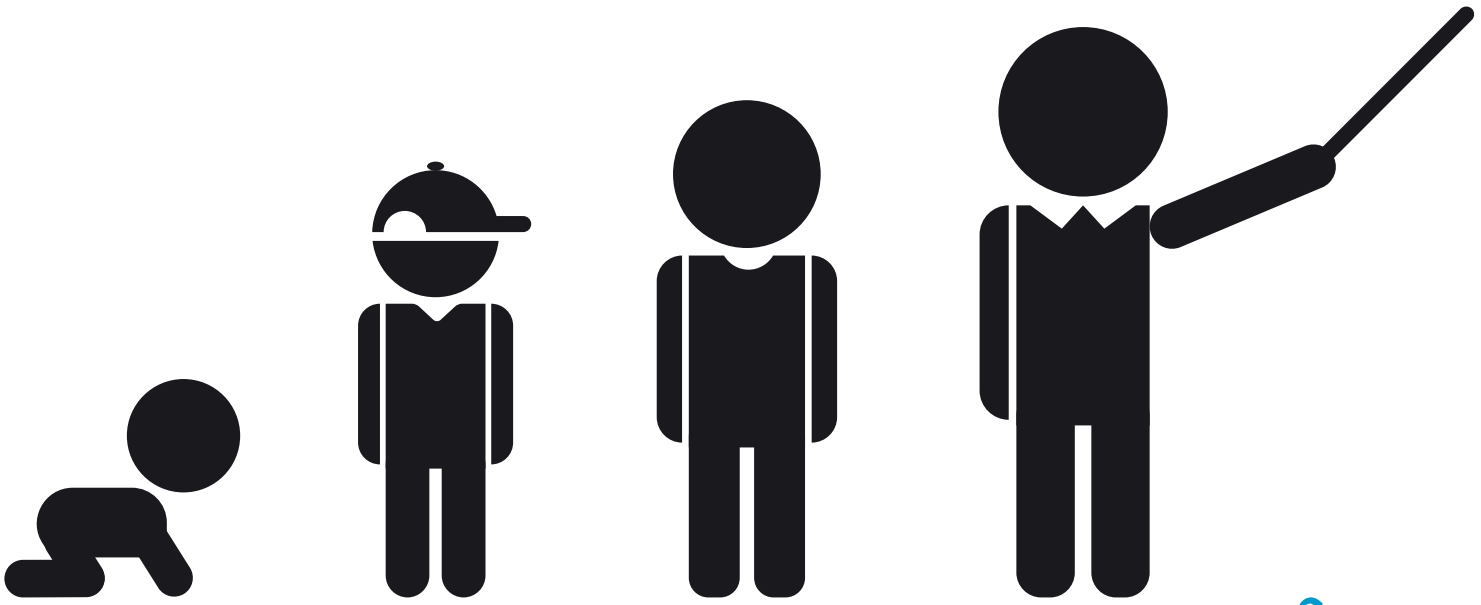
Sikkerhet og personvern i skole og klasserom

SENTER FOR IKT I UTDANNINGEN

NKUL 2017
Tommy Tranvik
Harald Torbjørnsen

Vi skal:


Øke kvaliteten i det pedagogiske arbeidet med digitale ferdigheter hos barn og unge
Øke den digitale kompetansen hos ansatte i barnehage og grunnskole
Øke kvaliteten i sektorens infrastruktur og administrative prosesser
Utvikle og drifte nasjonal portal for yrkes-, utdannings- og karriereveiledning



Barnehagen

Grunnskolen

Videregående skole

Lærerutdanningene

- Europa-parlamentets og Rådets forordning (EU) 2016/679 av 27. april 2016
  - gjennomgå noen viktige regler, fokus på informasjonssikkerhet
  - praktiske råd for etterlevelse av krav til risikovurderinger av informasjonssikkerheten

EUs personvernforordningen

- Gjelder fra 25. mai 2018
- Personvernforordningen erstatter
  - EUs personverndirektiv fra 1995
  - personopplysningsloven med forskrift
- Kjennetegn
  - mer omfattende og komplisert
  - mye gjenbruk
  - økt fokus på risikostyring

Oversikt

- 11 kapitler, 99 artikler
  - kapittel 1: generelle regler
  - kapittel 2: prinsipper
  - kapittel 3: den registrertes rettigheter
  -
  - kapittel 4: behandlingsansvarlig og databehandlers plikter
  - kapittel 5: overføring av personopplysninger til utlandet
  - kapittel 6 og 7: datatilsyn – oppgaver og overnasjonal samordning
  - kapittel 8: sanksjoner
  - kapittel 9: spesielle behandlingssituasjoner
  - kapittel 10 og 11: administrative bestemmelser

Når gjelder regelverket?

- Ved (elektronisk) behandling av personopplysninger
- Behandlinger
  - innsamling, lagring, overføring, sammenstilling, gjenbruk, publisering, sletting, osv.
- Personopplysninger
  - all informasjon og alle vurderinger som kan knyttes til bestemte ansatte, elever eller foreldre/foresatte
- Skoleeier er ansvarlig for at regelverket etterleves (behandlingsansvarlig)
- Skoleeiers ansvaret omfatter all bruk av eksterne tjenester eller nettressurser hvor personopplysninger behandles (databehandlere)
- Skoler etterspør og følger opp skoleeiers retningslinjer for ivaretakelse av regelverket

Rettigheter

- Kapittel tre i Forordningen
- De registrerte (ansatte, elever eller foreldre/foresatte) har rett til
  - informasjon (formkrav)
  - få innsyn i og kreve retting eller sletting av egne opplysninger
  - kreve begrensning av behandling av egne personopplysninger
  - motsette seg visse typer behandlinger
  - dataportabilitet
- Skoleeier har plikt til å ivareta rettighetene

Informasjonssikkerhet som grunnkrav

- Artikkel 5 i Forordningen
- Grunnleggende krav til behandling av personopplysninger, bl.a. lovlig grunn, formål og formålsbegrensning, dataminimering, datakvalitet og sletting/anonymisering
- Informasjonssikkerhet er et nytt grunnkrav
  - tilfredsstillende informasjonssikkerhet mht. konfidensialitet og integritet
  - tilfredsstillende sikring mot ulovlig eller uautorisert bruk av personopplysninger
  - tekniske og organisatoriske tiltak
- Krav til dokumentasjon av informasjonssikkerhet og andre grunnkrav
- Brudd på grunnkrav kan utløse de høyeste gebyrene

Hovedbestemmelsen

- Artikkel 32 i Forordningen
- Gjelder både for skoleeier (behandlingsansvarlig) og databehandler
- Tilfredsstillende konfidensialitet, integritet, tilgjengelighet og robusthet
- Risikostyrt arbeid
  - pseudonymisering og kryptering nevnes spesielt
  - krav til beredskap og kontinuitet
  - krav til testing og evaluering av sikringstiltak
- Krav til organisatoriske sikringstiltak (instrukser)

Varsling til Datatilsynet

- Artikkel 33 i Forordningen
- Varsling til Datatilsynet ved sikkerhetsbrudd som innebærer risiko for krenkelser av personvernet
  - så snart som mulig og senest innen 72 timer
  - krav til innholdet i varslingen
  - unntak for mindre alvorlige sikkerhetsbrudd
- Databehandler skal varsle skoleeier uten ubegrunnet opphold
- Krav til dokumentasjon, bl.a. omstendighetene rundt sikkerhetsbruddet, konsekvensene av sikkerhetsbruddet og gjenopprettende tiltak

Varsling til de registrerte

- Artikkel 34 i Forordningen
- Varsling til de registrerte (ansatte, elever, foreldre/foresatte) ved sikkerhetsbrudd som innebærer høy risiko for krenkelser av personvernet (artikkel 34)
  - hver enkelt registrert
  - umiddelbart etter at bruddet blir kjent
  - krav til tydelighet (forståelig språk)
  - krav til innholdet i varslingen
- Unntak for
  - mindre alvorlige sikkerhetsbrudd
  - effektive sikringstiltak allerede er iverksatt
- Hvis varsling er uforholdsmessig kostnadskrevende, kan de registrerte informeres via offentlige bekjentgjørelser

Personvernombud

- Artikkel 37-39 i Forordningen
- Skoleeiere pålegges å utnevne personvernombud
  - flere virksomheter kan ha samme ombud
  - ombudet kan være ansatt eller innleid
  - kan utøve rollen på heltid eller deltid
  - skal ha spesialkompetanse om personvern og regelverket

Ombudets oppgaver og posisjon

- Involveres i spørsmål vedrørende behandling av personopplysninger
  - informere og gi råd om regelverket
  - kontrollere praktisering av regelverket
  - kontrollere praktiseringen av interne rutiner og retningslinjer (organisering, bevisstgjøring, opplæring og revisjoner)
  - gi råd ved konsekvensutredninger (PIA)
  - bistå de registrerte
  - kontaktpunkt for og samarbeid med Datatilsynet
- Skal være uavhengig (ikke instrueres eller straffes)
- Rapporterer direkte til toppledelsen, for eksempel rådmannen
- Skoleeier (ikke personvernombudet) er ansvarlig for regeletterlevelsen

Databehandlere

- Artikkel 28 og 29 i Forordningen
- Mer detaljerte krav til bruk av databehandlere
  - krav om databehandleravtaler
  - krav til innhold
  - krav til informasjonssikkerhet hos og avtaler mellom leverandører og underleverandører
  - krav ved overføring av opplysninger til land utenfor EU/EØS
- Databehandlere får større selvstendig ansvar for informasjonssikkerheten
- Databehandlere kan bli ilagt sanksjoner ved brudd på sikkerhetsreglene

Sanksjoner

- Ved regelbrudd kan straffen maksimalt bli
  - 10 mill. euro, alternativt to prosent av årsomsetningen, eller
  - 20 mill. euro, alternativt fire prosent av årsomsetningen
- Avhenger blant annet av hvilke regler som brytes

Anbefalte tiltak fra Datatilsynet

- Vil gi et utgangspunkt for å oppfylle pliktene i regelverket dersom skoleeier
  - kartlegger personopplysninger de er ansvarlige for
  - utfører og dokumenterer risikovurderinger

Hvordan komme i gang?

- Avklar ansvar/roller som:
  - kartlegger og vurderer personopplysningene og systemene de ligger i.
  - gjennomfører risikovurderinger
  - inngår databehandleravtaler
  - informerer om brukernes rettigheter

System for internkontroll

- Viktig redskap for informasjonssikkerheten
  - dokumentasjon
  - vedlikehold/ oppdatering
  - kvalitet på data

”mangelfull internkontroll i skole og barnehage”

– Datatilsynet 2014 - ”Personvern i skole og barnehage”

Et stykke fram for mange...

- ”Digitalt internkontrollsystem innkjøpt etter tilsyn i skolen”
- ....skolen får avvik av Datatilsynet flere år etterpå for ikke å bruke internkontrollsystemet...

Risikovurderinger

- Kjernen i arbeidet med forebyggende informasjonssikkerhet
- Nøktern vurdering av:
  - hvilke problemer som kan oppstå?
  - hvor store problemene er?
  - hva kan gjøres med de viktigste problemene?
- Kompetansehevende effekt
  - kartlegger og diskuterer IKT-praksis i undervisning og administrasjon

Risikovurderingens 3 hovedfaser

1. Forberedelse
2. Gjennomføring
3. Oppsummering og etterarbeid

Risikovurdering av DVM

DEN VIRTUELLE MATEMATIKKSKOLEN

moodle

Adobe Connect

Eksempel på uønskede hendelser

- Feil ved tilgangsstyring fører til at personer får tilgang til sensitiv informasjon
- Lærer låner ut eget utstyr til elevene.
- Teknisk svikt fører til at innhold/systemer er utilgjengelig i kritiske perioder
- Elever får tak i læreren sin FeideID og gjør endringer på fravær og vurderinger

Etabler nødvendige tiltak

- Risikovurdering blir ofte et «byråkratisk ritual»
  - gjør vurderingen for å vise at den er gjort
  - lang vei fra vurdering til tiltak
  - ofte et spørsmål om økonomi

- Oppfølging med nødvendige tiltak krever
  - forpliktelse fra beslutningstakere
  - tydelig kommunikasjon av resultater
  - realistiske tiltaksforslag

Eksempel på tiltak

- Klasse 9B ønsker å ta i bruk skytjeneste for publisering.
  - Skolens rutine godt kjent blant lærerne
  - Feideinnlogging et krav
  - Egen skole/skoleeiergruppe risikovurderer
  - skoleeier inngår eventuell databehandleravtale.

Håndter daglige hendelser

- Risikovurderinger er ferskvare
- IKT-praksis i skolehverdagen er dynamisk

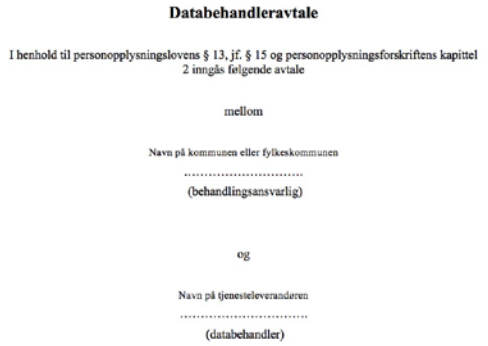
- Mye vil skje mellom risikovurderinger
  - rapporter og håndter uheldige hendelser
  - skriv opp hendelser og håndtering
  - legg frem og diskuter i formelle skolefora

Eksempel på daglige hendelser

- Digital mobbing
  - Elev mistenkes for å ha bevis på konto i skyplattform
    - Avviksmelding
    - IKT-reglement
    - Kap 9 forskrift til personopplysningsloven
    - Ordensregler
    - Skjønn

Databehandleravtaler

- Sjekk at leverandørene tilbyr databehandleravtaler



Databehandleravtale

I henhold til personopplysningslovens § 13, jf. § 15 og personopplysningsforskriftens kapittel 2 inngås følgende avtale

mellom

Navn på kommunen eller fylkeskommunen

.....

(behandlingsansvarlig)

og

Navn på tjenesteleverandøren

.....

(databehandler)

- Sjekk innholdet i databehandleravtalene, jf. mal for databehandleravtaler

Datatilsynet

SENTER FOR IKT I UTDANNINGEN

Rettigheter og informasjon

- Etabler rutiner for innsyn
- Publiser og kommuniser rettighetene og rutinene

Informasjon

- Veiledninger
- Brukerstøtte
- Programvare
- Retningslinjer for bruk av sosiale medier
- IKT-reglement med veiledning og samtykkeerklæring
- IKT-reglement signeringsskjema
- I beste mening

Personvern

- Din rett til informasjon og innsyn etter personopplysnings - loven
- Behandling av personopplysninger og rett til innsyn
- Rutiner for utlevering av informasjon ved begjæring om innsyn
- Elverumskolen samler inn personopplysninger
- Begjæring om innsyn

Om oss | Kontakt oss | in English

SENTER FOR IKT I UTDANNINGEN

Hjem | Barnehage | Skole | Lærerutdanning

Barnehage

Skole

Lærerutdanning

AKTUELT

Nyhet

Blogginnlegg

HVA SKJER

02 MAI

Frokostseminar: Lansering av Rammeverket for lærerens profesjonsfaglige digitale kompetanse

STED: Senter for IKT i utdanningen

Følg oss:

iktsenteret

iktsenteret

Nyhetsbrev (via iktsenteret.no)