



Spørsmål 180 (2021) fra Maud Sørum Vestnes, Linda Kristin Jakobsen og Herman Ekle Lund (V): Oppfølgingsspørsmål om personvern i skolen

Til: Rådmannen
Fra: Herman Ekle Lund (V)

Dato: 15.09.2021
Saksnr: 21/00070-182
Deres ref:

Vi viser til tidligere besvarte spørsmål 122 om personvern i skolen. <https://www.drammen.kommune.no/globalassets/politikk-og-samfunn/dokumenter/sporsmal-og-svar/2021spm122msvar.pdf>

Vi viser også til besvart muntlig spørsmål til kommunaldirektør Fredrik Holtan om liknende tema i partssammensatt samarbeidsutvalg 06.09.21, ved hans interessante orientering om «Oppfølging av digitaliseringsstrategien og status digitaliseringsprosjekter».

Kommunens nye digitaliseringsstrategi stiller høye forventninger til vårt arbeid med personvern av skoleelever, og andre innbyggere. Under «*Alle er trygge på at personvern er ivaretatt*» i digitaliseringsstrategien finnes følgende vedtatte målsetninger:

- *Drammen kommune skal prioritere investering i infrastruktur som kommer innbyggerne og næringslivet til gode.*
- *Drammen kommune skal ha et høyt digitalt sikkerhetsnivå som ivaretar personvern og sikrer IKT-infrastrukturen mot uønsket risiko.*
- *Innbyggere, næringslivet og kommunens brukere skal ha tillit at informasjonssikkerhet og personvern blir ivaretatt.*
- *All nødvendig investering skal ta utgangspunkt i hensynet til personvern og informasjonssikkerhet.*

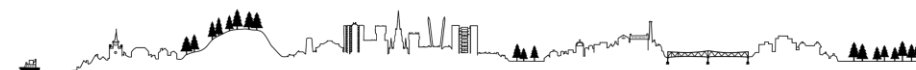
For å lykkes med disse og andre modige målsetninger må kommunen nødvendigvis etterstrebe å være «best i klassen» i alle praktiske formål. Dette har vi høy tillit til at rådmannen vil kunne oppnå, etter den offensive og kunnskapsrike tilnærmingen vi opplever å dømmе.

Strategiens ambisjonsnivå bidrar likevel at vi, på bakgrunn av ny, ekstern kunnskap, samt grunnet ønske om supplerings/utfylling av tidligere skriftlig og muntlig besvarelse, ønsker å stille rådmannen følgende oppfølgingsspørsmål.

Vi har forståelse for at spørsmålene er omfattende og forventer ikke hurtig besvarelse.

- Vi ber om innsyn i ROS- og DPIA-analysene som er utført, med henvisning til svaret på spm 122.

Styring og eierskap



- Bestemmer Drammen kommune, eller leverandør, innholdet i databehandleravtalene som er nevnt i svaret på spm 122, eller er det en forhandling mellom partene? Vi ber om innsyn i disse databehandleravtalene.
- Viser til rådmannens planlagte oppfølging av Kikora, som beskrevet i svaret på spm 122. Hva er resultatet av denne dialogen, og hvordan vurderer rådmannen Kikoras eventuelle svar?
- Viser til følgende, i svaret til spm 122: «*Drammen kommune har startet arbeidet med å skaffe seg en oversikt over alle kommunens databehandlere med henblikk på om det skjer overføring av data til tredjeland, samt hvilke overføringsmekanismer som benyttes der slik overføring skjer. Dette er et stort arbeid som i praksis startet opp rett før årsskiftet 2021. På grunn av pandemien har det vært vanskelig å øke intensiteten og fremdriften i dette arbeidet. Det forventes at dette arbeidet kan strekke seg inn i 2022.*» Hva er status på dette arbeidet?
- Konsulentselskapet Bouvet lanserte 12.08.21 en rapport om personvern i norsk skole: https://cdn.vev.design/private/hNjwDIts16ZNNuwMVdzd56NnMyz1/38XFoNiOFC_Digitalisering%20i%20skolen%20-%20Har%20vi%20glemt%20personvernet.pdf.pdf
Den fokuserer særlig på hvordan personvern ble ivaretatt i den norske skolen gjennom pandemitiden og den omfattende digitaliseringen som da skjedde «over natta». Tilbakemeldingene fra kommunene som er intervjuet i rapporten viser at skoleeiere i liten grad har hatt kontroll over bruken av gratisapplikasjoner i undervisning i skolen, særlig under pandemien. Bruk av gratisapplikasjoner medfører en betydelig risiko for at elevenes persondata kommer på avveie. I lys av denne rapporten ber vi rådmannen å svare ut det følgende:
 - ◆ Hvor mange og hvilke gratisapplikasjoner har blitt brukt i undervisningssammenheng i nye Drammen? (Rådmannen skrev i svaret på spm 122 at «Kommunen har kontroll på porteføljen av hva som brukes av skolene.»)
 - ◆ Hvilke systemer eller rutiner har / har rådmannen hatt for å føre tilsyn og kontroll med bruk av slike gratisapplikasjoner?
 - ◆ Hvis svaret på det foregående var at det ER blitt benyttet slike gratisapplikasjoner – hvilke tiltak er gjort for å kartlegge om persondata har kommet på avveie som følge av dette, og for å spore disse eventuelle lekkasjene?
 - ◆ Viser til Bouvet-rapporten som viser at ingen (!) lærere i datagrunnlaget vet hva de skal gjøre i en situasjon hvor elevenes persondata kommer på avveie, samt at svært få skoleeiere tror at disse rutinene er gjort kjent av skoleeier til lærere. Hvordan er Drammens system for avvismelding ved mistanke om persondata på avveie? Hva er rådmannens vurdering av hvor godt kjent, innlært og brukt dette systemet er opp mot lærere og skoleledere?
- Elever som tildeles egne epostkontoer står i utgangspunktet fritt til å benytte disse adressene til å registrere seg på andre sider og tjenester som ikke har noe med undervisning å gjøre. (Kasino, spill, nyhetsbrev, osv.) Besøk på slike landingssider og videre registrering derfra medfører svært høy risiko for at persondata kommer på avveie og videreselges, og at eleven deretter med høy sannsynlighet blant annet vil utsettes for målrettet markedsføring fra tredjeparter. Skolen har naturligvis ikke mulighet til å begrense hva elever gjør i sin private sfære med private verktøy, men så lenge det er skole-adresser som benyttes så mener vi dette er en del av skolens ansvar. Hvilke rutiner har derfor rådmannen for å forebygge at skole-epostadresser benyttes til denne typen risikofylt atferd?
- Datatilsynet kom med en ny veileder i september, for hva som skal til for at personopplysninger kan overføres til land utenfor EØS: <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos/overforingsgrunnlag/> Stiller denne veilederen noen av rådmannens tidligere vurderinger i et nytt lys, i tilfelle hvordan? Viser til refleksjonen rådmannen hadde rundt denne typen deling av persondata utenfor EØS i svaret på spørsmål 122.

- Disse spørsmålene gjelder skolesektoren spesielt, mens personvern er aktuelt for alle digitale brukere av Drammen kommunes ulike tjenester. Er svarene som rådmannen har gitt dekkende også for øvrige tjenester, eller vil det være andre utfordringer tilknyttet f.eks. helse, sosial og omsorg? Belys i så fall gjerne dette, hvis relevant.

Vi vil avslutningsvis gjenta at vi synes rådmannen viser en god og offensiv tilnærming til temaet, basert på den nevnte tidligere dialogen samt arbeidet med digitaliseringsstrategien. Vi er også klar over at mange av de beskrevne problemstillingene er utfordringer som kanskje med fordel bør løses på et høyere forvaltningsnivå og hvor det kan være urimelig å forvente at hver enkelt kommune skal klare å lage egne, perfekte rutiner og løsninger.

Samtidig kan det virke som Drammen, og andre kommuner, har et u-utløst potensiale for å møte og kommunisere med brukerne på en smart måte som sikrer trygghet og innsikt i møte med slike stadig mer aktuelle bekymringer rundt datasikkerhet og personvern. Vi ønsker derfor en avsluttende refleksjon rundt det følgende:

- Hvordan kan Drammen kommune skape en god, åpen og transparent kommunikasjon om disse problemstillingene med brukere (både elever/foreldre i skolen samt alle andre digitale brukere av kommunale tjenester) – og om mulig stimulere til å skape interesse og kunnskapsdeling rundt temaet?

Svar

Rådmannen vil innledningsvis beklage sent svar. Spørsmålene er til dels detaljerte og en uttømmende besvarelse av spørsmålene ville kreve utdypende svar om lokale, faglige systemer og nasjonale og internasjonale bestemmelser. For at svarene i denne saken ikke skal bli for omfattende og detaljerte, kan rådmannen evt gi ytterligere informasjon vår systemforvaltning og internkontroll i en muntlig orientering i egnet organ.

Kommuneloven har krav om internkontroll og opprettelse av kontrollutvalg. I tillegg til ordinære kontrollrutiner og rapportering, blir ulike områder i kommunen gjenstand for forvaltningsrevisjoner med jevne mellomrom. I 2020 ble det gjennomført forvaltningsrevisjon på personvern i Drammen kommune. Den ble initiert av kontrollutvalget og rapporten fra Viken kommunerevisjon forelå i februar 2021. Fire anbefalte oppfølginger ble vedtatt i kommunestyret 4. mai 2021.

Drammen kommune har etter hvert god kompetanse på IT-sikkerhet. Det er likevel slik at det selv for en stor kommune er svært krevende å til enhver tid holde seg oppdatert. Endringer skjer raskt, og det er snakk om svært komplekse problemstillinger. Derfor er det påkrevet at andre forvaltningsnivåer gjør informasjon tilgjengelig til rett tid, og på en måte som gjør det enkelt for kommunene å innarbeide regelverk i våre rutiner og at kommunene selv er proaktive og søker informasjon om utviklingen.

Kommunesammenslåingen har bidratt til en ytterligere gjennomgang av alle områdene i de 3 «gamle» kommunene som var utgangspunkt for nye Drammen kommune. Ett eksempel er IKT-området med prosjekt A4.2 hvor hele systemporteføljen ble gjennomgått og ryddet i, samtidig med ivaretagelsen av arkivering fra systemene i de tidligere kommunene. Dette er en opprydding som spesielt kommunene som ble berørt av kommunereformen har vært igjennom. Harmonisering og standardisering vil ikke automatisk bidra til økt informasjonssikkerhet, men vi har fått bedre oversikt og kjenner derfor sårbarhetene godt og kan slik sett si at informasjonssikkerheten er god.

1. Vi ber om innsyn i ROS- og DPIA-analysene som er utført, med henvisning til svaret på spm 122

Svar:

Viken kommunerevisjon behandlet spørsmålet om tilstrekkelige risiko- og sårbarhetsanalyser ganske inngående. Både ROS-analyser og gjennomførte DPIA (Data Protection Impact Assessment) var omfattet av revisjonen. De ble gitt innsyn i en rekke ROS-vurderinger og en DPIA. Overordnet var de fornøyd med innholdet i dokumentene og arbeidet rundt ROS-analyser. En oppsummering kan leses på side 16 i revisjonsrapporten, se [Forvaltningsrevisjon om personvern](#)

Både ROS og en DPIA vil inneholde opplysninger som etter sin art kan avsløre sårbarheter knyttet til organisering og tekniske løsninger, og dermed kunne være utsatt for cybertrusler. Derfor vil tilgjengeliggjøring av ROS-analyser og DPIA evt skje direkte mellom spørsmålsstillere og politisk sekretariat. Dette initieres av administrasjonen. For øvrig gir malene som brukes både til selve løsningsbeskrivelsen og ROS god oversikt over hvordan det jobbes. Disse kan tilgjengeliggjøres hvis ønskelig.

2. Bestemmer Drammen kommune, eller leverandør, innholdet i databehandleravtalene som er nevnt i svaret på spm 122, eller er det en forhandling mellom partene?

Vi ber om innsyn i disse databehandleravtalene

Svar:

Det vises også her til tidligere nevnte revisjonsrapport. Spørsmålet som ble stilt var: Har kommunen oppdaterte «databehandleravtaler»? Revisjonen var generelt middels fornøyd, se side 21 i [rapporten](#). Rådmann har derfor startet et arbeid på dette området. Dette er et eget oppfølgingspunkt gjennom kontrollutvalget, med neste rapportering juni 2022. Det kan videre nevnes at Drammen Kommune fortrinnsvis ikke godtar andre maler for databehandleravtaler enn de som Datatilsynet anbefaler.

Innsyn i databehandleravtaler vil måtte behandles på samme måte som nevnt i svaret ovenfor.

3. Viser til rådmannens planlagte oppfølging av Kikora, som beskrevet i svaret på spm 122. Hva er resultatet av denne dialogen, og hvordan vurderer rådmannen Kikoras eventuelle svar?

Svar:

Vi har vært i dialog med Kikora og vurderer svarene vi har fått som tilfredsstillende med ett unntak; lagringstid fra tidspunktet en elev slutter på skolen frem til innsamlede opplysninger om eleven slettes, vurderes som for lang. Vi er i kontakt med Kikora for å vurdere muligheten for redusert lagringstid. Dagens lagringstid er likevel en restrisiko som er akseptabel.

4. Viser til følgende, i svaret til spm 122: «Drammen kommune har startet arbeidet med å skaffe seg en oversikt over alle kommunens databehandlere med henblikk på om det skjer overføring av data til tredjeland, samt hvilke overføringsmekanismer som benyttes der slik overføring skjer. Dette er et stort arbeid som i praksis startet opp rett før årsskiftet 2021. På grunn av pandemien har det vært vanskelig å øke intensiteten og fremdriften i dette arbeidet. Det forventes at dette arbeidet kan strekke seg inn i 2022.» Hva er status på dette arbeidet?

Svar:

Overordnet kartlegging av status er gjort. Om lag halvparten av kommunens systemer har blitt knyttet til avtale, og på disse er status for DBA kjent. I øvrige avtaler vil det sendes en survey til systemeiere og forvaltere der de ansvarliggjøres for å oppdatere status for avtale og DBA på sine system. Denne er klar til testing, neste skritt er informasjon og utsendelse. Det kreves betydelig arbeid av systemeiere og

forvaltere der hver enkelt DBA må gås opp. Fremdrift avhenger av ressursituasjonen hos virksomhetene, men arbeidet er styrket ved at det er ansatt en person for å sikre fremdriften i arbeidet.

5. Konsulentselskapet Bouvet lanserte 12.08.21 en rapport om personvern i norsk skole: [lenke](#)

Den fokuserer særlig på hvordan personvern ble ivaretatt i den norske skolen gjennom pandemien og den omfattende digitaliseringen som da skjedde «over natta». Tilbakemeldingene fra kommunene som er intervjuet i rapporten viser at skoleeiere i liten grad har hatt kontroll over bruken av gratisapplikasjoner i undervisning i skolen, særlig under pandemien. Bruk av gratisapplikasjoner medfører en betydelig risiko for at elevenes persondata kommer på avveie. I lys av denne rapporten ber vi rådmannen å svare ut det følgende:

- a. Hvor mange og hvilke gratisapplikasjoner har blitt brukt i undervisningssammenheng i nye Drammen? (Rådmannen skrev i svaret på spm 122 at «Kommunen har kontroll på porteføljen av hva som brukes av skolene.»)**
- b. Hvilke systemer eller rutiner har / har rådmannen hatt for å føre tilsyn og kontroll med bruk av slike gratisapplikasjoner?**
- c. Hvis svaret på det foregående var at det ER blitt benyttet slike gratisapplikasjoner – hvilke tiltak er gjort for å kartlegge om persondata har kommet på avveie som følge av dette, og for å spore disse eventuelle lekkasjene?**
- d. Viser til Bouvet-rapporten som viser at ingen (!) lærere i datagrunnlaget vet hva de skal gjøre i en situasjon hvor elevenes persondata kommer på avveie, samt at svært få skoleeiere tror at disse rutinene er gjort kjent av skoleeier til lærere. Hvordan er Drammens system for avviksmelding ved mistanke om persondata på avveie? Hva er rådmannens vurdering av hvor godt kjent, innlært og brukt dette systemet er opp mot lærere og skoleledere?**

Svar:

Dersom persondata kommer på avveie, må elev/foresatte/lærer umiddelbart gi beskjed til skoleledelsen, slik at de får fulgt opp det enkelte tilfelle.

Slik sikrer man at sakene meldes inn som avvik og dermed registreres i kvalitetssystemet.

All programvare som brukes i skole er kartlagt og registreres i kommunens systemoversikt. Alle systemene har en dedikert systemeier. Det er ansatt en person i rollen systemforvalter, som tiltrer i 2022. Vedkommende får ansvar for å forvalte all pedagogisk programvare, dvs. å holde kontakt med leverandørene, å få informasjon og rutinebeskrivelser ut til skolene, å håndtere lisenser samt sikre at personvern og sikkerhet er ivaretatt.

Det gjenstår en del arbeid rundt revidering av ROS-analyser av ulike programvare som er i bruk på skolene. Dette etterslepet er planlagt innhentet i løpet av 2022.

Det pågår et kontinuerlig arbeid rundt personvern og sikkerhet både sentralt og ute på skolene. I forbindelse med utarbeidelse av handlingsplan for digitaliseringsstrategien, ble det gjennomført en kompetansekartlegging. Kartleggingen viser at mellom 70 og 78 % (avhengig av rolle; pedagogisk medarbeider/lærer/skoleleder) vet hvem de skal henvende seg til dersom de opplever sikkerhetsbrudd eller uventede hendelser på nett. Vi tolker svaret dithen at flertallet vet hva de skal gjøre dersom elevs persondata kommer på avveie. For å sikre at alle vet hva de skal gjøre i slike situasjoner, vil skoleeier, i samarbeid med IKT og personvernombudet, igangsette kompetansehevingstiltak i samsvar med Digitaliseringsstrategien i 2022.

Høsten 2021 er det gjennomført flere prosesser som danner godt grunnlag for videre arbeid rundt personvern og sikkerhet. Bl.a.:

- All pedagogisk programvare som tilgjengeliggjøres via FEIDE (påloggingsløsning for utdanningssektoren) er gjennomgått og vurdert.
- Programvare som ikke er i bruk, er fjernet fra FEIDE-pålogging.

- På iPad er det standardisert hvilke apper som er tilgjengelig for nedlasting for elevene.
- Det er igangsatt et arbeid for å få tilsvarende standardisering av apper på PC.
- For å ha enda bedre kontroll på hvilke app-er som benyttes, er det besluttet å fjerne App-Store fra alle enheter. Skolene vil da kun få tilgang til et utvalg app-er (inkluderer betal- og gratisapp-er). Disse app-ene kvalitetssikres og ROS-vurderes før de distribueres ut. Dette arbeidet fortsetter utover våren 2022.

Restriksjoner på PC / iPad er vurdert for ytterligere tiltak for kontroll på hva elevene har tilgang til. Det er alltid en balanse mellom å stenge ned og holde åpent ulike funksjoner på elevenes enheter. Det er dog en del av elevens opplæring å måtte manøvrere i en digital, uoversiktlig verden. Her gjøres det fortløpende hensiktsmessige valg og vurderinger.

Virksomhet IKT har overvåking, varsling og sporing av kommunens digitale enheter. Dersom uregelmessigheter på en enhet oppdages, blir elevens PC/iPad «wipet», dvs. at den tilbakestilles til opprinnelig oppsett. Med det fjernes alle programmer som er ulovlig installert.

6. Elever som tildeles egne epostkontoer står i utgangspunktet fritt til å benytte disse adressene til å registrere seg på andre sider og tjenester som ikke har noe med undervisning å gjøre. (Kasino, spill, nyhetsbrev, osv.) Besøk på slike landingssider og videre registrering derfra medfører svært høy risiko for at persondata kommer på avveie og videreselges, og at eleven deretter med høy sannsynlighet blant annet vil utsettes for målrettet markedsføring fra tredjeparter. Skolen har naturligvis ikke mulighet til å begrense hva elever gjør i sin private sfære med private verktøy, men så lenge det er skole-adresser som benyttes så mener vi dette er en del av skolens ansvar. Hvilke rutiner har derfor rådmannen for å forebygge at skole-epostadresser benyttes til denne typen risikofylt atferd?

Svar:

Det er en forutsetning for å kunne ta i bruk tjenester at elever har en e-post adresse, f.eks. for å kunne benytte seg av pedagogisk programvare som tilbys via FEIDE. Elevene skal som en del av undervisningen, lære hvordan e-postadressen deres kan brukes/ikke bør brukes.

Elever skal forholde seg til [Reglement for teknologisk utstyr | Drammen kommune.](#)

Virksomhet IKT har overvåking, varsling og sporing av kommunens digitale enheter. Dersom uregelmessigheter på en enhet oppdages, blir elevens PC/iPad wipet, dvs. at den tilbakestilles til opprinnelig oppsett. Med det fjernes alle programmer som er ulovlig installert.

7. Datatilsynet kom med en ny veileder i september, for hva som skal til for at personopplysninger kan overføres til land utenfor EØS: <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos/overforingsgrunnlag/> Stiller denne veilederen noen av rådmannens tidligere vurderinger i et nytt lys, i tilfelle hvordan? Viser til refleksjonen rådmannen hadde rundt denne typen deling av persondata utenfor EØS i svaret på spørsmål 122.

Svar:

Rådmannens tidligere vurdering endres ikke i nevneverdig grad. Men til forskjell fra tidligere så har EU-kommisjonene i mellomtiden vedtatt nye standard personvernbestemmelser¹. Disse omhandler lovlig overføringsgrunnlag og bl.a. bruk av de nye standardavtalene (SCC). De gamle standardavtalene, som en del leverandører har benyttet seg av, er opphevet. Reglene er slik at avtaler inngått før 27. September 2021, på gammel mal, er lovlig overføringsgrunnlag frem til 27. desember 2022. Nye anskaffelser etter 27. September 2021 skal følge de nye standardavtalene. Disse reglene er foreløpig kun bindende for EU-land, men det forventes at rettsakten snarlig blir også blir vedtatt innenfor EØS. Selv om reglene ennå ikke er norsk lov, må vi uansett ta hensyn til disse når leverandøren operer innenfor EU og har underleverandører utenfor EU.

8. Disse spørsmålene gjelder skolesektoren spesielt, mens personvern er aktuelt for alle digitale brukere av Drammen kommunes ulike tjenester. Er svarene som rådmannen har gitt dekkende også for øvrige tjenester, eller vil det være andre utfordringer tilknyttet f.eks. helse, sosial og omsorg? Belys i så fall gjerne dette, hvis relevant.

Svar:

De samme reglene for personvern og informasjonssikkerhet gjelder alle kommunens tjenesteområder. I tillegg er det slik som det poengteres i spørsmålet at f.eks. helseopplysninger gjør at journalsystemer og behandling av personopplysninger stiller ekstra krav til tjenesteområdene innen helse, sosial og omsorg. I tillegg har vi brukergrupper med ulik kompetanse når det gjelder digital atferd, kunnskapsnivå om trusler og bruk av digitale enheter.

9. Vi vil avslutningsvis gjenta at vi synes rådmannen viser en god og offensiv tilnærming til temaet, basert på den nevnte tidligere dialogen samt arbeidet med digitaliseringsstrategien. Vi er også klar over at mange av de beskrevne problemstillingene er utfordringer som kanskje med fordel bør løses på et høyere forvaltningsnivå og hvor det kan være urimelig å forvente at hver enkelt kommune skal klare å lage egne, perfekte rutiner og løsninger.

Samtidig kan det virke som Drammen, og andre kommuner, har et u-utløst potensiale for å møte og kommunisere med brukerne på en smart måte som sikrer trygghet og innsikt i møte med slike stadig mer aktuelle bekymringer rundt datasikkerhet og personvern. Vi ønsker derfor en avsluttende refleksjon rundt det følgende:

Hvordan kan Drammen kommune skape en god, åpen og transparent kommunikasjon om disse problemstillingene med brukere (både elever/foreldre i skolen samt alle andre digitale brukere av kommunale tjenester) – og om mulig stimulere til å skape interesse og kunnskapsdeling rundt temaet?

Svar:

Så langt det lar seg gjøre, bør Drammen kommune møte alle brukere ut fra deres individuelle behov. Det betyr at ansatte i møte med brukere som ytrer nysgjerrighet eller bekymringer om temaet, skal stille med et åpent sinn og lytte til det som blir lagt fram, og eventuelt bringe innspill videre ved behov. På et organisatorisk nivå, er det en ambisjon at innbyggere, næringslivet og kommunens brukere skal ha tillit at informasjonssikkerhet og personvern blir ivaretatt. Dette er nedfelt i digitaliseringsstrategien.

¹ https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

Kommunen benytter en rekke systemer i kontakten med brukere. Således er det sentralt for å lykkes, at kommunen har dialog med leverandører, slik at hver enkelt løsning legger til rette gjennom god og forståelig informasjon om personvern og informasjonssikkerhet.

Ved siden av tilrettelegging gjennom systemene i seg selv, gis det informasjon i direkte møter. Et eksempel er det informasjonsmøter med eldrerådet, og med andre brukergrupper. I skolen er kildekritikk og personvern tema. Det finnes blant annet en handlingsplan for digitalisering i grunnopplæringen (2020-2021). Videre er digitale ferdigheter videreført som en grunnleggende ferdighet i Kunnskapsløftet 2020. De digitale ferdighetene er tydeliggjort i de nye læreplanene og skal bidra til å styrke elevenes digitale kompetanse og teknologiforståelse. Dette handler for eksempel om at elevene skal utvikle godt digitalt medborgerskap, som inkluderer god digital dømmekraft, kildekritikk og informasjonssikkerhet. Temaet er derfor med i kommunens arbeid med implementering av nye læreplaner gjennom fagfornyelsen.

Fagfeltet er i rask utvikling, og det er uten tvil slik at kompetansen hos både innbyggere og ansatte ennå ikke er tilstrekkelig. Det blir derfor viktig i tiden framover å opprettholde oppmerksomheten på dette temaet i opplærings- og informasjonsarbeid, samtidig som kommunen bør oppfordre til at så mange som mulig viser egeninteresse for temaet.