Personvern i kulturskoler

Taisiia Demina
Strategisk rådgiver informasjonssikkerhet og personvern i Atea

07. september 2022
Førde

Agenda

1. Personvern og hvorfor det er viktig
2. Kulturskolens fremtid: digitalisering, løsninger og utfordringer
3. Den behandlingsansvarlige og den behandlingsansvarliges plikter
4. Risikovurderinger av digitale løsninger
5. Schrems II
6. Barnas personopplysninger
7. Spørreundersøkelse

Personvern og hvorfor det er viktig

Personvern er en grunnleggende rettighet og et fundament mange av de andre menneskerettighetene bygger på.

«Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse»
(Menneskerettskonvensjonens artikkel 8).

Grunnlovens §102: «Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller. Statens myndigheter skal sikre et vern om den personlige integritet»

Personvernet vil i noen tilfeller komme i konflikt med andre rettigheter, f.eks. med ytringsfrihet, men på den annen side kan det være en forutsetning for ytringsfrihet.

Personvern er en viktig ressurs i et fungerende demokrati

Kulturskolens fremtid: digitalisering, løsninger og utfordringer

Rapporten *«På vei mot fremtidens kulturskole»* understrekker fire verdiområder:

- Attraktiv og relevant
- Inkluderende og mangfoldig
- Utviklende og skapende
- Betydningsfull og mestringsorientert

«Innovasjon i kulturskolen kan være å endre prosesser for å gjøre ting bedre, gjøre noe smartere eller skape noe helt nytt".

Kulturskolen har som et mål å forsterke sin rolle som samfunnsaktør og samtidig bli relevant for flest mulig innbyggere. Dette kan oppnås gjennom digitaliseringen, men det skal ikke gå på bekostning av personvernet.

Kulturskolens fremtid: digitalisering, løsninger og utfordringer

Datatilsynet:

«Ved å bruke gratis tilgjengelige verktøy fra de store teknologiselskapene, inviterer nærmest offentlige virksomheter kommersielle aktører til å samle inn og bruke data om norske innbyggere. Samtidig skapes det et avhengighetsforhold som det kan bli vanskelig å fri seg fra ettersom det finnes få alternative tjenestetilbydere».

NOU 2022: 11:

"Mangel på tilstrekkelige sentrale føringer, i kombinasjon med varierende grad av kompetanse og ressurser ute i kommunene, medfører også en risiko for at tjenesteleverandører kan legge premissene for hvordan elevenes personvern ivaretas i skolen".

«Leverandører av tjenester til skole- og barnehagesektoren ikke kan benytte forretningsmodeller som profitterer kommersielt på barnas personopplysninger. I praksis betyr dette at det ikke er akseptabelt å benytte leverandører som forbeholder seg retten til å bruke data til kommersielle formål, særlig markedsføringsaktiviteter".

"For barn og unge i skolen, handler personvern om at foreldre og barn skal vite om og ha kontroll over hvordan opplysningene om barna blir brukt".

Den behandlingsansvarlige for kulturskolen

- Kulturskolene er både eid og drevet av kommunene, og det er kommunene selv som bestemmer innhold og omfang av tilbudet i sine skoler. Dette inkluderer valg av læringsverktøy.

- **Kommune er behandlingsansvarlige** for behandling av personopplysninger i kulturskoler. Den behandlingsansvarlige er den som fastsetter formålet med behandlingen av personopplysninger og bestemmer hvilke hjelpemidler (for eksempel IT-systemer) som skal benyttes.

- Datatilsynet understrekker at offentlige virksomheter har et særlig ansvar for innbyggernes personvern.

NOU 2022: 11:

«Offentlige myndigheter har et ansvar for å holde en høy standard, også når det gjelder personvern. Det innebærer at offentlige myndigheter må gjøre grundige personvernvurderinger og ta i bruk verktøy som respekterer innbyggernes personvern. Personvernkommisjonen anbefaler at offentlig sektor bruker sin innkjøpsmakt for å stimulere til fremveksten av personvernvennlige produkter og tjenester. Det bør gis føringer om hvordan personvern bør vektes i anskaffelser».

Den behandlingsansvarliges plikter

https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/

Personvernforordningen er basert på ansvarsprinsippet

- Dette prinsippet går ut på at virksomheten skal ha full oversikt over sin behandling av personopplysninger og iverksette tekniske og organisatoriske tiltak som gjør at loven følges.
- Hver enkelt virksomhet må gjøre mange viktige vurderinger før de samler inn og bruker personopplysninger.
- Særlig ansvar: offentlige virksomheter og barnas personopplysninger

Den behandlingsansvarliges plikter

- Ha en **behandlingsprotokoll** *(Excel-arket, digitale løsninger for protokollføring – eks. Visma Draftit, OneTrust).* Den skal inneholde det rettslige grunnlaget, formål, typer personopplysninger osv. Protokoll er grunnsteinen for personvernarbeidet og skal være tilgjengelig for tilsynsmyndighetene.
- Overholde **personvernprinsippene** (lovlighet, rettferdighet og åpenhet; formålsbegrensning, dataminimering, riktighetsprinsippet, lagringsbegrensning, prinsippet om integritet og konfidensialitet)
- **Informere** de registrerte (gjennom f.eks. personvernerklæring). Legge til rette for deres rettigheter.
- **Vurdere** leverandører/databehandlere jf. art. 24, 28, 32 GDPR. Samle bevis i dokumentasjonen (spørreskjemaer, inspeksjoner og sertifikater).
- **Vurdere løsninger** og behandlingsaktiviteter jf. art. 24, 32 og 35 GDPR.
- Ha en **oversikt** over hvem som behandler opplysninger på deres vegne og etablere **databehandleravtaler.**
- **Dokumentere** at dere følger lover.
- Ha **rutiner.**
- **Opplæring** av ansatte. De skal være i stand til å håndtere de registrertes begjæringer og oppdage avvik
- Involvere **personvernombudet**

Det er mulig å bruke **maler** fra andre virksomheter – f.eks. KS, KINS, Digdir, kommuner (f.eks. Bærum kommune).

Risikovurderinger av digitale løsninger

- GDPR lovfester et krav om å vurdere risiko og hvilke tiltak som kan settes inn for å redusere risikoen til et akseptabelt nivå (artikkel 24, 32). Kan gjøres i form av **risiko- og sårbarhetsvurdering (ROS)**

- Personvernforordningen stiller krav til å gjennomføre en **vurdering av personvernkonsekvenser (DPIA)** for noen behandlingsaktiviteter hvis det er «sannsynlig» at behandlingen vil medføre «høy risiko for fysiske personers rettigheter og friheter», jf. personvernforordningen artikkel 35 nr. 1.

- Risikovurderinger skal gjøres ved innføring av nye systemer, ved endringer av eksisterende systemer og gjentas regelmessig.

- Ikke inngå databehandleravtaler før risikovurderinger er gjennomført

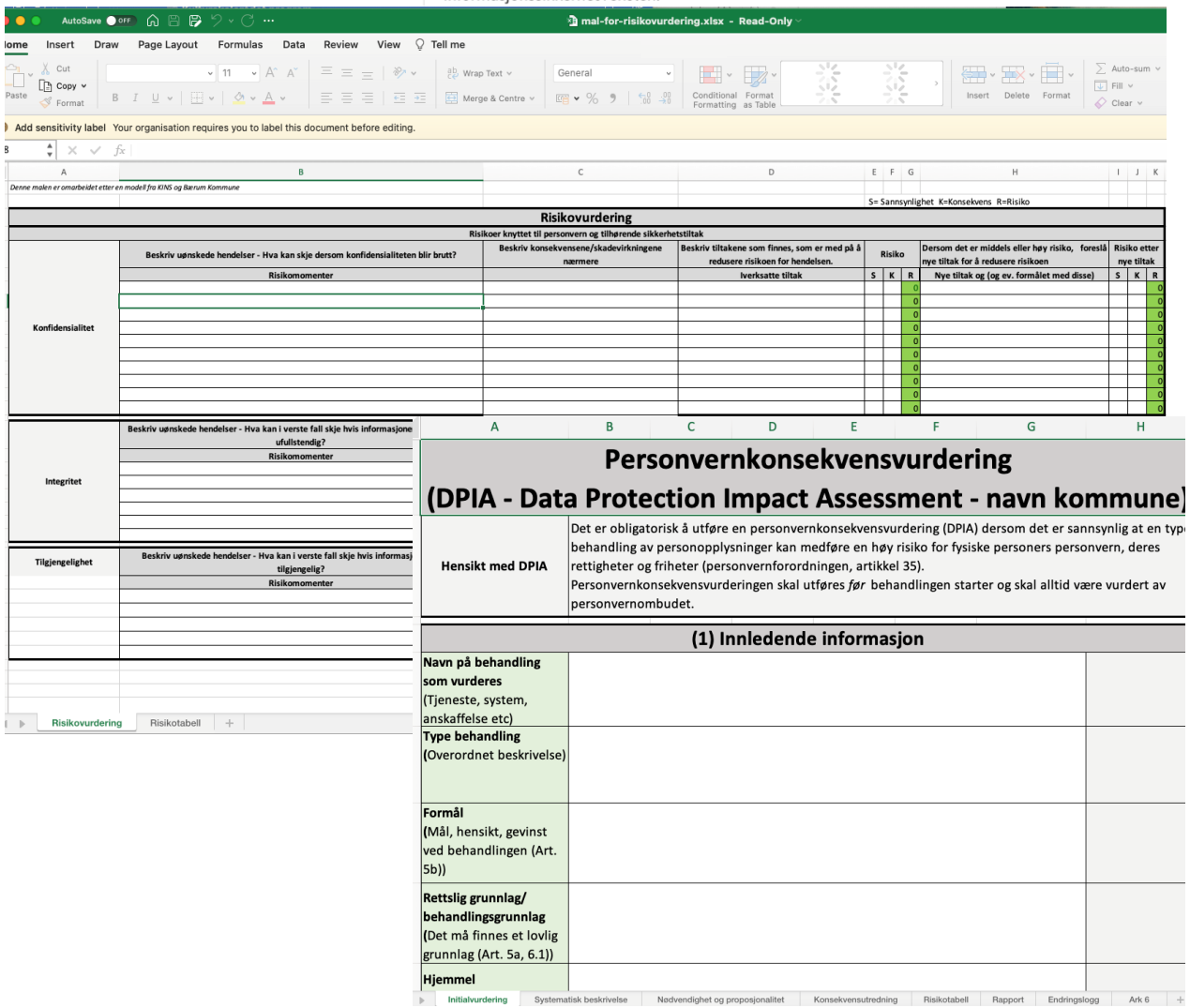
- Den behandlingsansvarlige skal iverksette tiltak som er nødvendige for at risikoen skal bli akseptabel. Tiltakene kan for eksempel være tekniske, organisatoriske og juridiske.

- Nettverk er viktig. Snakk i sektoren om hvilke tjenester som brukes, organiser workshops for å risikovurdere dem sammen. Dere har da større makt til å forhandle om justeringer med leverandøren.

- Barna er **sårbare** registrerte, dette skal alltid inngå i vurderinger.

- Bruk maler.

Fra KS:



Maler for databehandleravtale

Her finner du anbefalt mal for databehandleravtale. Se også digitaliseringsdirektoratets databehandleravtale.

- databehandlaravtale nynorsk →
- databehandleravtale bokmål →
- databehandleravtale engelsk →
- Digitaliseringsdirektoratets databehandleravtale - Oppdatert september 2021 →

Ressursbank for ROS arbeid

Her finner du anbefalt ressurser og maler som kan hjelpe deg med å forankre prosessene knyttet til ROS-arbeid med nye digitale ressurser.

- Spørreskjema til ROS arbeid →
- Mal for risikovurdering →

DPIA maler

Her finner du anbefalt mal for gjennomføring av personvernkonsekvensvurdering (DPIA). I tillegg har SkoleSec utviklet en «dummy»-DPIA som er et støtteverktøy som kan brukes i utarbeidelse av egne

Fra KINS

VERKTØYKASSE

KiNS vil her publisere nyttige verktøy for kommuner og fylkeskommuner. Innholdet er utarbeidet av KiNS, medlemskommuner eller samarbeidspartnere. Vektøyene er utarbeidet av kompetente fagpersoner og organisasjoner. Den enkelte bruker av verktøyene må selv vurdere nytteverdien og er ansvarlig for egen utnyttelse av verktøyene.

RELATERTE ARTIKLER
- KiNS e-læring
- Opplæringsfilmer fra KiNS
- CTF Norway
- Schrems II og leverandøroppfølging
- Maler for databehandleravtaler
- Mal for gjennomføring av DPIA
- Mal for gjennomføring av risikovurdering
- Risikobank
- Kravspec

KALENDER

SEPTEMBER

September 2022 - webinar i samarbeid med IMDi

29. sep 2022 kl 09.00 - kl 10.00

OKTOBER

Oktober 2022 - Sikkerhetstesting for

MAL FOR GJENNOMFØRING AV DPIA

BÆRUM KOMMUNE

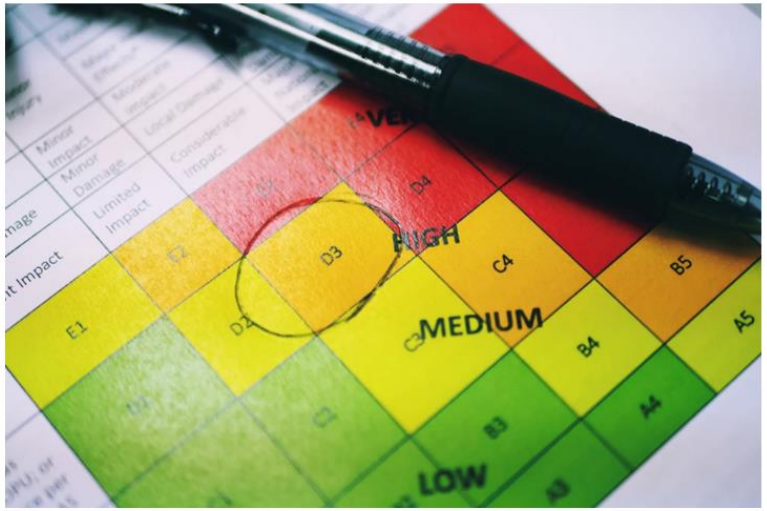
Bærum kommune har utarbeidet en mal for gjennomføring av personkonsekvensutredning, DPIA, som KiNS har fått lov til å dele med våre medlemmer og andre interesserte. Malen brukes på eget ansvar og er et godt utgangspunkt for å gjennomføre DPIA i egen organisasjon.

Å få på plass gode personvernkonsekvensutredninger krever kompetanse og erfaring som bygges opp over tid. KiNS mener malen fra Bærum er et godt utgangspunkt for å bygge kunnskap, erfaring og kompetanse på dette i egen organisasjon.

Den digitale utviklingen går raskt og det er derfor rimelig å anta at malen bør utvikles videre i tråd med behov og den praksis som etableres rundt dette. Vi vil derfor sette stor pris på å få tilbakemeldinger og konkrete forslag til forbedringer i malen.

MAL FOR GJENNOMFØRING AV DPIA

MAL FOR GJENNOMFØRING AV RISIKOVURDERING



Ringerike kommune har delt sin mal for gjennomføring av Risikovurderinger (ROS) med KiNS, og vi har fått lov til å dele den med våre medlemmer og andre interesserte. Malen brukes på eget ansvar og er et godt utgangspunkt for å gjennomføre ROS i egen organisasjon.

"Alt som deles i verktøykassen til KiNS kan fritt brukes av kommuner og fylkeskommuner i deres arbeid med informasjonssikkerhet og personvern. Innholdet i verktøykassen kan ikke videreselges eller på annen måte utnyttes kommersielt til egen vinning.
...
Ta kontakt med KiNS om det spørsmål i den forbindelse".

Fra Digdir

Digdir

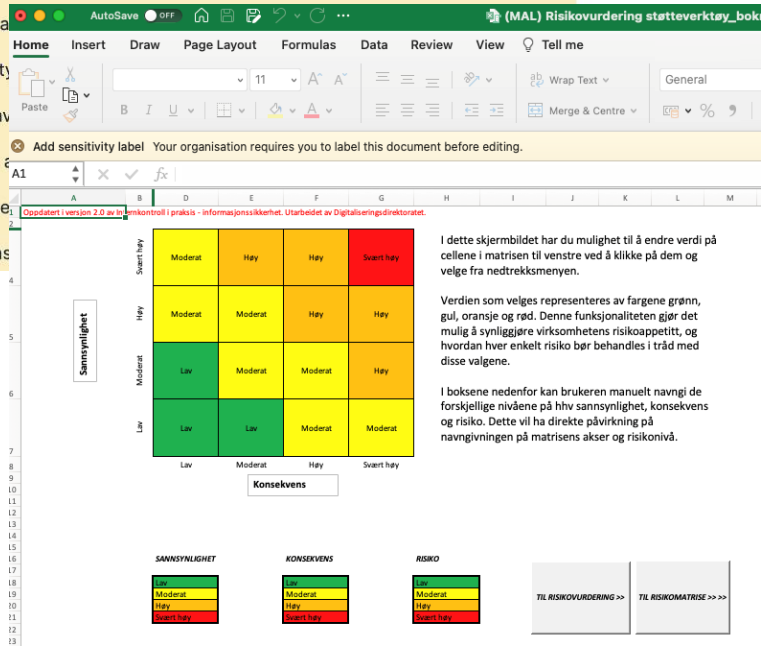
Heim > Informasjonssikkerhet > Internkontroll i praksis > Malar og eksempel

Malar og eksempel

Denne sida gir ein oversikt over alle malar, eksempel og støtteark som er presentert i denne rettleiaren. Malane og eksempla er og å finne under dei aktivitetene der dei naturlig hører heime i materiellet.

På denne sida

- Etableringsa
- Leiinga si sty
- Vurdering av
- Handtering a
- Kompetanse
- Kommunikas



Vurdering av risiko

Ha oversikt og prioritere		
[MAL] Foranalyse Trinn 1 - Oppgaver og informasjonstyper (docx)	Bokmål	Nynorsk
[EKSEMPEL] Typiske oppgaver og tilhørende informasjonstyper (docx)	Bokmål	Nynorsk
[MAL] Foranalyse Trinn 2 - Konsekvensnivå Risikoeier (xlsx)	Bokmål	Nynorsk
[MAL] Foranalyse Trinn 2 - Konsekvensnivå Systemeier Fellessystem (xlsx)	Bokmål	Nynorsk
[MAL] Foranalyse Trinn 3 - Trulser, farer og sårbarheter	Bokmål	Nynorsk
[MAL] Behov og plan for risikovurderinger (docx)	Bokmål	Nynorsk

Gjennomføre risikovurdering		
[MAL] Risikovurdering - støtteverktøy (xlsm)	Bokmål	Nynorsk
[STØTTE] Risikovurdering - støtteverktøy - brukerveiledning (pdf)	Bokmål	Nynorsk

Schrems II – skall inngå i vurderinger

Den 16. juli 2020 i den såkalte «Schrems II»- dommen vurderte EU-domstolen at Facebook brøt reglene i GDPR ifm at Facebook overførte personopplysninger om europeiske brukere til USA. Dommen har betydning for all overføring av personopplysninger fra land i EU til land utenfor EU ("tredjeland").

1. USAs overvåkningspraksis og regelverk strider mot flere av reglene i GDPR og EU-charteret. Privacy Shield ikke kan benyttes som overføringsgrunnlag.

2. Standard personvernbestemmelser (SCCs) er et gyldig overføringsgrunnlag, men i de fleste tilfeller vil det være nødvendig å vurdere beskyttelsesnivået I tredjeland, om dataimportøren er underlagt overvåkingslover, og implementere ytterligere beskyttelsestiltak for å unngå risikoene som følger med et utilstrekkelig beskyttelsesnivå i landet man overfører personopplysninger til.

3. Tiltakene kan være organisatoriske (f.eks. streng tilgangskontroll), tekniske (kryptering og pseudonymisering) eller juridiske (kontraktsforpliktelser)

4. For virksomhetene kan det være komplisert og krevende å vurdere hva som vil være et tilstrekkelig beskyttelsesnivå og hvilke tiltak som bør iverksettes.

5. Personvernrådet (EDPB) og Datatilsynet har gitt ut en veiledning om overføring av personopplysninger til tredjeland.

Særlig om barnas personopplysninger

- Stor fokus på personvern til barn i den Norske personvernpolitikken

- Barnekonvensjonen artikkel 16 (barns rett til personvern), artikkel 3 om hensynet til **barnets beste**, artik- kel 12 om retten til å si sin mening og å bli hørt, artikkel 2 om ikke-diskriminering og artikkel 6 om retten til liv og utvikling. Grunnloven §104: "Barn har rett til vern om sin personlige integritet"

- Spesifikke krav til samtykke fra barn:

✓ Hovedregelen er at barn kan samtykke alene til deling og behandling av egne personopplysninger først når de fyller 18 år. Før dette må de foresatte samtykke på barnets vegne. Likevel har barn rett til økt selv- og medbestemmelse med alderen, og de foresatte bør høre med barna selv før de samtykker på deres vegne (barneloven § 33).
✓ Barn under 18 år kan i noen situasjoner gi samtykke selv dersom de er i stand til å gi et informert og frivillig samtykke (jf. barneloven § 33 og de alminnelige kravene til gyldig samtykke).
✓ En tommelfingerregel kan være at jo større personvernkonsekvenser behandlingen av opplysninger vil kunne ha, desto høyere terskel bør det være for at barnet kan samtykke selv, uten foreldre.
✓ Vanligvis hvis barnet er 13 år eller mer, må det også underskrive erklæringen.

Bilder og videoer av barn

Bruk Datatilsynets veiledning

- Et portrettbilde er en personopplysning, og klassebilder/gruppebilder defineres også som portrettbilder.
- **Før** bildene tas, må man ha et samtykke fra de foresatte (bade for intern brud og hvis de skal deles på nett).
- Samtykkeskjema skal suppleres med erklæringen med all nødvendig informasjon om behandlingen.

Skjemaet bør inneholde relevante og konkrete spørsmål som de foresatte skal krysse av for:

1. Er det greit at det tas bilder/film av barnet?
2. Er det greit at bildene publiseres på åpne/passordbeskyttede nettsider?
3. Er det greit at bilder av barnet deles i sosiale medier? (Her må det spesifiseres hvor bildene vil kunne publiseres og om det er åpne eller lukkede *profiler*/grupper. Her bør det være mulig å velge hvilke kanaler man gir samtykke til.)
4. Er det greit at bildene publiseres i trykksaker relatert til skolen/barnehagen/organisasjonen?

...osv

Sjekkliste

Her er noen stikkord til hva man må vurdere før deling av barnebilder, og som vi vil gå nærmere inn på i denne veiledningen:

1. **Lovlighet**: Del aldri bilder av andres barn uten samtykke fra deres foresatte.
2. **Type bilde**: Tenk over innholdet og bruk filter eller dårligere oppløsning når det er mulig, det gjør bildene mindre interessante for andre.
3. **Mengde**: Del færrest mulig bilder.
4. **Kanalbruk**: Vær bevisst på hvordan du deler bildene. Alt må ikke ligge åpent. Bruk personverninnstillinger og lag lukkede grupper.
5. **Slett jevnlig**: Ta en vårrengjøring og slett tidligere bilder du har publisert med jevne mellomrom.
6. **Spør alltid barna**: Bruk spørsmål som "Synes du det er greit at jeg deler dette bildet med familien eller vennene mine?" Da gjør du det forståelig for dem. Respekter svaret.

https://www.datatilsynet.no/personvern-pa-ulike-omrader/skole-barn-unge/bilder-av-barn-pa-nett/samtykkeskjema/

Hvilke digitale løsninger brukes I kulturskoler?

1. Administrative verktøy (eks. administrative systemer, kommunikasjonsløsninger for foresatte)?

2. Læringsverktøy (applikasjoner, programvare)?

3. Plattformer (Microsoft (Windows PC), Apple (Mac, iPad), Google (Chromebook)).

4. Sosiale medier (Meta, Instagram, snapchat, TikTok, etc)

Intern risikovurdering: skal Datatilsynet ha egen side på Facebook?

Sluttrapport 2021

Datatilsynet

HVA SIER REGLENE? BORGER

Forside / Dommer / Dommer / 2021 / sep / Vedtak om brudd på personopplysningssikkerhet

Dommer

Dommer
2018
2019
2020
2021
Jan
feb
mar
april

Alvorlig kritikk av Helsingør kommune i Chromebook-saken

Dato: 10.09.2021

Beslutning | Offentlige myndigheter | Alvorlig kritikk | Kjennelse | Advarsel | Rapportert brudd på personopplysningssikkerhet | Behandlingsgrunnlag | Risikovurdering og konsekvensanalyse | Grunnleggende prinsipper | Databehandler | Barn

Datatilsynet har avgjort den første i en serie saker knyttet til bruk av Google Chromebooks og G Suite for Education (nå kalt Workspace) i grunnskolen.

Journalnummer: 2020-431-0061.

The New York Times

SUBSCRIBE FOR €

Meta Fined $400 Million for Treatment of Children's Data on Instagram

Irish regulators said Instagram violated European data protection rules. It was the latest move by authorities in Europe and the U.S. related to child protection online.

Give this article

10-year-old girl dies after TikTok blackout challenge

Friday, 22 January 2021

Credit: Belga

A ten-year-old girl died of asphyxiation in Parlermo, Italy, after

An Coimisiún um Chosaint Sonraí
Data Protection Commission

YOUR DATA | FOR ORGANISATIONS | RESOURCES | WHO WE ARE | NEWS AND MEDIA | DATA PROTECTION OFFICERS

News & Media

- Contact details
- Press releases
- Latest news
- Consultations

Home » News & Media

Irish DPC submits Article 60 draft decision on inquiry into TikTok

13th September 2022

The Data Protection Commission (DPC) submitted a draft decision in a large scale inquiry into TikTok Technology Limited to other Concerned Supervisory Authorities across the EU on 13 September 2022. This inquiry was commenced in September 2021 and it examined certain processing of the personal data of children by TikTok. The Inquiry focuses on processing of child users' personal data in the context of the platform settings of the TikTok platform, in particular public-by-default processing of such platform settings in relation to users under age 18 accounts and age verification measures for persons under 13. The Inquiry also considers whether TikTok has complied with the GDPR's transparency obligations in the context of the processing of personal data of users under age 18.

ATEA


Vi bygger **Norge med sikker IT**
ATEA

Taisiia Demina

Strategisk rådgiver sikkerhet & personvern

Kompetanseområder

- Personvern og etterlevelse av GDPR
- Vurdering av personvernskonsekvenser (DPIA)
- Etablering og implementering av policy, regelverk og organisering
- Risiko- og sårbarhetsanalyser (ROS)
- Personvernombud
- GAP-analyse
- Overføringskonsekvensvurdering (DTIA)/Shrems II
- Risikostyring og risikohåndtering
- Styringssystem for informasjonssikkerhet (ISMS)
- Program for bevissthet om personvern og digital sikkerhet
- Utarbeidelse av databehandleravtaler

Taisiia er utdannet **personvernjurist** som har fagekspertise i **personvernombudsrollen**. Taisiia har opparbeidet seg en variert erfaring som juridisk rådgiver både som internjurist i store selskaper og som ekstern rådgiver. Taisiia har de siste to årene jobbet som jurist og personvernombud i krysningsfeltet mellom personvern og informasjonssikkerhet, samt ledet implementering og etterlevelse av GDPR i bedriften.

Før hun startet i Atea har hun hatt stilling som personvernombud på Høyskolen Kristiania, med hovedansvar for virksomhetens **personvernprogram**, inkludert implementering og etterlevelse av retningslinjer og rutiner, samtidig som hun var ansvarlig for **opplæring og bevissthetsgjøring** av ledelsen, ansatte og studenter. I forbindelse med sin rolle i Kristiania har Tais god kjennskap til gjennomføring av **risikovurderinger, inkludert personvernkonsekvensvurderinger (DPIA)** angående anskaffelse og utvikling av tjenester/prosesser.

Taisiia har vært involvert i utarbeidelse av styrende, gjennomførende, og kontrollerende dokumentasjon innen personvern, oppfølging og opplæring, inkludert avvikshåndtering. Hovedformålet med arbeidet var å sørge for at informasjonssystemene som høyskolen bruker, oppfyller personvernprinsippene og krav til **innebygd personvern** samtidig som at de ivaretar de registrertes rettigheter. Dette innebærer bl.a. å iverksette tilstrekkelige tekniske og organisatoriske tiltak ved bruk av en risikobasert tilnærming.

Taisiia har sin masterutdannelse i informasjons- og kommunikasjonsteknologi rett (ICT Law LL.M), med spesialisering innen personvern, sikkerhet og digital forvaltning ved Universitetet i Oslo. Hun har også masterutdannelse i medieforvaltning og høyere utdanning på mastergradsnivå i internasjonal business jus. Taisiia er sertifisert som CIPM - Certified Information Privacy Manager og som CIPT - Certified Information Privacy Technologist.

Tais er strukturert og systematisk, med blikk for helhet og detaljer. Hun er også løsningsorientert, ansvarsfull, nysgjerrig, og brenner for fagfeltet hun jobber innenfor.