side, i

et vist omfang, er fokus på, at også denne type elevoplysninger kan være relevant "data" iht. databeskyttelsesloven.

På den anden side viser undersøgelsen også, at der blandt underviserne ikke nødvendigvis er et ønske om et større ledelsesfokus, da man frygter en standardisering, der ikke tager højde for deres pædagogiske hensyn. Blandt de 61 pct. af underviserne, der har angivet, at der ikke er procedurer på deres institutioner for opbevaringen af faglige produkter, er det fx kun 25 pct., der kunne tænke sig at institutionen indførte sådanne procedurer.

5. OPBYGNING

Rapporten er bygget op efter følgende struktur. I afsnittet **Ledelsens modtagelse af databeskyttelsesloven** sættes der overordnet fokus på den organisatoriske kontekst. Der redegøres for de tiltag som institutioner og kommuner tager med henblik på at øge sikkerheden omkring elevernes persondata.

Dernæst følger kapitlet **Digitale produkter i undervisningen** – med særligt fokus på hvor meget, hvorfor og hvordan grundskoler, erhvervsskoler og gymnasier, inddrager digitale produkter i undervisningen. Herunder hvilke udfordringer de har med at skabe sikker brug igennem regler, videndeling, databehandleraftaler og it-løsninger.

Derefter følger et mere dybdegående indblik i en række specifikke arbejdsgange, og hvordan den nuværende praksis fører udfordringer med sig, i kapitlet **Institutionernes håndtering af elevernes data.** Herunder opdelt med særligt fokus på hhv. de administrative arbejdsgange og udfordringer og pædagogiske arbejdsgange og udfordringer.

For at kunne svare på flere af undersøgelsesspørgsmålene, og generelt forinden kontekstualisere og efterfølgende perspektivere undersøgelsens fund, har der været foretaget en omfattende desk research. Opsummeringer heraf vil være at finde som selvstændige kapitler afslutningsvist. Et af desk researchens kapitler handler om **datatrafik og digitale produkter**, hvor projektteamet har gennemgået de 50 mest benyttede digitale produkter for at undersøge hvilke data de deler og med hvem, samt gennemgået forskningslitteratur om, hvad digitale produkter deler af data. Det sidste kapitel er en **sammenligning af internationale styringsstrukture**r i hhv. Holland, Norge, Sverige, USA og Danmark. Her undersøges hvordan myndigheder, foreninger og private aktører i forskellige lande, ud fra forskellige værdier og gennem forskellige typer af initiativer, har været med til at præge sikker datahåndtering i skolesystemerne.

6. LEDELSENS MODTAGELSE AF DATABESKYTTELSESLOVEN

6.1 INDLEDNING

I dette kapitel beskrives institutionsledelsernes opfattelse af databeskyttelsesloven og de nye sikkerhedskrav, samt hvilke tiltag de har indført som reaktion herpå. Det er tiltag med fokus på nye retningslinjer, vidensdeling og teknisk oprustning.

Besøg på caseinstitutionerne har vist, **at der er blevet gjort en del forskellige tiltag fra ledelsernes side**, særligt med fokus på det administrative arbejde og de administrative arbejdsgange. Ledelserne har særligt haft fokus på opbevaring og sletning af digitale elevdata, men også sikkerheden vedrørende deling af elevdata i de administrative arbejdsopgaver nævnes af størstedelen som et stort fokus. Til dette er særligt brugen af sikker og krypteret mail et centralt fokusområde. Blandt det administrative personale svarer 89 pct.[9], at de i løbet af det seneste år eller tidligere har øget deres brug af sikker eller krypteret mail, mens kun 2 pct[10]. svarer, at det ikke er sket eller planlagt.

Derudover er indtrykket fra casebesøgene, at ledelserne oplever, at databeskyttelsesloven har lagt et pres på dem, men et pres som i ledelsens øjne flere steder var nødvendigt.

It-ansvarlig leder, erhvervsskole: Det koster jo, der er nogle administrative arbejdsgange, som kan blive mere administrativt tunge. Men nej ikke flere end dem. Vil egentlig sige, det har været en kærkommen måde at få ryddet op på. Det er blevet mere legalt nu, at snakke sikkerhed. For det har altid været udfordrende at tale om det. For IT-afdelingens vedkommende er det blevet meget mere legalt. Det har tidligere været vanskeligt at trænge igennem overfor ledelse og personale. Derfor er det faktisk en gave for os, det en god mulighed for os at få løftet det. God anledning til at få ryddet op. For det er altså nødvendigt.

Ovenstående citat er et eksempel på, at it-afdelingerne kan bruge databeskyttelsesloven som en udefrakommende anledning til at minde medarbejderne om, at det er vigtigt, at de retningslinjer, der er blevet udstukket for håndtering af data, bliver overholdt. Det bliver også mere legalt for lederne eksempelvis at eksplicitere overfor medarbejderne, at de ikke kan have fraværsnotater mv. liggende fremme**. Flere af ledelserne på caseinstitutionerne ser databeskyttelsesloven som en kærkommen lejlighed til at få både ryddet og strammet op i sikkerhedsstrategier**, og loven kan fungere som et overbevisende redskab hertil.

Udover denne modtagelse af databeskyttelsesloven, viser spørgeskemaundersøgelsen, at mere end 6 ud af 10 ledere på selvejende institutioner samt 5 ud af 10 folkeskoleledere er enige i, at databeskyttelsesloven har givet en kærkommen anledning til at kvalificere institutionernes brug af digitale produkter. Flere skoleledere bemærker, at de kan bruge databeskyttelsesloven aktivt, som et redskab til at kvalificere deres retningslinjer for brug at digitale produkter, samt øge fokus på håndteringen af elevdata.

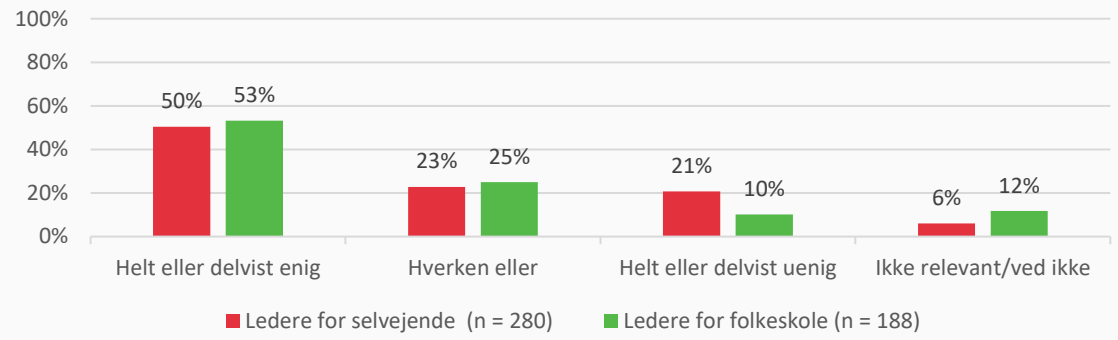
At databeskyttelsesloven af nogle kan bruges aktivt til at skabe fokus, er dog ikke ensbetydende med, at det altid kan bruges til at skabe klare retningslinjer. **En overordnet pointe blandt alle undersøgelsens respondenter er, at der stadig er flere elementer, der er uklare**. Det handler især om,

[9] Spørgsmålsformulering – *"Hvilke af følgende tiltag er blevet taget på din arbejdsplads med henblik på at øge datasikkerheden"*
[10] Spørgsmålsformulering – *"Hvilke af følgende tiltag er blevet taget på din arbejdsplads med henblik på at øge datasikkerheden"*

hvad man præcis skal og ikke skal gøre med persondata, og det er ikke alle ledere, der synes at rammerne for fortolkning, er stillet skarpt nok op af de relevante ministerier og styrelser.

Spørgeskemaundersøgelsen viser hertil, at halvdelen af de selvejende ledere er **enige i, at der er fare for overimplementering** i arbejdet med at sikre elevernes persondata, hvilket over halvdelen af folkeskolelederne ligeledes mener (jf. figur 1).

Figur 1: Hvor enig eller uenig er du i følgende udsagn om jeres arbejde med at sikre elevernes persondata: Der er fare for overimplementering (flere tiltag end nødvendigt for at leve op til loven)



Kilde: Ledere på folkeskoler og selvejende institutioner, n=468.
Note: Kun ledere for selvejende institutioner har haft mulighed for at svare "ikke relevant".

Faren for overimplementering kommer også til udtryk i det kvalitative materiale, hvor flere ledere beskriver det som et opmærksomhedspunkt:

Vicerektor, gymnasium: Jeg er opmærksom på risikoen for over implementering. Fx ift. [læringsplatform], nu har jeg begyndt at indføre et nyt system, og hvis det så viser sig om nogle måneder at der ikke er nogle problemer, så har jeg overimplementeret. Også ift. lærerne er jeg i tvivl ift. udmelding. Jeg havde lige 30 min. Inden ferien med dem. Når en elev går ud, skal opgaver osv. Slettes eller anonymiseres. Praksis har ændret sig, folk har enorme mængder materialer liggende. Men altså der er blevet gjort meget ift. administrationen, og studievejledningen har gjort meget, men ikke så meget med lærerne. De har haft en halv time før sommerferien omkring sletning af gamle ting som fx elevopgaver.

Ledelserne på caseinstitutionerne beskriver, at de på den ene eller den anden måde har forsøgt at kommunikere, hvilke arbejdsgange, der ideelt set bør følges i arbejdet med håndteringen af elevdata. Dette kunne eksempelvis være på personalemøder, via oplysningsplakater eller skriftlige meddelelser.

FAKTABOKS: Hvornår skal opgaver slettes?

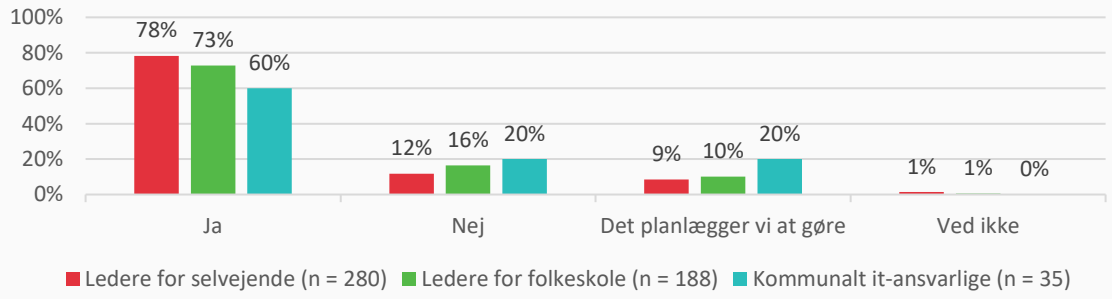
Opgaver skal slettes, når det ikke længere er nødvendigt at opbevare dem. En lærer kan tidsubegrænset gemme en gammel opgave og bruge den som vejledende eksemplar uden samtykke, fordi opbevaringen af den specifikke opgave er en legitim interesse for læreren. Hvis der dog er tale om et essay, hvor eleven eventuelt har beskrevet oplysninger om sig selv, der betragtes som følsomme, skal læreren dog nøjes med at anonymisere opgaverne. Hvis det er en opgave, som i forvejen tydeligt er offentliggjort af eleven selv, har læreren lov til at gemme opgaven uden at anonymisere.

Indtrykket fra de kvalitative interviews understøttes af spørgeskemaundersøgelsen blandt de kommunale it-ansvarlige og lederne på de selvejende institutioner. Heraf fremgår det, at hhv. **60 pct. og 78 pct. af de kommunalt it-ansvarlige og ledere for selvejende institutioner har sendt informationsmateriale ud til underviserne om datasikkerhed**, og at 20 pct. af de kommunale it-ansvarlige planlægger at gøre det (jf. figur 2).

Dilemma:

Institutionsledelserne er i flere henseender usikre på, hvilke regler og retningslinjer, der gør sig gældende omkring sikker håndtering af elevernes persondata. Derfor oplever nogle ledere et dilemma imellem på den ene side at agere således, at man rent juridisk er "på den sikre side" og omvendt at overimplementere i en sådan grad, at det går ud over personalets mulighed for at løse deres egentlige kerneopgaver.

Figur 2: Har I på skolen/gymnasiet udført ét eller flere af følgende tiltag? Uddelt informationsmateriale til lærere om datasikkerhed

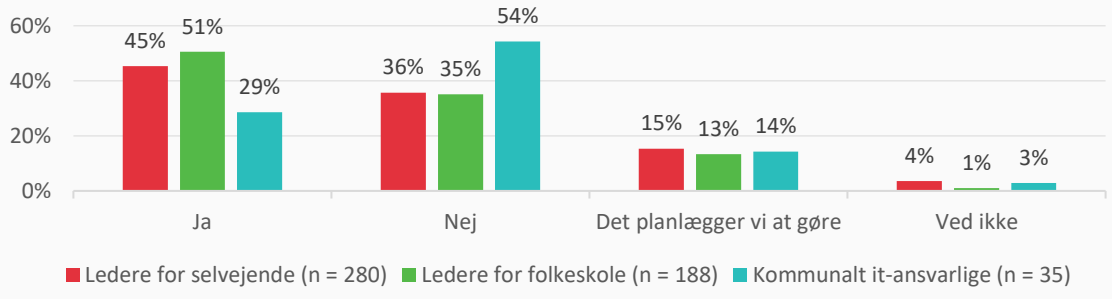


Kilde: Ledere på folkeskoler og selvejende institutioner samt kommunalt it-ansvarlige, n=503.

Note: De kommunalt it-ansvarlige har fået spørgsmålet: Har kommunen udført ét eller flere af følgende tiltag? Uddelt informationsmateriale til lærere om datasikkerhed

Udover at sende information til underviserne har 45 pct. af de selvejende ledere angivet at have haft undervisere på kursus i datasikkerhed, mens 29 pct. blandt de kommunale it-ansvarlige svarer, at skolerne i kommunen har haft underviserne på datasikkerhedskursus:

Figur 3: Har I på skolen/gymnasiet udført ét eller flere af følgende tiltag? Haft lærere på kursus i datasikkerhed



Kilde: Ledere på folkeskoler og selvejende institutioner samt kommunalt it-ansvarlige, n=503.

Note: De kommunalt it-ansvarlige har fået spørgsmålet: Har kommunen udført ét eller flere af følgende tiltag? Haft lærere på kursus i datasikkerhed?

For de frie grundskolers vedkommende, er det kun en femtedel (21 pct.), der har været på kursus. De frie grundskoler har også i mindre grad (24 pct.) tilkøbt konsulentydelser for at imødekomme kravene i databeskyttelsesloven (jf. figur 3).

6.2 AFDÆKNING OG RISIKOANALYSE AF ARBEJDSGANGE

Det kan være vanskeligt for en ledelse og medarbejdere at overskue, hvilke arbejdsgange der rent faktisk berøres af et skærpet fokus på sikkerhed ift. håndteringen af elevdata. Derfor har flere institutioner gennemgået deres arbejdsgange for at identificere eventuelle risici og behov. En GDPR-ansvarlig medarbejder på et erhvervsgymnasium beskriver, hvordan institutionen systematisk har arbejdet netop sådan og på den baggrund formuleret og iværksat handlingsplaner på området:

GDPR-ansvarlig, gymnasium: Vi har lavet en risikovurdering, og vi har lavet handlingsplaner for to områder, hvor vi er i det røde felt. Når vi kommer tilbage fra sommerferien bliver alle præsenteret for, hvad vi arbejder med – vi går 'live' for alle. Samme dag frigiver vi en datasikkerhedshåndbog med spørgsmål og svar, hvor vi kortlægger, hvordan vi håndterer ting her.

På en case-erhvervsskole har man gennemført en tilsvarende arbejdsgangsanalyse, hvor institutionen systematisk har forholdt sig til, hvilke persondata institutionen nødvendigvis må håndtere for at kunne gennemføre sagsbehandlingen af eleven fra indmelding til udmelding – hvad de kalder "fra vugge til grav". Her har institutionen undersøgt, hvilke data institutionen bruger i de forskellige faser i et typisk elevforløb, og hvem adgang til disse data er relevant for i de forskellige faser:

Datafortegnelse – Pædagogisk administration

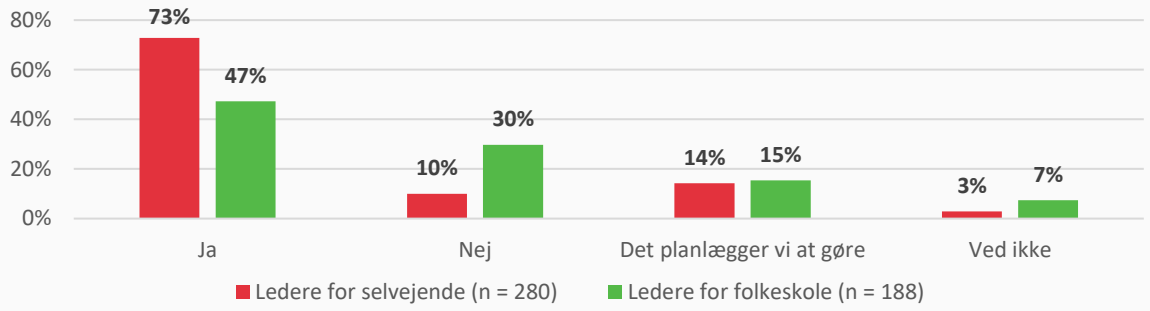
Dataansvarlig	Institutionens navn, cvr.nr. og kontaktoplysninger	[redacted]
	Den fælles dataansvarlige	[redacted]
	Den dataansvarliges repræsentant	[redacted]
Formål	Håndtering af elever, studerende og kursister "fra vugge til grav"	Pædagogisk administration
Kategorier af registrerede	Kategorier af registrerede personer	Elever/studerende/kursister Virksomheder Forældre/værge Alle person- og øvrige data, der er nødvendige for at gennemføre sagsbehandlingen
Kategorier af personoplysninger om disse	Oplysninger, som behandles om de registrerede personer	

	Elever/ studerende	Kursister	Virksomheder	Forældre/ værge
Identifikationsoplysninger	x	x	x	x
Grundskoleadgang	x			
Statsborgerskab	x			
Fravær	x	x		
Sygdom / Barsel	x			
Advarsler	x			

Det er dog ikke alle institutioner, der på denne måde har gennemført systematiske analyser af egne arbejdsgange. **Det er i højere grad de selvejende institutioner, der har foretaget systematiske beskrivelser og risikoanalyser.**

Spørgeskemaundersøgelsen viser, at 73 pct. af lederne på de selvejende institutioner svarer, at de har lavet systematiske beskrivelser og risikovurderinger af administrationens håndtering af forskellige datatyper, mens det samme gør sig gældende for 47 pct. af folkeskolelederne (jf. figur 4).

Figur 4: Har I på skolen udført ét eller flere af følgende tiltag? Lavet systematiske beskrivelser og risikovurderinger af administrationens håndtering af forskellige datatyper (indsamling, opbevaring og deling)



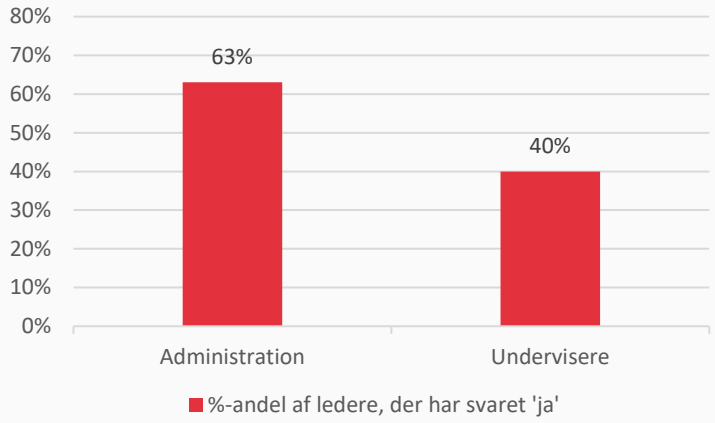
Kilde: Ledere på folkeskoler og selvejende institutioner, n=468.

En del af forklaringen på variationen mellem folkeskoler og selvejende institutioner kan findes i at kommunerne påtager sig ansvaret for opgaver såsom risikovurderinger men "skåner skolerne for information om dette", som det blev udtrykt på workshops afholdt med deltagelse af ansatte fra kommunale forvaltninger.

6.3 LEDELSENS FOKUS PÅ DE ADMINISTRATIVE ARBEJDSGANGE

Det fremgår af spørgeskemaundersøgelsen, at der generelt – både på de selvejende institutioner og på folkeskolerne – er **et større fokus på at lave systematiske beskrivelser og risikovurderinger af det administrative personales arbejdsgange sammenlignet med undervisernes arbejdsgange**. Figur 5 viser, at 40 pct. af lederne på tværs af selvejende institutioner og folkeskoler har lavet systematiske beskrivelser af undervisernes datahåndtering, men også at betragtelig flere (63 pct.), har lavet beskrivelser for administrationens håndtering af forskellige datatyper.

Figur 5: Har I på skolen/gymnasiet udført ét eller flere af følgende tiltag? Lavet systematiske beskrivelser og risikovurderinger af undervisernes/administrationens håndtering af forskellige datatyper (indsamling, opbevaring og deling)



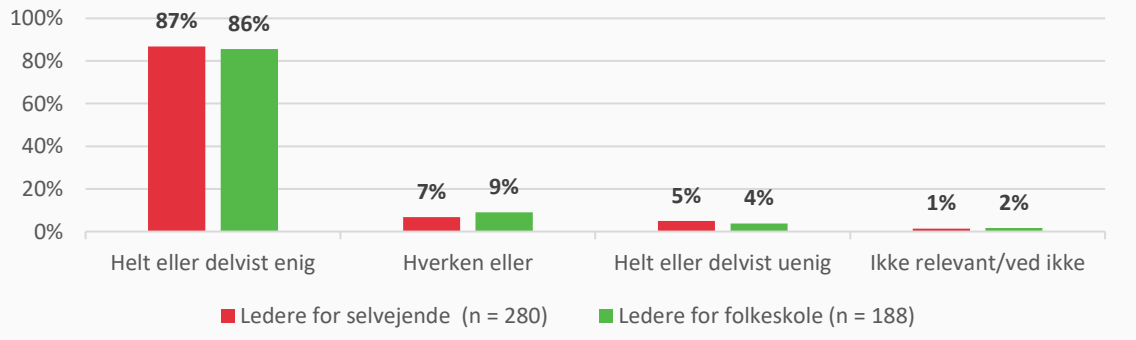
Kilde: Sammenlagt ledere på folkeskoler (n=187) og selvejende institutioner (n=282). N=469.
Note: Procentandelen er en sammenlægning af de ledere på tværs af institutionstyper, der har svaret 'ja' til spørgsmålet i figurtitlen.

Forskellen på det ledelsesmæssige fokus på hhv. administrative arbejdsgange og pædagogiske arbejdsgange understøttes af de kvalitative interviews på caseinstitutionerne. Her er det på flere casebesøg kommet til udtryk, at ledere som det første tænker på de administrative arbejdsgange, når samtalen falder på databeskyttelsesloven og generel datasikkerhed. Arbejdsgange, der knytter sig til undervisning, fx i forbindelse med brug af digitale produkter, er et område, som er i mindre fokus.

6.4 INTERNE ARBEJDSGRUPPER OG EKSTERNE SAMARBEJDER

På de fleste institutioner har lederne adgang til vidanspersoner, der kan afklare de fleste spørgsmål omkring sikring af elevernes persondata. Det gælder på både de selvejende institutioner og på folkeskolerne, hvor figur 6 viser, at hhv. 87 pct. og 86 pct. angiver at have adgang til vidanspersoner:

Figur 6: Hvor enig eller uenig er du i følgende udsagn om jeres arbejde med at sikre elevernes persondata: Vi har adgang til vidanspersoner, der kan afklare de fleste spørgsmål om sikring af elevernes persondata



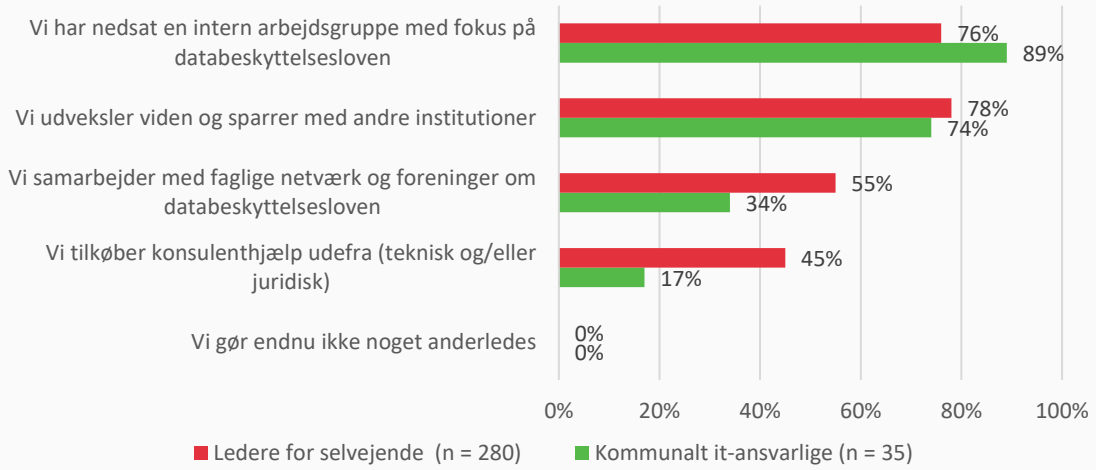
Kilde: Ledere på folkeskoler og selvejende institutioner, n=468.
Note: Kun ledere for selvejende institutioner har haft mulighed for at svare "ikke relevant".

På 76 pct. af de selvejende institutioner og i 89 pct. af de kommunale forvaltninger, er der blevet nedsat interne arbejdsgrupper med fokus på databeskyttelse. Specifikt for de frie grundskoler er

vurderingen noget lavere, i det 71 pct. af ledere på frie grundskoler angiver at have adgang til vidanspersoner.

Udover at trække på interne ressourcer, inddrager institutionerne også eksterne ressourcer. Det sker dels i form af uformel sparring med andre institutioner, dels med mere formaliserede samarbejder i faglige netværk og foreninger eller som tilkøb af specialiseret konsulenthjælp udefra.

Figur 7: Hvordan har I forberedt jer for at leve op til databeskyttelseslovens krav pr. 25. maj 2018 (GDPR)



Kilde: Ledere på selvejende institutioner samt kommunalt it-ansvarlige, n=315.
Note: De kommunalt it-ansvarlige har fået spørgsmålet: "Hvordan har kommunen forberedt sig på at leve op til databeskyttelseslovens (GDPR) krav, der trådte i kraft pr. 25. maj". Lederne på de selvejende institutioner har fået spørgsmålet: "Hvordan har din institution forberedt sig for at leve op til databeskyttelseslovens krav pr. 25. maj 2018 (GDPR)?"

Som det kan ses i figur 7, **er der en tendens til, at særligt de selvejende institutioner søger viden udenfor organisationen**. Over halvdelen af de selvejende institutioner deltager i it-fællesskaber og foreninger, og 45 pct. tilkøber konsulenthjælp udefra. Flere går også sammen om at hyre eller blive tilknyttet en ekstern DPO (Data Protection Officer) ordning:

Administrativt personale, gymnasium: Vi har talt meget om de her procedurer. Vi er en del af gymnasiefællesskabet [it fællesskab], som har en jurist ansat til kun at kigge på GDPR. Vi har deltaget i alt der har været udmeldt. De har gjort rigtig meget og været herude og tale med os om hvilke forretningsgange vi har og hvor vi skal være opmærksomme. Og hvad det er for nogle aftaler som skal på plads. Vi er hjulpet meget via gymnasiefællesskabet. Også hende som er jurist der, der er vores DPO.

Administrationschef, gymnasium: Vi har selv fundet sammen med fire andre skoler, som vi deler DPO med. Når der laves tiltag der, så er det i den kreds som kan mødes i en arbejdsgruppe. Det er en stor fordel, for man har brug for at sparre med nogle andre som står i samme situation. Men ingen af os er jurister jo. Nogle gange føler man, at man famler lidt i blinde.

En forklaring på at de selvejende institutioner i høj grad søger om konsulentbistand eksternt kan være, at man på særligt mindre institutioner, ikke har det juridiske know-how i egen organisation. **I de kommunale forvaltninger vil der givetvis være en større juridisk kapacitet qua deres organisatoriske størrelse.**

Når man som selvejende institution går med i en fælles DPO-ordning med andre institutioner, er det ikke kun for at afklare juridiske spørgsmål. DPO'erne kommer også forbi på institutionerne og gennemgår arbejdsgangene og udstyret på institutionen og medvirker således til at fællesskaberne ensretter arbejdsgangene og giver it-tekniske løsninger på tværs af institutionerne. Denne ensretning gør det lettere for institutionerne indenfor fællesskabet at samarbejde og udveksle data på en sikker måde på tværs af institutioner, fordi institutionerne bruger de samme sikre produkter til eksempelvis mailsystemer og SharePoints.

Nogle caseinstitutioner har startet deres egne fællesskaber op, og andre igen er med i flere. Dertil kommer at institutionernes forskellige fagforbund, samt KL for folkeskolerne, også udbyder materialer og afholder konferencer.

Overordnet set forsøger ledelserne på tværs af caseinstitutionerne at holde sig opdateret på datasikkerhed og fortolkning af databeskyttelsesloven, gennem disse mere eller mindre formaliserede fællesskaber, men som ovenstående administrationschef siger, så føler de også, at de nogle gange famler i blinde.

En anden udfordring som opstår i den forbindelse, er når ledelsen deltager i flere sammenhænge og flere fællesskaber**. For forskellige fællesskaber tolker forskellige ting ud af lovgivningen, hvilket gør lovgivningen mere uigennemsigtig for institutionerne**. Det bliver derfor nogle gange uklart for lederne, hvem de skal lytte til og udarbejde retningslinjer på baggrund af.

Vicerektor, gymnasium: Det er ikke tydeligt for mig 100 pct. hvornår vi overholder lovgivningen, og hvornår vi ikke gør. Vi har databeskyttelsesrådgiver i [it-fællesskab X], men jeg sidder også med i [it-fællesskab Y], hvor der er en anden rådgiver. Og de forskellige databehandlerrådgivere er ikke altid enige. Det gør mig usikker på, hvordan det skal tolkes.

Dilemma:

Der bliver flere steder givet udtryk for en oplevelse af, at den juridiske ramme for håndtering af elevernes persondata er præget af "myter" og tvetydige retningslinjer om, hvordan man skal agere. Selv når institutionerne tyer til professionel rådgivning i fx hos DPO'er i it-fællesskaber, kan de møde modsatrettede tolkninger. I den forstand oplever nogle institutionsledere således rent juridiske dilemmaer i arbejdet med elevernes persondata.

6.5 GRUNDSKOLERNES INDDRAGELSE AF SKOLEBESTYRELSEN

Udover lederne, er også grundskolerne bestyrelser blevet spurgt om deres syn på datasikkerhed som hensyn. Besvarelserne fra skolebestyrelsesformænd viser, at omkring en tredjedel af de adspurgte skolebestyrelsesformænd svarer, at de ikke har haft fokus på sikker håndtering af elevdata eller at de ikke har diskuteret datahåndtering i bestyrelsen det seneste år. **Samtidig svarer halvdelen af de skolebestyrelsesformænd, der ikke har diskuteret datahåndtering i bestyrelsen, at procedurer for, hvordan skolen opbevarer personoplysninger, er blandt de tre vigtigste emner som skolen bør prioritere det næste år.** Resultaterne fra undersøgelsen blandt skolebestyrelsesformænd tyder altså på, at der blandt skolebestyrelserne er et stigende fokus på, hvordan skolerne håndterer opbevaring af elevernes personoplysninger.

EPINION

7. DIGITALE PRODUKTER I UNDERVISNINGEN

7.1 INDLEDNING

Digitale produkter er en integreret del af undervisningen på landets skoler og gymnasier. 99 pct. af landets elever på tværs af gymnasier, grundskoler og erhvervsskoler bruger i dag digitale produkter i undervisningssammenhæng[11]. Så meget desto mere er det også vigtigt i en sikkerhedsoptik at forstå, hvilke digitale produkter, der bruges, på hvilke præmisser, af hvem og til hvad i undervisningen.

Det er ikke muligt at få et fuldstændigt overblik over, hvilke digitale produkter der bruges i undervisningen. I denne analyse tages der udgangspunkt i et øjebliksbillede, hvor elever og undervisere har angivet, hvilke digitale produkter de bruger. Dette giver en samlet bruttoliste på 373 produkter[12].

I analysen arbejdes der med begrebet om digitale produkter. Der findes en lang række af betegnelser (fx platforme, læremidler, teknologier, materialer, værktøjer eller ressourcer), der refererer til forskellige pædagogiske og tekniske traditioner og brugsaspekter. I denne analyse bruges begrebet digitale *produkter.* Det er fordi betoningen i analysen ligger på det aspekt af teknologierne, der handler om, at den er udviklet med henblik på at imødekomme en forbrugers (fx institution, elev eller undervisers) behov. **Det, der karakteriserer et produkt er, at det stilles til rådighed for brugeren på baggrund af en udveksling. Det kan fx være af penge eller af data.**

Med betoning af det *digitale* understreges det, at analysen fokuserer på de produkter, som er uhåndgribelige og immaterielle. I praksis er det hjemmesider, software og apps som brugen i undervisningen. Der kigges altså i mindre grad på de fysiske enheder, såsom computere, tablets og telefoner. Der kigges altså i mindre grad på de fysiske enheder, såsom computere, tablets og telefoner.

Kapitlet falder i tre afdelinger. Først afdækkes det, hvilke kategorier af digitale produkter der aktuelt bruges af elever og undervisere i undervisningssammenhænge. Det analyseres, hvor mange af disse produkter, der er danske eller udenlandske og er gratis eller betalte.

Derpå gives et overblik over brugsfrekvens, hvad produkterne bidrager med til undervisningen og på hvis initiativ, de bruges.

Herefter gives der et overblik over holdninger og tillid blandt undervisere og elever til de forskellige produktkategorier, og en oversigt over hvilke aktuelle sikkerhedsmæssige tiltag, der tages på institutionerne i forhold til at håndtere de digitale produkters sikkerhed. De igangsatte initiativer sammenholdes med en undersøgelse af, hvilke datakilder forskellige produktkategorier tilgår, og hvor mange eksterne parter, de deler data med.

---

[11] Spørgsmål – *"Hvilke af følgende danske forlagsprodukter har du brugt i forbindelse med undervisning eller hjemmearbejde? Jeg har ikke brugt nogle produkter … i undervisningen"*

[12] På en workshop afholdt i forbindelse med undersøgelsen gjorde en it-vejleder opmærksom på, at han på sin skole havde registreret over 600 forskellige apps installeret på skolens tablets. Dette vidner om, at der florerer en betragtelig større mængde digitale produkter, og at det ikke lade sig gøre at danne et fuldstændigt overblik.

7.2 KATEGORISERING AF PRODUKTER

I analysen arbejdes der med forskellige produktinddelinger. Det drejer sig om danske og udenlandske produkter, licensform og kategorier. De udsendte spørgeskemaer har også taget afsæt i disse produktinddelinger. Tidligere kategoriseringer af digitale produkter i undervisning har ofte taget udgangspunkt i brugsformål[13] i den pædagogiske kontekst, forstået på den måde, at det afgøres af brugskonteksten, om fx en online tekst editor er et kreativt samarbejdsredskab eller et testværktøj.

En stor del af de konkrete produkter er karakteriseret ved at være multifunktionelle på denne måde, og en kategorisering efter brugsformål er derfor vurderet som uhensigtsmæssig, da undervisere og elever vil betragte samme produkt som tilhørende forskellige kategorier, afhængigt af, hvordan de bruger det. For at undgå mest mulig overlap kategorierne i mellem, har vi **udviklet en produktinddeling på baggrund af de kvalitative casebesøg, som er inddelinger som undervisere og ledere på tværs af institutionstyper har kunnet se deres egen praksis i relation til**.

Derudover er kategorierne informeret af, at de hver især har deres egne datasikkerhedsmæssige udfordringer, som ligeledes er blevet anskueliggjort gennem de kvalitative casebesøg og via eksisterende forskning. Med henblik på at reducere antallet af kategorier, som undervisere og elever har skullet forholde sig til i spørgeskemaerne, er vi landet på følgende fem kategorier:

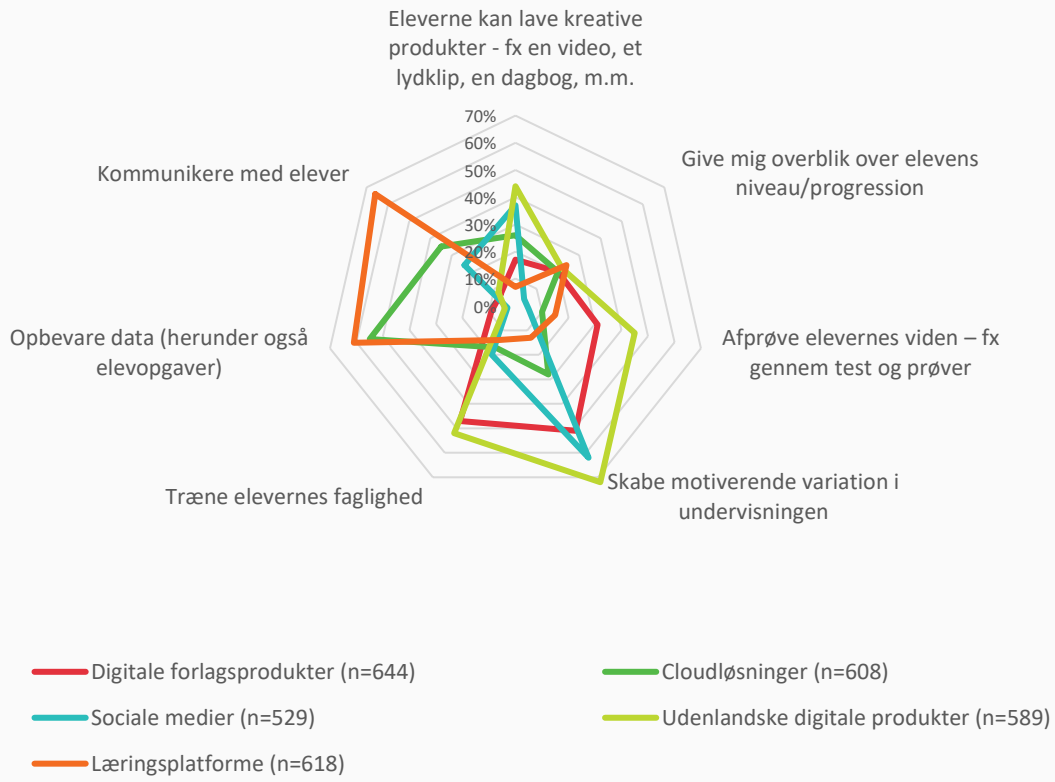
1. **Digitale forlagsprodukter**
   Platforme og læremidler med digitalt tilrettelagt undervisningsindhold og som oftest er danske og koster penge. Sikkerhedsmæssigt er disse produkter karakteriseret ved at udbyderne er proaktive i forhold til indgåelse af databehandleraftaler.
2. **Sociale medier**
   Større platforme med det formål at forbinde folk, facilitere kommunikation og markedsføring. Sikkerhedsmæssigt karakteriseret ved lav tillid og udfordringer med at vurdere sikkerheden og udfordringer med indgåelse af databehandleraftaler. De er oftest udenlandske og gratis.
3. **Cloud- og dataopbevaring**[14]
   Løsninger, der gør det muligt at dele, uploade og downloade filer. Sikkerhedsmæssigt karakteriseret ved, at institutionerne ofte har retningslinjer for, hvad de må bruges til og under hvilke betingelser. Disse er både danske og udenlandske og kan både være gratis og betalte.
4. **Øvrige digitale produkter**
   Øvrige apps og produkter, der tilbyder muligheder for fx quiz, træning, spørgeskemaer eller præsentationer m.v. Sikkerhedsmæssige risici er ofte underbelyst, da de typisk benyttes på undervisere og elevers eget initiativ og ikke vurderes ud fra sikkerhedshensyn. Disse er overvejende udenlandske og gratis.
5. **Læringsplatforme**
   Produkter der er tiltænkt tilrettelæggelse af undervisningsforløb. Ofte omfattet af databehandleraftaler og reguleret/indkøbt på institutionelt niveau. Disse er oftest danske og betalte. Af respondentgrupperne er det kun underviserne, der er blevet spurgt ind til læringsplatforme som særskilt kategori.

[13] Fx https://www.emu.dk/sites/default/files/Helle%20Mathiassen%20-%20slides.pdf og Personal Learning Environments.
[14] I den videre analyse forkortet til cloudløsning.

7.3 PRODUKTER TIL FORSKELLIGE FORMÅL

Underviserne tager ofte forskellige produktkategorier i brug, fordi de tjener forskellige formål i forhold til at få undervisningen til at hænge sammen. Figur 8 viser, at digitale forlagsprodukter bruges især med henblik på at skabe motiverende variation i undervisningen (51 pct.) og træne faglighed-den (47 pct.). Det samme mønster ses for de udenlandske digitale produkter, som dog desuden karakteriseres ved især at bruges til at afprøve elevernes viden (52 pct.) og til at eleverne kan lave kreative produkter (44 pct.). Dette står i kontrast til læringsplatforme og cloudløsninger, hvis formål er at opbevare data og kommunikere med eleverne. Slutteligt er der de sociale medier, som især udmærker sig ved at bidrage til motiverende undervisning, men samtidig også er den produkttype, der oftest lader underviserne lave undervisning, hvor eleverne producerer kreative produkter (62 pct. og 37 pct.).

Figur 8: Produkternes primære bidrag til undervisningen



Kilde: Undervisere, n=722.

Note: Underviserne er blevet stillet spørgsmålet: "Hvad er de vigtigste formål de angivne [produktkategori] bidrager med til din undervisning? (Prioritér op til 5)". Figuren angiver andelen af lærere, som har angivet, at de respektive produktkategorier bidrager til de forskellige aspekter af undervisningen. Hvert produkt er angivet ved en streg. Jo længere stregen er mod midten, desto færre undervisere angiver, at produktet bidrager til den angivne bidragskategori.

Sammenhængen mellem de digitale produkter og kreativitet i undervisningen betoner også formand i Danmarks it-vejleder, John Klesner, der samtidig kæder en begrænsning i brugen af disse sammen med usikkerhed omkring, hvordan sikkerheden vurderes.

John Klesner, Danmarks it-vejlederforening: Det [databeskyttelseslovens implementering i hverdagen] vil nok lægge begrænsninger på noget kreativ aktivitet i den pædagogiske sammenhæng, fordi både lærere og elever er bange for at lave noget, der ikke er helt legalt. Det skyldes jo usikkerhed i den her sammenhæng. Det er rigtig, rigtig vigtigt at vi får klædt ledelse og personale på til at tage de nødvendige skridt hver dag.

De forskellige brugsformål og bidrag til undervisningen siger også noget om, hvilke datatyper det er særlig relevant at fokusere på ift. de forskellige produkter. Digitale forlagsprodukter har fx især med data om fagligt niveau at gøre, mens læringsplatforme indeholder personlig kommunikation. De sociale medier og øvrige produkter vedrører især datatyper, hvor eleven udtrykker sig selv – fx video og billeder.

Lærer, gymnasium: Jeg bruger [socialt medie] til alt muligt. Til taleøvelser, skriveøvelser, refleksionsøvelser. Småopgaver. For at løfte det lidt, så de ikke bare sidder med pen og papir. På [sociale medie] får man også hørt nogle af de lidt mere stille elever.

Dette resonerer med den gennemførte desk research af digitale produkter, der viser, at de øvrige digitale produkter i appformat er dem, der hyppigst forespørger om adgang til datakilder på enheden (telefon eller tablet) såsom kamera og "skrive til hukommelsen" (dvs. mulighed for at tilgå og redigere indhold på enheden). Desuden vedrører øvrige produkter også personoplysninger i form af test og resultater, idet de oftest bruges til at afprøve elevernes niveau.

Når de forskellige produktkategorier bruges til forskellige formål i undervisningen, betyder det også at de producerer og håndterer forskellige typer af data. Kreative elevproduktioner tyder fx på video- og billeder, mens træning af faglighed peger på datatyper såsom test- og præstationsresultater.

7.4 EN UNDERSKOV AF ØVRIGE PRODUKTER

Igennem spørgeskemaerne er undervisere og elever for hver produktkategori blevet spurgt, om de har brugt de forskellige produktkategorier i forbindelse med undervisning eller hjemmearbejde[15]. Den totale bruttoliste er på 373 produkter på tværs af kategorier og svar fra undervisere og elever.

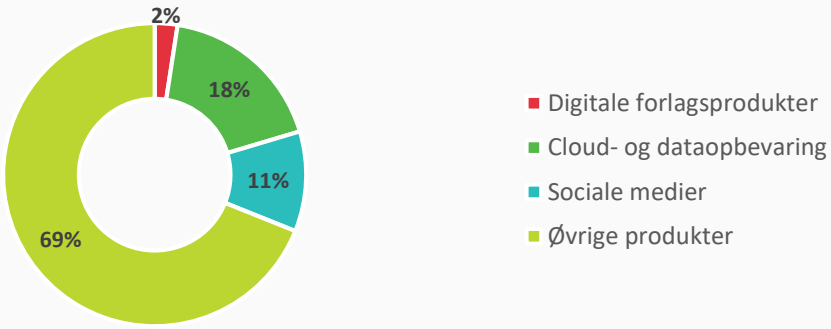
I figur 10 fremgår det, hvor stor en andel af de 373 produkter, som falder ind under de fem kategorier. **Som det ses, er andelen af digitale forlagsmaterialer relativ lille, når den sammenholdes med brug af cloudløsninger og sociale medier.**

Endeligt er der kategorien øvrige, som tegner sig for langt størstedelen ift. diversitet i produkter brugt af undervisere og elever i undervisningen. En del af forklaringen er, at kategorien er bredt defineret, men samtidig er det samlende for disse, at der er distinkte formål, de tjener i undervisningen

[15] Eksempel på formulering fra elevsurvey: *" Hvilke af følgende danske forlagsprodukter har du brugt i forbindelse med undervisning eller hjemmearbejde? Sæt kun kryds ved de produkter, du har brugt i forbindelse med undervisning eller hjemmearbejde."*

jf. ovenstående. Som det fremgår af næste afsnit, er det endvidere et samlende karaktertræk for disse, at de ofte er gratis og udenlandske.

Figur 10: Fordeling af produkter i de fire produktkategorier



Note: Fordelingen er lavet på baggrund af de kategorier, elever og lærere selv har angivet, de mener de pågældende konkrete produkter tilhører.

7.5 FLEST GRATIS OG UDENLANDSKE DIGITALE PRODUKTER

På tværs af produktkategorierne figurerer både danske og udenlandske produkter, samt betalings- og gratisprodukter. For at afdække dette aspekt, er undervisere blevet spurgt ind til, under hvilke licensbetingelser, de bruger de forskellige produkter, hvorefter produkterne er blevet kodet som enten udenlandske eller danske[16]. Produkterne fordeler sig således, at 68 pct. af produkterne bruges fortrinsvist under en gratislicens, mens 32 pct. fortrinsvist bruges under en betalingslicens. Samtidig er 57 pct. af de disse udenlandske, mens 43 pct. er danske.

Samlet tegner der sig et billede af, at størstedelen af de digitale produkter anvendt på gymnasier, erhvervsskoler og grundskoler er udenlandske og gratis (42 pct.). I den anden ende af spektret tegner antallet af produkter, der er udenlandske og betalingsprodukter sig for den mindste andel.

Tabel 4: Fordeling af øvrige digitale produkter efter oprindelsesland og primær licenstype

	Udenlandsk	Dansk
Gratis	42 %	26 %
Betaling	15 %	17 %

Kilde: Lærere, n=722

Note: Dertil er 1 pct. af de danske og 1 pct. af de udenlandske produkter angivet som brugt i en udgave, der både rummer en betalings- og gratislicens.

Sammenholdes licens- og oprindelsesoversigten med de forskellige produktkategorier, **er der et sammenfald mellem sociale medier og øvrige produkter og dem, der er udenlandske og gratis.** I den anden ende af spektret er de digitale forlagsprodukter og læringsplatformene, som oftest er

[16] Oprindelseslandet på de enkelte produkter er afgjort ved opslag i domæneregister (WHOIS) på leverandøren og efterfølgende kvalitetstjekket manuelt.

danske og betalingsprodukter. Midt imellem disse er cloudløsningerne, der fortrinsvist er udenlandske, men både bruges som betalings- og gratisudgaver.

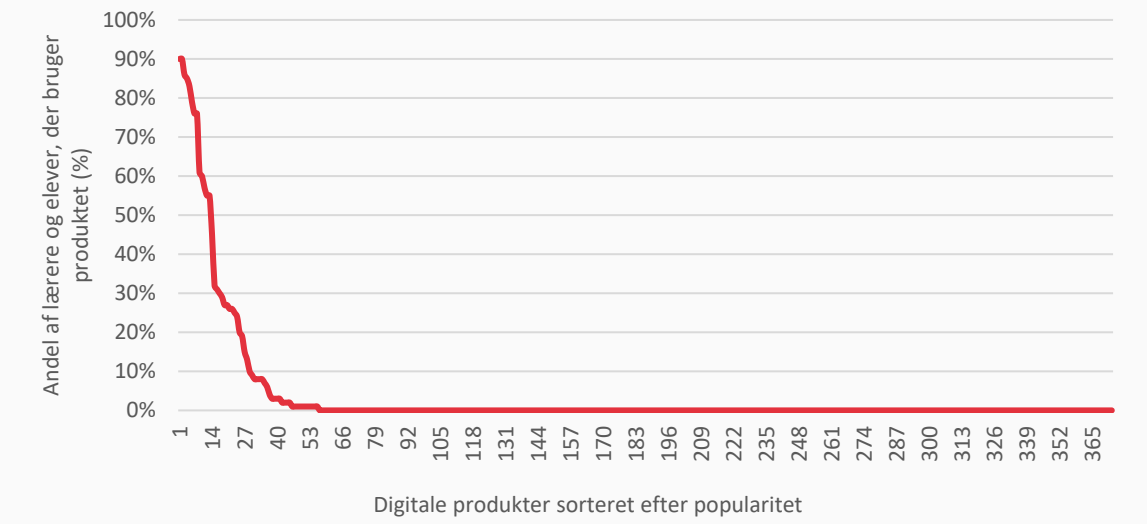
7.6 UDBREDELSE

Ovenstående siger noget om variationen af produkter. Men tallene kan ikke stå alene, da der dermed dels ikke tages højde for, hvor *mange* (elever og undervisere) der bruger dem, og dels hvor *ofte* de bruges. Nedenfor kigger vi derfor på udbredelse og brugsfrekvens.

7.6.1 Få produkter bruges af mange – mange produkter bruges af få

Kigger vi på, hvor mange, der bruger de 373 angivne digitale produkter, ser fordelingen ud som i figur 11:

Figur 11: Andel af elever og lærere, der bruger de 373 angivne digitale produkter



Kilde: Undervisere og elever, n=7.756.

Som det fremgår af figur 11, er de mest udbredte produkter (plads 1-10) brugt af mellem 75-90 pct. af de adspurgte undervisere og elever. Der sker dog et drastisk fald i, hvor udbredte de digitale produkter er, således at det 50'ende mest udbredte produkter kun bliver brugt af 1 pct. af respondenterne. Udfladningen skal forstås på den måde, at der bruges en lang række af forskellige digitale produkter ude på institutionerne, men at mange af disse har relativt få brugere, og for 161 af produkterne er det kun én underviser eller elev, der har angivet, at de bruger dem.

Det kan på den baggrund konkluderes, at **på den ene side er variationen af digitale produkter stor, men at der på den anden side er en stor andel af produkterne, som kun få undervisere eller elever har angivet, at de har brugt i undervisningen.** Samtidig er der en lille gruppe af produkter, som langt størstedelen bruger.

På casebesøg og i interviews med undervisere har forklaringen på dette mønster ofte været, at de fleste undervisere og elever bruger de digitale produkter – fx cloudløsninger eller forlagsplatforme –

der stilles rådighed af institutionen, men derudover supplerer med apps eller hjemmesider, de hører om fra en kollega, eller en elev selv finder:

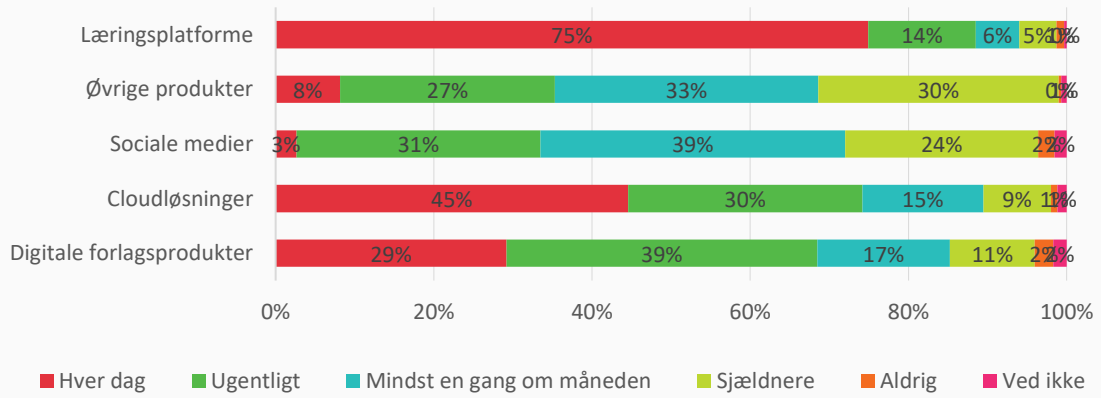
> **Lærer, folkeskole**: Hvis det skal betales for, så kommer det op i budgetmøder. Er det gratis så downloader vi det selv bare. Måske er det de unge, der har erfaringer med det eller også er det noget, kollegaer anbefaler.

Det er altså udbredt praksis, at **størstedelen af underviserne på institutionerne bruger de indkøbte eller institutionsbesluttede produkter, og derudover supplerer med af kollegaer eller elever anbefalede produkter.** Det er sidstnævnte type produkter, der udgør den lange række af produkter, der har få brugere og som oftest er øvrige produkter.

7.6.2 Dagligdags- og lejlighedsvise produkter

Læringsplatforme, cloudløsninger og forlagsprodukter er de kategorier, der oftest bliver anvendt i undervisningen. Over halvdelen af samtlige undervisere bruger disse tre enten dagligt eller ugentligt. **De øvrige produkter og sociale medier bliver kun brugt lejlighedsvist – enten ugentligt eller månedligt (figur 12).**

Figur 12: Underviseres brugsfrekvens af forskellige produktkategorier

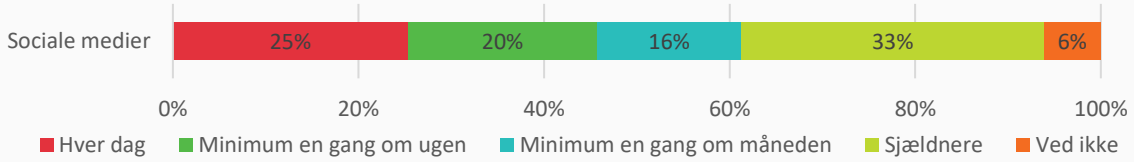


Kilde: Undervisere, n=722.

Note: Underviserne er blevet stillet spørgsmålet: "Hvor ofte har du brugt et eller flere af de valgte [Produkttype] i din undervisning sidste skoleår?"

Undersøgelsen viser også, at selvom underviserne svarer, at de bruger forskellige produkter i varierende grad, kan dette ikke tages som entydigt udtryk for, hvor ofte forskellige digitale produkter bruges i undervisningssammenhænge. **Eleverne angiver, at 45 pct. af dem bruger sociale medier enten dagligt eller ugentligt i forbindelse med undervisning- og skolearbejde. Dette indikerer, at eleverne i et vist omfang selv tager initiativ til at bruge de sociale medier til skolearbejde (figur 13)**.

Figur 13: Elevers brugsfrekvens for sociale medier i undervisning og lektiearbejde

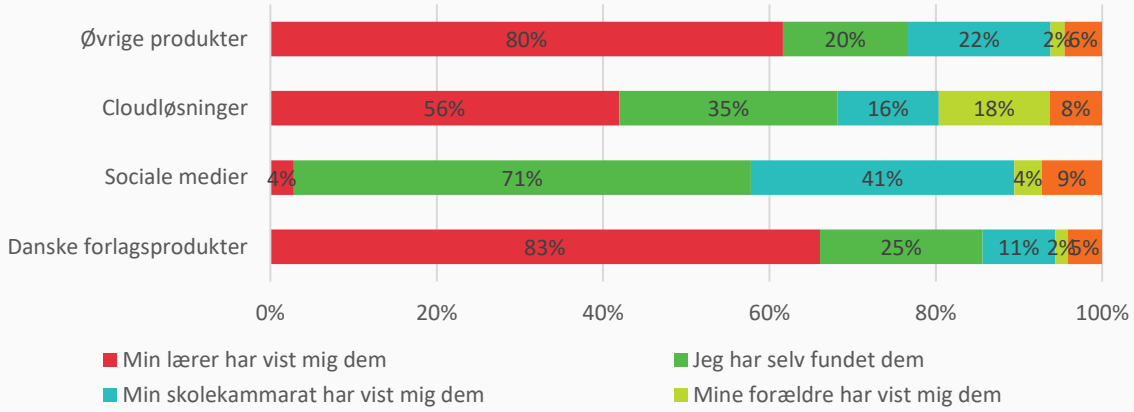


Kilde: Elever, n=7.042.

Note: Hvor ofte har du i løbet af det seneste skoleår, brugt følgende typer af hjemmesider og apps i undervisningen?

I en datasikkerhedsmæssig optik giver det anledning til at rejse spørgsmål ved, hvornår det ligger inden for institutionens opgave at håndtere, hvilke data der deles med eventuelle tredjeparter – såsom sociale medier, når eleverne bruger dem på eget initiativ. Adspurgt om, hvem der har vist eleverne de forskellige kategorier af produkter, fordeler svarene sig som i figur 14:

Figur 14: Hvor kender du de hjemmesider og/eller apps fra, som du har brugt i skolen/gymnasiet eller ved hjemmearbejde?



Kilde: Elever, n=7.042.

Forlagsprodukter og øvrige produkter er oftest introduceret af institutionen gennem underviseren. Det samme gælder cloudløsninger – dog i et mindre omfang (56 pct.). For de sociale mediers vedkommende gælder det til gengæld, at eleverne typisk finder dem selv (71 pct.) eller via klassekammerater (41 pct.), mens underviseren næsten aldrig er den, der viser eleverne sociale medier (4 pct.).

Dilemma:

Digitale produkter anvendes i undervisningen ofte på direkte foranledning af underviseren. Men i andre tilfælde foregår det på initiativ af eleverne selv (fx brugen af sociale medier). Potentielt deler eleverne data om dem selv via disse digitale produkter. Dette rejser et ansvarsmæssigt dilemma om, hvilken rolle uddannelsesinstitutionerne skal spille mht. at fastsætte regler for elevernes brug af digitale produkter i undervisningssituationer – dels når det sker på foranledning af underviserne og dels når det sker på elevernes eget initiativ.

Om brugen af sociale medier i undervisning ift. datasikkerhed nævner John Klesner, formand for Danmarks it-vejlederforening i et telefoninterview, at det er et særligt gråzoneområde:

John Klesner, it-vejlederforeningen: En udfordring har været, at vi har taget SoMe til os og i den sammenhæng har det været et gråzoneområde for mange typer data. Det har været meget uklart, hvorvidt og hvornår der var tale om at praksis var privatsfære og hvornår det var i erhvervssfæren. Man delte bare data.

7.7 TILLID OG KOMPETENCER TIL VURDERING AF DATASIKKERHED

Det er forskelligt, hvor mange overvejelser, lærere gør sig omkring brugen af digitale produkter i forhold til datasikkerhed. **En gennemgående rød tråd, der har vist sig i fokusgrupperne med lærere er, at det hensyn, der vejer tungest i forhold til at bruge digitale produkter, er de pædagogiske.** En lærer fra mobiletnografien udtrykker dette således:

Lærer, gymnasium: Hvis der sker en ændring, hvor læremidlerne bruger oplysninger fra fx elevernes profil på [socialt medie], ville jeg sandsynligvis søge andre alternativer. Det er dog ikke en ny praksis, da jeg mener, at jeg har et ansvar for, at eleverne ikke skal dele oplysninger med diverse undervisningsrelaterede værktøjer, med mindre det er strengt nødvendigt for at gennemføre undervisningen.

Læreren udtrykker her den dilemmafyldte balance mellem på ene side at sørge for, at eleverne ikke deler unødige eller private oplysninger gennem undervisningen, og på den anden side foretage de nødvendige valg for at gennemføre og tilrettelægge den bedst mulige undervisning. Samtidig udtrykker lærerne også et generelt behov for at kunne vurdere sikkerheden ved de enkelte produkter. **Kun 6 pct. ser ikke noget behov for at blive klædt på til at vurdere datasikkerheden ved digitale produkter[17].**

Tilsvarende er 69 pct. helt enige eller enige i, at de mangler viden om hvordan de forskellige udbydere af gratis, digitale produkter deler data med tredjeparter. Kun 30 pct. angiver, at de selv har den fornødne viden til at informere eleverne om, hvordan de sikkert bruger internet og apps i undervisningen[18]. **Det er altså en generel udfordring, at på trods af en ansvarsfølelse blandt lærerne, har de sjældent de fornødne kompetencer til også at kunne vurdere eller tage datasikkerhedsmæssige hensyn,** når det kommer til valg og brug af digitale produkter.

Dilemma:

Digitale produkter er ofte et velegnet redskab til at gennemføre undervisning, der er mere interessant og vedkommende for eleverne. Det gælder fx brugen af sociale medier, der kan bidrage til at skabe en ramme for elementer i undervisningen, der foregår, hvor "de unge er". Samtidigt er mange undervisere også klar over, at der ved at anvende disse produkter, potentielt er en datadelingsrisiko. Derved opleves et dilemma mellem pædagogiske hensyn på den ene side og dataetiske og -sikkerhedsmæssige overvejelser på den anden side.

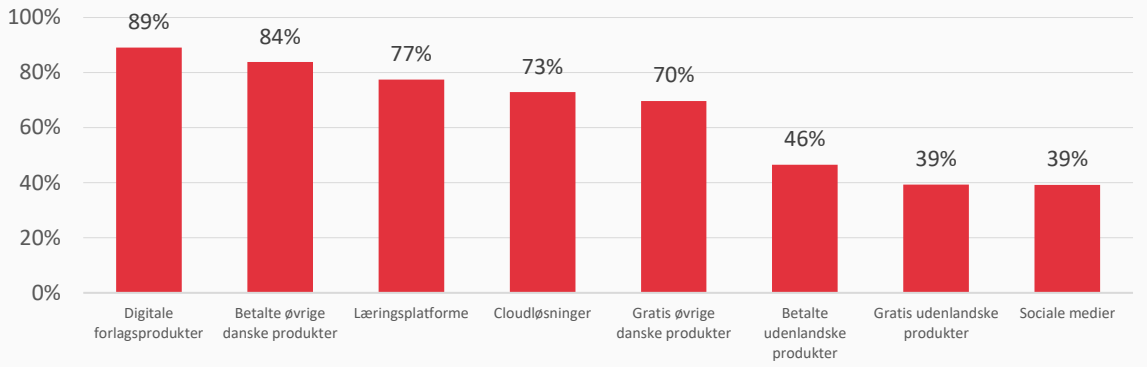
Flere lærere angiver, at deres tillid til, hvorvidt produkterne lever op til lovkrav om datasikkerhed varierer meget på tværs af de forskellige produktkategorier (jf. figur 15). Det mønster, der viser sig er,

[17] Spørgsmålsformulering – *"Har I på skolen foretaget følgende tiltag i forhold til at klæde dig på til at vurdere datasikkerheden ved digitale produkter"*

[18] Spørgsmålsformulering – *"Hvor enig eller uenig er du i følgende udsagn om din skoles arbejde med at skabe digital sikkerhed for eleverne"*

at **tilliden til øvrige produkter og sociale medier er betragtelig lavere end læringsplatforme, forlagsprodukter og cloudløsninger**.

Figur 15: Undervisernes tillid til, at de digitale læringsprodukter lever op til lovkrav om datasikkerhed.



Kilde: Undervisere, n=722.

Note: Figuren viser andelen, der har svaret "Helt enig" eller "enig" til spørgsmålet: "Jeg har generelt tillid til, at [produktkategori] lever op til lovkrav om datasikkerhed".

Nogle af de interviewede lærere taler med kollegaer eller gør sig overvejelser omkring, hvor vidt det er hensigtsmæssigt at bruge sociale medier i undervisningen ud fra et datasikkerhedsmæssigt perspektiv:

Lærer, gymnasium: Men jeg har da tænkt, om det er en god idé at fortsætte med [socialt medie]. Det er jo ikke sikkert, de har en profil på [socialt medie]. Så trækker jeg dem jo derind, og jeg vil jo gerne være lidt kritisk overfor den platform. Der findes jo også andre programmer, men det her er nemt. Det er jo unge elever, og det her er nemt for dem. Det er noget de kender.

Det er dog ikke normen, at lærere gør sikkerhedsmæssige overvejelser til grundlag for vurderingen af digitale produkter. Både i mobiletnografi og fokusgrupper med lærere giver de udtryk for, at det er uvant for lærerne at forholde sig til de sikkerhedsmæssige aspekter ved digitale øvrige produkter og sociale medier.

Lærer, folkeskole: Jeg har ikke tænkt over, at de måske bruger data. Måske man lige skulle vende den med chefen, hah. […]. Det giver da stof til eftertanke, men det [datadeling] er ikke noget, vi er blevet informeret om, og derfor har jeg ikke skænket det en tanke.

Udover at vælge og prioritere på baggrund af pædagogiske eller sikkerhedsmæssige overvejelser, fremhæver flere, at **det, der ligger til grund for deres beslutninger, er deres egen private holdning til og erfaring med produkterne**. Hvis en lærer privat ikke har for vane at dele eller bruge sociale medier privat, er det heller ikke nærliggende at bruge det professionelt:

Gymnasielærer 1:	Det handler meget om mig selv. Jeg gider ikke figurere i offentligheden. Jeg synes ikke det er fedt, man kan søge mig frem om ti år. Jeg hader selv at blive eksponeret. Måske eleverne heller ikke synes, det er fedt, når de skal søge et job senere. Du er jo ligeglad, ikke?
Gymnasielærer 2:	Ja, jeg ligger alt muligt pjat ud på [socialt medie], jeg håber folk ikke kan finde om ti år, haha.

Således er der for disse produkttyper et vist overlap mellem private holdninger og viden, og hvad der overføres til den professionelle praksis, og måden lærerne bruger det med eleverne. **Flere lærere udtrykker bekymring over, at eleverne ikke altid er klar over, hvilke konsekvenser deres handlinger kan have** og hvem, de deler hvilke oplysninger med:

Interviewer:	Hvad med datadeling i forhold til digitale produkter i undervisningen?
Gymnasielærer 1:	Man bliver hurtigt den gamle. Men det tror jeg der er meget få, der reflekterer over, hvor meget de smider væk af data. Og oveni købet ikke kan se et problem i det.
Gymnasielærer 2:	De logger ind med alt muligt gennem deres profil på [socialt medie]. Uden at vide, at de giver samtykker til, at alle muligt informationer videregives.

På den ene side udtrykker lærerne en forholdsvis lav tillid til især sociale medier og de øvrige produkter, på den anden side er det sjældent datasikkerhed fylder noget som hensyn, når de skal vælge. Forklaringen på dette kan være, at de ikke har de fornødne kompetencer og værktøjer til at gøre dette. En anden forklaring er, at de vurderer det ligger ude for deres ansvarsområde.

Når de fravælger at bruge forskellige digitale produkter, kan det også være andre hensyn, der ligger til grund – fx private eller økonomiske. Det betyder også, at det ofte er uklart for lærerne, hvornår deres praksis med digitale produkter også eventuelt kan være problematisk i en sikkerhedsoptik.

7.8 HVAD GØR INSTITUTIONERNE FOR AT HÅNDTERE DATASIKKERHED VED DIGITALE PRODUKTER?

Ovenfor er det blevet afdækket, hvilke produkter, der bruges, under hvilke licensbetingelser, deres geografiske ophav og på hvis initiativ de ofte finder vej ind i undervisningen. Der er peget på en række dilemmaer, disse praksisser foranlediger fra et datasikkerhedsmæssigt perspektiv. I det følgende vil det blive adresseret, hvilke forholdsholdsregler og tiltag, der i praksis allerede er taget for at håndtere datasikkerheden omkring brugen af digitale produkter i undervisningen. **Den type initiativer, der oftest er taget med henblik på at håndtere sikkerheden omkring persondata om elever i undervisningen er: Databehandleraftaler, tekniske tiltag, institutionelle procedurer og personlige forbehold hos elever og lærere.**

7.8.1 Indgåelse af databehandleraftaler

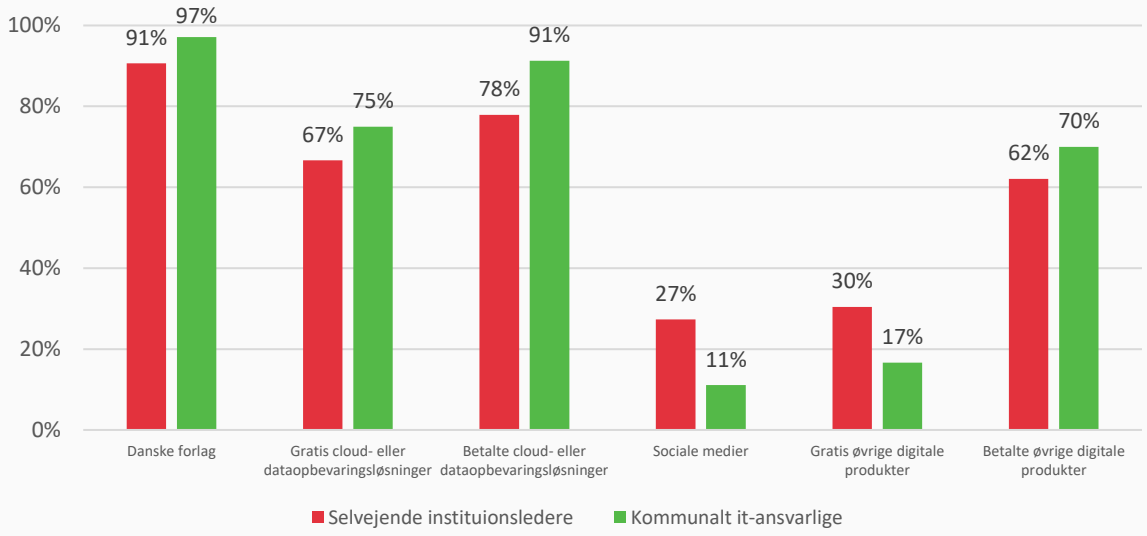
På de kvalitative casebesøg er der blevet givet udtryk for, at der er et sammenfald mellem, hvilke produktkategorier, der er betalt for, og hvilke der også foreligger databehandleraftaler på. Som en it-chef fortæller på et casebesøg på et gymnasium er den primære årsag til dette *ikke* nødvendigvis, at de gratis, øvrige og udenlandske produkter ikke er relevante i en datasikkerhedsmæssig optik.

Det handler snarere om det lavpraktiske forhold, at **regninger på de digitale produkter ofte er administrationens primære kilde til indsigt i, hvilke produkter, der bruges ude i undervisningen**. Det betyder, at når 57 pct. af de øvrige produkter bruges i gratisudgaver, så bliver dem, der har ansvar for indgåelse af databehandleraftaler, heller ikke altid adviseret om eventuelle behov herfor med leverandører af gratis produkter.

Det kan danne forklaringsgrundlag for tendensen til, at lederne i mindre grad har erfaring med eller ved, om det er muligt at indgå databehandleraftaler med de øvrige produkter og sociale medier.

Eksempelvis oplever ledere på de selvejende institutioner, at det på den ene side er overvejende **muligt at indgå databehandleraftaler med danske forlag omkring deres digitale produkter og platforme (91 pct.), mens markant færre oplever, at dette er tilfældet med øvrige produkter (30 pct. og særligt sociale medier (27 pct.):**

Figur 16: Det er generelt muligt at få en databehandleraftale på plads, hvis det er nødvendigt



Kilde: Selvejende institutionsledere, n=280; kommunalt it-ansvarlige, n=35.

Note: Søjlerne angiver andelene der har svaret "Helt enig" eller "Delvis enig" til spørgsmålet: "Det er generelt muligt at få en databehandleraftale på plads, hvis det er nødvendigt".

Som figur 16 viser, er det overvejende muligt at indgå databehandleraftaler med danske forlag omkring deres digitale produkter og platforme. I interview med tre større danske forlag er det da også blevet beskrevet, hvordan forlagene selv har henvendt sig til institutionerne med udkast til aftaler. Disse har taget udgangspunkt i Datatilsynet og/eller KOMBITs udkast, og forlagene melder tilbage om, at de oftere afventer tilbagemeldinger fra institutionerne og kommunerne end den anden vej rundt.

Samtidig tegner der et billede af, at ledelser og kommuner **i mindre grad har erfaring med at indgå databehandleraftaler med de gratis udenlandske produkter i kategorien øvrige samt sociale medier.** Især på kommunalt niveau angives det også, at det er vanskeligt at indgå aftaler med sociale medier (45 pct.). For de øvrige produkter svarer størstedelen på både de selvejende institutioner (73 pct.) og kommunerne (77 pct.) enten "ved ikke" eller "hverken/eller" til, om det er muligt at indgå aftaler[19].

[19] Spørgsmålsformulering – *"Hvor enig eller uenig er du i følgende udsagn om de sociale medier / øvrige produkter, skolerne bruger: Det er generelt muligt at få en databehandleraftale på plads, hvis det er nødvendigt"*

7.8.1.1 Hvem skal træffe beslutning om, hvorvidt der skal indgås databehandleraftale?

70 pct. af lederne på de selvejende institutioner angiver, at de er uenige eller helt uenige i, at de mangler viden om, hvem der skal træffe beslutning om indgåelse af en databehandleraftale[20]. Der er dermed blandt lederne for de selvejende institutioner en relativt veletableret konsensus om, hvis ansvar det er at indgå databehandleraftaler.

Blandt folkeskoleledere er der mindre klarhed omkring ansvarsplaceringen. Her oplever kun 53 pct.[21], at de ikke mangler viden om, hvem der skal træffe beslutninger omkring indgåelse af databehandleraftaler.

Forskellen på oplevelsen af klarhed omkring ansvaret for indgåelse af aftaler på de to institutionstyper kan delvist forklares med, at kommunerne for folkeskolernes vedkommende påtager sig en del af ansvaret. Her angiver 74 pct.[22] af de kommunalt it-ansvarlige, at de er uenige eller helt uenige i, at de mangler viden om ansvarsfordelingen.

Ikke desto mindre indikerer resultaterne, at der generelt ikke er fuld klarhed om hvem – på tværs af alle institutionstyper – der har ansvaret for at afgøre eller indgå en databehandleraftale. På casebesøgende kommer det i nogle af de kvalitative interview til udtryk, at en del af forklaringen kan være, at grundet forlagenes pro-aktive og opsøgende indsats, er ledelser nogle steder af den overbevisning, at ansvaret for at initiere indgåelse af aftaler ikke kun påhviler institutionen, men er delt med leverandørerne af de digitale produkter.

Et andet forhold der er vigtigt at have in mente i vurderingen af processen med indgåelse af databehandleraftaler er, at **det varierer i hvilken grad, kommunalt it-ansvarlige og ledere vurderer, at databehandleraftaler er nødvendige.**

Halvdelen af de kommunalt it-ansvarlige vurderer, at mellem tre-fjerdedele af digitale produkter brugt i undervisningen kræver en databehandleraftale (54 pct.). En fjerdedel (23 pct.) mener, det er alle[23]. Dette kan dels tolkes som udtryk for, at det varierer på tværs af kommuner, hvilke produkter der bruges, og derfor også hvor nødvendige aftaler er.

En anden forklaring kan være, at der ligger forskellige kriterier til grund for vurderingen af, om aftaler er nødvendige. Slutteligt er det også normen, at hverken ledelse eller kommuner har fuldt overblik over, hvilke produkter, der bruges i undervisningen. **En fjerdedel af lederne på selvejende institutioner og folkeskoleledere angiver, at de i nogen eller høj grad har overblik over de anvendte produkter (24 pct.). Lidt over halvdelen af de kommunalt it-ansvarlige har i nogen eller høj grad et overblik (60 pct.)[24]**

Kommunalt it-ansvarlig, spørgeskema: Vi har ikke helt overblikket over hvad der bruges af gratis produkter af personalet på skolerne

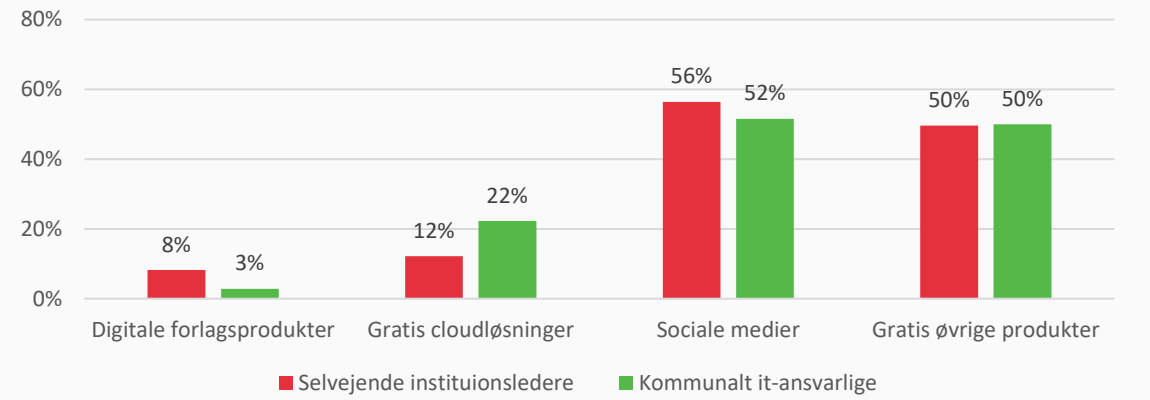
---

[20] Spørgsmålsformulering – *"Datahåndtering handler ofte om juridiske tolkninger. Vi vil gerne vide, hvor enig eller uenig du er i, at I mangler viden om, hvem der skal træffe beslutning om, hvorvidt der skal indgås en databehandleraftale"*
[21] Ibid
[22] Ibid
[23] Spørgsmålsformulering – *"Hvor stor en del af de digitale produkter, som skolerne bruger, vurderer du: kræver en databehandleraftale"*
[24] Spørgsmålsformulering – *"I hvilken grad vurderer du, at du har fuldt overblik over, hvilke digitale produkter lærerne generelt bruger i undervisningen"*

7.8.1.2 Erfaring med indgåelse af databehandleraftaler

Når det kommer til foreløbige erfaringer med indgåelse af aftaler, oplever lederne på de selvejende institutioner og kommunalt it-ansvarlige, at **processen går overvejende problemfrit med forlag og cloudløsninger (figur 17)**.

Figur 17 Andel af kommunalt it-ansvarlige og ledere på selvejende institutioner, der ikke har forsøgt at indgå databehandleraftale med forskellige produktkategorier



Kilde: Selvejende institutionsledere, n=280; kommunalt it-ansvarlige, n=35.

Som figur 17 viser, har langt størstedelen forsøgt at indgå aftaler med forlag og tilsvarende har over to-tredjedele forsøgt at indgå aftaler med cloudløsninger**. Når det kommer til sociale medier og øvrige, gratis produkter har over halvdelen ikke forsøgt at indgå databehandleraftaler**.

Enkelte institutioner skiller sig ud, og har forsøgt at indgå en databehandleraftale med sociale medier, men uden et frugtbart resultat:

GDPR-ansvarlig, erhvervsskole: Vi har databehandleraftaler med 30 stykker. Både nationalt og internationalt, EU primært. Udover de 30 er der nogle, vi gerne vil indgå samtaler med, men som vi ikke lykkes med. Primært de sociale medier såsom [eksempel 1] og [eksempel 2]. Vi har forsøgt at kontakte dem på flere forskellige måder.

Forklaringen på de blandede erfaringer med indgåelse af aftaler med sociale medier kan dels forklares ved, at det – som eksemplet viser – **ikke kan lade sig gøre at komme i kontakt med virksomhederne eller forhandle indholdet**. En anden forklaring kan være, at institutionerne i stedet laver lokale retningslinjer for, hvordan sociale medier må (og ikke må) bruges i undervisningen, som afsnittet nedenfor om tiltag og procedurer omhandler.

Dilemma:

De fleste digitale produkter, der anvendes til undervisningen, tilhører kategorien gratis digitale produkter. Samtidigt er denne produkttype blandt de produkttyper, som flest angiver, at de ikke har forsøgt at indgå databehandleraftaler med. Der er således et dilemma, der knytter sig til det forhold, at de gratis produkter på den ene side ofte – i højere grad end betalingsløsningerne – opfylder specifikke pædagogiske behov, mens de på den anden side kan være vanskelige at indgå databehandleraftaler med.

Hensyn til datasikkerhed medfører også et andet potentielt dilemma. Det kan afstedkomme en central regulering af, hvilke produkter, lærerne får mulighed at vælge i mellem. Der er ikke mange empiriske indikationer på dette som en aktuel problemstilling, men it-vejlederforeningens formand John Klesner udtrykker en bekymring for, at dette meget vel kan blive et reelt scenarie. **Problemet med centralisering er, at det begrænser de pædagogiske muligheder for lærerne og skaber ulige vilkår for små udviklere af nye digitale produkter**:

John Klesner, Danmarks it-vejlederforening: Kravene til datasikkerhed begrænser umiddelbarheden og lysten til at eksperimentere med noget nyt, der dukker op og som kunne have potentiale. Hvis man ser på de små producenter på det danske marked. Det er svært for dem at sende apps på gaden og få dem udbredt fordi det bliver de store gængse, velkonsoliderede løsninger man vælger, fordi de er standard. Det er pædagogisk begrænsende i aller højeste grad. Men sikkerhedsmæssigt mere forsvarligt.

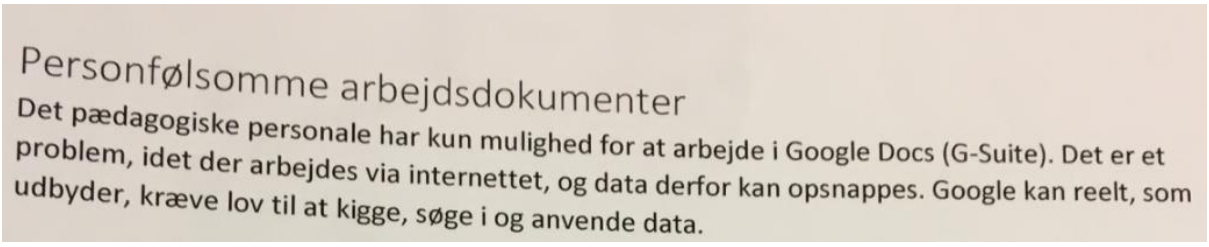
Flere af de forlag, der er blevet interviewet i forbindelse med undersøgelsens desk research bemærker også, at det papirarbejde databehandleraftaler kræver, er en meget stor opgave for små virksomheder at håndtere.

Dilemma:

En måde at håndtere datasikkerheden på er centralt at styre og regulere, hvilke produkter der stilles til rådighed for lærere og elever. Det betyder imidlertid, at det kun er de virksomheder, der har ressourcer og kapacitet til at leve op til de juridiske betingelser og det oplevede bureaukrati databeskyttelsesloven medfører, som vil nå ud til lærerne. Det konflikter med lærernes metodefrihed. Udover at begrænse de pædagogiske muligheder for underviserne, er en faldgrube, at dette skævvrider markedsvilkårene for nye aktører og teknologiudviklere.

7.8.2 Institutionelle og kommunale procedurer og tiltag

Spørgsmålet om, hvorvidt et givent digitalt produkt brugt i undervisningen er relevant fra et sikkerhedsmæssigt perspektiv afhænger af, hvordan det bruges og under hvilke betingelser**. På flere institutioner og i kommunalt regi har man truffet beslutninger og taget tekniske initiativer med henblik på at minimere risiko og øge sikkerheden**. Et sådant et eksempel fra en caseinstitution er hand outs udarbejdet af skoleledelsen på baggrund af information fra kommunen. Dette bliver distribueret lokalt på institutionen til lærerne med henblik på at korrigere deres brug af cloudløsninger:


Personfølsomme arbejdsdokumenter

Det pædagogiske personale har kun mulighed for at arbejde i Google Docs (G-Suite). Det er et problem, idet der arbejdes via internettet, og data derfor kan opsnappes. Google kan reelt, som udbyder, kræve lov til at kigge, søge i og anvende data.

Kilde: Billede fra casebesøg på folkeskole

Dokumentet beskriver videre, at lærerne skal henvende sig til skolekontoret, hvis de har tvivlsspørgsmål eller brug for at opbevare personfølsomme dokumenter sikkert.

Der er på caseinstitutionerne også gjort flere tiltag, der vedrører brugen af digitale produkter i undervisningen. Indtrykket er, at disse ikke tages af lærerne selv, men af enten ledelsen, kommunen eller institutionens it-vejleder med henblik på at sikre, at de produkter, enheder og vilkår, lærerne

får stillet til rådighed er teknisk konfigureret, samt angive hvad man må bruge bestemte produkter til, så datarelaterede risici minimeres.

7.8.2.1 Tekniske tiltag

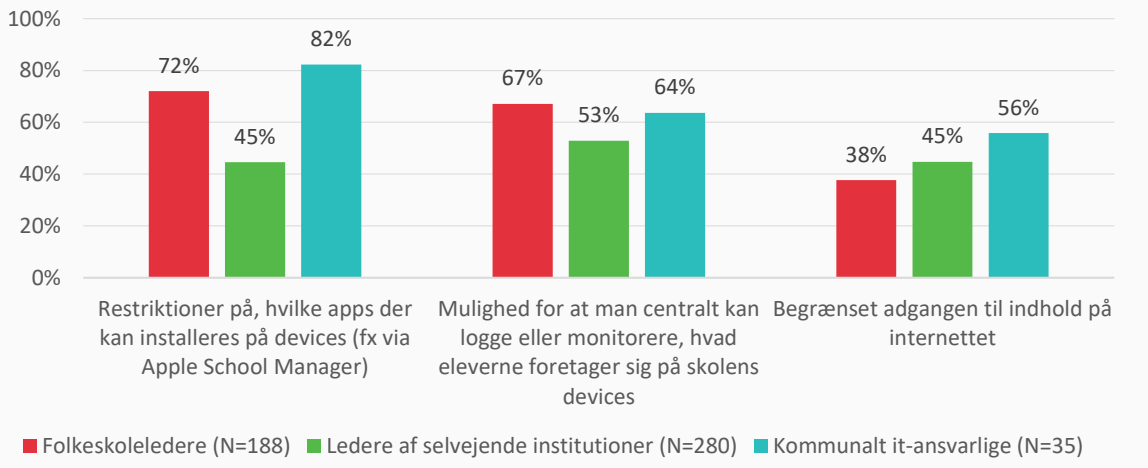
De fleste institutioner har indført forskellige tekniske tiltag med henblik på at optimere datasikkerheden. Dette drejer sig især om netværksindstillinger, forskellige blockere og firewalls, samt hvilke enheder der arbejdes på.

På ungdomsuddannelser er det betragtelig mere udbredt, at eleverne kun bruger egne enheder, mens det på grundskoleområdet er mere almindeligt, at eleverne får stillet computere eller tablets til rådighed af institutionen. Dog betyder institutionernes forskellige politikker for, hvad der stilles til rådighed ikke, at der nødvendigvis udelukkende arbejdes på enten institutionens eller private enheder.

80 pct. af folkeskolelederne angiver således, at eleverne både bruger institutionens og private enheder. Det samme er tilfældet for 61 pct. af de selvejende institutioner[25]. Denne overvejende "både-og-praksis" er blevet omtalt på forskellige måder på caseinstitutionerne. På nogle folkeskoler stiller institutionen tablets til rådighed i de mindre klasser, mens mellemtrin og udskoling fungerer som 'Bring Your Own Device'. På andre institutioner får alle elever en computer, men mange elever bruger stadig private telefoner i undervisningen.

Når eleverne arbejder på de enheder, institutionerne har stillet rådighed, bliver der imidlertid taget forskellige tekniske tiltag med henblik på at kontrollere brug og datasikkerhed, herunder især hvilke produkter og apps, der kan installeres. Over halvdelen af institutionerne har også mulighed for at logge, hvad eleverne foretager sig på institutionens devices (figur 18):

Figur 18: Tekniske tiltag på institutionens devices



Kilde: Folkeskoleledere, n=188; Selvejende institutionsledere, n=280; kommunalt it-ansvarlige, n=35.

Note: Søjlerne angiver andelen der har svaret "Ja, det er udbredt" eller "Ja, i nogle situationer" til spørgsmålet: "Har I indført et eller flere af følgende tekniske tiltag på institutionens enheder?"

[25] Spørgsmålsformulering – *"Hvilke enheder (dvs. smartphone, tablet, computer mv.) arbejder eleverne med i undervisningen"*

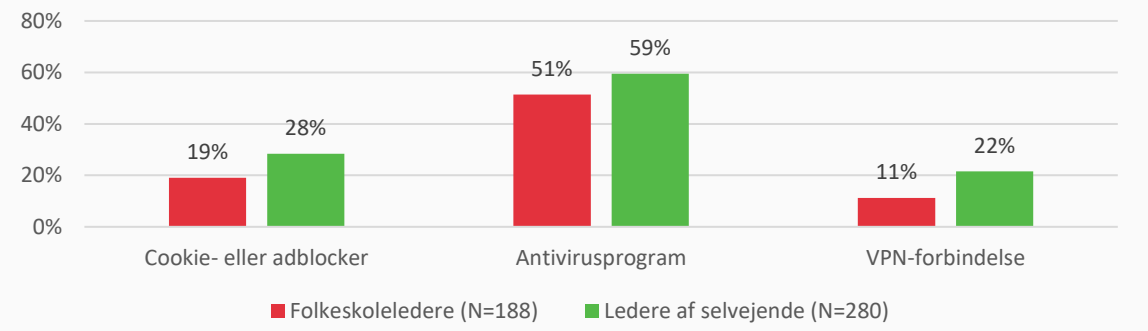
De forskellige reguleringer tjener flere formål. Dels at sikre, at uvedkommende ikke trænger ind i den digitale infrastruktur, dels at beskytte eleverne mod indhold og endeligt at sikre, at der ikke unødigt deles data om eleverne. Af interviewene på caseinstitutionerne kommer det imidlertid til udtryk, at sidstnævnte sjældent årsagen til at, de tekniske initiativer bliver taget. Det handler i højere grad om beskyttelse af elever mod indhold og sikring mod hackerangreb, malware m.v.

Når det kommer til elevernes brug af egne enheder, bliver der oftest taget færre tekniske forholdsregler. På casebesøg blev dette begrundet på flere måder. Dels har institutionerne ikke de tekniske ressourcer og kompetencer til at ensarte kontrol og sikkerhed på tværs af forskellige modeller af computere og styresystemer. Dels mente flere ledere, at det ikke var institutionens opgave at sikre, at elever har styr på sikkerheden på private computere, telefoner og tablets.

Forskning i Bring Your Own Device har peget på, at der typisk er fokus på sikkerheden, mens privatlivsaspekter ofte er oversete, men i høj grad relevante**. Når en og samme enhed bruges til private og skoleformål samtidig "mingles" data fra forskellige kontekster også potentielt sammen[26].**

Adspurgt om, hvad institutionerne stiller til rådighed af forskellige tiltag for at sikre elevernes private enheder, fordeler det sig som på figur 19:

Figur 19: Har institutionen i forbindelse med, at eleverne laver skolearbejde på egne devices, anbefalet eleverne, at installere...



Kilde: Folkeskoleledere, n=188; Selvejende institutionsledere, n=280

Generelt er mønstret således, at institutionerne er mere proaktive med forskellige tekniske indsatser, når det handler om de enheder, de selv stiller til rådighed sammenlignet med enheder, eleverne selv medbringer.

På casebesøgene peger nogle i forlængelse heraf på, at **ansvaret fordeles efter, hvem der ejer enhederne, mens andre peger på, at ansvaret for datasikkerhed fordeles efter, hvilken type aktivitet der laves**:

Leder, gymnasium: Det er vores ansvar hvis vi siger, at de skal hente og arbejde på et særligt program. Men hvis de selv vælger det, så kan det ikke være os, bare fordi de sidder herude. Men i det øjeblik det indgår i undervisningen, så må det være vores ansvar.

[26] Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and privacy considerations. *It Professional*, *14*(5), 53-55.

7.8.2.2 Procedurer for brug af bestemte produktkategorier

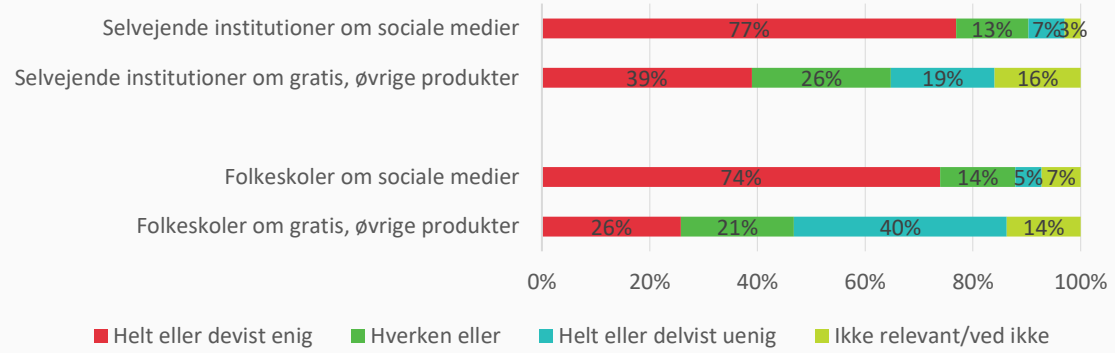
Analysen har indtil videre peget på øvrige produkter (der ofte er gratis og udenlandske) og sociale medier, som de produktkategorier, der er særligt kritiske ift. datadeling og som tit "går under radaren", når det kommer til kontrol og overblik med datadeling samt indgåelse af databehandleraftaler.

Dilemma:

På institutioner, der praktiserer Bring Your Own Device, kan det opleves som et dilemma at afgøre, hvornår det falder indenfor og udenfor institutionernes ansvar at sørge for, at sikkerheden omkring deling af data er sikker. Trækkes linjen ved hvis enhed det er (privat eller institutionens), hvilken type aktivitet (undervisning eller fritid) eller ved hvilket netværk man er koblet på (institutions eller privattelefonens 4G).

For at håndtere risici med disse produktkategorier har nogle institutioner udarbejdet forskellige retningslinjer og procedurer for underviserne. Disse procedurer vedrører især, hvilke produkter, der må bruges, under hvilke betingelser, og hvordan der oprettes profiler.

Figur 20: Har institutionerne procedurer for brugen af sociale medier og øvrige produkter?



Kilde: Folkeskoleledere, n=188; Selvejende institutionsledere, n=280. Lederne er blevet spurgt for hver produktkategori: "Vi har procedurer for, hvordan [produktkategori] må bruges".

På tværs af institutionstyperne angiver tre-fjerdedele af lederne, at de har procedurer for, hvordan sociale medier må bruges (figur 20). Øvrig analyse viser, 25 pct. af folkeskolerne har pålagt underviserne slet ikke at bruge sociale medier i undervisningen, mens dette er tilfældet for 15 pct. på de selvejende institutioner. Figur 20 viser, at institutionerne i mindre grad har procedurer for brugen af øvrige, gratis produkter (39 pct. på selvejende institutioner og 26% på folkeskoler).

Flere af caseinstitutionerne har også en politik for brugen af sociale medier i undervisningen. Her viser det sig dog, at **ophavet til lokale procedurer eller retningslinjer sjældent er begrundet med hensyn til datasikkerhed, men ofte pædagogiske hensyn såsom forstyrrelser i undervisningen** eller at kommunikationen mellem institution, forældre og elever ikke skal spredes udover unødige platforme. Et andet hensyn til at reducere brugen af sociale medier i undervisningen, der blev nævnt til workshoppen med selvejende institutioner er, at der ikke må spredes ophavsretsbeskyttet materiale på disse platforme.

Kigger vi på de øvrige produkter, angiver de kommunalt it-ansvarlige i spørgeskemaets åbne svarkategorier**, at kommunens undervisere bruger flere af de gratis produkter gennem forlagsløsninger, som giver adgang til premium-udgaver, og som de har indgået databehandleraftaler med**. Derfor kan samme produkt bruges under forskellige licensmæssige og juridiske forudsætninger, uden undervisere og elever nødvendigvis er klar over det.

Derudover enten har eller planlægger 42 pct. af folkeskolelederne og 40 pct. af de selvejende institutioners ledelser at udarbejde en liste over produkter, underviserne må bruge ("whitelist") eller en liste over produkter, de bør undgå ("blacklist")[27].

Øvrige produkter er altså et område der er reguleret i lavere grad end fx brugen af sociale medier og cloudløsninger. Forklaringen på dette er ofte, at lederne ikke har et overblik over, hvilke produkter, der bliver brugt, i hvilket omfang og til hvad. 24 pct. af lederne på selvejende institutioner har i høj eller nogen grad overblik over produkterne. For kommunalt it-ansvarlige er tallet 60 pct.[28] Igen hænger det sammen med, at når produkterne er gratis, bliver ledelse eller administration sjældent konfronteret med brugen af disse – eller at det potentielt kunne være problematisk i forhold til datasikkerhed.

På tværs af interviews med ledelse og undervisere, er produkterne, de anvender, ofte noget, de ikke har overvejet kunne være relevant i forhold til deling af data. Flere påpeger, at det er et område, de godt kunne tildele større opmærksomhed, ligesom de har gjort gennem retningslinjer for brug af cloudløsninger og sociale medier. En folkeskoleleder udtaler om undervisernes valg af gratis produkter:

> **Leder, folkeskole:** Er vi kildekritiske nok? Bordet fanger jo nok med meget af det. Når vi bruger de her ting [gratis produkter i undervisningen] er det vigtigt, at vi er kritiske for hvem kilden er. Men umiddelbart tager lærerne det første [søgemaskinen] viser. Det er ureflekteret, og deraf også det, der følger.

Samlet set kan det konkluderes, at der på både kommunalt og ledelsesniveau bliver taget forskellige initiativer – især for brugen af enheder, tekniske tiltag og brugen af sociale medier. **Omvendt er brugen af øvrige digitale produkter i undervisningen stadig et "blind spot" i praksis, når det kommer til vurdering af risici og håndtering af data, der produceres, deles og lagres gennem disse**. I det følgende behandles både elevers og undervisernes egne forholdsregler – og mangel på samme – mere nærgående.

7.8.3 Undervisere og elevers individuelle forholdsregler

To gode indikationer på, om der gennem øvrige udenlandske og gratis produkter deles data, der potentielt kan være personligt er 1) om eleverne opretter en bruger med navn eller mail eller 2) de downloader en app til deres enhed[29], der kan dele data med tredjeparter. **Blandt eleverne svarer 94**

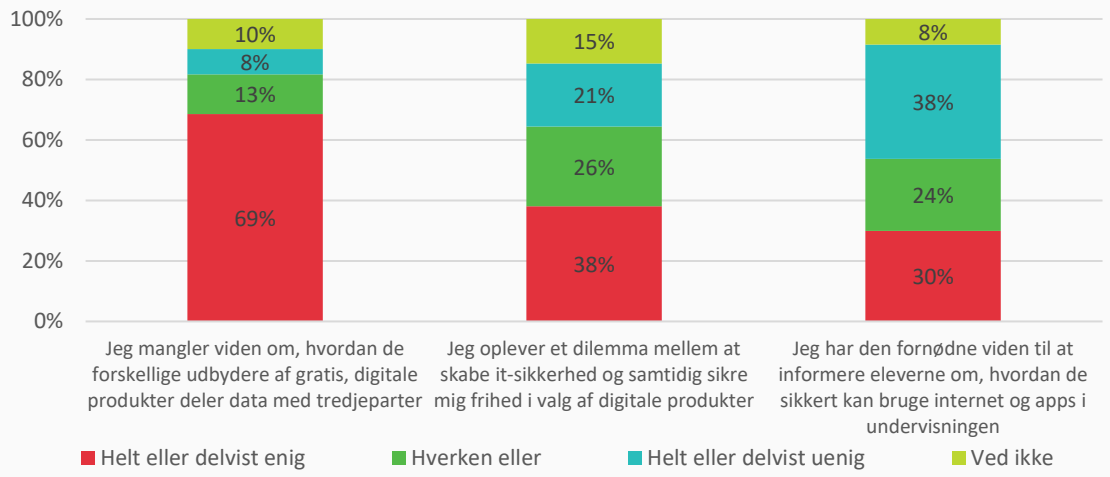
---

[27] Spørgsmålsformulering – *"Har I på institutionen udført ét eller flere af følgende tiltag: Udarbejdet en liste …"*
[28] Spørgsmålsformulering – *"I hvilken grad vurderer du, at du har fuldt overblik over, hvilke digitale produkter lærerne generelt bruger i undervisningen"*
[29] Se desk research om hvordan der muliggøres datadeling gennem apps. Se også artiklen:

pct. af dem, at de i forbindelse med skolearbejde har oprettet en profil, hvor de skulle angive navn og/eller mail (det kan også indbefatte fx forlagsprodukter) og 89 pct. har downloadet en app på deres egen eller institutionens enhed[30]. Der er altså tale om særdeles udbredte praksisser.

Samtidig angiver underviserne også, at de ofte ikke har den fornødne viden til at vurdere, hvilke risici der kan være forbundet med brugen af digitale produkter. **Som figur 21 viser, er underviserne sjældent klædt på til at vurdere eller afgøre, hvorvidt deres praksis er forbundet med et datasikkerhedsmæssigt aspekt.** Generelt angiver underviserne, at de ofte ikke har de fornødne kompetencer til at vurdere sikkerheden af digitale produkter. Fx angiver 69 pct., at de er helt eller delvist enige i, at de mangler viden om, hvordan udbydere af digitale produkter deler data med tredjeparter.

Figur 21: Hvor enig eller uenig er du i følgende udsagn om din skoles/dit gymnasiums arbejde med at skabe digital sikkerhed for eleverne?



Kilde: Undervisere, n=722.

Dette stemmer godt overens med indsigterne fra de kvalitative datakilder. En gruppe undervisere siger om det at forholde sig til datasikkerhed i forbindelse med brug af apps:

Interviewer:	Hvad med fx apps og datasikkerhed. Har I overvejet relationen?
Folkeskolelærer 1:	Nej
Folkeskolelærer 2:	Nej. Når vi henter noget ned, er det jo lige præcis dér, det er interessant. Der er vi som lærere ligesom alle andre udsatte.

Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T., & Shadbolt, N. (2018). Third Party Tracking in the Mobile Ecosystem. *arXiv preprint arXiv:1804.03603*.

[30] Spørgsmålsformulering – *"Har du i forbindelse med skolearbejde prøvet at oprette en profil til en app eller hjemmeside, hvor du skulle indtaste din mail og andre oplysninger (f.eks. navn, e-mail, adresse mv.)"*

Folkeskolelærer 3: Vi er jo ikke it-eksperter.

Når underviserne forholder sig til, hvordan eleverne gebærder sig, refererer flere af dem, at eleverne nogle gange selv tager forholdsregler, såsom altid at oprette brugere med dæknavne, uden at det nødvendigvis er en vedtaget politik. **Den forholdsregel eleverne oftest tager er ved app-download, hvor 40 pct.[31] foretager ændringer i de personlige indstillinger, fx ved at slå kamera fra.**

Men generelt er det sparsomt med forholdsregler og overvejelser, udtrykt ved at 92 pct. har download apps og accepteret betingelser uden at læse dem, mens kun 10 pct. har brugt pseudonym eller dæknavn ved profiloprettelse[32]. Generelt fremhæver forskningen dog også, at privatlivspolitikker er svært læselige i det hele taget og tilnærmelsesvist uforståelige for unge[33].

Der er altså et dilemma, der vedrører, hvilke kompetencer og ressourcer, der er nødvendige for at undervisere kan træffe datasikkerhedsmæssige kvalificerede valg, og hvor grænsen går mellem, hvad der skal gøres "uden for klasserummet", dvs. ledelsesmæssige eller kommunale beslutninger, og hvad der er underviserens og evt. elevens ansvar.

Dilemma:

Det er ikke alle undervisere, der er klar over, at brugen af digitale produkter i undervisningen kan indebære deling af elevernes persondata. Men selv når underviserne er bevidste om den potentielle udfordring, så oplever nogle undervisere fortsat ikke at have tilstrækkelige kompetencer til at kunne vurdere, hvilke forholdsregler der evt. kan tages i undervisningssituationerne. Derfor oplever relativt mange lærere et dilemma mellem på den ene side at praktisere friheden til at vælge de didaktisk eller pædagogisk bedste produkter og hensynet til it-sikkerhed på den anden side.

7.9 "THERE AIN'T NO SUCH THING AS A FREE LUNCH"

På baggrund af ovenstående kan de digitale produkter overordnet inddeles i to kategorier, med hver deres karakteristika set fra et datasikkerhedsmæssigt perspektiv. For at bruge en talemåde fra økonomien viser denne tabel også, at der *ain't no such thing as a free lunch*. Med andre ord er de mindre kontrollerede produkter nok økonomisk gratis, men der betales ofte i stedet med data.

[31] Spørgsmålsformulering – *"Gjorde du følgende, da du sidst downloadede en app i forbindelse med skolearbejdet: Foretog ændringer i personlige indstillinger"*

[32] Spørgsmålsformulering – *"Anbefalede læreren dig at gøre følgende, da du sidst downloadede en app i undervisningen"*

[33] Das, G., Cheung, C., Nebeker, C., Bietz, M., & Bloss, C. (2018). Privacy Policies for Apps Targeted Toward Youth: Descriptive Analysis of Readability. *JMIR mHealth and uHealth*, *6*(1).

	De mere kontrollerede produkter	De mindre kontrollerede produkter
Kategorier	Læringsplatforme, cloudløsninger*, digitale forlagsprodukter, sagshåndteringssystemer	Sociale medier og øvrige produkter
Karakteristiske brugsformål	Kommunikation med elever, journalisering, dokumentopbevaring, træne elevers faglighed, motiverende og varierende undervisning	Skabe motiverende og varierende undervisning, afprøve elevernes viden, kreative elevproduktioner
Overvejende niveau for beslutning om brug	Institutionsledelse eller kommune	Undervisere og elever
Tillid til datasikkerheden blandt undervisere	Højere	Lavere
Produktvariation	Lille	Stor
Oprindelse	Overvejende danske	Overvejende udenlandske
Licensformer	Overvejende betaling	Overvejende gratis
Databehandleraftaler	I overvejende grad indgået eller påbegyndt	I lavere grad indgået eller påbegyndt
Relevante datatyper (der potentielt kan være personlige)	Resultater, diagnoser, navn, adresse, mail, CPR, billeder, fravær, intern kommunikation m.v.	Billeder, video, lydoptagelse, geolokation, ip-adresse, tekniske indstillinger og id, e-mail, telefon nr., søgehistorik.
Initiativ til deling af data	Brugeren er i højere grad intiativtager til at dele data	Produktet deler i højere grad data uden initiativ fra brugeren

* Cloudløsninger adskiller sig fra de andre "mere kontrollerede produkter" ved også at være gratis og udenlandske.

En talemåde lyder også, at *data er det nye olie*. Ved dette skal der forstås, at gennem brugen af digitale produkter giver brugeren også ofte en række oplysninger om sig selv væk – fra tekniske til personlige. Disse oplysninger genererer en værdi for leverandøren af produktet, fordi data kan bruges til videresalg og målrettet reklame og på et mere generelt plan forudsige fremtidig adfærd. **Den generelle forretningsmodel bag gratis, digitale produkter betyder også, at et vilkår for, at brugeren kan benytte sig af dem (økonomisk set) gratis, er, at brugeren afgiver data, produktet eller leverandøren kan tjene penge på**. Modellen beskriver tænketanken DataEthics således:

> *Many consumer tech and social media giants have built their business models on personal data. They may be search engines, social media, digital trading platforms, streaming services and health trackers. But they are, more than anything else, big data companies that generate profit on personal data.*[34]

[34] Hasselbalch, G., & Tranberg, P. (2016). *Data ethics: The new competitive advantage*. Publishare. Side 25.

I relation til institutionernes håndtering af persondata om elever, bliver det derfor relevant at se nærmere på, hvilke licensbetingelser, elever og undervisere bruger forskellige produkter på. En tese på baggrund af ovenstående er, at hvis produkterne er gratis, betales der i stedet med data om eleverne. I den gennemførte desk research underbygges denne tese, men samtidig er der tale om et broget og svært tilgængeligt område.

Resultaterne indikerer overvejende, at produkter i gratisudgaver gennemsnitligt etablerer forbindelse til adskillige tredjeparter (trackere) med henblik på datadeling både i browser og app-udgaver, og dette gælder især øvrige digitale produkter, der er gratis og udenlandske. **De tredjeparter, der etableres forbindelse til gennem brugen af produkterne er ofte karakteriseret ved at bruge data til målrettet markedsføring.** Når elever og undervisere bruger gratis produkter i undervisningen, er der altså tale om, at de ikke kun potentielt deler data med leverandøren af produktet, men også alle de tredjeparter, som produktet deler data med (en slags "fjerdeparter").

Som det fremgår af desk researchen, angiver leverandørerne af digitale produkter i meget varierende grad hvilke typer af data de deler og med. **Dertil kommer, at der ikke lader til at være konsensus om, hvad der forstås ved personoplysninger blandt leverandørerne** (nogle sætter i deres privatlivspolitikker modsætningsforhold mellem ip-adresse og personoplysninger, selvom ip-adresse jf. databeskyttelsesloven forstås som personoplysninger). Undersøgelser peger på, at i forhold til at forstå omfanget og problemerne forbundet med datadeling i apps, er der "challenges ahead both for regulators aiming to enforce the law, and for companies who intend to comply with it."[35]

Der er altså både ledelsesmæssige og tekniske udfordringer i at begribe og afgøre, i hvilken udstrækning den data, der deles om elever gennem apps og hjemmesider er problematisk fra et databeskyttelseslovsperspektiv.

7.10 ELEVPERSPEKTIVET

Det er i ovenstående allerede indikeret, at også elevernes egen adfærd med brugen af digitale produkter spiller en helt central rolle i problematikken. **Eleverne er ofte direkte involverede i delingen af data – bevidst eller ubevidst og med eller uden underviserens kendskab.**

I de følgende afsnit præsenteres undersøgelsens resultater om datasikkerhed set fra elevernes perspektiv. Afsnittet trækker på resultater, der dels vedrører elevernes generelle syn på håndtering af data i skolesammenhæng som de kommer til udtryk i spørgeskemaundersøgelsen. Dels vedrører resultaterne elevernes vidensniveau baseret på deres besvarelse af en specialudviklet test om datasikkerhed.

7.10.1 Elevernes bekymringer, viden og adfærd

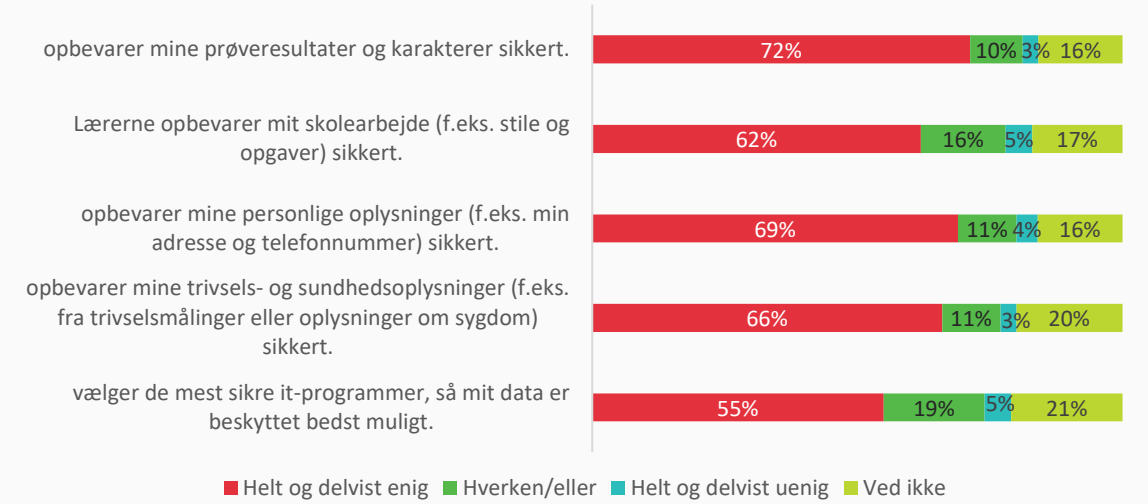
7.10.1.1 Bekymringer vedr. institutionens og undervisernes håndtering af elevdata

Overordnet set har de fleste af eleverne tillid til, at deres institution og undervisere håndterer deres elevdata sikkert (figur 23). Tilliden fordeler sig dog relativt ujævnt på tværs af forskellige

[35] Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T., & Shadbolt, N. (2018). Third Party Tracking in the Mobile Ecosystem. *arXiv preprint arXiv:1804.03603*. Side 8.

parametre. Den er højest, når det gælder spørgsmålet om, hvorvidt institutionerne opbevarer elevernes prøveresultater og karakterer samt personlige oplysninger sikkert (72 pct.). **Omvendt er tilliden mindst, når det gælder spørgsmålet om, hvorvidt eleven oplever, at institutionerne vælger de mest sikre it-programmer (55 pct.)**

Figur 23: Hvor enig eller uenig er du i følgende udsagn?



Kilde: Elevsurvey. n=7048

Følgende hjælpetekst indgår i spørgsålet: "I løbet af et skoleår får din [institution] mange forskellige informationer om dig. Det kan f.eks. være dine prøveresultater, stile, personlige oplysninger såsom telefonnummer, resultater fra trivselsmåling osv. De første spørgsmål handler om, hvordan du tror, at [institution] opbevarer sådan nogle informationer."

Selvom størstedelen af eleverne har tillid til, at deres institution og undervisere håndterer elevdata sikkert, så er der dels en relativt stor gruppe, der svarer "ved ikke", og dels en gruppe elever der er helt eller delvist uenige i udsagnene.

De elever, der giver udtryk for, at de i et eller andet omfang er uenige i udsagnene, er blevet bedt om at beskrive konkrete situationer, som ligger til grund for deres manglende tillid[36]. I elevernes besvarelser henvises der til situationer af meget forskelligartet karakter og svarer i høj grad til de udfordringer, som også institutionens personale peger på (jf. rapportens øvrige resultater). Nogle af eleverne peger således på situationer, hvor problemet er af relativt lavpraktisk karakter, som fx situationer hvor det har været muligt at se andre elevers karakterer og opgaver:

Elev: Ofte har læreren en liste med alle elevernes navne og en karakter udfor. Derefter bliver vi kaldt ud på gangen og får vores resultat. Man skal altså ikke være atomfysiker, for at kunne læse de andres karakterer, på hovedet.

Elev: Vores lærer lægger tit vores stile og opgaver i deres dueslag, så alle kan hente dem

[36] Spørgsmålsformulering: *"Du har svaret [x] til spørgsmålet [y]. Kan du give et eksempel på en situation, hvor du har oplevet, at oplysninger om dig eller dine klassekammerater ikke blev opbevaret sikkert af [institution]?"*

Men andre elever reflekterer også over situationer eller forhold, der knytter sig til mere komplekse og tekniske udfordringer. Nedenstående citat illustrerer eksempelvis, hvordan en elev oplever et dilemma imellem institutionens retningslinjer/tekniske foranstaltninger til eksamen på den ene side og hensynet til sin egen datasikkerhed på den anden side:

Elev: Vi skal til eksamen bruge et program, som overvåger alt, vi laver, og det er svært med garanti at vide, at programmet forsvinder helt, og hvordan de data, programmet overvåger, bliver gemt. Jeg kunne for eksempel have et program i baggrunden, som sender data i baggrunden. Dette eksamensprogram ville så have den data, og hvis de ikke blev gemt og beskyttet rigtigt, kunne der være information om mig på nettet, som jeg ikke selv havde godkendt skulle lægges ud.

Nedenstående citater illustrerer en lignende pointe, idet de viser, hvordan nogle elever forholder sig kritiske over for institutionens valg af it-løsninger:

Elev: Skolen bruger [e-mail klient fra større it-virksomhed], som er ejet af en koncern, der har en udveksling af oplysninger med udenlandske regeringer. Ligeledes kan man finde vores fulde navn på [læringsplatform], uden at logge ind. Slutteligt bruger vi også et net, som tracker vores brug på nettet. Disse data kan i værste fald også misbruges.

Elev: Skolen benytter fx [online tekstbehandling], som har i sine betingelser, at alt der skrives i [tekstbehandlingen], har [leverandøren] rettighederne til at dele. Det er ikke en konkret situation, hvor data er behandlet usikkert, men chancen er der.

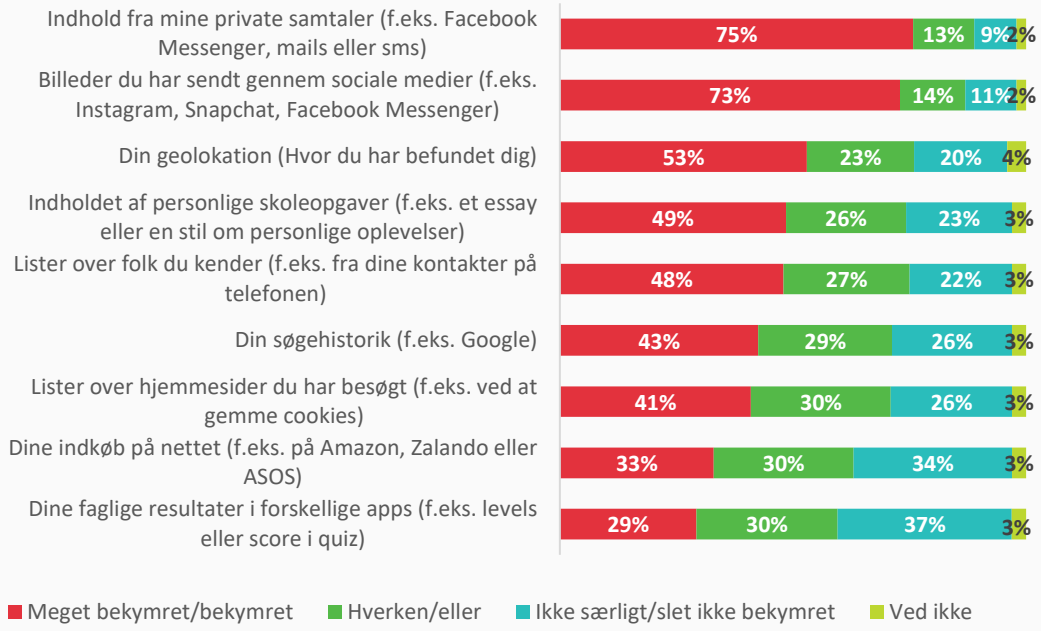
Netop blikket for den "usynlige" datadeling er noget, der i et vist omfang spiller en vigtig rolle for eleverne, når de spørges ind til det. 77 pct. af eleverne er således helt eller delvist enige i, at det er vigtigt for dem, at hjemmesider til undervisning ikke deler oplysninger, som de afgiver, mens kun 6 pct. er helt eller delvist uenige[37].

Ser vi videre på, hvad bekymringerne konkret handler om, så knytter de sig først og fremmest til adfærd på de sociale medier – dvs. deling af tekst (75 pct.) og billeder (73 pct.) (figur 24). Dermed understøtter resultaterne, de fund, der viser, at det især er brugen af sociale medier, som har været i institutionernes søgelys.

[37] Spørgsmålsformulering: *Mange digitale produkter gemmer ofte oplysninger om dig. Det gælder både, hvad du lægger op eller skriver af indhold, men også hvad du klikker på. Du bedes i de næste spørgsmål vurdere i hvilket omfang virksomhederne behandler dine oplysninger ordentligt.*

Først vil vi gerne bede dig forholde dig til følgende udsagn om hjemmesider, der bruges i undervisningen (eksempelvis [forlag]). Hvor enig eller uenig er du i følgende udsagn: Det er vigtigt for mig, at hjemmesider til undervisning ikke deler de oplysninger, jeg afgiver"

Figur 24: Mange apps og hjemmesider deler data om dig og din adfærd med andre virksomheder. Hvor bekymret eller ubekymret er du for at dele følgende informationer med andre virksomheder?



Klide: Elevsurvey, n=7.048

I forlængelse heraf er det nærliggende at se på, hvad det er, eleverne er bekymrede for, at deres data rent faktisk bruges til (figur 25). Her viser undersøgelsen, at det særligt er risikoen for, at data kan bruges til at vurdere elevens humør/psykiske tilstand (55 pct.) samt brugen af data i anonymiseret form til forskning og rapporter (49 pct.), der bekymrer flest elever. Målretning af politiske kampagner (43 pct.), nyheder (40 pct.) og især reklamer (33 pct.) er færre bekymrede for, men forskellene på tværs af kategorierne er begrænset.

Figur 25: Mange forskellige slags data fra din søgehistorik, billeder, SMS'er mv. kan bruges til at lave en profil, som beskriver, hvem du er. En sådan profil kan bruges af virksomheder til forskellige formål. Hvor bekymret eller ubekymret er du for, at en sådan profil bliver brugt til følgende?

Klide: Elevsurvey, n=7.048

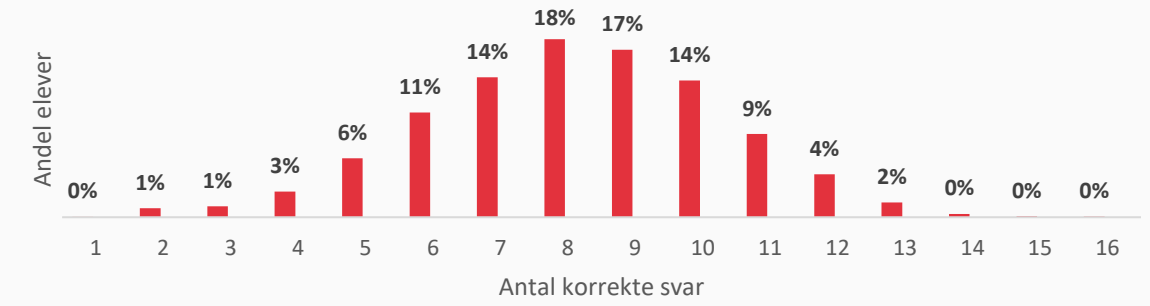
Ét aspekt er imidlertid elevernes *bekymringer*, et andet er elevernes *viden* om datasikkerhed. For at få et indtryk af elevernes viden har Epinion udviklet en test, som eleverne har taget i forbindelse med besvarelsen af spørgeskemaet.

I det følgende afsnit præsenteres analysen af testresultater – herunder koblingen mellem elevernes videns - og bekymringsniveau.

7.10.2 Viden om datahåndtering

Alle elever, der har deltaget i spørgeskemaundersøgelsen, er samtidigt blevet bedt om at besvare en test, som Epinion har udviklet til at måle elevernes viden inden for en række konkrete forhold om datasikkerhed. **Opgjort ved antallet af korrekte svar fordeler eleverne sig normalfordelt, sådan at de fleste elever har svaret rigtigt på mellem 8-9 spørgsmål ud af 16**, mens færre elever har svaret enten rigtigt eller forkert på hhv. alle eller næsten alle spørgsmål (jf. figur 26). På tværs af alder og køn er forskellene små. Drengene har gennemsnitligt 0,5 flere rigtige besvarelser end pigerne, mens der på tværs af aldersgrupper ikke er et entydigt mønster eller store udsving i resultaterne.

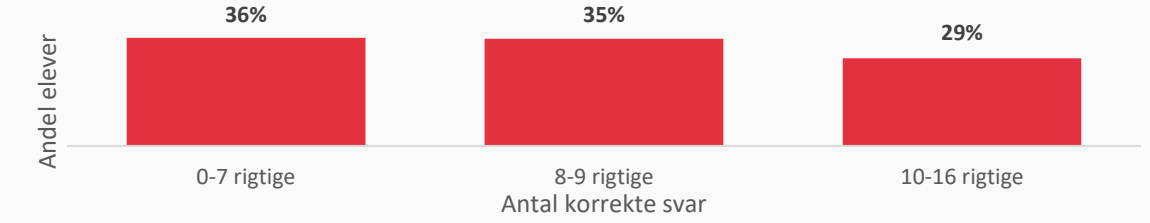
Figur 26: Prøveresultater opgjort ved antallet korrekte svar



Klide: Elevsurvey, n=7.048

Det er på den baggrund muligt at sondre mellem eleverne i tre overordnede grupper: Elever, der svarer rigtigt på hhv. 1-7 spørgsmål, 8-9 spørgsmål og 10-16 spørgsmål. Inden for denne sondring fordeler elevernes resultater sig nemlig i tre næsten lige store grupper, som kan sammenlignes (figur 27).

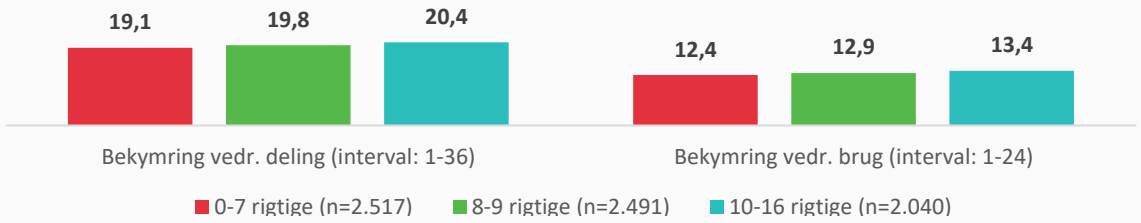
Figur 27: Prøveresultater opgjort ved antallet korrekte svar (kategoriseret tre ca. lige store grupper)



Klide: Elevsurvey, n=7.048

Når vi sammenligner de tre gruppers grad af bekymring (figur 28) (ved en indeksering af survey-spørgsmålene fra sidste afsnit), fremgår det, at der er en signifikant forskel på tværs af de tre grupper – både mht. bekymringer vedr. deling af data og den efterfølgende brug af data. Forskellen er beskeden, men indikerer en tendens til, at **elever med større viden om datasikkerhed generelt også er en smule mere bekymrede mht. deling af deres digitale data via apps og hjemmesider.**

Figur 28: Prøveresultater opgjort ved antallet korrekte svar krydset med samlet grad af bekymring ved hhv. datadeling og -brug



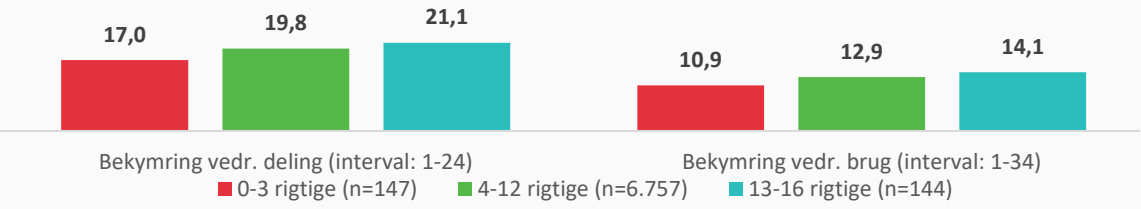
Klide: Elevsurvey, n=7.048

Note: De to bekymringsindeks er konstrueret ved at score (Meget bekymret=4; bekymret=3; Ikke særligt bekymret=2; Slet ikke bekymret=1) og summere besvarelserne for spørgsmålene i de to batterier vedr. deling og brug (ekskl. "ved ikke"- og "hverken-eller "-besvarelser.). De mest bekymrede elever scorer således 4 X antallet af spørgsmålet i batteriet (dvs. hhv. 9 og 6 spørgsmål). De mindst bekymrede elever scorer 1, da de har svaret "slet ikke bekymret" til ét enkelt spørgsmål, mens de til de resterende spørgsmål har svaret enten "ved ikke" eller "hverken-eller").

Ser man imidlertid på forskellen på de elever med *allerflest* rigtige svar (13-16 rigtige) på den ene side og elever med *allerfærrest* rigtige svar (0-3 rigtige) på den anden side, så er billedet en smule anderledes.

Forskellen på graden af bekymring mellem elever, der svarer rigtigt på hhv. 4-12 spørgsmål (mellemgruppen) og 13-16 spørgsmål (gruppen med allerflest rigtige) er nemlig ikke signifikant. Til gengæld er både mellemgruppen og gruppen med allerflest rigtige svar signifikant mere bekymrede end den gruppe elever, der svarer rigtigt på 0-3 spørgsmål (jf. figur 29). **Dette kan indikere, at elever, der ved relativt lidt om datasikkerhed, kun skal højne deres vidensniveau relativt lidt for at blive bekymrede i sammen grad, som de elever der scorer højest i testen om datasikkerhed**.

Figur 29: Prøveresultater opgjort ved antallet korrekte svar krydset med samlet grad af bekymring ved hhv. datadeling og -brug (allerflest vs. allerfærrest rigtige svar)



Klide: Elevsurvey, n=7.048

Note: De to bekymringsindeks er konstrueret ved at værdisætte (Meget bekymret=4; bekymret=3; Ikke særligt bekymret=2; Slet ikke bekymret=1) og summere besvarelserne for spørgsmålene i de to batterier (ekskl. "ved ikke"- og "hverken-eller "-besvarelser.). De mest bekymrede elever scorer således 4 X antallet af spørgsmålet i batteriet (dvs. hhv. 9 og 6 spørgsmål). De mindst bekymrede elever scorer 1, da de har svaret "slet ikke bekymret" til ét enkelt spørgsmål, mens de til de resterende spørgsmål har svaret enten "ved ikke" eller "hverken-eller").

8. PERSONALETS HÅNDTERING AF ELEVDATA

I dette kapitel beskrives, hvordan medarbejderne på institutionerne ser på deres praksis efter databeskyttelseslovens ikrafttræden, og hvilke udfordringer de møder i hverdagen. Disse udfordringer kan være opstået i kraft af nye tiltag, der fx har besværliggjort arbejdsprocesser. Men det kan også være udfordringer forbundet med, at der ikke har været tiltag, der har kunnet sikre arbejdsgangene og større selvsikkerhed i medarbejderens håndtering af elevens persondata.

Der sondres i kapitlet mellem arbejdsgange og udvalgte udfordringer for hhv. administrative arbejdsgange på den ene side og undervisningsrelaterede og pædagogiske arbejdsgange på den anden side. Der trækkes på såvel surveydata som konkrete kvalitative eksempler på håndtering af elevdata.

8.1 PRAKSIS OG UDFORDRINGER FOR ADMINISTRATIVE ARBEJDSGANGE

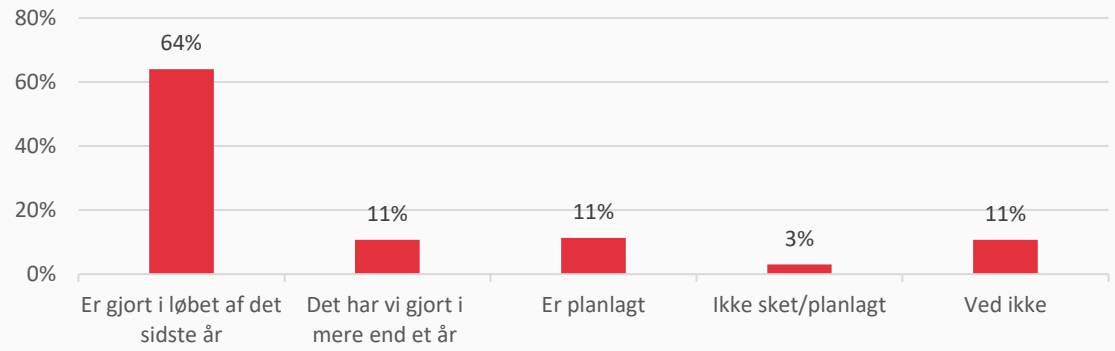
Administrative arbejdsgange skal forstås som arbejdsgange hvori elevdata indgår, der *ikke* knytter sig direkte til undervisningssituationer. De knytter sig derimod til processer som fx registrering, dokumentering eller arkivering. Administrative arbejdsgange foretages således typisk af institutionernes teknisk-administrative personale (fx sekretærer, it-ansvarlige eller ledelse), men også undervisere vil have administrative opgaver, når de fx melder karakterer ind som censorer. Konkrete eksempler på administrative arbejdsgange er:

- Indskrivning af nye elever
- Udstedelse eller arkivering af karakterbeviser
- Fraværsregistrering
- Bortvisninger
- Opbevaring eller udveksling af stamkort
- Behandling af CPR-numre
- Registrering og opbevaring af pårørendeoplysninger

I de fleste tilfælde har de interviewede medarbejdere, når de er involveret i administrative arbejdsgange, ikke været i tvivl om, at den type data, der arbejdes med, kan karakteriseres som elevdata (i modsætning til flere af de datatyper, der indgår i de undervisningsrelaterede og pædagogiske arbejdsgange, jf. forrige kapitel). Det er data, som personalet på institutionerne altid har arbejdet med at arkivere og journalisere, og hermed også har opfattet som data iht. fx persondatalovgivningen. Derfor fortæller de interviewede medarbejdere også, at de er vant til at håndtere oplysningerne relativt systematisk og med blik for datasikkerhed.

Overordnet set fortæller de fleste administrative medarbejdere på casebesøgene da også, at de ikke oplever, at det aktuelle fokus på datasikkerhed har medført *radikale* ændringer i institutionernes administrative arbejdsgange. Flere caseinstitutioner har allerede i en årrække arbejdet med et mere eller mindre intensivt fokus på datasikkerhed. Enten direkte med henblik på at kunne imødekomme databeskyttelseslovens ikrafttræden eller som led i et mere overordnet strategisk fokus på digitalisering og datasikkerhed. I figur 30 kan det ligeledes ses, at **64 pct. af de administrative medarbejdere vurderer, at der er blevet indført nye interne procedurer indenfor de sidste par år for at øge datasikkerheden**:

Figur 30: Hvilke er følgende tiltag er blevet taget på din arbejdsplads med henblik på at øge datasikkerheden? Nye interne procedurer for tjek af sikker datahåndtering



Kilde: Administrativt personale, n=167.

Hos de administrative medarbejdere, der har oplevet, at man har gennemført forskellige sikkerhedstiltag såsom fået sikker, krypteret mail, makuleringsmaskiner og aflåste skabe, viser spørgeskemaundersøgelsen, at det for nogen har haft en positiv effekt i deres daglige arbejde.

58 pct. af de administrative medarbejdere er helt enige eller enige i, at have fået et bedre overblik over de elevdata som de sidder med, og 51 pct. er helt enige eller enige at de har fået større ansvarsfølelse. **Samtidig rapporterer 55 pct., at de er helt enige eller enige i, at tiltagene også har besværliggjort deres arbejde**[38].

Administrationen har traditionelt set haft som daglig opgave at tænke i sikre og standardiserede arbejdsgange. Det harmonerer med, at de på casebesøgene giver udtryk for, at de ofte allerede har fokus på, hvor der er udfordringer med sikkerheden. I nedenstående eksempel fremgår det, hvordan administrationen nok ser, at databeskyttelsesloven medfører en mere besværlig proces mht. eksempelvis udlevering af eksamensbeviser, men allerede tænker konstruktivt imod, at der må findes en sikker løsning – enten gennem digitalisering eller indførsel af nye procedurer:

[38] Spørgsmålsformulering – *"Hvordan har tiltagene påvirket dit daglige arbejde? Det har… "*
Note: Der er ikke nogen klar sammenhæng mellem, hvilke respondenter der har fået større ansvarsfølelse, fået bedre overblik, og vurderer, at det er blevet mere besværligt. Det ene udelukker ikke det andet.

Mobiletnografisk opgave: Tag et billede eller en video af en situation, hvor du synes, at det aktuelle fokus på datasikkerhed har medført, at du er blevet usikker på, hvordan du bør udføre dit arbejde?

Administrativt personale, erhvervsskole: Vi laver rigtig mange beviser. AMU beviser, uddannelsesbeviser osv. Vi er en skole med flere afdelinger, så beviserne sendes her fra studieadministrationen og ud til afdelingerne. Da beviserne ikke er digitale, skal de sendes i papirformat ud til vores afdelinger, og der synes vi håndteringen er lidt besværlig. Hvem må vi sende det med osv.

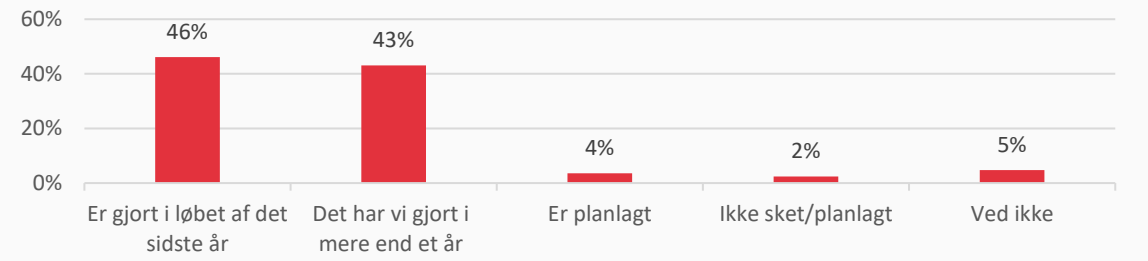
Det ender med, at vi sender det med vores kantine eller en anden medarbejder, når de skal ud på de enkelte afdelinger. Det bliver sendt med dem i en lukket kuvert.
Det nemmeste og sikreste vil jo helt sikkert være at beviserne bliver digitaliseret, så de ikke længere skal printes ud. Ellers mangler vi en hel klar procedure for, hvordan vi håndterer papirgangen mellem afdelingerne.

I det følgende fremlægges de mest centrale tiltag, praksissituationer og mest presserende udfordringer, som kendetegner de administrative arbejdsgange.

8.1.1 Udfordringer med ekstern kommunikation

Både det kvalitative og kvantitative data viser, at der på institutionerne er kommet **øget fokus på at skabe mere sikkerhed, når det gælder kommunikation ind og ud af huset**. Næsten alle fra det administrative personale angiver, at man har øget brugen af krypteret eller sikker mails i sin kommunikation (jf. figur 31).

Figur 31: Hvilke af følgende tiltag er blevet taget på din arbejdsplads med henblik på at øge datasikkerheden? Øget brug af sikker eller krypteret mail (TLS-forbindelse, e-Boks m.v.)



Kilde: Administrativt personale, n=167.

Det er desuden værd at bemærke, at en relativt stor andel (46 pct.) af det administrative personale angiver, at brugen af sikker eller krypteret mail er et tiltag, som institutionen har taget *inden for det seneste år*. Dette bekræfter indtrykket fra caseinstitutionerne og mobiletnografien, hvor netop den

øgede brug af sikre datadelingskanaler fremhæves som et af de mest centrale nye fokusområder for de administrative arbejdsgange efter databeskyttelsesloven.

Mobiletnografisk opgave: Optag en lille film, hvor du viser eller beskriver en arbejdsgang, procedure eller et værktøj, som er blevet indført inden for det sidste år - enten af dig selv eller af ledelsen - som har øget datasikkerheden.

Administrativt personale, erhvervsskole: En af de arbejdsgange, vi har ændret her det seneste år, er administrationen af uddannelsesaftaler. Der er cpr-numre på uddannelsesaftaler, og de blev tidligere sendt med posten, men i dag sender vi dem i e-Boks, netop pga. cpr-nummeret.

Selvom sådanne tiltag medvirker til at gøre deling af elevdata mere sikkert *internt* i organisationen, så er institutionerne også afhængige af at kunne dele data *eksternt*. **Datadeling med eksterne aktører kan af forskellige årsager være vanskelig at håndtere sikkert.** Det kan fx dreje sig om andre institutioner, praktiksteder, andre myndigheder (fx sundhedsvæsenet) eller forældre, hvor enten modtageren eller afsenderen af data ikke har adgang til (eller er klar over, at de har adgang til) sikre datadelingskanaler, som fx sikker mail:

Administrativ medarbejder 1, folkeskole: Forældre kan jo fx ikke modtage sikker mail, så hvordan skal vi sende personhenførbare oplysninger til dem? Lige nu sender vi det typisk til vores skoleleder, og så tager han sig af det på en eller anden måde. Men det er jo ikke holdbart i længden.

Administrativ medarbejder 2, folkeskole: Men det kan også være andre skoler, der ikke er up-to-date endnu. Jeg skulle fx sende nogle oplysninger til en anden skole, der arbejder med et andet system, og der bad modtageren på den anden side mig om at strege alle CPR-numre ud, inden jeg skulle sende det, fordi han ikke havde sikker mail. Det er jo enormt tidskrævende.

Problemstillingen handler således om, at man som institution langt hen ad vejen godt kan sikre sine egne kommunikationskanaler. Samtidigt er de afhængige af, at de eksterne parter (andre institutioner, praktiksteder, forældre m.m.), også kan spille med på institutionens nye kommunikationsveje. Konkret set virker organisationens tiltag hen imod en mere sikker kommunikation kun, hvis de eksterne parter tilsvarende har:

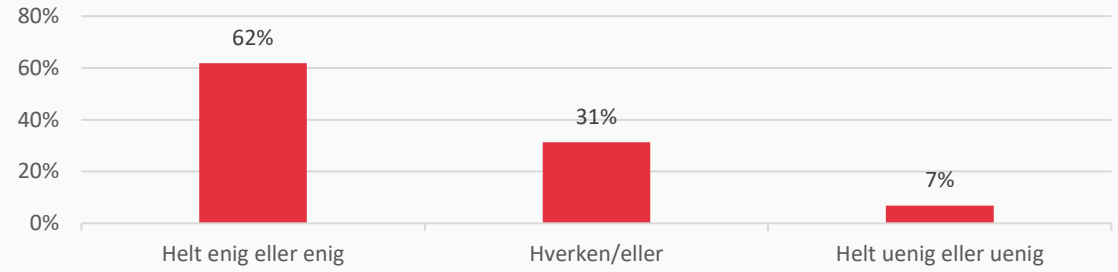
1. Teknisk adgang til at modtage og kommunikere sikkert
2. Viden om, at de faktisk har mulighed for at kommunikere sikkert tilbage
3. Anerkendt vigtigheden af, at man bør kommunikere sikkert om elever

I interviewene har det administrative personales fokus på, at der må gøres "noget" når elevdata deles med aktører, der ikke opfylder disse kriterier. **Det er også ud fra pædagogiske og etiske hensyn, at institutionen ikke bare kan lukke ned for kommunikationen med alle de eksterne parter** og fx nægte at svare fx praktiksteder eller elever, der kommunikerer til dem via usikre mails. Et eksempel kunne ifølge en sekretær på en erhvervsskole være, elever der gerne vil melde sig ind efter fristen for den koordinerede tilmelding udløber på optag.dk (som er en sikker platform) via elevens egen mail, som de føler sig nødsaget til at kommunikere med på - selvom eleverne gør det via forkerte kanaler.

Spørgeskema-resultaterne viser, at der er tale om en relativt udbredt udfordring, når det kommer til at dele data eksternt. Det er ikke blot ift. elever, forældre og praktikvejledere, at sikker deling er

udfordret – det gælder også deling af elevdata med andre myndigheder. **Blandt det adspurgte administrative personale svarer 62 pct. således, at de er helt enige eller enige i, at det i deres daglige arbejde er udfordrende at dele elevdata med andre skoler, institutioner eller myndigheder**, mens kun 7 pct. svarer, at de er uenige eller helt uenige (jf. figur 32).

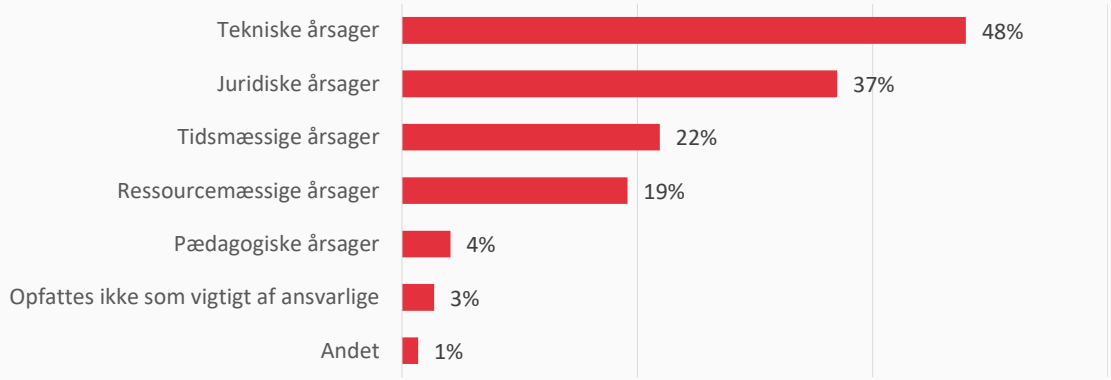
Figur 32: Hvor enig eller uenig er du i, at følgende er udfordrende i dit daglige arbejde, når det kommer til at håndtere elevdata sikkert? At dele elevdata med andre skoler eller myndigheder



Kilde: Administrativt personale, n=118.
Note: Respondenter der har svaret "ikke relevant" indgår ikke i beregningerne

Ud af de administrative medarbejdere, der opfatter deling af elevdata med andre skoler eller myndigheder som en udfordring, peger halvdelen på, at dette skyldes tekniske årsager (figur 33).

Figur 33: Du har skrevet, at følgende er udfordrende. Hvorfor? At dele elevdata med andre skoler eller myndigheder



Kilde: Administrativt personale, n=73.
Note: Kun respondenter der har svaret "Helt enig" eller "enig" til spørgsmålet: "Hvor enig eller uenig er du i, at følgende er udfordrende i dit daglige arbejde, når det kommer til at håndtere elevdata sikkert? At dele elevdata med andre skoler eller myndigheder" indgår i beregningerne.

Samtidigt peger mere end en tredjedel på juridiske årsager og omkring en femtedel på, at det skyldes tidsmæssige - og/eller ressourcemæssige årsager. Men som følgende beskrivelse fra det mobiletnografiske studie illustrerer, så er det ofte også sådan, at når tekniske årsager udfordrer sikkerheden ved at kommunikere ud af huset, **så løses det ofte af medarbejderne ved at skrue op for øget brug af tid og ressource**r:

Administrativt personale i en mobiletnografisk opgave, folkeskole: Så sent som i dag er der en forælder til en tidligere elev, der ringer og spørger til en ordblindetest, der blev taget på eleven af vores vejleder. Den følger eleven via unilogin, men det kan vejlederen på den nye skole ikke finde ud af.

Vi skal så elektronisk hive eleven ind igen (med unilogin) for at trække testen. Vejlederen printer den ud, og går så over ved kontorets printere og sender en pdf til mig. Jeg skal så finde morens cpr frem fra sidste år, for at kunne sende til hendes e-boks, da hun jo ikke har sikker mail. Derefter skal jeg så sende den sikkert til den nye skole. Alt dette tager oceaner af tid. I stedet for at det bare kan drønes afsted på den mail, moren har spurgt på.

I det konkrete tilfælde gør de juridiske rammer dels, at elevens gamle skole ikke længere må ligge inde med data om eleven, og dels at den administrative medarbejder på den gamle skole (fortællingens ophavsperson) ikke må sende data til forældre via almindelig mail. Den tekniske udfordring i at systemer ikke taler sammen, udfordrer således administrationens tilrettelæggelse af arbejdsdagen og opgaveprioritering.

Dilemma:

Det administrative personale oplever i en vis grad udfordringer med at udveksle informationer med eksterne aktører, der ikke har adgang til (eller har viden om, at de har adgang til) samme sikkerhedsløsninger. Derfor opleves der i administrative arbejdsgange til tider at være dilemmaer mellem sikkerhedshensyn på den ene side og etiske hensyn til den enkelte elev, der måske står og skal bruge oplysninger fra skolen "her og nu", på den anden side.

8.1.2 Opbevaring og sletning af fysisk og analog data

Institutionernes fokus på databeskyttelsesloven har medført iværksættelsen af en række konkrete tiltag med henblik på at gøre især de administrative arbejdsgange mere sikre. **Når det gælder data i fysisk form – fx printede dokumenter, lister eller lignende – så er der på de fleste institutioner godt styr på, hvordan de administrative arbejdsgange bør foregå sikkert.** En vicerektor på et gymnasium beskriver eksempelvis, hvordan institutionen har formuleret helt konkrete handlingsanvisninger til sine medarbejdere.

Vicerektor, gymnasium: Vi har lavet nogle retningslinjer med 10 punkter – fx lås altid din computer, dit kontor og de nye kabinetter. Så alle ting kan låses inde, når man går derfra.

Tilsvarende beskriver en erhvervsskoleunderviser i det mobiletnografiske studie sin typiske arbejdsgang, når det gælder sikker opbevaring af elevdata. Eksemplet illustrerer, hvordan mange institutioner har relativt klare procedure for, hvordan personhenførbare fysisk data skal håndteres i de administrative arbejdsgange:

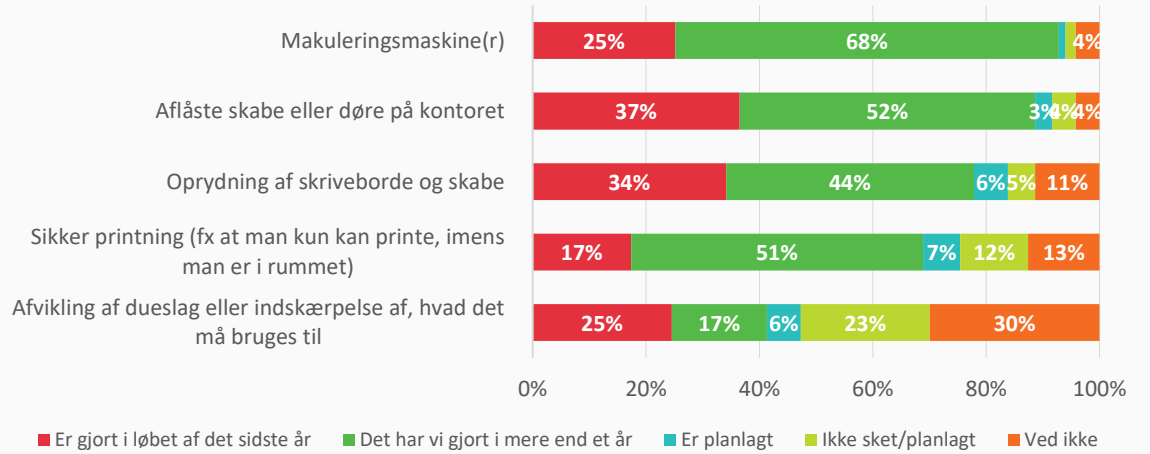
Mobiletnografisk opgave: Forestil dig, at du får udleveret noget elevdata, der er printet på papir og noget elevdata i digital form (fx en pdf-fil). Du får at vide, at du skal opbevare data sikkert. Tag et billede af de steder, hvor du typisk opbevarer disse typer data.

Underviser, erhvervsskole: Jeg har vedlagt et par eksempler på, hvad jeg ville gøre med de printede oplysninger.

1. Gennemse dem og lave en personlig vurdering af vigtighed.
2. Men fordi jeg skulle gemme dem, vil jeg låse dem inde i skuffe eller skab.
3. Eventuelle ikke vigtige vil jeg destruere i makulator.

De kvalitative inputs understøttes af resultaterne fra spørgeskemaundersøgelsen blandt det administrative personale (jf. figur 34). Heraf fremgår det, at **størstedelen af institutionerne i løbet af det seneste år eller tidligere har indført konkrete lavpraktiske foranstaltninger for at øge datasikkerheden.** Langt de fleste institutioner arbejder med makuleringsmaskiner, aflåsning af skabe og døre, oprydning på skriveborde samt "sikker print" for at øge datasikkerheden.

Figur 34: Hvilke af følgende tiltag er blevet taget på din arbejdsplads med henblik på at øge datasikkerheden?



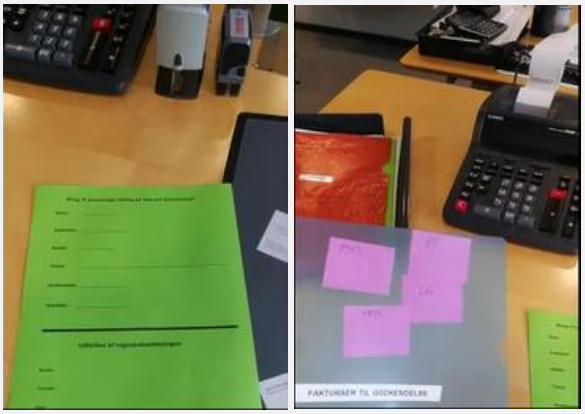
Kilde: Administrativt personale, n=167.

Som det fremgår af resultaterne, er der også tale om tiltag, som mange af institutionerne allerede inden ikrafttrædelsen af databeskyttelsesloven havde foretaget. En administrativ medarbejder beskriver da også i et kvalitativt interview, hvordan de som administrativt personale er "opdraget" og vant til at håndtere den type data forsvarligt:

Administrativt personale, erhvervsskole: Vi har jo fra day one skrevet under på en tavshedspligterklæring. Så det er jo noget, vi er blevet opdraget med. Og vi har jo haft erhvervsret i handelsskolen og sådan. Så det har altid ligget i underbevidstheden, at man fx vender et papir, der ligger på skrivebordet, hvis der kommer nogen ind på kontoret.

Det er også den vanetænkning, der gør, at man tager databeskyttelsesloven alvorligt, og fokuserer på hvordan problemer med deling af data løses, selvom det besværliggør de administrative arbejdsgange. I næste eksempel ses fx hvordan en medarbejder organiserer en simpel ting som, at en underviser skal godkende et elevudlæg, i flere forholdsvis besværlige faser med forskellige opbevaringssteder, for at leve op til databeskyttelsesloven:

Administrativ medarbejder, gymnasium: Vi har jævnligt elever der har personlige udlæg i forbindelse med en fest eller i forbindelse med noget de laver i undervisningen. Og så udfylder de en grøn blanket her hos mig, hvor de skriver navn og klasse på og hvad det er til. Og så skal jeg have deres bankkontooplysninger, for at kunne overføre pengene til dem. Når de har afleveret den til mig, så kan jeg ikke lægge den i den pågældende læreres dueslag, som skal godkende, som jeg før jeg kunnet, da det er fyldt med personlige oplysninger. Så jeg har nu oprettet et chartek, hvor jeg lægger de her bilag ned i og så skriver jeg ud til lærerne at de skal komme ind til mig og godkende udlæggene. For at jeg så derefter kan overføre pengene til eleverne.



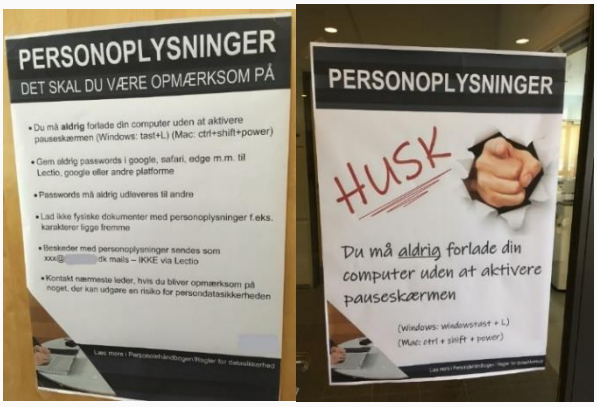
(Kilde: Mobiletnografi, billederne er screenshots fra video)

Kilde: Mobiletnografi. Spørgsmål/opgave: Optag en lille film, hvor du viser eller beskriver en arbejdsgang, procedure eller et værktøj, som er blevet indført inden for det sidste år - enten af dig selv eller af ledelsen - som har øget datasikkerheden.

8.1.3 Sikker opbevaring af *digitale* data

Sikker håndtering af *fysiske* data har længe været en relativt integreret del af de administrative arbejdsgange. **Men de fleste institutioner har i et vist omfang også i de senere år arbejdet med sikker håndtering af *digitale* data via *digitale værktøjer*.** Her er det typisk to grundlæggende parametre ved digitale værktøjer, som institutionerne har fokuseret på:

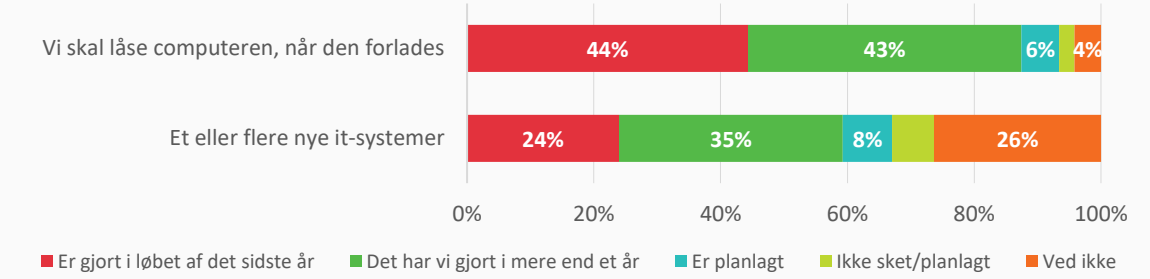
- Dels den **tekniske side af de digitale værktøjer:** Dvs. hvilke muligheder for at skabe bedre sikkerhed, der er teknisk indbygget i et specifikt værktøj og kan udnyttes it-kompetence medarbejdere gennem indstillinger, adgangstildelinger, m.m.
- Dels de **arbejdskulturelle vaner eller adfærd omkring disse digitale værktøjer**: Dvs. hvordan personalet kan arbejde manuelt med sikkerheden omkring det fysiske værktøj, dvs. ikke lade det stå uden opsyn, huske at logge af, ikke vise skærmen til andre, m.m. Disse vaner forsøges på flere af institutionerne at internaliseres vha. påmindelser i kontorer og printerrum, som i nedenstående plakater:



Kilde: Billeder fra casebesøg på gymnasium.

Mht. den tekniske side af de digitale værktøjer svarer 59 pct. af det administrative personale, at der er indkøbt ét eller flere nye it-systemer med henblik på at øge datasikkerheden i løbet af det seneste år eller tidligere. **Mht. de arbejdskulturelle tiltag er det at skulle låse sin computer, når den forlades et godt eksempel på, hvordan nogle institutioner arbejder med at øge datasikkerheden gennem opdyrkning af nye vaner**. Her svarer hele 87 pct., at dette tiltag er blevet ekspliciteret i løbet af det seneste år eller tidligere (jf. figur 35).

Figur 35: Hvilke af følgende tiltag er blevet taget på din arbejdsplads med henblik på at øge datasikkerheden?



Kilde: Administrativt personale, n=167.

Der er således et fokus på at øge muligheden for sikker digital opbevaring og deling, og hvordan administrationen i deres praktiske omgang med computere og kopimaskiner, også skaber sikkerhed igennem omtanke og vaner.

Generelt tilstræbes en øget digitalisering i de administrative arbejdsgange, da det forbindes med øget sikkerhed. En af caseinstitutionerne arbejder fx på at blive fuldstændig papirløs. Sådanne bestræbelser er dog ikke uden udfordringer. **Nogle gange er det dog også sådan hos administrationen, at brugen af sikre it-systemer bliver så udfordret, at man paradoksalt nok går tilbage til de mere analoge processer.**

8.1.4 Dataopbevaring og tidsfrister

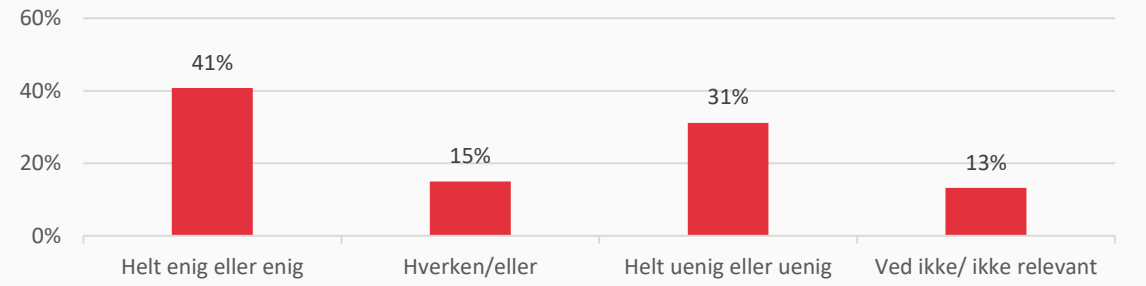
Hvad enten persondata om eleverne opbevares fysisk eller digitalt, så er der nogle fælles udfordringer ift. at have klar viden om i hvor lang tid forskellige typer af data generelt må – eller skal – opbevares. Fx skal elevens personlige og følsomme persondata som udgangspunkt slettes efter udmelding, imens deres karakterbeviser og udtalelser skal opbevares fremadrettet, hvis der skulle komme henvendelser herom eller eventuelt af hensyn til forskellige lovgivningers krav om dokumentation.

FAKTABOKS: Hvad er tidsfristerne for, hvornår forskellige data skal slettes?

GDPR kræver, at data skal slettes eller anonymiseres, når der ikke længere er behov for at opbevare dem i personhenførbar form. Det er derfor ikke nødvendigt med en specifik slettefrist til de forskellige persondata, men dog nødvendigt med en velbegrundet slettepolitik.

Som det ses i figur 36, er **4 ud af 10 administrative medarbejdere enige eller helt enige i, at de mangler viden om, hvor længe forskellige datatyper må opbevares** i henhold til lovgivningen:

Figur 36: Hvor enig eller uenig du er i, at du mangler viden om… i hvor lang tid forskellige datatyper må opbevares?



Kilde: Administrativt personale, n=167.

På nogle institutioner er man også blevet opmærksom på udfordringer mht. sletning af elevdata. Det har nogle steder medført både tekniske og adfærdsorienterede tiltag, der har til formål at sikre systematisk oprydning og sletning af digitale data. Dette gælder særligt når det kommer til at få ryddet op i sin mailindbakke:

Interviewer: Hvad så når folk sender oplysninger til jer vedrørende elever?

TAP, erhvervsskole: Vi har lavet det sådan på SharePoint, at der er en mappe per elev. Når informationer sendes på mail til os, så smider vi det på SharePoint og sletter mailen.

Vicerektor, gymnasium: I vores mail har vi fået gjort det sådan, at man kan markere mails med personfølsomme oplysninger, som bliver markeret fortrolig og slettes automatisk efter 30 dage.

Ovenstående citater afspejler, hvordan man kan lave tekniske procedurer, der fremadrettet kan hjælpe medarbejderen med at sørge for at data ikke ligger i uhensigtsmæssig lang tid. Dette gælder

dog mails, hvor den enkelte medarbejder hver dag åbner op og kan forventes at have overblik, samt har et klart ansvar for oprydning.

Andre datatyper er sværere at håndtere, både pga. størrelsen på datamængden og måden hvorpå de traditionelt har været opbevaret gennem årerne. Et eksempel på en sådan type kunne være fraværsdata:

Viceerektor, erhvervsskole: Fraværsdata kommer i et administrativt system, så vi kan se hvilke dage og hvilke timer elever har fravær i. Den type digitale data er der i lang tid. Lovmæssigt skal vi have det i 5 år, men det er der i længere tid. Jeg tror, man er nødt til at slette det manuelt.

Som viceerektoren her peger på, så har flere institutioner igennem året opsamlet en stor historisk mængde data. Uanset om den er opbevaret i digital eller analog form (typisk arkivskabe), kræver det en større manuel gennemgang. Sådanne datatyper kan – alt efter det lokale arkiveringssystem – tænkes at være filtret sammen med andre datatyper, hvor andre tidsfrister gælder. I den sammenhæng vil manuelle gennemgange derved også kræve stillingtagen til, hvad der skal slettes nu, hvad der skal gemmes, og på hvilken ny måde man skal gemme det teknisk, ift. at lette fremtidige gennemgange.

Generelt er der tale om et stort oprydningsarbejde, som institutionerne først oplever at kunne gøre noget ved, når de har dannet sig overblik over reglerne for data og for tidsfrister, og evt. har et nyt, gennemtænkt arkiveringssystem, at overføre data til.

8.1.5 Indhentning af samtykkeerklæringer til markedsføring og brug af billeder

Markedsføringsdata er i denne sammenhæng oplysninger om eleverne, som bruges i aktiviteter, der har til hensigt at tiltrække nye elever til institutionen. På caseinstitutionerne har der typisk været tale om billeder af elever i undervisningssituationer, til gallamiddage, på studieture eller lignende, der skal signalere et attraktivt miljø på institutionen.

Der er på flere caseinstitutioner udpeget en medarbejder, som er ansvarlig for at lægge billederne op på institutionens hjemmeside eller på sociale medier. Typisk bliver billederne dog også taget af andre undervisere eller sågar af elever, når situationerne opstår. Herefter videregives billederne til den markedsføringsansvarlige medarbejder, der fx lægger billederne op på institutionens hjemmeside.

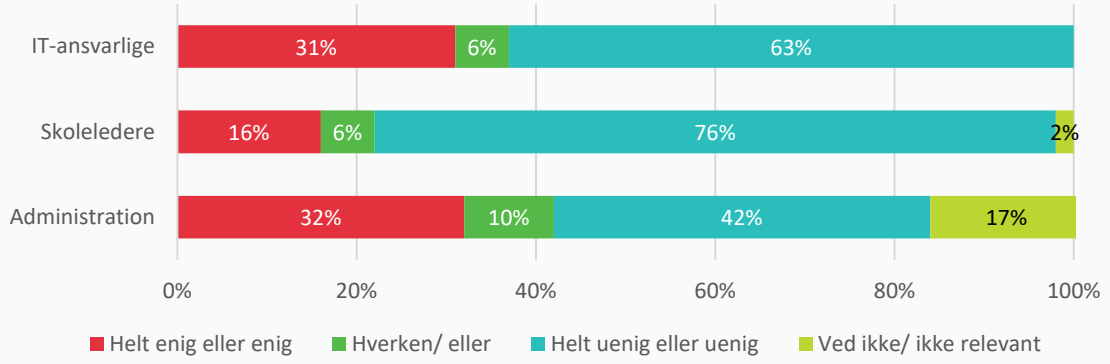
De fleste af caseinstitutionerne er særligt efter databeskyttelsesloven og diverse nyhedshistorier blevet opmærksomme på, at billedmateriale af eleverne kan udgøre en udfordring iht. databeskyttelsesloven. Derfor er der flere steder indført nye rutiner og procedurer for, hvordan denne type elevdata håndteres teknisk og praktisk – at man fx skal bruge institutionens officielle kameraer i stedet for sin egen mobil, hvis man tager billeder af elever i undervisningen. Selvom der indføres restriktioner og ressourcekrævende, nye arbejdsgange til fx at indhente samtykke fra de elever, der måtte optræde på billeder, så kan det stadig opleves som en udfordring for institutionerne at fortolke, hvilke slags billeder der er tale om fra tilfælde til tilfælde:

Vicerektor, gymnasium: Så vidt jeg forstår, er der en kattelem omkring situationsbilleder. For i praksis kan vi nærmest selv beslutte, hvad der er situationsbilleder. Men der burde jo være en vejledning. Man kan jo ikke bare sige, at det skal vi selv finde ud af. Så kan vi jo komme frem til, at alt er situationsbilleder.

Citatet illustrerer et billede som tegner sig på flere caseinstitutioner. **Der kan være udfordringer med juridisk at tolke og skelne mellem situationsbilleder og portrætbilleder, samt i forlængelse heraf at finde ud af, hvornår et billede kræver samtykke fra eleven eller ej.** Vicerektoren ovenfor oplever eksempelvis ikke, at der findes tilstrækkeligt klare kriterier for, hvornår et billede kan karakteriseres som hhv. et situations- eller portrætbillede, og oplever usikkerheden som frustrerende.

I spørgeskemaerne på tværs af vores respondentgrupper ses det, at 32 pct. af det administrative personale er helt enige eller enige i, at de mangler juridisk viden om de betingelser, hvorunder man skal håndtere elevbilleder (jf. figur 37):

Figur 37: Hvor enig eller uenig du er i, at du mangler viden om… under hvilke betingelser man må bruge billeder af eleverne?



Kilde: Administrativt personale, n=167; Skoleledere, n=382; kommunalt it-ansvarlige, n=35.

På nogle caseinstitutioner har man, som en konsekvens af denne usikkerhed omkring fortolkning og for at sparre på ressourcer ift. indhentning af samtykke, valgt at gardere sig ved at indhente skriftlige samtykkeerklæringer fra samtlige elever. Det fungerer på den måde, at eleven i begyndelsen af skoleåret giver samtykke til, at institutionen må tage og bruge billeder af vedkommende.

Administrativt personale, gymnasium: Alle skal udfylde en 4-siders samtykkeerklæring, inden de starter på skolen. […] De [eleverne] bliver orienteret om, hvordan skolen håndterer data, billeder m.m. At billeder kan ryge på [socialt medie]. Også at de til enhver tid kan få billedet taget af [socialt medie]. Der er også et billede af eleven i [læringsplatform], så læreren kan se klassen og lære navne.

På trods af denne procedure kan det dog fortsat være en udfordring at håndtere elevbillederne retmæssigt. For som det påpeges af en administrativ medarbejder, så er det ikke altid, at de markedsføringsansvarlige er klar over, hvem der faktisk er på billedet. Derfor kan det i praksis være vanskeligt at undgå, at der bliver lagt billeder op af elever på institutionens hjemmeside eller profil på sociale medier, der ikke har givet samtykke til, at institutionen må bruge billeder af eleven til markedsføringsformål.

Administrativt personale, gymnasium: Men det kræver jo, at man ved hvem, der er hvem – man kan sagtens komme til at lægge billeder op af nogen, som man ikke ved, hvem er. Men vi siger også til elever, at de endelig skal komme og sige, hvis der er noget, de vil have taget af. Men fx med [socialt medie] kan det selvfølgelig være svært at tage et billede af igen, hvis det først er lagt op.

Den administrative medarbejder i ovenstående citat reflekterer samtidigt over, at det kan være vanskeligt at fjerne ting permanent fra internettet. Det kan fx være blevet delt andre steder, og sociale medier ligger måske fortsat inde med billedet, selvom det er slettet fra profilen.

Dilemma:

Billeder som personhenførbare data om eleverne opfattes på flere institutioner som kilde til usikkerhed. På nogle institutioner har man løst udfordringen ved at bede om samtykkeerklæringer fra samtlige elever i begyndelsen af skoleåret. Men som det også bliver påpeget medfører denne formaliserede løsning en mere lavpraktisk udfordring mht. i praksis at administrere og agere efter, hvilke elever der har hhv. givet/ikke givet samtykke til brug af billeder af dem. Særligt på større institutioner vil det være vanskeligt for den enkelte medarbejder (fx hjemmesideansvarlige medarbejder) at holde overblik over, hvem der har/ikke har givet samtykke.

En anden tilgang, der imødegår denne udfordring, er at fokusere indhentningen af samtykkeerklæringer på udvalgte elever - i modsætning til at bede om samtykkeerklæringer fra alle. En it-ansvarlig for en case-erhvervsskole beskriver, hvordan det øgede fokus på persondata har ført til en mere selektiv praksis:

It-ansvarlig, erhvervsskole: Vi gør brug af samtykkeerklæringer i markedsføringsafdelingen, hvis de fx tager billeder. Vi gør det nu, at vi vælger nogle elever ud. Og det er en ændring i proceduren for, hvordan der bliver taget billeder af eleverne. De få, der bliver fotograferet, har nu samtykket til det. Vi tager ikke bare billeder som før.

Fx skal vi afholde et skilz-arrangement. Her udvælges så en klasse, der må tages billeder af. Nu tænkes der over, at det er dem, der bliver brugt, og dem der bliver fulgt hele dagen. Før ville man løbende have taget billeder af det hele

På et af casegymnasierne har man, som en konsekvens af det større fokus på datasikkerhed, valgt en helt tredje strategi. Her har man nemlig besluttet at anvende stock-fotos hvor det giver mening (hvis der fx skal bruges et portrætbillede af en student til markedsføringsindsatser på hjemmesider eller i publikationer). Den administrative medarbejder, som sidder med markedsføringen på dette gymnasium, beskriver dog alligevel, at de i nogle situationer gerne vil bruge billeder, de selv tager, fx i forbindelse med konkrete arrangementer på institutionen. I disse situationer er de fortsat i tvivl om, hvordan de reelt skal håndtere det:

Administrativt personale, gymnasium: Ofte skal vi have samtykkeerklæringer. Vi ville normalt gerne have mange billeder, men nu er vi begyndt at begrænse antallet, og så får vi kun de samtykkeerklæringer, vi har brug for. Vi er i stedet begyndt at gøre brug af "shutterbox" og "colourbox" [-modeller], hvor man kan købe billeder. Men hvis vi har noget, vi skal bruge i annoncer, så indhenter vi også samtykkeerklæringer.

Hvis vi har haft fællesarrangementer, så vil vi også gerne tage billeder, og dér er det meget genkendeligt, så der skal vi også begynde at lave samtykkeerklæringer. Så fremadrettet bør vi have samtykkeerklæring på sådan noget, tænker vi. Og her kunne man godt tænke sig nogle retningslinjer. Gør alle skoler det? Der er andre gymnasier, der smider mange billeder op, hvor man godt kan tvivle på, hvorvidt de har samtykkeerklæringer fra alle.

På andre caseinstitutioner opfattes det som tilstrækkeligt, hvis underviseren får elevens mundtlige samtykke, inden billedet tages. På en caseinstitution beskriver en underviser fx, hvordan vedkommende aldrig har opfattet det som problematisk at tage billeder af eleverne, så længe eleven mundtligt går med til det. Det er derimod en praksis, som vedkommende ofte gør brug af, som han her beskriver:

Underviser, folkeskole: Vi var fx på tur og tager billeder af eleverne ved Nyhavn, Amaliehaven, Den lille havfrue og osv. osv. – billeder af forskellige situationer og ting. Og der er jo både elever og lærere med på de her billeder. Og hvis det er fuldstændigt ulovligt, så er der mange, der bryder loven. De ligger på min egen mobil, indtil eleverne går ud. Og de kan også ligge på computeren. Så sletter jeg dem, når de går ud.

Citatet belyser desuden endnu en potentiel udfordring, som er blevet påpeget på flere af case-skolebesøgende, nemlig at **nogle medarbejdere typisk bruger deres private mobiltelefon til at tage billeder af eleverne**. Nogle undervisere beskriver, at de sletter billederne, når de er lagt op på hjemmesiden eller lignende – eller som i ovenstående, når eleverne er gået ud. Men andre fortæller, at de ikke har en fast procedure for, at de ikke har nogen fast procedure for sletning af elevbilleder på deres private telefon.

FAKTABOKS: Hvad siger loven om at tage billeder af elever på ens private telefon?

Hvis læreren tager et portrætbillede til brug for sin undervisning eller for at markedsføre skolen på hjemmesider og sociale medier, skal der indhentes samtykke til offentliggørelsen. Hvis der derimod er tale om et situationsbillede kan billedet – alt efter konteksten – offentliggøres uden samtykke, da det er et legitimt hensyn for skolen at markedsføre sig selv online. Læreren og skolen skal dog være opmærksomme på, hvordan den enkelte elev er udstillet på billedet, fordi eleven kan anmode om at få billedet slettet, hvis eleven føler sig krænket over, hvordan man er udstillet. Derudover bør læreren være opmærksom på, at lærerens private telefon muligvis ikke er sikker til opbevaring.

Læreren bør altid oplyse eleverne på forhånd, hvis denne har tænkt sig at tage et billede med henblik på offentliggørelse.

Hvis læreren derimod tager billedet på en studietur eller et fagligt arrangement udelukkende til privat brug som et personligt minde, er man uden for GDPR's anvendelsesområde – også selvom man anvender en privat telefon.

Dilemma:

Flere undervisere beskriver, hvordan de typisk bruger kameraet på deres private telefon til at tage billeder af elever i undervisningssituationer. Dermed opstår et dilemma, der handler om hvorvidt underviserne må bruge deres egen telefon til at tage og opbevare billeder af eleverne – fx for at samle gode minder fra en ekskursion eller en lejrskole med henblik på senere at dele minderne med eleverne.

8.1.6 Tvivl om sikkerhedsniveau på centrale administrative systemer

En overordnet udfordring, handler om, at institutionerne i senere år har flyttet flere af deres aktiviteter over på få, samlende platforme og datadelingsløsninger. Samlingen af aktiviteterne og data gør arbejdsgangene effektive og overskuelige for personalet, da den digitale indgang til data dermed indsnævres til én eller få platforme.

Men det gør samtidigt arbejdsgangene sårbare, såfremt disse ikke møder de nye sikkerhedskrav. Der er blevet investeret tid og ressourcer i licensaftaler, implementering og kompetenceoprustning i disse løsninger, og det ville være en besværlig og dyr proces, at finde nye alternativer.

I følgende citat fortæller en administrativ medarbejder om udfordringerne ved at have bundet sig på en leverandør. Medarbejderne har svært ved at vurdere, hvorvidt løsningen lever op til de nye sikkerhedskrav.

Administrativt personale, gymnasium: Når vi taler om elevdata og opbevaring af det, så er vores primær redskab [læringsplatform]. Her foregår al vores kommunikation med elever via et mail-system. Og det har selvfølgelig begrænset sig noget, hvor meget man kan udtrykke sig der. Så ofte er man nødt til at skrive til eleverne at de skal komme ned, så man kan sige tingene til dem i stedet for.

Opbevaring af elevdata handler om personlige oplysninger, hvilke klasser, fag, studieretninger de går i, karakterer, værgeoplysninger, al den form for oplysninger.

Vi ved ikke, om vi bliver ved med at bruge [læringsplatform], for det er ikke sikkert. De har godt nok – så vidt jeg ved – underskrevet en databehandleraftale, men [læringsplatformen] er ikke specielt lukket.

Men jeg kunne forestille mig I har hørt om problemet før. Det jeg så er begyndt at gøre nu, når jeg skal kommunikere med eleverne, det kunne være elever, som får støtte til studieture eller af personlige årsager skal oplyse bankkonto oplysninger, der er jeg begyndt at sende dem beskeder i e-Boks eller kalde dem ned på kontoret – bare skrive, om de ikke lige vil kigge end til mig. Det er blevet lidt omstændeligt.

Kilde: Mobiletnografi. Spørgsmål/opgave: Forestil dig, at du får udleveret noget elevdata, der er printet på papir og noget elevdata i digital form (fx en pdf-fil). Du får at vide, at du skal opbevare data sikkert. Tag et billede af de steder, hvor du typisk opbevarer disse typer data.

Dilemma:

Der er store ressourcemæssige fordele ved at samle flere funktioner i én eller få digitale løsninger. Men når først personalet har "vænnet" sig at bruge denne/disse, så vil det kunne have store ressourcemæssige konsekvenser at skifte løsning. Derfor oplever nogle skoler det som et dilemma, når der til en sådan løsning florerer rygter om, at løsningen ikke lever op til krav om it-datasikkerhed. Skal man som skoleleder prioritere løsningens it-sikkerhed eller de store ressourcemæssige fordele det har fortsat at anvende den etablerede løsning?

Fordelen ved platformen har tidligere været, at man kunne have et samlet overblik over udmøntningen af undervisningen alt inklusive, samtidig med at man kunne kommunikere samlet omkring platformen. **Med det øgede fokus på sikker kommunikation er platformens fordele blevet mindre, og der foretages kommunikative tiltag udenom platformen.** Flere caseinstitutioner i undersøgelsen afventer at få mere sikker viden om "hvor lukket" denne platform er, ift. databeskyttelseslovens krav, og afventer en aktiv stillinstagen til sagen længere oppe i systemet.

8.2 PRAKSIS OG UDFORDRINGER FOR UNDERVISNINGSRELATEREDE OG PÆDAGOGISKE ARBEJDSGANGE

I dette afsnit beskrives institutionernes praksis og udfordringer mht. undervisningsrelaterede og pædagogiske arbejdsgange. Undervisningsrelaterede og pædagogiske arbejdsgange foretages i udgangspunktet af institutionernes undervisere og er kendetegnet ved den aktive inddragelse af viden i forbindelse med at undervise eller formativt evaluere eleven og elevens læring, trivsel og udvikling. Der kan konkret være tale om arbejdsgange, der vedrører:

- Undervisning
- Planlægning og afholdelse af studieture
- Bedømmelser af og feedback på faglige opgaver
- Censoropgaver
- Pædagogisk håndtering af elevers personlige eller familiære udfordringer
- Udarbejdelse af elevplaner o.l.
- Skole-hjemsamtaler
- Opbevaring og udveksling af faglige produkter, fx en stil

Overordnet set varierer det på tværs af caseinstitutionerne, hvor opmærksomme underviserne generelt er på datahåndtering og datasikkerhed. **I forlængelse af de foregående afsnit er det administrative personale mere fokuseret på datasikkerhed end det pædagogiske personale er.** En forklaring, der italesættes blandt det administrative personale, er, at de sammen med ledelsen altid har haft som en kerneopgave at skulle forholde sig til dét, som databeskyttelsesloven nu blot sætter yderligere fokus på og krav for: Standarder for registrering, deling, arkivering og opbevaring af data om elever. Selvom disse procedurer nu bliver mere digitaliserede, og informationer nu i højere grad omtales som "data", så er principperne og tilgangen for personalegruppen stadig den samme. **Når det kommer til underviserne, kan der tales om en anden fagkultur og profession, som historisk set har haft en mere autonom tilgang til deres arbejdsgange, og hvis kerneopgave ikke er registrering og arkivering, men undervisning, læring og udvikling**.

Viceerektor, gymnasium: Her er en gruppe mennesker, der er relativt afslappede. Folk tænker ikke i de baner. De vil gerne rykke deres elever, og de synes ikke, at administration, skemaer osv. er noget, de har valgt eller prøvet at finde hoved og hale i. Hvis de bare kan få at vide, hvad de skal, så er de glade. De vil gerne lære deres elever noget.

På nogle af caseinstitutionerne beskrives det på den ene side, hvordan underviserne allerede har været igennem en proces eller er ved at tage tilløb hertil, der har til formål at rydde op i undervisningsrelateret elevdata – fx makulere dokumenter eller slette gamle opgaver, som ikke længere bliver brugt. **Men på den anden side beskriver flere undervisere, at der stadig er nogle områder af databeskyttelsesloven, der står uklart for dem. I den forbindelse er det særligt uklart hvilke typer af faglige bedømmelser og produkter, der skal håndteres med blik for databeskyttelsesloven.** Ikke mindst, hvorfor noget der kan virke ufarligt, som opbevaringen af en elevopgave hjemme i skuffen, skal skabe så meget besvær.

FAKTABOKS: Hvornår er elevers faglige bedømmelser og produkter persondata?

EU-domstolen har slået fast, at selve indholdet af en eksamensbesvarelse og opgave kan anses som persondata, fordi indholdet af besvarelsen afspejler eksaminandens "*viden og kompetence inden for et givent område samt i givet fald [elevens] tankegang, dømmekraft og kritiske sans.*" Domstolen har også slået fast, at "*i tilfælde af, at prøven skrives i hånden, indeholder besvarelserne tillige oplysninger vedrørende [elevens] håndskrift.*"[39]

I det følgende gennemgås tre centrale fokusområder for de undervisningsrelaterede arbejdsgange, der skaber udfordringer ift. håndtering af elevernes persondata.

8.2.1 Anonymisering og sletning af gamle opgaver

Gamle opgaver gemmes typisk af pædagogiske eller læringsmæssige hensyn og bruges af underviserne til at vise eksempler på "den gode besvarelse" til eleverne. Denne praksis beskrives dog på flere caseinstitutioner som en central kilde til tvivlstilfælde og generel usikkerhed omkring, hvor grænserne for datasikkerhed går.

Opgaverne kan dels indeholde almindelige personoplysninger om eleven (navn, klassetrin, cpr-nummer o.lign.), men vil også kunne indeholde personlige oplysninger, der knytter sig til det indholdsmæssige i opgaven – fx en danskstil om "min barndom" eller en samfundsfagsopgave, hvor elevens politiske holdninger eller religiøsitet kommer til udtryk. På flere institutioner er underviserne derfor blevet bedt om at slette eller anonymisere gamle opgaver:

Underviser 1, gymnasium: Det, vi blev bedt om, var at gennemgå og fjerne ting, vi havde derhjemme, der var mere end et år gammelt – opgaver osv. … Eller i hvert fald anonymisere det.

Underviser 2, gymnasium: Ja, det kan være eksemplariske opgaver fx. Og hvis vi VILLE beholde det, så skulle det anonymiseres. Men det kan være rart som lærer, at man har de her opgaver liggende til at sammenligne – er den her for eksempel til 7 eller til 12?

39 pct.[40] af de adspurgte undervisere svarer i spørgeskemaundersøgelsen, at deres institution har procedurer for, hvordan elevernes faglige produktioner skal opbevares. Dette indikerer dermed på den ene side, at der i et vist omfang er fokus på, at også denne type elevoplysninger kan være relevant "data" iht. databeskyttelsesloven.

På den anden side kan også ses, at der blandt underviserne ikke nødvendigvis er ønske om et større fokus på at institutionen standardiserer procedurerne for opbevaring af opgaver**. Blandt de 61 pct. af undervisere, der har angivet, at der ikke er procedurer på deres institutioner for opbevaringen af faglige produkter, er det 25 pct.[41], der kunne tænke sig at institutionen indførte sådanne procedurer.**

[39] Sag C-434/16 (Nowak-dommen)
[40] Spørgsmålsformulering – *"Har I på skolen procedurer for, hvordan oplysninger om eleverne håndteres"*
[41] *Spørgsmålsformulering – "Kunne du tænke dig , at I på skolen indførte en eller flere af følgende procedurer: Hvordan elevernes faglige produktioner skal opbevares"*

At en større andel af underviserne ikke oplever, at institutionen har indført procedurer for opgaveopbevaring og blot et mindretal kunne tænke sig, at institutionen gjorde det, kan hænge samme med, at faglige produktioner blandt flere undervisere opfattes som et gråzonetilfælde. Underviserne beskriver på caseinstitutionerne, at man altid har arbejdet med elevernes faglighed relativt åbent over for hinanden – fx elevernes bidrag til gruppearbejder og gennem fremlæggelser – og at det derfor ikke er intuitivt at tænke på deres produkter som "data". Nedenstående uddrag fra et kvalitativt interview illustrerer, hvordan en leder undervejs i interviewet bliver opmærksom på, at de på institutionen måske har overset faglige produktioner som elevdata:

Interviewer: Har i lavet nogle retningslinjer eller talt med lærere om elevopgaver, hvor der måske er personfølsomme ting i?

Leder, erhvervsskole og gymnasium: Det har vi ikke retningslinjer om, hvad de må. Vi har altid taget stile med hjem, man har altid haft det med i tasken. Men det som du formulerer dér, kunne man godt have retningslinjer om. For ja, danskstile kan meget nemt indeholde personfølsomme ting.

Interviewer: Hvad med gamle stilehæfte, opgavebøger. Hvem har det?

Leder, erhvervsskole og gymnasium: Det har de [lærerne] selv. Engang imellem rydder de op, og det bliver smidt ud i skraldespande. Men det kunne man da godt tænke over. Vi har jo ikke en skraldespand, der kan låses. Det kan man få nu. Det er jo faktisk elevens data og elevens ejendom.

Men selv på nogle af de institutioner, hvor underviserne *er* opmærksomme på, at elevernes faglige produktioner kan opfattes som elevdata, opfattes det ikke nødvendigvis som meget presserende at behandle det som sådan i praksis. I nedenstående uddrag peges der også på, at der dels kan være tale om en ressourcemæssig udfordring, da **det kan opleves som en tidskrævende opgave at efterleve krav om at slette eller anonymisere opgaver**. Men uddraget illustrerer også en pointe, som kommer til udtryk af flere undervisere under casebesøgene, nemlig at nogle undervisere har vanskeligt ved at forstå begrundelsen for, hvorfor gamle opgaver i det hele taget skal slettes eller anonymiseres:

Underviser 1, gymnasium: Jeg ved, at jeg ikke arbejder helt inden for lovgivningen. Men jeg er ved at gøre antræk til at gøre det, for det tager jo en hel ferie at rense computeren for elevnavne osv.

Underviser 2: Altså jeg har også opgaver med elevnavne liggende stadigvæk. Men hvis jeg nu bruger dem, så fjerner jeg navnene først og anonymiserer dem, når jeg viser de gode eksempler til andre elever.

Underviser 1: Men du må jo faktisk heller ikke gemme det under et navn – "Mogens fra '87, der skriver så godt"

Underviser 2: Nej, det ved man jo godt. Vi har jo fået at vide, at vi i princippet ikke må have sådan noget liggende. Men tror du, det bliver overholdt? Jeg synes, det er rart at gemme opgaver, som er fremragende. Men jeg gemmer jo ikke de dårlige. […] De fleste elever er jo sådan lidt halvstolte, når jeg nogle gange spørger, om jeg må bruge deres opgave.

Nogle undervisere peger – som i ovenstående uddrag – på, at eleverne oftest opfatter det som en anerkendelse, at få vist et fagligt produkt frem som det gode eksempel. Andre peger på, at indholdet i faglige produktioner oftest næppe kan karakteriseres som følsomme persondata eller "farlig" data, som en underviser udtrykker det (fx en matematikaflevering eller en fysikrapport).

Dilemma:

Flere undervisere er i tvivl om, hvorvidt faglige produktioner skal håndteres som data. Der hersker da også forskellige tolkninger heraf, men ikke desto mindre beskriver flere lærere det som en central udfordring for dem – dels at skulle gøre noget ved (pga. rent ressource-/tidsmæssige forhold), men i endnu større grad, fordi underviserne har svært ved at forstå, hvorfor det er relevant. Underviserne opfatter det således som et dilemma mellem de pædagogiske fordele ved at gemme gamle opgaver på den ene side, og de institutionelle retningslinjer om sletning af gamle opgaver, som flere institutioner har indført, på den anden side.

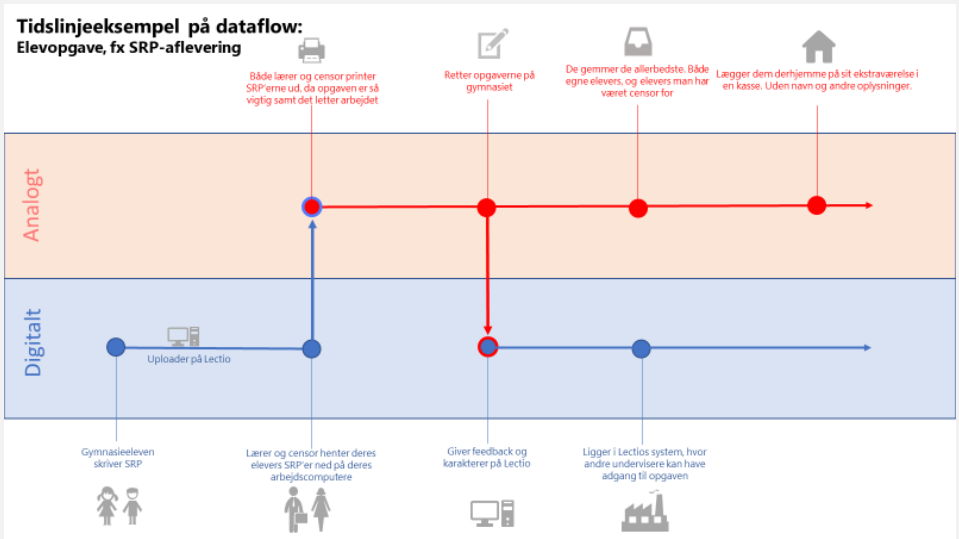
Nogle undervisere peger desuden på, hvordan opgaver over tid kan antage både digitalt og analogt format, hvilket øger mængden af data, man skal efterse og sikre. Til at illustrere dette, ses der nedenfor et interviewuddrag og en visualisering af en SRP-opgaves dataflow, som afspejler et typisk forløb omkring aflevering og vurdering af en SRP-prøve. Beskrivelsen illustrerer samtidigt omfanget af den række af systemer og procedurer, som der skal bruges ressourcer på at efterse, når en opgave afleveres:

Underviser 1, gymnasium: En elev skriver en stil. Afleverer stilen via [læringsplatform] til læreren. Læreren henter den ned på computeren både privat eller på skolecomputer. Stilen lægges ind på [cloud]. Den kunne også godt lægges privat, hvis man ville. Læreren retter og læser stilen på computeren. Nogle lærere kan godt finde på at printe stilen ud – især med årsprøver… der skal være særlig anledning. Når der printes, kan der bedre skrives længere kommentarer. Eller hvis der er særlige pædagogiske hensyn, som at de skal overstrege alle deres citater med grøn, så de synligt og tydeligt kan se, hvor få citater de har med.
Herefter uploades den rettede opgave på [læringsplatform]. Jeg ved ikke, om den slettes, eller om det stadig ligger der. Lærerne sletter den i hvert fald ikke. De [opgaverne] ligger der i hvert fald i de tre år, eleverne går på skolen. Hvis opgaven er blevet printet, så lægges den i en kasse på ekstraværelset derhjemme.
På [læringsplatform] kan man også se andre elevers opgaver – andre end sine egne elevers. Det kan man bruge, hvis man fx overtager et hold, hvor man skal samle op og se, hvad de tidligere har afleveret og fået respons på i 2.g, og hvordan der skal samle op i 3.g. Andre lærere går typisk ind og ser karakterer i [læringsplatform] – af samme grund.

Underviser 2, gymnasium: Jeg har også store mængder SRP'er og DIO-opgaver liggende derhjemme

Underviser 3, gymnasium: Det har jeg også. Men så er navn, personnummer og skole streget ud med tusch.

Underviser 2, gymnasium: Jeg har også [opgaver] liggende fra andre skoler, hvis jeg har været ude og være censor. Særligt gode opgaver. Men jeg printer også synopser ud, når jeg skal være censor, så jeg kan være klar til den mundtlige del og ikke sidde med en computerskærm. Jeg skal kunne sætte gule streger osv. på printet.



Som det kan ses i eksemplet, bevæger opgaven sig igennem formater og duplikeres undervejs. Den lagres potentielt på underviserens og censorens arbejdscomputer, på læringsplatformen og i diverse analoge udskrifter og kopier. Sådanne kopier kan så igen ligge flere steder, fx i underviseres dueslag eller i underviserens hjemmearkiv som "det eksemplariske opgaveeksempel".

Underviser, gymnasium: Der er nogle gange, at eleverne printer en stil og lægger den i dueslag og så ligger den jo frit for alle. Nogle lærere kræver, at de bliver printet ud faktisk.

8.2.2 Deling af følsomme personoplysninger om elever

Ud fra et pædagogisk hensyn kan det være hensigtsmæssigt, at det pædagogiske personale deler viden om elever, som oplever sociale eller personlige udfordringer, der kan have indflydelse på, hvordan der skal arbejdes pædagogisk med dem. Det kan være oplysninger om forhold i hjemmet, helbredsmæssige oplysninger (sygdomme og diagnoser) o.l. – dvs. oplysninger, der ikke bare er person*henførbare*, men ofte også *følsomme* personoplysninger.

De interviewede undervisere giver på den ene side udtryk for en grundopfattelse af, at denne type elevoplysninger altid skal håndteres med den største forsigtighed og fortrolighed mellem underviser og elev. En underviser beskriver eksempelvis, hvordan man aldrig ville dele følsomme personoplysninger om en elev uden elevens (mundtlige) samtykke:

Interviewer: Hvordan forholder man sig til deling af personfølsom information om elever?

Underviser og studievejleder, gymnasium: Det gør man kun, hvis man har fået samtykke af eleverne. Og det er et mundtligt samtykke. Hvis det er skriftligt samtykke, sidder de typisk og er med til at skrive mailen.

Overordnet set beskriver interviewpersonerne således arbejdet med følsomme personoplysninger som noget, de helt naturligt behandler med forsigtighed – og ikke et fokus, der nødvendigvis er forårsaget af databeskyttelsesloven. Flere interviewpersoner henviser bl.a. til tavshedspligten eller mere overordnet *"hensynet til den enkelte elev"* som hensyn, som også før databeskyttelsesloven har været gældende for skolepersonalet:

Administrativ medarbejder, Erhvervsskole: Altså i virkeligheden har tavshedspligten jo været vores lille datalov. Vi har jo egentlig lavet vores egen lille datalov inden GDPR, på baggrund af tavshedspligten. Vi har bare altid overholdt det.

Studievejleder og underviser, gymnasium: Det vigtigste hensyn er, at man skal kunne se alle elever i øjnene, så de får den følelse, at der er styr på det. Og man må stole på, at ledelsen har ansat folk, der ved, at de er ansat under tavshedspligt.

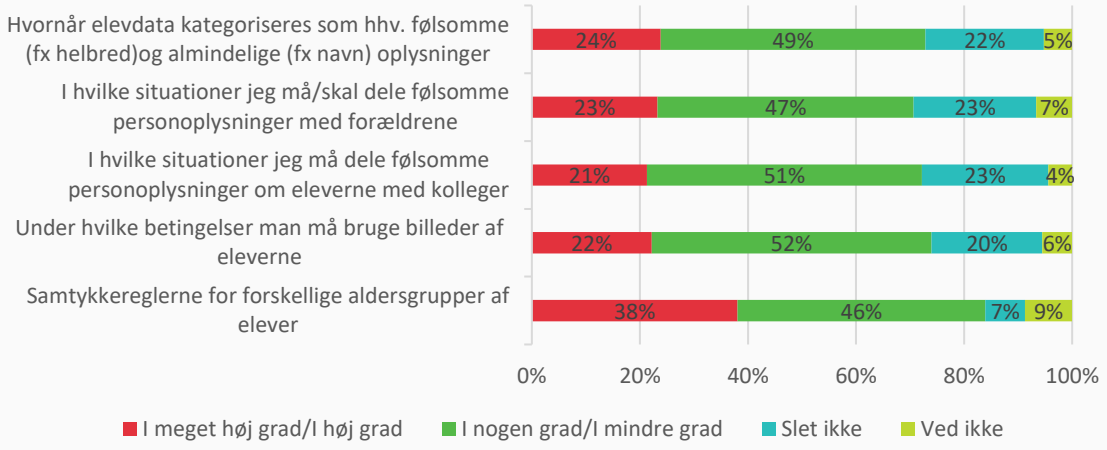
Men selvom undervisere på den måde efterstræber – og også før databeskyttelsesloven har efterstræbt – kun at dele følsomme personoplysninger med elevens samtykke, **så har databeskyttelsesloven flere steder alligevel skabt øget opmærksomhed på potentielle udfordringer**. Disse udfordringer kan være af både teknisk/ressourcemæssig karakter, som første af nedenstående citater viser. Men de kan også være udfordringer ift. arbejdsvaner/kultur, som det nederste citat illustrerer:

Underviser, gymnasium: Hvor skal jeg opbevare de her oplysninger? Jeg har jo ikke et lukket system. Jeg kan jo også få papirer fysisk tilsendt. Men vi har ikke rigtig en sagsgang. Optimalt set skulle det jo være i et pengeskab. Men jeg har det ofte både digitalt og på papirer i en mappe, der fx hedder "Elever til læsevejledning" […]. Vi indhenter jo også bemyndigelseserklæringer fra forældre og elever. Så dem har jeg også liggende. Så der er lidt noget information, som jeg ikke rigtig ved, hvad jeg skal gøre med.

Underviser, gymnasium: Det er udfordrende, når jeg modtager mails. Nogle gange modtager jeg noget på min private mail, som er Gmail. Og hvis nogle er dumme nok til at sende mig noget til min private mail, så må det være deres ansvar. Ikke elever, men andre lærere, som sender noget her. Det er irriterende. Hvis vi skal passe på alt det her, så skal de da ikke sende det ud i Gmailen. Vi har også fået at vide, at vi ikke må skrive om elever og elevers navne i [læringsplatform], som vi tidligere har gjort. Det sker også stadig, og jeg har modtaget både fra ledelsen og andre kolleger på [læringsplatform]. Lidt modstridende signaler.

Som det kan ses, er der udfordringer med at få adgang til sikre strukturer for elevdatadeling og nogle steder også at få kollegaer til at benytte dem. Dertil kommer også juridisk tvivl om, i hvilke situationer man som underviser i første omgang overhovedet må dele sin viden om elevens følsomme personoplysninger med andre. Hertil viser spørgeskemaundersøgelsen i figur 39, at mellem 21-24 pct. af underviserne i *meget høj grad* eller i *høj grad* vurderer at mangle viden om, hvornår oplysninger i det hele taget kategoriseres som følsomme personoplysninger, samt under hvilke betingelser man må dele dem med fx forældre og kollegaer:

Figur 39: Datahåndtering handler ofte om juridiske tolkninger. Vi vil gerne vide, i hvilken grad du vurderer, at du mangler viden om…



Kilde: Undervisere, n=722.

Denne problemstilling er ikke nødvendigvis ny. Men med databeskyttelsesloven er der kommet fornyede refleksioner over, hvad man egentlig tænker, at data er, og hvordan man må dele dem. Som følgende to undervisere sætter spørgsmålstegn ved, er der tvivl om, hvad man må dele, selvom sigtet er pædagogisk – og særligt hvis det foregår mundtligt, er det så stadig data?

Underviser, gymnasium: Fx ift. mistrivsel. Må man så omtale problematiske elever på møder? Må elever nævnes i forbindelse med en diagnose? Må man overhovedet sige et navn, så kontaktlæreren kan fortælle det videre?

Underviser, gymnasium: Når man er på lærerværelset så får man ofte samtaler om eleverne, men de skal altså være fortrolige. De er mere uskrevne, end skrevne"

I interviews med undervisere har flere også været kontaktpersoner for elever, og har derfor kendskab til deres personlige historik. De oplever, at deres kollegaer på den ene siden har brug for at vide noget om eleven, men at det samtidig ikke kan blive konkret. **Så i stedet for at dele elevens historie (data) med kollegaerne, kommer de med mere handleanvisende tips omkring specifikke elever:**

Interviewer: Kan man dele personfølsomme oplysninger i mere løse termer?

Underviser, gymnasium: Nej, i princippet må man ikke gøre det. Men man kan jo fortælle sine kollegaer (hvis en elev fx har opført sig udadreagerende i den seneste tid), at det bliver der taget hånd om. Eller: Vær gerne opmærksom på, at eleven er i en situation, der gør, at de ikke bryder sig om at blive udspurgt i klassen. Jeg synes det er vigtigt at holde tingene for sig selv. Som lærer er det vigtigste at overholde den tavshedspligt, man har – også selv om man kan se, at andet ville være bedre for eleven.

Såfremt underviserne gerne vil dele noget om eleven, vurderer alle underviserne, at dertil kræves samtykke. Som figuren før viste, **er der 38 pct. der vurderer, at de i meget høj eller høj grad mangler viden om, hvordan samtykkereglerne gælder for forskellige aldersgrupper.**

Dilemma:

Der er ofte væsentlige pædagogiske fordele og hensyn forbundet med at dele viden med sine kollegaer om eleverne. Denne viden kan eksempelvis handle om elevers sociale eller helbredsmæssige udfordringer og kan dermed have karakter af følsomme personoplysninger. Derfor deler underviserne sjældent denne type oplysninger uden elevens samtykke. Men alligevel har det øgede fokus på databeskyttelsesloven medført en usikkerhed hos nogle medarbejdere omkring, hvordan denne type oplysninger må håndteres. Er det tilstrækkeligt med mundtligt samtykke? Og må man dele informationerne både mundtligt og skriftligt?

8.2.3 Retningslinjer vis-à-vis hverdagen

Som det fremgår af ovenstående, håndterer nogle undervisere udfordringen med opbevaring af gamle opgaver ved at anonymisere navn, CPR-nummer o.l. Men på enkelte caseinstitutioner er det blevet påpeget, at der kan være tilfælde, hvor anonymisering ikke umiddelbart er en mulig løsning.

Konkret drejer det sig om situationer i forbindelse med eksamensbedømmelser, hvor eleven har klageret. Udfordringen beskrives i følgende citat som et "clash" mellem to hensyn: At underviseren/censoren på den ene side bliver nødt til at opbevare eksamensopgaver i ikke-anonymiseret form for senere at kunne forsvare en bedømmelse i tilfælde af, at eleven klager, mens vedkommende på den anden side har fået at vide, at man ikke må opbevare ikke-anonymiserede opgaver overhovedet. Citatet illustrerer dermed en pointe omkring **det krydspres, som nogle undervisere oplever mellem, hvad der opfattes som korrekt adfærd, ifølge de opstillede retningslinjer på den ene side, og hvad der praktisk og ressourcemæssigt er mest hensigtsmæssigt**:

Underviser 1, gymnasium: Men vi har jo en forpligtelse til at opbevare noter i forbindelse med votering osv. i op til et år. Af hensyn til mulige klagesager. Og der kan vi jo ikke slette navne, for så ved vi jo ikke, hvem den tilhører. Så der synes jeg, det clasher lidt. Jeg har hørt, at i princippet skulle man gemme det i et pengeskab.

Underviser 2, gymnasium: Men det er jo en utopi. Det skal jo være et stort pengeskab så! Og så skulle vi alle sammen have et pengeskab?

Underviser 1, gymnasium: Ja, så der VIL være tidspunkter, hvor det flyder rundt – uanset hvordan man gør det.

FAKTABOKS: Hvad er situationsbilleder og portrætbilleder?

Der er en udbredt misforståelse om at sletning skal ske ligeså snart eleven har fået sin bedømmelse. Hvis der er legitime grunde til at fortsætte opbevaringen, og det er foreneligt med det oprindeligt indsamlede formål (bedømmelsen), så må man gerne fortsætte opbevaringen. Så længe der er en klagefrist og klageret over en bedømmelse, så er der ikke krav på sletning.

Eksemplet illustrerer samtidigt en pointe, der kendetegner flere underviseres oplevelse af kravene om sikker håndtering af elevdata. For som det fremgår af den første del af citatet fra underviser 1, **så er retningslinjerne for sikker håndtering af elevdata i nogle henseender omgærdet af rygter eller uklare tolkninger af, hvordan institutionerne og personalet ideelt set skal agere**. Vendinger som *"jeg har hørt, at i princippet skal man… "* eller *"Det bliver tolket anderledes på andre skoler… "* går igen i flere af underviserinterviewene. På andre institutioner oplever underviserne eksempelvis ikke klagemuligheden som en udfordring:

Underviser 1, gymnasium: Altså hvis der kommer en klage, så ved man det inden for ret kort tid, og hvis der ikke er kommet nogen, så smider jeg dem bare [opgaverne] ud. […]

Underviser 2, gymnasium: Når et nyt skoleår er startet, så betragter jeg den der klageperiode som overstået.

Interviewer: Er det så lidt et tænkt problem det her med klager?

Underviser 2, gymnasium: Jeg har aldrig oplevet, at der kommer en klage, når det nye skoleår først er begyndt.

Underviser 1, gymnasium: Nej, ellers ville man have fået at vide, at der var en klage undervejs.

Dilemma:

Flere undervisere er i tvivl om, hvorvidt faglige produktioner skal håndteres som persondata. Der hersker da også forskellige tolkninger heraf, men ikke desto mindre beskriver flere lærere det som en central udfordring for dem. Udfordringen består dels i at finde tid til at skulle gøre noget ved det, men for mange i højere grad, at de oplever det som svært at se, hvorfor sletning af gamle opgaver overhovedet er relevant – særligt når det holdes op imod et pædagogisk hensyn. Underviserne opfatter det således som et dilemma mellem både ressourcemæssige hensyn og pædagogiske fordele ved at gemme gamle opgaver på den ene side, og institutionelle retningslinjer om sletning af gamle opgaver, som flere institutioner har indført i kølvandet på databeskyttelsesloven, på den anden side.

De forskellige opfattelser af, hvordan institutionerne og personalet bør håndtere dilemmaer som dette, bliver i interviews på tværs af personalegrupper forklaret med manglen på klare, centralt givne retningslinjer. En efterlysning vi ligeledes har hørt blandet de deltagende ledere, tekniske/administrative personale og undervisere ved de to workshops. For som en administrativ medarbejder udtrykker det i det mobiletnografiske studie, så får institutionerne deres oplysninger om og input til retningslinjer for, hvad man må og ikke må, fra mange forskellige kilder, hvilket kan skabe forvirring på tværs af institutionerne:

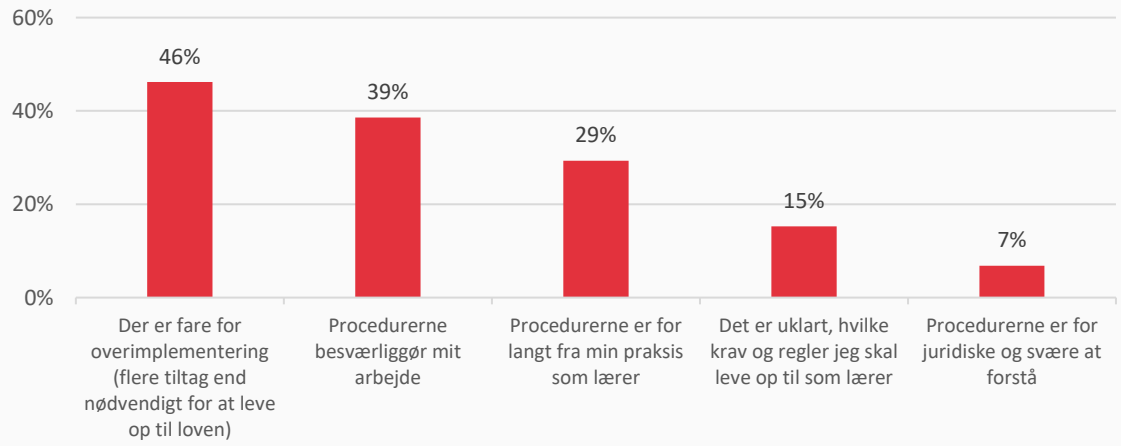
Administrativ medarbejder, gymnasium : ALLE vil gerne gøre det rigtigt, men det kan ikke undgås, at skolerne tolker forskelligt og har forskelligt fokus, og det gør, at vi indimellem "forvirrer" hinanden. [Medarbejderens gymnasium] er med i Gymnasiefællesskabet Y, og vi er løbende blevet orienteret om loven – og om hvad vi skal vi være opmærksomme på. Der er en jurist ansat i Y, der har haft persondataforordningen som sit primære arbejdsområde det sidste halvandet år. Tillige har vi orienteret os via Danske Gymnasier, Faglige organisationer og diverse netværker.

Andre skoler får oplysninger og informationer fra andre fællesskaber, foreninger og netværker - og vi har ikke altid "hørt og forstået" vedledningerne og oplysningerne ens.

Det samme gør sig gældende for underviserne, der ift. opbevaring af elevopgaver i hjemmet også spørger, lettere ironisk, om de skal have dem i et aflåst pengeskab. **Forvirringen omkring hvad man præcist må og ikke må, fx hvad angår opbevaring af elevprodukter, kunne paradoksalt nok være med til at delvist forklare, hvorfor nogle undervisere er tøvende med at forlange klare regler fra ledelsen omkring opbevaring af gamle opgaver** (som nævnt tidligere, "kun" 25 pct.).

For at se på hvilke grunde undervisere generelt kan have til at tøve med at indføre klare regler, kan i figur 40 ses hvad undervisere, der tidligere har svaret, de ikke kunne tænke sig at ledelsen indførte en række sikkerhedsprocedurer, giver af begrundelse herfor:

Figur 40: Hvorfor kunne du ikke tænke dig, at skolen/gymnasiet indfører procedurer?



Kilde: Undervisere, n=249.

Note: Spørgsmålet her er et forgreningsspørgsmål, der blev givet til de undervisere, der præsenteret for en række procedurer deres institution ikke havde indført, svarede at de ikke kunne tænke sig at institutionen indførte dem. I alt svarede 46 pct. (249 undervisere) at de ikke kunne tænke sig at institutionen indførte en eller flere af disse procedurer.

Som det her kan ses, er den hyppigste årsag til at underviserne kan være påpasselige ved at få indført nye procedure, at 46 pct. mener, at der er fare for, at der vil blive tale om overimplementering.

Tanken om overimplementering særligt ift. håndteringen af elevopgaver, var også noget der fyldte i diskussionerne til den 1. workshop med medarbejdere fra de selvejende institutioner:

Underviser til 1. workshop: Det er et felt præget af myter om, hvad man må, og hvad man ikke må – snarere end noget man ved. Det kan skabe usikkerhed, også fordi at ledelsen er i tvivl, men gerne vil være på den sikre side. Så bliver meldingen ofte, at man vil være på den sikre side og derfor bør slette gamle opgaver, når en underviser kommer og spørger.

Som det kan ses ifølge ovenstående underviser, kan man forstå, at undervisernes frygt for overimplementering hænger sammen med at de oplever et vidensunderskud ift. reglerne. I stedet for klar viden opstår der myter, hvor undervisere kan være bange for at ledere som en automatreaktion vil overimplementere for at være på den sikre side.

8.2.4 Kulturforandring

I forrige afsnits eksempel med underviseren, der fortsat oplever, at elevdata deles via potentielt usikre kanaler, illustreres også en pointe, som flere andre undervisere på caseinstitutionerne peger på: Behovet for en ændring af arbejdskulturen i arbejdet med elevdata.

En underviser beskriver i følgende citat, hvordan man i de daglige undervisningssituationer let kan komme til at glemme god datahåndterings-praksis:

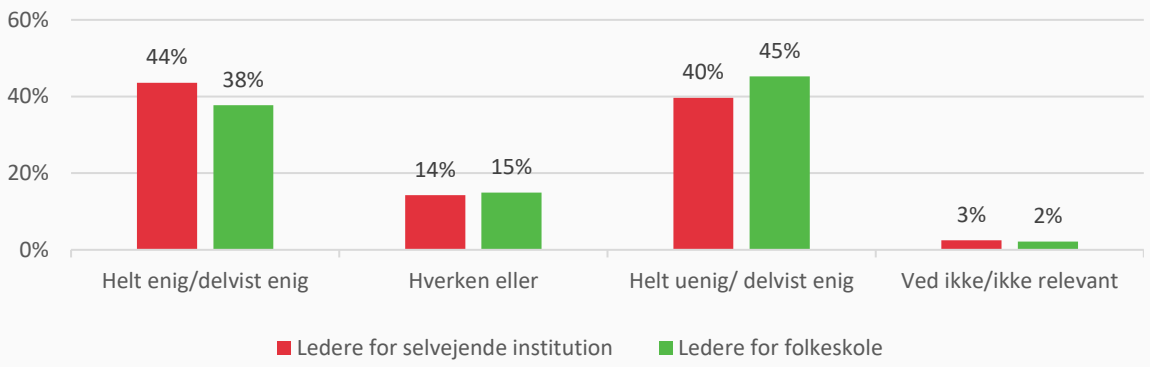
Underviser, gymnasium: Hvis nu en gruppe elever arbejder udenfor, og jeg lige vil ud og tjekke til dem. Så skal jeg jo huske at slukke min computer inde i klasselokalet. Men der er det nemt at komme til at glemme. Og man vil jo også gerne bare stole på hinanden… Så bliver det lidt skørt. Hvis man skal langt væk, så har jeg selvfølgelig altid låst min computer. Men man kan nemt komme til at glemme det, hvis det bare er "korte distancer".

Arbejdet med tilpasning af arbejdskulturen er et fokusområde, der kan være relevant for både de administrative og undervisningsrelaterede arbejdsgange. **Men især underviserne, der ikke på samme måde som det administrative personale er vante til at se informationer som data, kan opleve det øgede fokus på datasikkerhed, som et fokus, der kræver et opgør med gamle vaner** – en pointe, der bl.a. kommer til udtryk i følgende citat:

Administrativ medarbejder, gymnasium: Jeg tror, at lærerne har sværere ved at se logikken i det. […) Det er nemmere for det administrative personale, fordi vi er ikke i tvivl om, hvad der er personfølsomt. Det knytter sig tættere til vores primære arbejdsopgaver. Jeg kunne godt forestille mig, at de [lærerne] synes, at kommunikationen omkring, hvad man skal gøre, skal være bedre.

At det kan være vanskeligt at få underviserne til at vænne sig til nye arbejdsgange mht. sikker håndtering af persondata, understøttes også af spørgeskemaresultaterne i figur 41. Her svarer hhv. **44 pct. af lederne for selvejende institutioner og 38 pct. af lederne for folkeskoler nemlig, at de oplever det som en udfordring at få underviserne til at forstå vigtigheden af den nye databeskyttelseslov**:

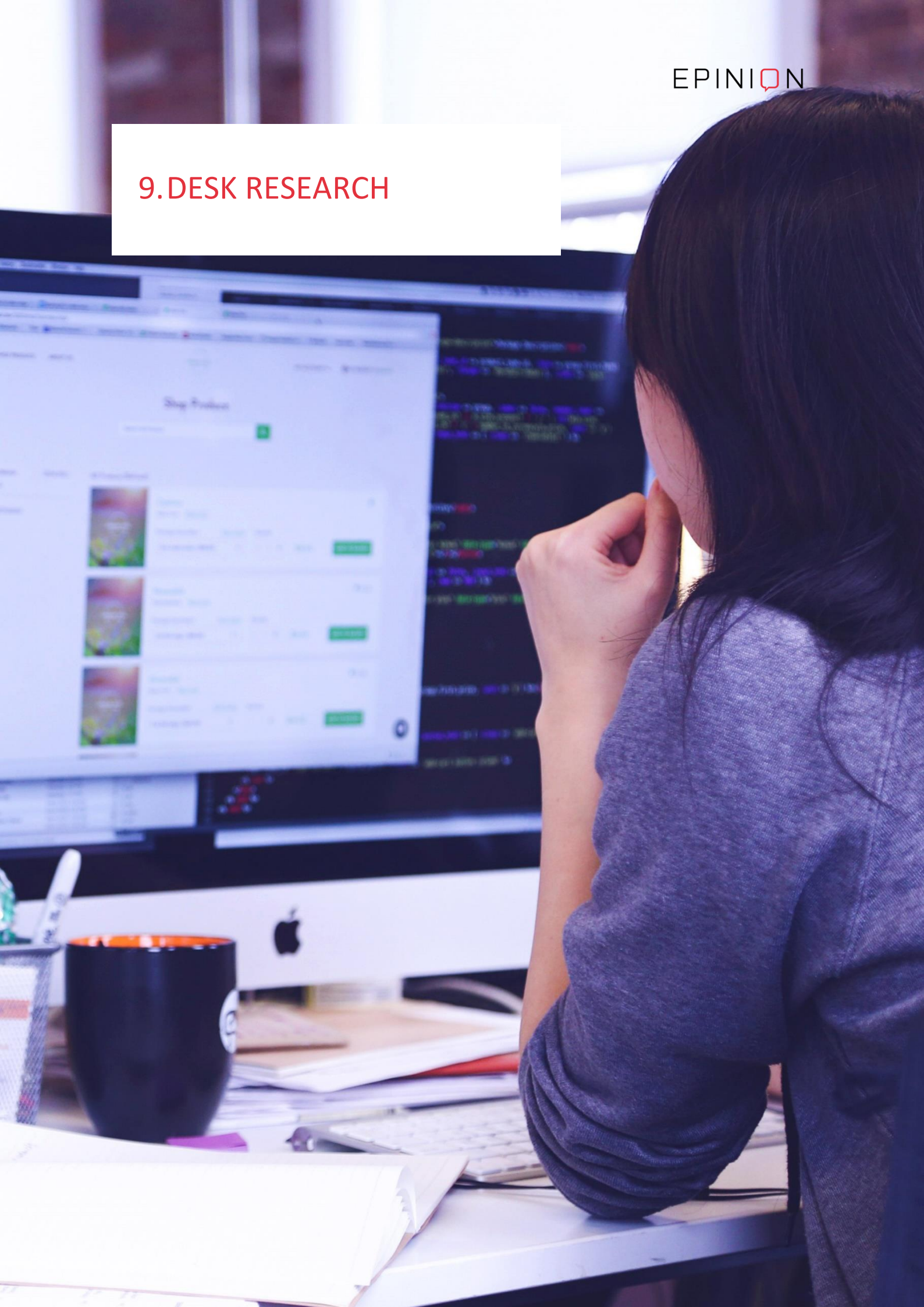
Figur 41: Hvor enig eller uenig er du i følgende udsagn om jeres arbejde med at sikre elevernes persondata: Det er en udfordring at få lærerne til at forstå vigtigheden af den nye databeskyttelseslov



Kilde: Ledere på folkeskoler og selvejende institutioner, n=468.
Note: Kun ledere for selvejende institutioner har haft mulighed for at svare "ikke relevant".

Omvendt oplever både det administrative personale og ledelserne på flere af caseinstitutionerne som tidligere beskrevet, at databeskyttelsesloven i et vist omfang har bidraget til at gøre sikkerhedshensynet mere legitimt at påpege over for underviserne.

9. DESK RESEARCH



9.1 INTERNATIONALE GOVERNANCESTRUKTURER – EN SAMMENLIGNING

Som en del af undersøgelsen, blev Epinion bedt om at foretage en landesammenligning mellem Danmark og lande, der normalt sammenlignes hermed. Sammenligningens omdrejningspunkt var at se på ligheder og forskelle på de enkelte landes governancestrukturer – dvs. en sammenligning af hvordan institutionernes rum for at håndtere data bliver influeret, understøttet eller begrænset af forskellige lovstrukturer, styringsmæssige praksisser, offentlige initiativer, private aktører, m.m.

I denne undersøgelse har Epinion taget udgangspunkt i nationale governancestrukturer i fem udvalgte lande. Disse lande udgøres af Sverige, Norge, Holland og Danmark der politisk/kulturelt og lovgivningsmæssigt minder om hinanden, samt USA, der er medtaget for at få et anderledes perspektiv på variationer i datagovernance.

Overordnet set er indtrykket fra landesammenligningen, at **Danmark er et af de lande, der har en højere grad af lokal selvbestemmelse**, når det gælder kommuners og institutioners beslutning om at anvende forskellige digitale produkter og imødekomme databeskyttelsesloven. I Danmark søges primært, gennem vejledninger og informationsmaterialer, at gøre institutionerne bevidste om, hvad man juridisk set skal være opmærksom på og hvilke procedurer, man skal følge. Hvis der fx skal vælges et digitalt produkt på institutionelt eller kommunalt plan, kan der findes skabeloner for databehandleraftale hos fx KL eller hos foreninger og tips til indgåelse af denne.

I andre lande har man på nogle områder en mere centraliseret rammesætning for, på hvilke måder skoler og selvejende institutioner samarbejder med udbydere af digitale produkter – fx bliver elevdata i norske grundskoler ikke opbevaret af udbyderen, men skal opbevares af den enkelte kommune. **Ligeledes er grundskoler i Holland også underlagt et krav om at foretage databeskyttelseskonsekvensanalyser på deres databehandlingspraksis**. I andre lande kan det også ses, at informationsmaterialet omkring særligt brugen af digitale produkter, også går fra at være mere juridisk og processuelt orienteret som i Danmark, til decideret at anbefale mere datasikre produkter ved navns nævnelse**. I USA arbejdes der fx med officielle sikkerhedscertificeringer af produkter, som hjælper institutionerne til at træffe sikre valg**, og gennem et privat-offentligt samarbejde i Holland, har man også udarbejdet en "white-list" over skoleprodukter, der er blevet vurderet som sikre.

Ligeledes er den praktiske overholdelse af databeskyttelsesloven relativt decentraliseret i Danmark sammenlignet med Sverige og Norge. Til trods for, at ansvaret for grundskolernes overholdelse af persondataforordningen formelt set ligger hos kommunerne – ligesom i Sverige og Norge –, er det i Danmark den enkelte skoles ansvar at indhente samtykke fra elever og forældre, samt sikre overholdelsen af oplysningspligten og indsigtsretten.

I det følgende bringes udvalgte nedslag fra det vidensnotat, der blev afleveret på baggrund af desk researchen. I gennemgangen refereres der til institutioner som samlebetegnelse for både grundskole og ungdomsuddannelse. Når andet er tilfældet, angives dette ved at nævne den konkrete institutionstype (fx grundskole eller gymnasium).

9.1.1 Nationale governancestrukturer

I kraft af at Sverige, Norge, Holland og Danmark er medlemmer i EU og EØS-samarbejdet, har persondataforordningen (General Data Protection Regulation (GDPR)) medført ændringer i landenes nationale lovgivning, for at sikre, at landenes styringsmæssige praksisser er i overensstemmelse med den overstatslige dataforordning.

USA er ikke underlagt GDPR og adskiller sig således væsentligt fra de fire andre lande. USA's lovgivning har dog været med til at inspirere indholdet i GDPR f.eks. i forhold til samtykke. I USA handler Children's Online Privacy Protection Act (COPPA) om forældresamtykke for børn under 13 år og indbefatter alle onlineservices, der har et kommercielt udgangspunkt. Family Educational Rights and Privacy Act (FERPA) og Protection of Pupil Rights Amendment (PPRA) har til formål at beskytte elevernes og forældrenes personoplysninger.

I Norge, Sverige og Danmark har kommuner og bestyrelser på de selvejende institutioner hver i sær ansvaret for at skolen eller institutionen overholder databeskyttelsesloven. Holland har dermed et mere decentraliseret system end de øvrige europæiske lande, idet de lader det være op til institutionerne selv, at sikre styringsmæssige praksisser i overensstemmelse med dataforordningen. I USA har staternes Local Education Agencies ansvaret sammen med institutionerne.

I Holland er alle uddannelsesinstitutioner forpligtede til at udnævne en databeskyttelsesansvarlig (DPO), der har til opgave at sikre, at institutionen agerer i overensstemmelse med persondataforordningen. I Sverige, Norge og Danmark udpeges den databeskyttelsesansvarlige på kommunalt niveau for folkeskolerne, således at en overordnet agerer databeskyttelsesansvarlig for samtlige grundskoler i kommunen. Institutionerne på det selvejende område i Danmark – gymnasier, friskoler, erhvervsskoler osv. – har deres egen DPO. Oftest i form af en fælles DPO.

Til trods for, at ansvaret for folkeskolernes overholdelse af databeskyttelsesforordningen formelt set ligger hos kommunerne, er det i Danmark den enkelte skoles ansvar at indhente samtykke fra elever og forældre, samt sikre overholdelsen af oplysningspligten og indsigtsretten. **Danmark har dermed decentraliseret de styringsmæssige praksisser ift. håndtering af persondata i skolen sammenlignet med Sverige og Norge.**

9.1.2 Aktører på uddannelses- og lovgivningsområdet ift. institutioners håndtering af persondata

De nationale governancestrukturer udarbejdes af forskellige statslige, regionale, kommunale og private aktører, der agerer indenfor uddannelses- og lovgivningsområdet.

I de fire europæiske lande agerer et statsligt organ som datatilsyn (i Danmark; Datatilsynet) samtidigt med, at en anden statslig myndighed udstikker retningslinjer for institutionerne på uddannelsesområdet (i Danmark; Undervisningsministeriet). I USA findes ikke ét datatilsyn. Det betyder, at lovgivningen i forbindelse med håndteringen af elevernes personoplysninger kontrolleres af de myndigheder, der udsteder lovgivningen. Her har Danmark (og de øvrige tre europæiske lande) i stedet én

særskilt og uvildig aktør til, at føre tilsyn med institutionernes praksisser ift. håndtering af elevernes persondata.

I de europæiske lande har flere offentlige aktører indgået samarbejder på tværs, for at understøtte institutionerne i en hensigtsmæssig brug af persondata. Dette dækker særligt over samarbejder mellem datatilsyn og myndigheder på uddannelsesområdet samt tværkommunale samarbejder.

I Danmark udgør disse samarbejder bl.a. Undervisningsministeriet og Kommunernes Landsforenings (KL) lancering af fem dataetiske principper for brug af persondata i folkeskolen[42]; Digitaliseringsstyrelsen, KL og Danske Regioners "Vi holder hackerne ude"-informationskampagne[43]; samt Datatilsynet, Digitaliseringsstyrelsen, Erhvervsstyrelsen og Justitsministeriets vejledning til databeskyttelsesforordningen[44]. Produktet af disse samarbejder udgør vejledninger, retningslinjer og principper, som institutionerne kan anvende og søge at efterleve, for at sikre daglig praksis i overensstemmelse med den nationale og overstatslige lovgivning på området.

Derudover er der en række private aktører, der er med til at udarbejde informationsmateriale og digitale værktøjer til institutionerne. Særligt i Holland og USA eksisterer en række private aktører, der udarbejder undervisningsmateriale og yder rådgivning og vejledning ift. retsmæssig håndtering af persondata. I Danmark er særligt handletænketanken DataEthics synlig ift. at udarbejde vejledninger samt fremme dialog omkring dataetik, datasikkerhed og privatlivsrettigheder.

9.1.3 Indsatser og initiativer på uddannelses- og lovgivningsområdet

De forskellige initiativer og indsatser i denne undersøgelse er klassificeret som informationsinitiativer, uddannelsesprogrammer og digitale værktøjer. I alle de fem lande anvendes særligt informationsinitiativer, der har til formål at vejlede og guide skoleejere og institutionerne i deres håndtering af data**. I Norge, Holland og Danmark findes derudover flere digitale værktøjer, mens der i Sverige og i USA i højere grad udbydes uddannelsesforløb.**

Danmark har en relativt decentraliseret tilgang til overholdelse af dataforordningen sammenlignet med de øvrige europæiske lande. **Statslige aktører i Sverige, Norge og Holland har udarbejdet fortolkninger af loven, der fastlægger retningslinjer for, hvorledes institutioner kan sikre praksis i overensstemmelse med persondataforordningen.** Her forholder statslige aktører i Danmark sig mere diplomatisk, og udbyder primært informationsmateriale, som kommuner og skoler kan læse sig ind i.

Dertil har mellemstatslige og statslige aktører i Sverige og Holland udarbejdet white-listings af hhv. apps og software-leverandører, der agerer i overensstemmelse med persondataforordningen. **Danske aktører lader det derfor være op til den enkelte uddannelsesinstitution eller kommune at tage stilling til brugen af digitale produkter.**

[42] https://uvm.dk/aktuelt/nyheder/uvm/2018/sep/180927-regeringen-og-kommunerne-lancerer-fem-dataetiske-principper
[43] https://digst.dk/sikkerhed/kampagner-og-analyser/informationsindsatser/undervisningsmateriale/
[44] https://www.datatilsynet.dk/media/6559/generel-informationspjece-om-databeskyttelsesforordningen.pdf

I det følgende præsenteres udvalgte initiativer ifm. institutioners håndtering af persondata i de fem lande.

Tabel 5. Udvalgte initiativer ifm. institutioners håndtering af persondata i Sverige, Norge, Holland, USA og Danmark

Sverige
• **Fokus på uddannelse**: Både statslige og kommunale aktører samt lærernes fagforening udbyder uddannelsesforløb, kurser og e-kurser med fokus på GDPR, privatlivets fred samt anvendelse af digitale værktøjer i undervisningen. • **Ti informationsinitiativer**: Sveriges Kommuner og Landsting har igangsat ti informationsinitiativer med informationer, tjeklister, vejledninger og begrebslister samt webinars og træning i databeskyttelsesforordning med fokus på kommunale spørgsmål. • **Digital platform:** Skolverket.se er en platform, der rummer værktøjer, gratis digitale materialer og inspiration til undervisning, der integrerer digitale værktøjer i undervisningen. Den indeholder bl.a. forslag til klassediskussioner om brugen af digitale data og smartphones samt grænser for deling af personlige data.
Norge
• **Fælles elektronisk indgang til digitale programmer:** Felles Elektronisk IDEntitet (FEIDE) giver institutionerne én elektronisk indgang til digitale tjenester på uddannelsesområdet, så lærere og elever kun skal bruge ét log-in. Derudover opbevares data hos skoleejeren (kommuner/fylkeskommuner) frem for leverandøren af læremidler og platforme. • **Utdanningsdirektoratets og Datatilsynets vejledningsmateriale**: Omfattende vejledningsmateriale med klare retningslinjer for institutionernes håndtering af personoplysninger, praksiseksempler og skabeloner. Materialet spænder fra overordnede retningslinjer til specifikke, lavpraktiske anbefalinger. • **Organisatoriske forandringer**: Omorganisering, hvor Senter for IKT, der tidligere havde ansvaret for den digitale indsats på uddannelsesområdet, blev indlejret i Utdanningsdirektoratet for at satse på it og digitalisering på tværs af alle afdelinger.
Holland
• **Databeskyttelses konsekvensanalyse**: Alle institutioner skal foretage en databeskyttelseskonsekvensanalyse (DPIA), der har til formål at kortlægge privatlivets risici ved databehandling. • **Whitelist over tjenester:** Liste med tjenester og softwareleverandører, der har underskrevet en såkaldt privatlivs-kontrakt, der forpligter dem til at sikre behandling af persondata i overensstemmelse med dataforordningen. Institutioner kan dermed trygt bruge tjenester på listen. • **Dokumentationstjeneste med anonyme pseudonymer**: I EDK iD får hver elev et anonymt pseudonym, der gør det muligt at følge den enkelte elevs fremskridt, udveksle persondata i overensstemmelse med GDPR samt påvise denne sikre udveksling af persondata.
USA
• **Leverandørerne har ansvar:** Lovgivningen (COPPA) regulerer og stiller krav til serviceudbyderne af uddannelsesværktøjer, så ansvaret for passende håndtering af elevdata ikke ligger ved institutionerne. • **Løfter og certifikater:** Serviceudbyderne kan afgive løfter eller opnå certifikater, som giver skoleledere, lærere, forældre og elever viden om, at udbyderen behandler elevernes persondata forsvarlig. • **Help desk om datasikkerhed:** Privacy Technical Assistance Center er en hjælpeservice, som skoleledere og lærere kan rette henvendelse til vedrørende datasikkerhed og -systemer. De tilbyder derudover teknisk support ude på institutionerne.
Danmark
• **E-læringsmodul**: Digitaliserings-styrelsen, KL og Danske Regioner har udarbejdet et E-læringsmodul som led i deres "Vi holder hackerne ude"-informationskampagne. Kampagnen har fokus på sikker adfærd på nettet, og består af computer-, mobil- og fællesøvelser henvendt lærere og elever.

- **Digital platform:** dataethics.eu er en platform, der rummer lister over dataetiske værktøjer, værktøjer til digitalt selvforsvar og gratis digitale materialer. Specifikt på uddannelsesområdet rummer platformen bl.a. Q&As om skoleområdet, information om skoleforedrag om digitale fodspor, 15 dataetiske must-do's ift. ansvarlig brug af skolebørns data.
- **Fælles samarbejdsplatform**: Aula er fremtidens kommunikationskanal i folkeskoler, SFO'er og dagtilbud, der i 2019 erstatter SkoleIntra. Aula udgør en kombineret læringsplatform og samarbejdsplatform, hvorigennem elever, forældre og lærere opnår sikker adgang til og udveksling af informationer fra skoledagen.
- **Dataetiske principper:** I samarbejde med Kommunernes Landsforening har Undervisningsministeriet udarbejdet fem dataetiske principper til at vejlede folkeskolernes håndtering af data.

Oversigt over samtlige initiativer i de respektive lande findes i særskilt vidensnotat.

9.2 DATATRAFIK OG DIGITALE PRODUKTER

I forbindelse med undersøgelsen er der foretaget en gennemgang af datatrafikken blandt de 53 digitale produkter, der oftest angives i elev og lærerbesvarelserne i spørgeskemaerne. Gennemgangen af datatrafikken handler om, hvem de forskellige produkter deler data med og hvilke typer data, der deles. Der er tale om en form for undersøgelse, der giver et tentativt indblik i, hvad det er for en type datatrafik der finder sted gennem hjemmesider og apps, som ikke nødvendigvis er synlig for brugeren selv. Desk researchen her har været retningsgivende for undersøgelsens fokus på den datadeling der foregår 'bag om ryggen' på elever og lærere. Den handler om de data, de ikke nødvendigvis selv er klar over, de deler (og med hvem, hvornår og hvordan).

Metodisk har gennemgangen bestået af tre trin:

1. Gennem Android-appen Lumen Privacy Monitor (LPM) er de produkter, der er tilgængelige som Android-apps testet mhp. at afdække hvor mange tredjepartstrackere, de etablerer forbindelse til og hvilke datakilder, appen kræver adgang til. Den gennemførte LPM-analyse er suppleret med tilsvarende forsøg gennemført af AppCensus.mobi.
2. Gennem browserplug-innet TrackingObserver er produkt- og leverandørhjemmesider blevet besøgt for at se, hvor mange tredjepartstrackere besøgende forbinder og evt. deler data med.
3. Læsning af udvalgte privatlivspolitikker mhp. indblik i deling og datatyper.

Metoden skal tages med en række forbehold. Dels at det forskningsmæssigt er komplekst at monitorere datatrafik[45], dels at sådanne test altid er lavet under tekniske forudsætninger, der ikke nødvendigvis mimer dem, fx institutioner har. Der kan derfor ikke direkte sluttes fra resultaterne i gennemgangen her til, hvilke data der deles og med hvem blandt lærere og elever lokalt på skoler og institutioner. Der er tale om en såkaldt lav økologisk validitet[46]. Institutioner kan gennem lokale

[45] På datatransparencylab.org findes en række udviklingsprojekter, der arbejder på metodisk at synliggøre datatrafik og digital infrastruktur.
[46] Økologisk validitet dækker over, om fænomenet også er undersøgt i det miljø, hvor det naturlig forekommer. Laboratorieforsøg (ligesom dette) har lav økologisk validitet sammenlignet med fænomenet undersøgt i 'in the wild'.

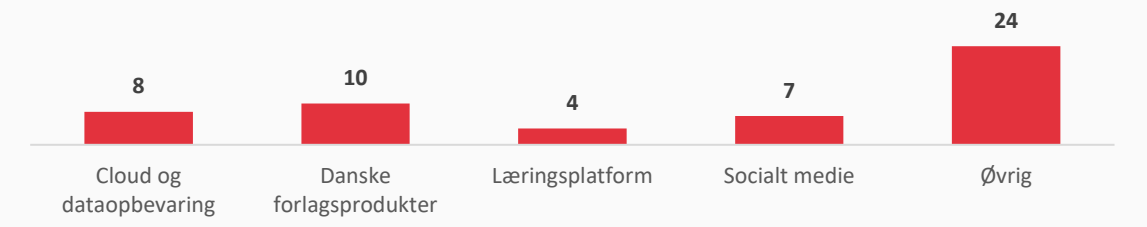
restriktioner, andre devices m.v. havde andre forudsætning eller betingelser for datadeling. Et eksempel herpå er, at mange bruger ellers digitale, gratis produkter gennem forlagsløsningen SkoleTube, der garanterer ordnede forhold ift. datadeling.

9.2.1 Datagrundlag og platforme for adgang

Ikke desto mindre giver analysen et indblik i omfanget og typerne af data, der deles gennem apps og hjemmesider. Resultaterne viser, at både apps og hjemmesider har en pågående udveksling af data, og der er tale om forskellige typer af data. Det kræver en kontekstuelt vurdering, om der er tale om persondata (og om yderligere handling derfor er påkrævet, fx indgåelse af databehandleraftaler).

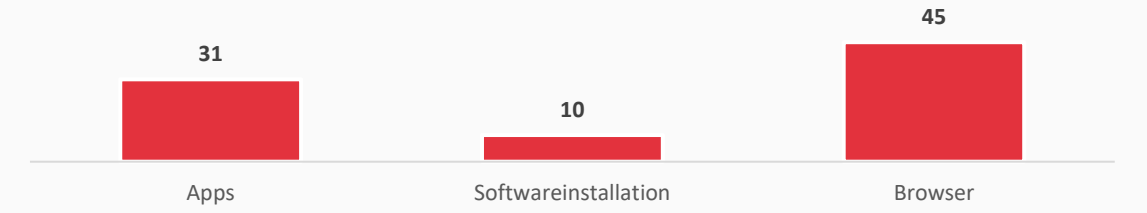
De 53 hyppigst angivne produkter fordeler sig således på tværs af analysens produktkategorier:

Figur 42: Fordeling af de 53 mest populære produkter fordelt på kategorier



Produkterne kan tilgås på forskellig vis. Dette er vigtigt, fordi måden brugeren tilgår produktet på giver forskellige betingelser for, hvordan og med hvem data deles[47]. Nogle produkter er tilgængelige gennem forskellige platforme, andre findes eksklusivt som fx app eller hjemmeside. Tilgængeligheden fordeler sig således:

Figur 43: Fordeling over hvilke måder, de forskellige produkter kan tilgås (samme produkt kan tilgås på flere måder)



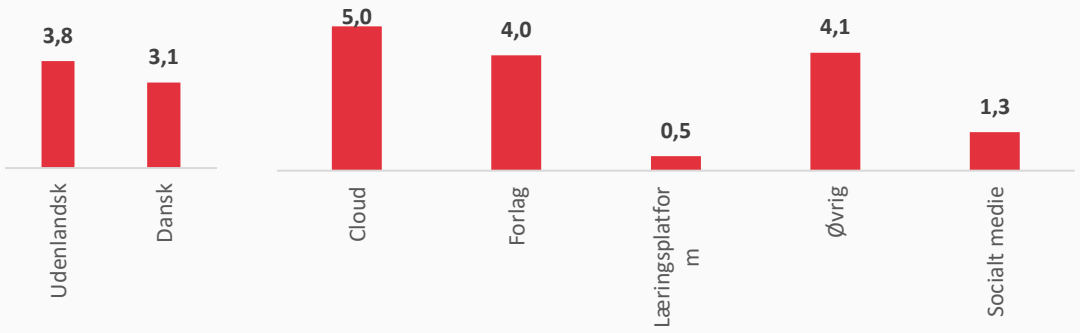
[47] Leung, C., Ren, J., Choffnes, D., & Wilson, C. (2016, November). Should you use the app for that?: Comparing the privacy implications of app-and web-based online services. In *Proceedings of the 2016 Internet Measurement Conference* (pp. 365-372). ACM.

9.2.2 Datadeling i browser

Når man besøger hjemmesider, herunder også de digitale produkter i undervisningen, sker der en række udvekslinger af data, brugeren ikke nødvendigvis er klar over. For det første afgiver brugeren gennem sin browser en række oplysninger. Det drejer sig om adfærd på hjemmesiden, såsom click, scroll og besøgstider[48]. Derudover afgiver brugeren gennem browseren en række oplysninger om styresystem, tidszone, ip-adresse m.v.[49] Studier viser, at disse faktorer i sig selv ofte er tilstrækkeligt til at identificere en bruger unikt gennem ens 'browser fingerprint'[50].

Udover adfærd og systemindstillinger, er også oplysninger om brugeren lagret og delt i cookies, et vigtigt aspekt ift. datasikkerhed. Cookies har fået særligt stor opmærksomhed i diskussioner om privatliv og datasikkerhed. Dette drejer sig især om cookieindhold og hjemmesiders deling af oplysninger om brugeren gennem trackere, især såkaldte tredjepartstrackere. Et større studie af hjemmesiders sikkerhed i forbindelse med cookies konkluderer bl.a., at "GDPR is making the web more transparent, but there is still a lack of both functional and usable mechanisms for users to consent to or deny processing of their personal data on the Internet"[51]. En undersøgelse foretaget af Reuters inden for nyhedsmedier viser, at siden GDPR's ikrafttræden er antallet af tredjepart-cookies faldet med 22 %[52]. Ved afprøvning i TrackingObserver viser det sig, at produkterne etablerer forbindelse til trackere i varierende grad jf. figur 44. Forlag, cloud og øvrige produkter er særligt udslagsgivende. Disse tal siger dog ikke noget om persondata i sig selv, da antallet af trackere, der forbindes med i sig selv ikke er et problem.

Figur 44: Gennemsnitligt antal tredjepartstrackere, produkthjemmesider forbinder med fordelt på geografisk ophav



Kilde: Ledere på folkeskoler og selvejende institutioner, n=468.

[48] Se fx https://clickclickclick.click/ for en live-afrapportering af, hvilke oplysninger man afgiver gennem sin digitale adfærd.
[49] Efterprøv via www.amiunique.org
[50] Laperdrix, P., Rudametkin, W., & Baudry, B. (2016, May). Beauty and the beast: Diverting modern web browsers to build unique browser fingerprints. In *Security and Privacy (SP), 2016 IEEE Symposium on* (pp. 878-894). IEEE.
[51] Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2018). We Value Your Privacy... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. *arXiv preprint arXiv:1808.05096*.
[52] Libert, T., Graves, L., & Nielsen, R. K. (2018). Changes in third-party content on European news websites after GDPR.

Det er derfor vigtigt at have in mente, at fordi en given hjemmeside etablerer forbindelse til en tredjepartstracker, er det ikke ensbetydende med, at der også finder en dataudveksling sted eller at denne data skulle indeholde personoplysninger. Endvidere er denne test lavet på de åbent tilgængelig versioner af hjemmesiderne. Bag betalingsmur på fx forlag vil tracking-profilen givetvis se anderledes ud.

Det er teknisk svært at bestemme præcist hvilken type data, der udveksles, og endeligt skal det afgøres kontekstuelt om den delte data er persondata, og om dette er dækket ind under eksisterende databehandleraftaler eller afgivne samtykker i forbindelse med accept af fx en hjemmesides cookiepolitik. De tredjepartstrackere, der modtager data om brugerne, pointerer selv, at de aldrig indsamler persondata[53], men samtidig registrerer de brugerens ip-adresse[54], der i en databeskyttelseslovskontekst oftest betragtes som en personoplysning[55].

9.2.3 Datadeling i apps

Tilsvarende browsere, kommunikerer apps efter installation på enheden (tablet eller telefon) oftest også med en række trackere/servere i baggrunden. Der er en lang række forskellige datakilder, apps kan tilgå på enheden. Gennemgangen her viser, at det i høj grad varierer, hvilke datakilder apps tilgår på telefonen.

Af de 53 produkter er 31 tilgængelige i appformat. Jf. metodeafsnittet er det kun muligt at gennemteste apps tilgængelige på Android. Af de 31 er 24 tilgængelige i Android-format. Disse fordeler sig geografisk således, at der kun er ét dansk produkt, 6 er europæiske og de øvrige 17 er fra USA.

Blandt disse 31 produkter er der forskellige datakilder, de beder om adgang til lokalt på telefonen. Fordelt på LPMs risikovurdering ser antallet af forespørgsler og kilder til data, appsne forespørger adgang til, således ud:

[53] https://www.theguardian.com/technology/2012/apr/23/doubleclick-tracking-trackers-cookies-web-monitoring

[54] Shuford, E., Kavanaugh, T., Ralph, B., Ceesay, E., & Watters, P. (2018, August). Measuring Personal Privacy Breaches Using Third-Party Trackers. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (pp. 1615-1618). IEEE.

[55] Fx på https://fpf.org/wp-content/uploads/2017/06/FPF_Visual-Guide-to-Practical-Data-DeID.pdf

Figur 45: Gennemsnitligt antal adgangsforespørgsler fra apps til forskellige datakilder på enheden, fordelt på kategori

Først og fremmest er der tale om en bred variation af datakilder, der potentielt deles gennem apps. De strækker sig fra fx geolokation til kontaktpersoner, netværksoplysninger og enhedsindstillinger. Tendensen er, at appsne i lavere grad forespørger adgang til højrisikable datakilder. Dog beder både de testede cloudløsninger (gratisudgaver) og sociale medier begge gennemsnitligt om adgang til 6-9 højrisikable datakilder på telefonen. Det er gennem LPM ikke muligt at afgøre, om de pågældende apps også benytter sig af den forespurgte adgang. Men sammenholdes resultaterne med tilgængelige gennemgange via AppCensus.mobi, hvor det også registreres om appsne benytter sig af de forespurgte adgange, fordeler det sig således:

Figur 46: Gennemsnitlig antal forespørgsler og tilfælde af tilgåede personoplysninger jf. AppCensus.mobi (AppCensus har afprøvet 16 af de 24 apps)

De kilder til persondata, som de sociale medier og cloudløsninger benytter sig af er fortrinsvist kontaktoplysninger, e-mail samt enhedens unikke device-id og fingeraftryk.

9.2.4 Datadeling jf. privatlivspolitikker

Læsningen af privatlivspolitikker viser, at størstedelen af de digitale produkter angiver, at de deler data med tredjeparter, men på forskellige betingelser. Størstedelen angiver, at de kun deler (person)data med tredjeparter, såfremt brugeren har samtykket eller at det er på myndigheders

forlangende. Imidlertid antager formuleringerne som oftest en generel karakter, der gør det svært at gennemskue, hvilke former for (person)data der er tale om og hvem konkret, den deles med.

Nogle produkter diskriminerer i deres privatlivspolitikker mellem data og persondata, mens andre blot skriver "data" eller "information". Det er uklart, i hvilken udstrækning de enkelte udbyderes forståelse af (person)data stemmer overens med en juridisk. Et eksempel på dette er fx data såsom ip-adresser, som ofte også klassificeres som persondata. Enkelte produkter (gratis/udenlandsk/øvrig) sætter modsætningsforhold mellem persondata og ip-adresse.

9.2.5 Konklusion og diskussion

Ovenstående gennemgang af datakilder, typer og deling åbner ligeså mange spørgsmål, som den besvarer. Overordnet kan det konkluderes, at der især for udenlandske og gratis produkter er tale om en større aktivitet – forstået som adgang til data og etablerede dataforbindelser til tredjeparter – end for danske betalingsprodukter. Imidlertid fremstår det ikke klart, præcis hvilke typer data, der deles hvornår og med hvem. Forklaringen på disse uklarheder bunder i, at det metodisk er svært at opnå mere præcis indblik i datatrafikken, og at det kræver en kontekstuel, juridisk vurdering at afgøre, om der er tale om persondata.

Det er aktuelt omdiskuteret, hvor problematisk disse typer af datadeling er. Diskussionerne går dels på et etisk spørgsmål, om hvorvidt det er i orden, at den gængse bruger af et digitalt produkt ikke kan gennemskue, hvad der finder sted af deling uden vedkommendes vidende. Dels er der et juridisk aspekt der handler om, hvorvidt mere teknisk orienteret data også rubriceres som personligt, og at samkøring af forskellige data, der i sig selv er anonymiseret/de-personaliseret, ved samkøring kan blive personligt.

10. METODE

10.1 KVALITATIV DATAINDSAMLING

I det følgende beskrives de forskellige kvalitative metoder, som er blevet anvendt i undersøgelsen. For at oparbejde en nuanceret viden, som både kunne indfange institutionernes berøring med og håndtering af elevers persondata samt belyse medarbejdernes udfordringer og behov, har Epinion gennemført en kvalitativ dataindsamling i to dele, som både har givet empiri til selvstændige analyser, men som også har skabt et solidt udgangspunkt for den kvantitative dataindsamling. De to kvalitative dataindsamlinger har på forskellig vis afdækket, hvilke udfordringer og dilemmaer skoleledere, lærere, it-ansvarlige samt administrativt personale møder i omgangen med persondata.

I alt har projekt-teamet været ude på 9 caseinstitutioner, fordelt på hhv. 3 grundskoler, 3 erhvervsskoler og 3 gymnasier. Metodisk har været anvendt dybdeinterview, typisk med ledere og fokusgruppeinterviews med administration og undervisere. I alt blev 52 personer interviewet. Alle interviews er blevet optaget på lydfiler og senere transskriberet og kodet.

Tabel 6: Fordeling af interviews på institutions- og medarbejdertyper på afholdte interviews

Dybde og fokusgruppeinterviews	Ledere	Undervisere	Administration
Grundskoler	8	6	6
Erhvervsskoler	4	11	7
Gymnasier	4	9	7
I alt:	**16**	**26**	**20**

Derudover har også været anvendt et mobiletnografisk studie, hvor af ledelsen udvalgte administrative medarbejdere og undervisere fra caseinstitutionerne henover en arbejdsuge skulle modtage forskellige opgaver og spørgsmål, som de skulle løse omkring datahåndtering og datadilemmaer i praksis. Nogle deltagere i dette studie deltog også i interviews, imens andre udelukkende deltog her. Alle svar og billeder fra det mobiletnografiske studie er blevet transskriberet og kodet. Der blev opnået en besvarelsesprocent på 83 pct. af opgaverne stillet.

Tabel 7: Fordeling af deltager på institutions- og medarbejdertyper i det mobiletnografisk studie

Mobiletnografi	Lærere	Administration
Grundskoler	2	2
Erhvervsskoler	3	3
Gymnasier	2	3
I alt:	**7**	**8**

10.1.1 Rekruttering

Institutionerne fordeler sig geografisk over det meste af landet og fordeler sig på i alt tre grundskoler, tre gymnasier og tre erhvervsskoler. Som et led i rekrutteringen af caseinstitutioner foretog en kvalitativ konsulent fra Epinion et forberedende opkald for at aftale et besøg. Derefter blev der sendt et

uddybende skriv, hvor Epinion præsenterede hvad casebesøget skulle bruges til, samt hvilke interviews Epinion gerne ville foretage under besøget. Lederne lagde så et dagsprogram med interviewrækkefølge, samt planlægningen af en lille rundtur på institutionen, hvor teamet kunne observere og tage noter til inventar og rummenes indretning ift. datasikkerhed.

Rekrutteringen til mobiletnografien blev foretaget af ledelsen på caseinstitutionerne, men også lokalt på institutionerne under casebesøgene, havde de enkelte konsulenter til ansvar at sikre deltagere. Herefter fik Epinion kontaktoplysninger på de udvalgte deltagere. Efter den endelige rekruttering til mobilforaet, sendte en konsulent fra Epinion en-to orienterende e-mails ud til de enkelte deltagere, som beskrev undersøgelsen, samt som blev brugt til at indhente deltagernes skriftlige samtykker. Hertil gennemførte Epinion personlige telefoniske opkald til alle deltagere med endnu en orientering, samt med det formål at sikre at alle fik downloaded appen og aktiveret den.

10.1.2 Formål

Formålet med de kvalitative casebesøg på institutionerne var dels at afdække institutionernes overvejelser, udfordringer og behov i forbindelse med brug af digitale læremidler, samt dels deres mere generelle håndtering af elevdata.

Casebesøgene har således spillet en vigtig rolle i afdækningen af institutionernes håndtering af persondata, institutionernes anvendelse af gratis digitale produkter, omfanget af institutionernes databehandleraftaler samt uddannelsessektorens udfordringer og behov på området.

På hver af de ni caseinstitutioner er der blevet foretaget interview med skoleleder/viceskoleleder, den it-ansvarlige, lærere samt teknisk-administrativt personale. Den it-ansvarlige var flere steder enten leder eller lærer. Interviews med lærere og administrativt personale blev afholdt som fokusgruppeinterviews - dog med undtagelser, da det ikke er alle institutioner som har haft kapacitet hertil - mens interview med ledelse og it-ansvarlig er blevet afholdt primært individuelt. Dog har ledelsen enkelte steder, sat sig sammen i det GDPR-ledelsesteam, der arbejdede med implementeringen.

Formålet med det mobiletnografiske studie med deltagende lærere og administrativt personale var at komme ekstra i dybden med medarbejdernes hverdagspraksis med elevdata. Ved at dokumentere og reflektere over egen praksis som den udfolder sig, hjalp det konsulenterne til at få indsigter i gråzonetilfælde, dilemmaer og udfordringer i arbejdet på praksisnært hold.

10.1.3 Dybdegående casebesøg

Første del af den kvalitative dataindsamling har bestået af casebesøg på ni uddannelsesinstitutioner. For at opnå en valid dataindsamling startede den kvalitative del af undersøgelsen med et forstudie på en erhvervsskole op til skolernes sommerferie 2018, med henblik på at kvalificere mere lukkede spørgerammer til brug for undersøgelsen på de resterende otte caseinstitutioner efter sommerferie.

Formålet med casebesøgene var at få et nuanceret indblik i institutionernes brug af elevernes persondata, herunder hvilken type af data, de er i berøring med, hvordan det deles, gemmes og efter hvilke aftaler. Casebesøgene gav således indblik i institutionernes praksis, og blev brugt til at undersøge dette endnu dybere gennem mobiletnografi. Derudover dannede casebesøgene baggrund for temaer og spørgsmål i det kvantitative studie.

Alle interviews er startet med en datahjuls-øvelse, hvor Epinion har lavet en oversigt over forskellige typer af data, som institutionerne kan være i kontakt med – dog ikke udtømmende. Dette "hjul" blev lagt frem og der blev sat krydser ud for de typer af data, som hver enkelt er i berøring med. Konsulenterne fra Epinion udvalgte herefter nogle af disse til en videre samtale omkring den pågældende type datas berøring med forskellige aktører, devices m.m. På den baggrund blev det muligt at tegne forskellige typer af data og deres "flow" eller "rejser" mellem mennesker og medier, og deres oversættelse til analoge eller digitale data undervejs.

10.1.3.1 Fokusgruppeinterview med administrativt personale

På hver caseinstitution blev der foretaget fokusgruppeinterview med 2-3 administrativt personale af en times varighed. Interviewene blev afholdt med henblik på kvalitativt at afdække institutionernes syn på håndteringen af elevernes data, hertil hvilke dilemmaer, udfordringer og administrative byrder som institutionerne oplever at stå over for. På grund af deres kendskab til institutionernes it – og datapolitik kunne det administrative personale give indsigter i hvilken type data de som administration er i berøring med GDPR-implementering, databeskyttelsesloven og udfordringer i den forbindelse, samt indgåelse af databehandleraftaler.

10.1.3.2 Enkeltmands – eller gruppeinterview med lærere

Der blev på hver caseinstitution også gennemført interview med lærere, enten som enkeltmands eller som et fokusgruppeinterview af en times varighed, alt efter hvad der var kapacitet til på de enkelte institutioner.

Interviewene blev afholdt med henblik på kvalitativt at afdække, om lærerne bemærker et øget fokus på datasikkerhed og hvordan, samt få indsigt i deres syn på håndteringen af elevernes data herunder hvilke dilemmaer og udfordringer de møder i deres pædagogiske arbejde. På grund af lærernes nære kontakt til eleverne, kunne de særligt give indsigter ind i hvilke typer af elevdata, som de er i berøring med og hvilke udfordringer det giver, samt hvilke digitale produkter de særligt benytter og hvilke overvejelser de har i den forbindelse.

10.1.3.3 Enkeltmands – eller gruppeinterview med skoleledelse og/eller it-ansvarlig

Derudover blev der også på hver caseinstitution gennemført interview med skoleledelsen enten som enkeltmands – eller gruppeinterview af en times varighed. På en del af caseinstitutionerne var den it-ansvarlige også en del af ledelsen, hvorfor de to interviewguides ofte har flydt sammen.

Interviewene blev afholdt med henblik på kvalitativt at afdække ledelsens og/eller den it-ansvarliges syn på håndtering af elevernes data, herunder hvilke administrative byrder der er forbundet hermed, hvilke udfordringer de møder i arbejdet, hvilke retningslinjer de arbejder med, om de har indført nye procedurer og hvilke databehandleraftaler der er blevet indgået, hvordan og hvorfor.

10.1.4 Mobiletnografisk studie

Den anden del af den kvalitative dataindsamling bestod af et mobiletnografisk logbogsstudie. Metoden er benyttet, da den som antropologisk metode er særligt velegnet til at give indblik i en kultur, her lærerens og de administrative personales viden, tanker, værdier og tvivl i deres daglige arbejde med elevdata, med et særligt fokus på deres udfordringer, dilemmaer og behov.

Konsulenter fra Epinion har faciliteret og administreret det mobiletnografiske forum, som forløb over to uger efter en drejebog med 6 hovedopgaver, disse blev lagt op cirka hver anden dag med undtagelse af weekenden. Hertil fulgte Epinion op med spørgsmål, som blev brugt til at moderere besvarelserne og skærpe fokus på de relevante problemstillinger.

Det mobiletnografiske studie foregik i et lukket online forum, Revelation fra FocusVision, som kun kunne tilgås af personer, som var blevet oprettet med brugernavn og password af Epinion. Ved undersøgelsens start modtog deltagerne en invitations-e-mail fra forummet med et brugernavn og en guide til at vælge password, samt en opfølgende guide fra Epinion til hvordan de hentede app'en trin for trin.

I alt deltog 15, hhv. 7 lærere og 8 administrative personale fra 7 caseinstitutioner, hvilket i alt blev til 81 besvarelser. Dette giver en samlet svarprocent på 83 pct. af alle opgaverne. Alle besvarelser er blevet behandlet og kodet efter samme kodninger som interviewene fra casebesøgene. Deltagerne skulle dokumentere deres omgang med elevdata i løbet af deres hverdag. De seks opgaver som blev stillet omhandlede hvilken type elevdata de er i kontakt med, deres opbevaring af elevdata, deres arbejdsgange og procedurer i forbindelse med at øge datasikkerheden, de programmer og produkter de bruger og hvor de er usikre i forbindelse med håndteringen af elevdata.

10.1.5 Bearbejdning af kvalitative data

Alle optagelser af interviews er blevet meningstransskriberet med henblik på at blive kodet i Nvivo. Under alle interviews på caseinstitutionerne har der siddet en referent, som har kunnet meningstransskribere fra start, dertil er alle lydfiler blevet gennemlyttet igen efterfølgende. Der er ved denne form for transskribering i højere grad udarbejdet referater af lydfilerne end ord-for-ord-transskriberinger.

Databehandlingen af de forskellige kvalitative datakilder har taget udgangspunkt i en udarbejdet kodebog i Nvivo, indeholdende koder og definitioner af koderne med henblik på en konsistent og systematisk kodning af datamaterialet. Der har været tale om en åben kodning, så nye perspektiver, der ikke på forhånd var kendskab til, kunne blive medtaget i kodningen. Der er blevet kodet efter om det angår håndtering af elevdata i hhv. administrations-, undervisnings-, markedsførings- eller personfølsomme elevdata øjemed, samt hertil om det omhandler løsninger, udfordringer, behov eller at der udtalt ikke var ændret adfærd fra respondentens side. Ligeledes er der kodet efter digitale produkter, og herunder forlags- og gratis produkter samt om der er en viden om dataafgivelse i forbindelse med at benytte nogle læremidler og udtalelser omkring sikkerhedsstrategier på institutionerne. Derudover har vi haft koder som er benyttet når der har været talt om datahandleraftaler, samt når vi har talt om særlige typer af datas rejse igennem forskellige aktører og devices.

Ved at kode i Nvivo gav det mulighed for analyser både internt på caseinstitutionerne, men også på tværs af flere caseinstitutioner.

10.2 KVANTITATIV DATAINDSAMLING

Der er gennemført kvantitative dataindsamlinger på fem forskellige målgruppeniveauer fordelt på i alt 11 populationer. I tabellen nedenfor er undersøgelsens populationer inddelt efter målgruppeniveau.

Tabel 8: Oversigt over undersøgelsens målgrupper og populationer

Overordnet målgruppe	Populationer
Kommuner	• Kommunale skolechefer eller it-ansvarlige
Institutioner	• Skoleledere på grundskoler • Rektorer på gymnasier • Direktører på erhvervsskoler
Personale	• Lærere og administrativt personale på grundskoler • Undervisere og administrativt personale på gymnasier • Undervisere og administrativt personale på erhvervsskoler
Elever	• Elever i 8.-9. kl. på grundskoler • Elever på gymnasier • Elever på erhvervsskoler
Forældre	• Skolebestyrelsesformænd på grundskoler

Dataindsamlingen blandt lærere, administrativt personale og elever er sket blandt 35 tilfældigt udvalgte uddannelsesinstitutioner. Dataindsamlingen blandt elever og personale er således indlejret i de samme rekrutterede institutioner[56]. De 35 institutioner er fordelt som:

4 erhvervsskoler	**13** folkeskoler	**5** frie grundskoler	**13** gymnasier

10.2.1 Sampleudvælgelse og dataindsamlingsmetoder

I det følgende redegøres for udvælgelsen af undersøgelsens sample, samt fremgangsmåden for dannelsen af kontaktgrundlaget. Derudover vil dataindsamlingsmetoden for hver population kort blive gennemgået.

10.2.1.1 Skolechefer eller kommunale it-ansvarlige

Dataindsamlingen blandt de kommunale it-ansvarlige er gennemført blandt skolechefer eller it-ansvarlige i 60 simpelt tilfældigt udvalgte kommuner. Kontaktgrundlaget er dannet ved hjælp af opslag på kommunens hjemmeside samt telefonisk henvendelse til kommunerne.

Blandt de 60 udvalgte kommuner er alle skolechefer blevet inviteret til at deltage i undersøgelsen. I invitationen er skolechefen blevet bedt om at besvare spørgeskemaet eller uddelegere opgaven til den relevante it-ansvarlige i kommunen. Skolecheferne har modtaget op til 2 påmindelser, hvorefter vi har forsøgt at påminde dem om at deltage i undersøgelsen telefonisk, hvis de endnu ikke har besvaret.

[56] Ikke alle 35 institutioner har sørget for, at de tre målgrupper har besvaret spørgeskemaet. På 24 institutioner har alle tre målgrupper besvaret spørgeskemaet. På fem institutioner har lærere og administrativt personale besvaret, men ikke elever. På to institutioner har lærere, men hverken administrativt personale eller elever besvaret. På fire institutioner har kun elever besvaret undersøgelsen. Det vurderes ikke, at dette forhold påvirker resultaternes repræsentativitet.

I alt har 35 skolechefer eller kommunale it-ansvarlige besvaret spørgeskemaet, hvilket udgør en svarprocent på 58 %.

Tabel 9: Oversigt over svarprocenter blandt kommunale it-ansvarlige

Population	N	n	Svarprocent
Skolechefer eller kommunale it-ansvarlige	**60**	**35**	**58%**

10.2.1.2 Ledere på uddannelsesinstitutioner

Dataindsamlingen blandt ledere er gennemført blandt landets i alt 1.022 uddannelsesinstitutioner. Heraf er 600 ledere på grundskoler, mens de resterende 622 er ledere på enten erhvervsskoler eller gymnasier. De 600 ledere på grundskoler er tilfældigt udvalgt blandt alle landets grundskoler med proportionel sampling så fordelingen af folkeskoler og frie grundskoler er proportionel med den nationale fordeling. De resterende ledere udgør den samlede population af ledere på erhvervsskoler og gymnasier.
Kontaktgrundlaget er dannet på baggrund af institutionsregistret.

Alle institutionsledere har elektronisk modtaget en invitation og op til 2 påmindelser om at deltage i undersøgelsen. De institutionsledere, som ikke har svaret, er blevet telefonisk påmindet om at besvare undersøgelsen.

I alt har 468 ledere på uddannelsesinstitutioner besvaret spørgeskemaet, hvilket udgør en svarprocent på 46 %.

Tabel 10: Oversigt over svarprocenter blandt ledere på uddannelsesinstitutioner

Målgruppe	N	n	Svarprocent
Ledere	**1.022**	**468**	**46%**
Folkeskoler	413	188	46%
Frie grundskoler	187	90	48%
Erhvervsskoler m.v.	289	95	33%

10.2.1.3 Personale på uddannelsesinstitutioner

Dataindsamlingen blandt lærere og øvrigt personale er gennemført blandt 2.148 lærere og 392 personer fra det administrative personale fra de 35 forhåndsrekrutterede institutioner. Kontaktgrundlaget er dannet ved at institutionerne har udleveret en liste til Epinion med navn og e-mailadresse på de relevante undervisere og øvrige personale.

Lærerne og det administrative personale har modtaget en invitation og op til to påmindelser om at deltage i undersøgelsen.

I alt har 708 lærere og 167 fra det administrative personale besvaret undersøgelsen, hvilket udgør en svarprocent på hhv. 33 % og 43 %.

Tabel 11: Oversigt over svarprocenter blandt personale på uddannelsesinstitutioner

Målgruppe	N	n	Svarprocent
Lærere	**2.148**	**708**	**33%**
Folkeskoler	432	136	31%
Frie grundskoler	152	28	18%
Erhvervsskoler m.v.	484	193	40%
Gymnasier og HF-kurser	1.080	351	33%
Administration	**392**	**167**	**43%**
Folkeskoler	51	12	24%
Frie grundskoler	20	6	30%
Erhvervsskoler m.v.	174	71	41%
Gymnasier og HF-kurser	147	78	53%

10.2.1.4 Elever

Dataindsamlingen blandt elever er sket blandt de omkring 36.421[57] elever i målgruppen blandt de 35 rekrutterede institutioner. Blandt grundskolerne er kun elever i 8.- og 9.- klasse blevet inviteret til at deltage i undersøgelsen, mens alle elever på erhvervsskolerne og gymnasier er blevet inviteret.

Institutionerne har distribueret fælles informationsmateriale til institutionens lærere som afsæt for, at de enkelte klassers elever kan besvare undersøgelsen som led i en lektion/time. Eleverne har modtaget et åbent link, hvor de har haft mulighed for at angive hvilken institution de er tilknyttet.

I alt har 7.048 elever besvaret spørgeskemaet, hvilket udgør en svarprocent på 19 %.

Tabel 12: Oversigt over svarprocenter blandt elever

Målgruppe	N	n	Svarprocent
Elever	**36.421**	**7.048**	**19%**
Folkeskoler	2.035	481	24%
Frie grundskoler	413	175	42%
Erhvervsskoler m.v.	23.671	1.417	6%
Gymnasier og HF-kurser	10.302	4.975	48%

[57] Antallet af elever er estimeret på baggrund af institutionernes officielle opgørelser over antallet af elever i målgruppen.

10.2.1.5 Skolebestyrelsesformænd

Dataindsamlingen blandt skolebestyrelsesformænd er sket blandt 86 skolebestyrelsesformænd blandt de grundskoler, hvis ledere har besvaret skolelederundersøgelsen. I forbindelse med skoleledernes besvarelse af spørgeskemaet, har lederne haft mulighed for at angive skolebestyrelsesformændenes kontaktinformationer.

De 86 skolebestyrelsesformænd har modtaget en invitation og op til to påmindelser om at deltage i undersøgelsen.

I alt har 30 skolebestyrelsesformænd besvaret undersøgelsen, hvilket udgør en svarprocent på 30 %.

Tabel 13: Oversigt over svarprocenter blandt skolebestyrelsesformænd

Målgruppe	N	n	Svarprocent
Skolebestyrelsesformænd	86	30	35%

10.2.2 Udvikling af spørgeskemaer

Der er udviklet i alt 7 selvstændige spørgeskemaer til ledere af folkeskoler, ledere af selvejende institutioner, IT-chefer, elever, administrativt personale, lærere og skolebestyrelsesformænd. Som fremhævet i rapporten er tematikkerne dog ens på tværs af målgrupperne, og i de fleste tilfælde er det samme spørgsmål stillet med hhv. en leder-, lærer- administrations- og elevvinkel.

Spørgeskemaerne er udarbejdet og kvalitetssikret af Epinions konsulenter og efterfølgende i videre dialog med STIL og relevante interessenter. Produktkategorier er udviklet med afsæt i de indsigter fra kvalitative casebesøg. Spørgeskemaerne er ligeledes blevet pilottestet af 2 repræsentanter fra hver målgruppe, dog med undtagelse af skemaet til IT-chefer, som kun er pilottestet af én repræsentant og spørgeskemaet til skolebestyrelsesformænd, som ikke er pilottestet.

10.2.3 Repræsentativitet

I det følgende vurderes repræsentativitet af undersøgelsens datagrundlag. Dette gøres på baggrund af ovenstående svarprocenter, samt uddybende analyser.

10.2.3.1 Skolechefer eller kommunale it-ansvarlige

Svarprocenten blandt skolechefer og de kommunale it-ansvarlige er 58 %, hvilket indikerer en høj grad af repræsentativitet. Dette bakkes desuden op af en opgørelse over den geografiske repræsentativitet af skolechefer og de kommunale it-ansvarlige, som viser at der kun i meget lav grad er forskel på den geografiske spredning i populationen af kommunale skolechefer og dem der reelt har besvaret spørgeskemaet.

Tabel 14: Geografisk repræsentativitet af skolechefer og kommunale it-ansvarlige

Region	Population	Besvarelser	Difference
Region Hovedstaden	25%	17%	-8%
Region Midtjylland	20%	26%	6%

Region Nordjylland	12%	11%	-1%
Region Sjælland	18%	17%	-1%
Region Syddanmark	25%	29%	4%

På baggrund af disse analyser vurderes repræsentativiteten af datagrundlaget blandt skolechefer eller kommunale it-ansvarlige at være høj.

10.2.3.2 Ledere på uddannelsesinstitutioner

Svarprocenten blandt ledere på uddannelsesinstitutioner er samlet set 46 %. På tværs af institutionerne er der en relativ stor forskel, idet svarprocenten blandt ledere på gymnasier er på 71 % og 33 % for ledere på erhvervsskoler. Den relativt høje svarprocent taler samlet set for, at datagrundlaget blandt ledere i høj grad af repræsentativt for ledere på uddannelsesinstitutioner.

Påstanden om, at datagrundlaget af ledere på uddannelsesinstitutioner, understøttes desuden af, at der kun er en meget lille forskel i den geografiske spredning blandt de institutioner, som har besvaret undersøgelsen og populationen.

Tabel 15: Geografisk repræsentativitet af ledere på uddannelsesinstitutioner

Institutionstype	Region	Population	Besvarelser	Difference
Erhvervsskoler m.v.	Region Hovedstaden	24%	22%	-2%
	Region Midtjylland	24%	28%	4%
	Region Nordjylland	13%	8%	-4%
	Region Sjælland	17%	18%	1%
	Region Syddanmark	22%	23%	1%
Folkeskole	Region Hovedstaden	27%	28%	1%
	Region Midtjylland	23%	24%	1%
	Region Nordjylland	13%	15%	2%
	Region Sjælland	15%	12%	-3%
	Region Syddanmark	22%	20%	-1%
Friskoler og private grundskoler	Region Hovedstaden	24%	28%	4%
	Region Midtjylland	26%	21%	-5%
	Region Nordjylland	12%	10%	-2%
	Region Sjælland	15%	16%	1%
	Region Syddanmark	22%	26%	3%
Gymnasier og HF-kurser	Region Hovedstaden	31%	32%	1%
	Region Midtjylland	23%	21%	-2%
	Region Nordjylland	11%	11%	0%
	Region Sjælland	14%	14%	0%
	Region Syddanmark	21%	23%	2%

Den samme tendens ses, når man ser på forskellen i skolestørrelser blandt ledere der har besvaret undersøgelsen og den samlede population.

Tabel 16: Institutionsstørrelsernes repræsentativitet af ledere på uddannelsesinstitutioner

Institutionstype	Størrelse	Population	Besvarelser	Difference
Erhvervsskoler m.v.	Over 400	68%	71%	-2%
	Under 400	32%	29%	2%
Folkeskole	Over 400	56%	61%	-5%
	Under 400	44%	39%	5%
Friskoler og private grundskoler	Over 400	13%	19%	-6%
	Under 400	87%	81%	6%
Gymnasier og HF-kurser	Over 400	87%	88%	-1%
	Under 400	13%	12%	1%

10.2.3.3 Personale og elever på uddannelsesinstitutioner

Dataindsamlingen blandt personale og elever er sket blandt 35 udvalgte institutioner. Disse institutioner kan ikke siges at udgøre et repræsentativt udsnit af de danske uddannelsesinstitutioner, om end udvælgelsen er disse er sket tilfældigt. Dette forhold bør der tages forbehold for, når der fortolkes resultaterne fra undersøgelserne blandt personale og elever.

Svarprocenten blandt disse målgrupper er dog relativt høj. Således ses det, at svarprocenten blandt lærere og administrativt personale på uddannelsesinstitutionerne er på hhv. 33 % og 43 %. Svarprocenten på 19 % blandt elever anses for at være god sammenlignet med lignende undersøgelser. Der bør dog taget forbehold for, at hovedparten af elevbesvarelser er fra gymnasieelever. Dette bør især tages in mente, når der laves opgørelser for alle elever.

10.2.3.4 Skolebestyrelsesformænd

Svarprocenten blandt skolebestyrelsesformænd er 35 %, hvilket er relativt godt. Alligevel bør analysens resultater tages med forbehold for, at disse data ikke udgør et repræsentativt udsnit af skolebestyrelsesformænd. Dette skyldes, at de 86 skolebestyrelsesformænd kun er et udsnit blandt dem, der har besvaret undersøgelsen blandt grundskoleledere og som har indvilget i at videregive kontaktoplysninger på skolebestyrelsesformanden på deres skole.

EPINION

WWW.EPINIONGLOBAL.COM

EPINION AARHUS
Hack Kampmanns Plads 1-3
8000 Aarhus C
Denmark
+45 87 30 95 00
aarhus@epinionglobal.com

EPINION COPENHAGEN
Ryesgade 3f
2200 Copenhagen N
Denmark
+45 87 30 95 00
copenhagen@epinionglobal.com

EPINION HAMBURG
Ericusspitze 4
20457 Hamburg
Germany
+43 (0)699 13180416
hamburg@epinionglobal.com

EPINION LONDON
D'Albiac House (Room 1015-1017)
Cromer Road, Heathrow Central Area
Hounslow, TW6 1SD
+44 (0) 7970 020793
london@epinionglobal.com

EPINION MALMÖ
Adelgatan 5
21122 Malmö
Sweden
+45 87 30 95 00
tv@epinionglobal.com

EPINION OSLO
Biskop Gunnerus Gate 2
0155 Oslo
Norway
+47 90 11 73 50
oslo@epinion.no

EPINION SAIGON
11th Fl, Dinh Le Building,
1 Dinh Le, Dist. 4, Hcmc
Vietnam
contact@epinionglobal.com

EPINION STAVANGER
Klubbgaten 4
4006 Stavanger
Norway
+47 90 17 18 99
stavanger@epinion.no

EPINION VIENNA
Hainburgerstrasse 20/7
1030 Vienna
Austria
+43 (0)699 13180416
vienna@epinionglobal.com