Bruk av skytjenester og sosiale medier i skolen

Martha Eike | senioringeniør | Datatilsynet

13.11.2015

Datatilsynet

Agenda

- Hva er personvern?
- Datatilsynets skole- og barnehageprosjekt
- Skytjenester
- Sosiale medier

Thinkstock.com

Hvem har ansvaret?

«Behandlingsansvarlig»

= skoleeier

= kommunens øverste administrative ledelse

= rådmannen

~ delegasjon til skolens ledelse

Hva handler personvern om?

- Autonomi / selvbestemmelse
- Å vite = retten til å velge
- Forutsigbarhet
- Tillit
- Informasjonssikkerhet

Thinkstock.com

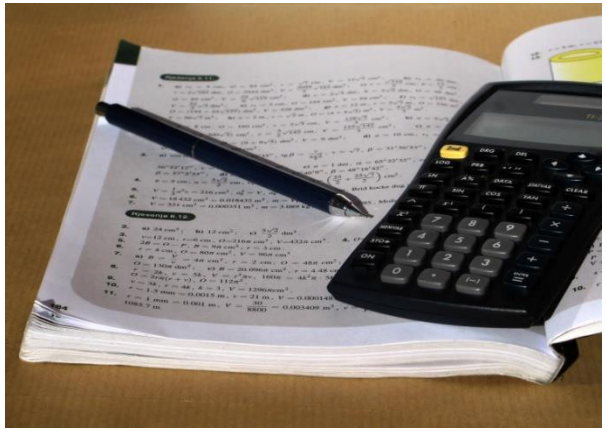
Skole- og barnehageprosjektet 2013-14

- Hvilke opplysninger samles inn om barna og hvordan blir de behandlet?
- Møter med ulike aktører innen opplæringssektoren
- Kontroller:
  - Brevlige tilsyn (9 grunn- og videregående skoler)
  - Stedlige tilsyn (11 grunnskoler, 4 videregående og 5 barnehager)
- Sluttrapport med tilstandsbeskrivelse og anbefalte tiltak
- Norm for personvern i skolen -verktøy for å hjelpe skole- og barnehageeiere til å ivareta personvernet i en digitalisert hverdag

Personopplysninger – hva er det?

Peder Aas
2020 Lillevik

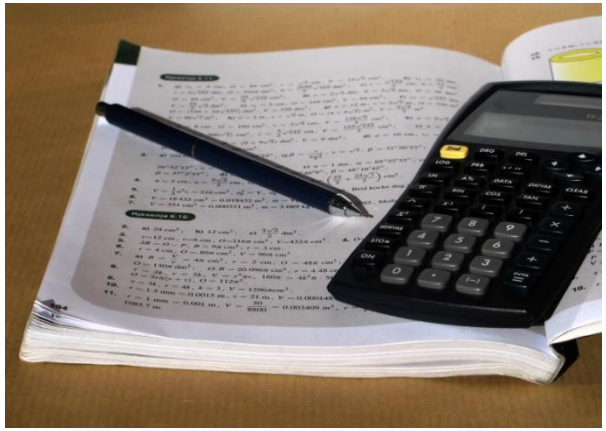
F.nr 180262 34997



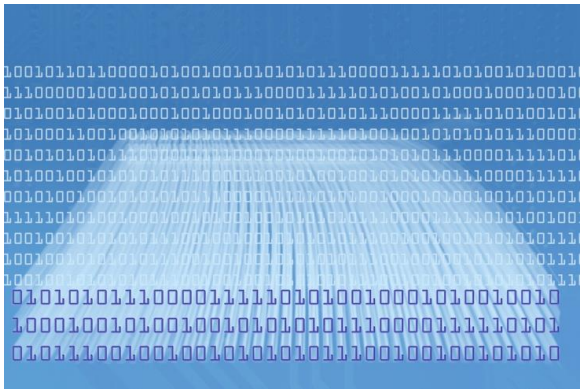
Sensitive personopplysninger – hva er det?

Peder Aas
2020 Lillevik

F.nr 180262 34997

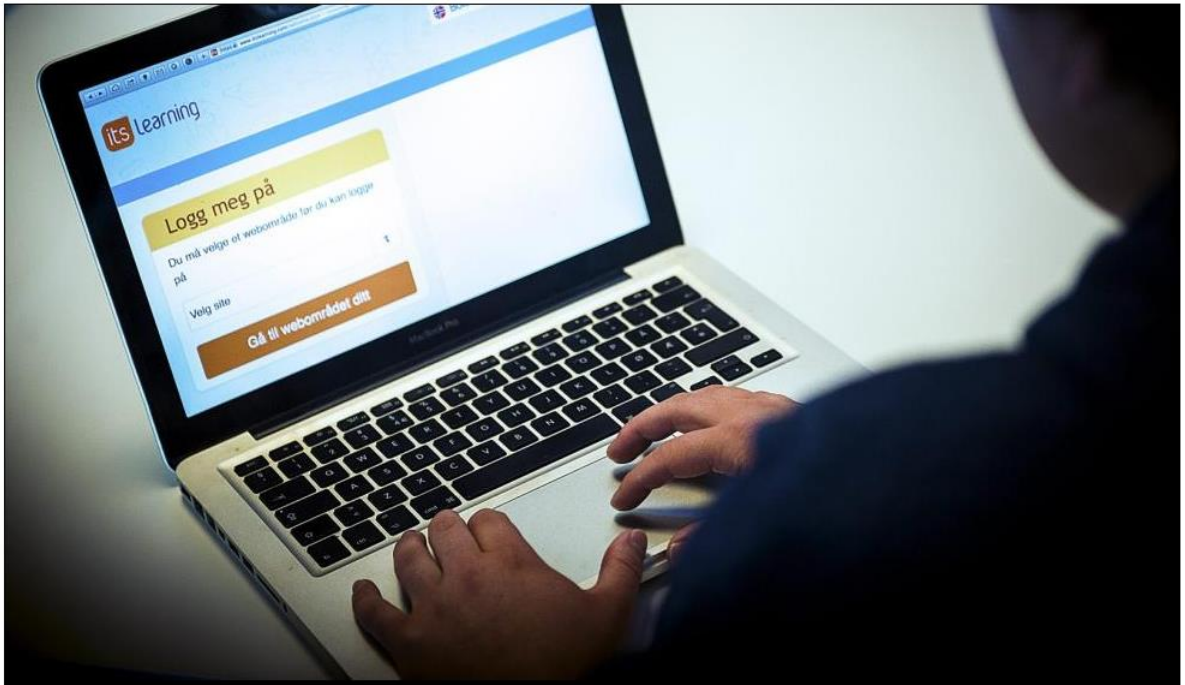


Personopplysninger er også…



- Fødselsnummer: `13087846271`
- Telefonnummer: `22396900`
- IP-adresse: `195.159.103.82`
- Bilnummer: `BL 23456`
- Bluetooth MAC: `17:35:52:78:4B:CA`
- Wi-Fi-adresse MAC: `12:44:32:45:7B:C9`
- Autpass-brikke-ID: `7483920983278394`
- UDID: `f7426bd759856431d9ae2c99175407a0dcd67ab5`

Lærers passord på avveier



DATAINNBRUDD: De to guttene plukket opp en av lærernes passord til skolens databaser, og kom seg deretter inn i databasen hvor skolen setter sine karakterer. Dermed sørget de for kraftige karakterhopp for seg selv, mens andre elevers karakterer ble satt ned. Den videregående skolen oppdaget selv jukset. (FOTO: CICILIE S. ANDERSEN)

Karakterjuks ender i retten

Guttene brøt seg inn på skolens databaser og bedret sine egne karakterer. De satte samtidig ned andres. Nå havner karakterjukset i retten.

Klasserommet i skyen

Kort om skytjenester

- Er det egentlig noe nytt?
  - ASP, Fjerndrift, stormaskin, hosting, …

- Rokker ikke ved ansvarslinjene
  Virksomhet ⟹ Leverandør
  Behandlingsansvarlig ⟹ Databehandler

- Skytjenester betyr ikke fravær av kontroll
  (i så fall er det uforenlig med regelverket)

Ulike typer av skytjenester

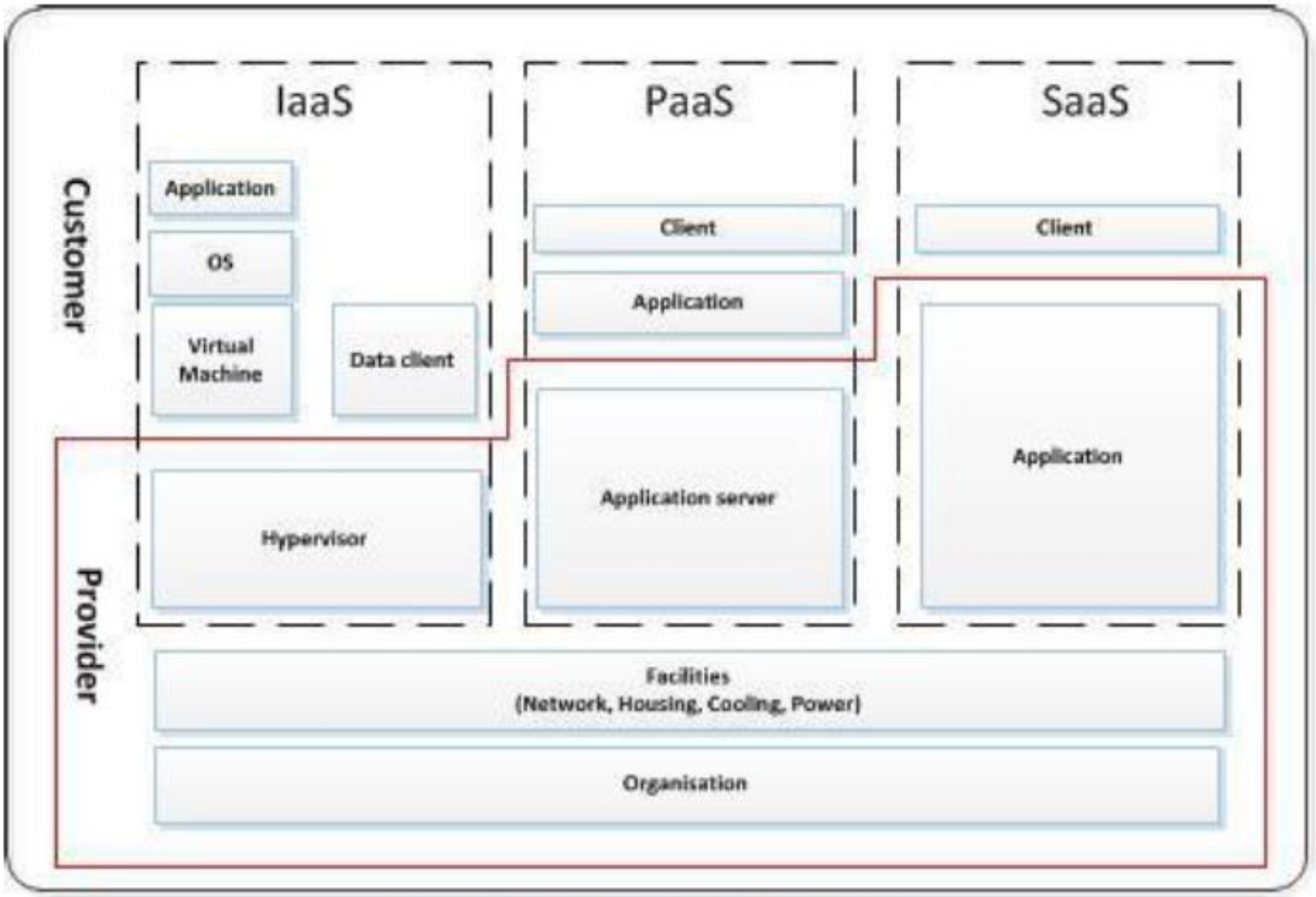


Figure 1: Asset in cloud computing

 Kilde: Enisa «Cloud Security Guide for SMEs»

Outsourcing av oppgaver er forskjellig i ulike tjenestetyper

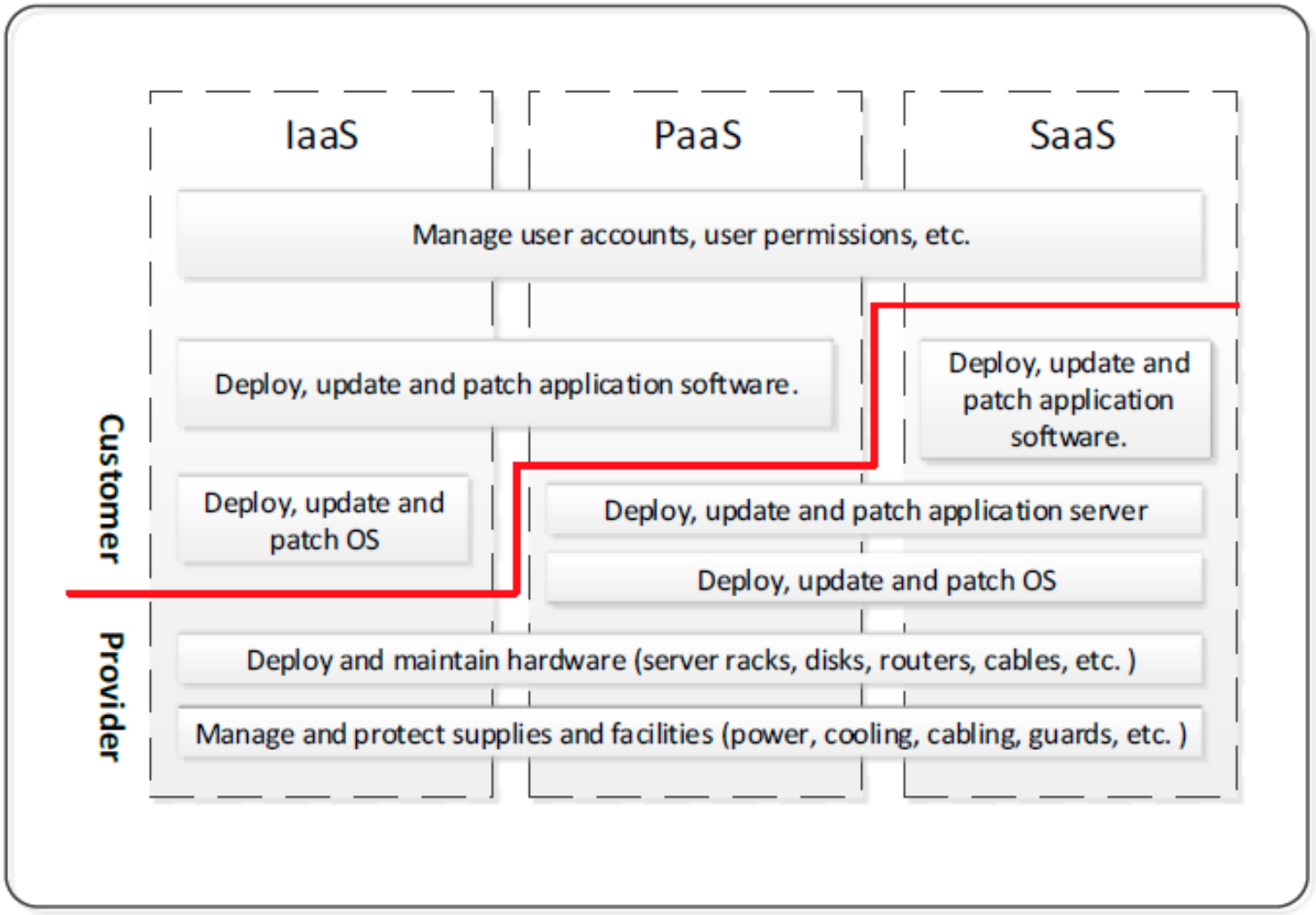
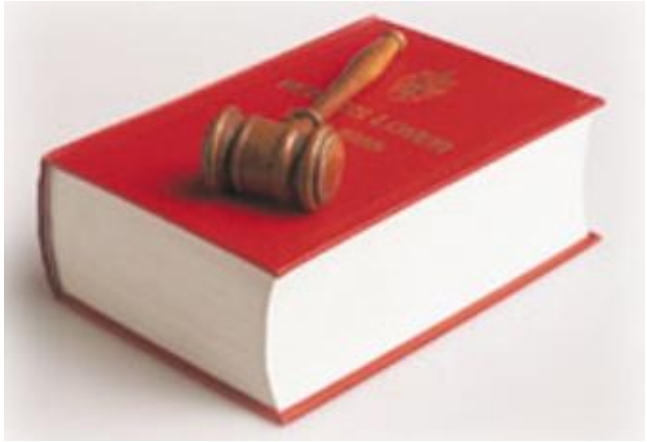


Figure 2: Outsourcing of tasks is different for different types of services

 Kilde: Enisa «Cloud Security Guide for SMEs»

Viktige lovkrav ved bruk av skytjenester

- Internkontroll
  - Personopplysningsloven § 14
  - Personopplysningsforskriften 3. kap
- Informasjonssikkerhet
  - Personopplysningsloven § 13
  - Personopplysningsforskriftens 2. kap
- Databehandlere
  - Personopplysningsloven §§ 15 og 13
  - Personopplysningsforskriften § 2-15 og hele 2. kapittel
- Andre relevante krav
  - Personopplysningsloven § 11 b) «uttrykkelig angitt formål»
  - Pol §§ 29, 30 - overføring til utlandet



Informasjonssikkerhet i forskriften

- § 2-3 Sikkerhetsledelse
- § 2-4 Risikovurdering
- § 2-5 Sikkerhetsrevisjon
- § 2-6 Avvik
- § 2-7 Organisering
- § 2-8 Personell
- § 2-11 Sikring av konfidensialitet
- § 2-12 Sikring av tilgjengelighet
- § 2-13 Sikring av integritet
- § 2-14 Sikkerhetstiltak
- § 2-15 Sikkerhet hos andre virksomheter

Hvordan etterleve loven?

Internkontroll

- Få oversikt over hvilke personopplysninger som behandles og klassifiser dem fra sensitive til ikke-sensitive.
- Lag rutiner og regler for:
  - Innsyn
  - Samtykke
  - Retting og sletting
  - Informasjon

Kartlegge virksomhetens behandlinger

Virksomheten skal ha oversikt over personopplysningene

- Nødvendig for å ivareta sine plikter.
- Grunnlag for sikkerhetsmål og sikkerhetsstrategi.
- Underlag for risikovurderinger.

Informasjon Formål	Behandlings-grunnlag	Melding/ Konsesjon	Klassifikasjon	Sikkerhets-tiltak	Lagring og kommuni-kasjon	Opplysningenes omfang	Avdeling	Databehandler
Lønn og personal: lønnsopplysninger personalopplysninger	Personopplysning sloven, § 8f	Unntatt i forskriftens § 7-16	Person-opplysninger			Ca. 130 ansatte		
Barnevern: vurdering og tiltak	Barnevernloven, § 3-1	Meldt 14.01.2009	Sensitive person-opplysninger			Ca. 68 barn og foresatte		
Helseopplysninger: pasientjournal	Helsepersonel-loven § 39	Meldt 14.01.2009	Sensitive person-opplyninger			Ca. 413 pasienter		
Elevadministrasjon elever / foresatte lærere	Opplæringsloven § 13-5		Person-opplyninger			Ca. 219 søkere		
Hendelsesregister: logg over brudd	Personopplysning sloven, § 13	Unntatt i forskriftens § 7-11	Person-opplyninger			Arkivlogg, nettverkslogg og serverlogg, PC-logger		

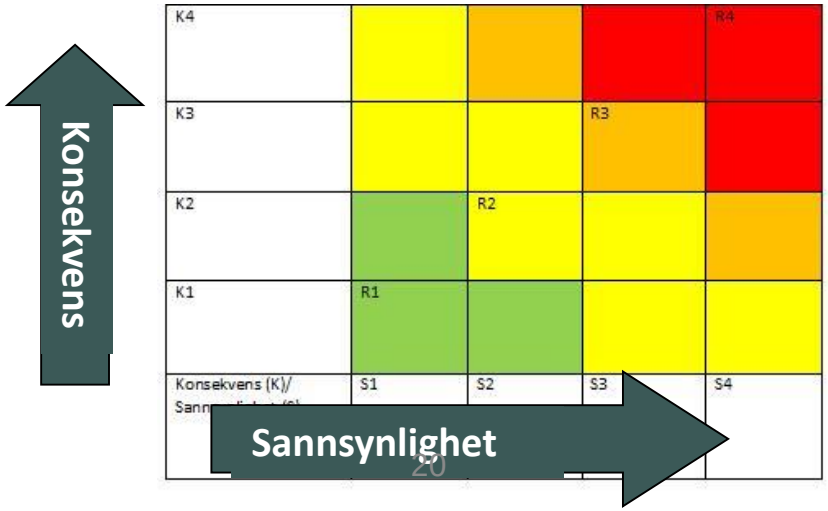
Risikovurdering

Thinkstock.com

Risikovurdering – trinn for trinn

- Kartlegg og klassifiser alle behandlinger
- Identifiser uønskede hendelser (og årsaker!)
- Konsekvensvurdering (1-4)
- Sannsynlighetsvurdering (letthet 1-4)

Sammenlign resultater og iverksett tiltak for å komme innenfor akseptabel risiko.



Sikkerhetsrevisjon

Sikkerhetsrevisjon av bruk av informasjonssystemet skal:

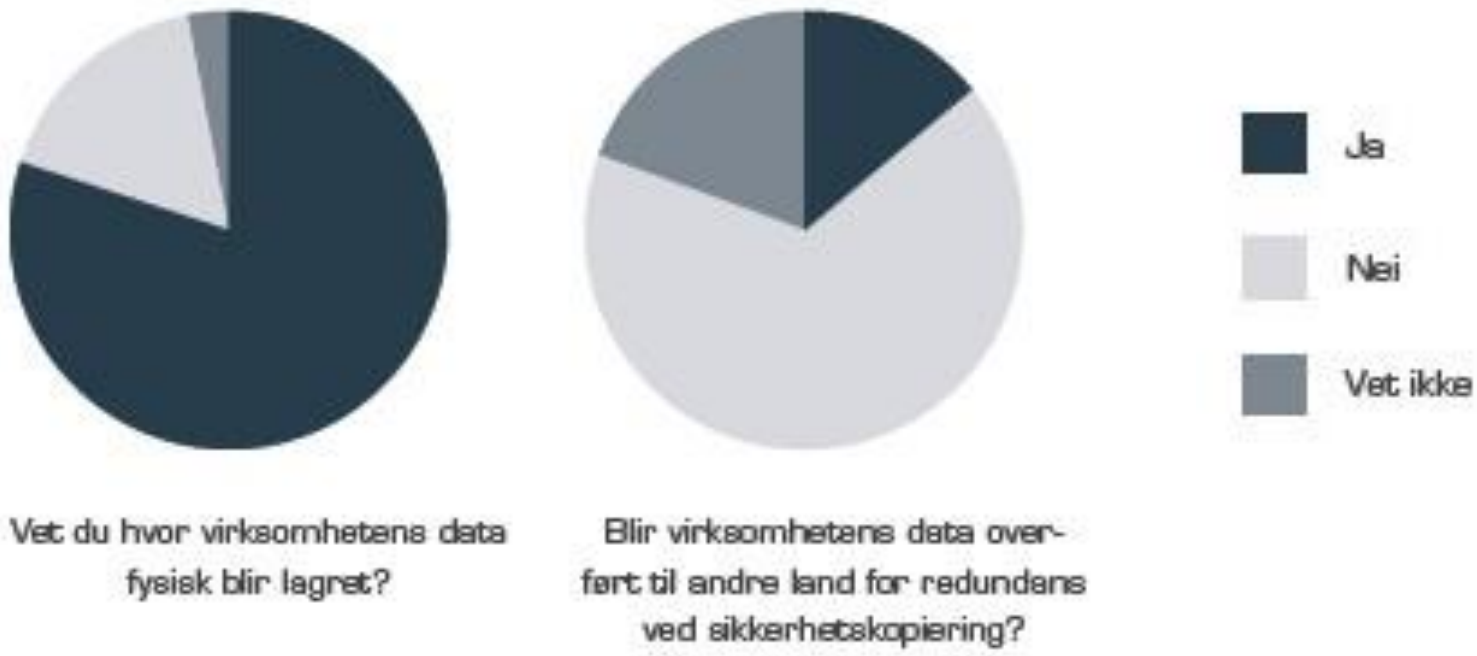
- Gjennomføres jevnlig
- Omfatte:
  - Vurdering av organisering
  - Sikkerhetstiltak
  - Bruk av sikkerhetsparter og databehandlere
- Bestå av:
  - Egenkontroller
  - Internrevisjon
  - Revisjon med sikkerhetsparter og databehandlere
- Dokumenteres

Dersom sikkerhetsrevisjonen avdekker bruk som ikke er forutsatt, skal det behandles som avvik.

Databehandleravtaler

Fra Mørketallsundersøkelsen 2014

Økt bruk av nettskytjenester



Fra Mørketallsundersøkelsen 2014: Avtale med driftsleverandør

Elementer med i avtalen?	Privat	Offentlig
1. Krav til tilgangskontroll til informasjon	58 %	45 %
2. Krav til taushetsplikt	65 %	62 %
3. Krav til tekniske sikringstiltak (kryptering etc.)	49 %	43 %
4. Krav til tilgjengelighet/oppetid	65 %	49 %
5. Rett til innsyn i relevante sikringsrutiner og dokumentasjon om f.eks. måling av sikkerhetsstatus	39 %	31 %
6. Kontraktsfestet et økonomisk ansvar ved informasjonssikkerhetshendelse eller manglende leveranser fra driftspartners sid	33 %	22 %
7. Sanksjoner dersom krav ikke oppfylles	29 %	20 %
8. Databehandleravtale etter regler i personopplysningsloven §13 og helseregisterloven §16	22 %	46 %
9. Nei, ingen av disse	7%	6%
10. Vet ikke	20%	27%

Minimumskrav til databehandleravtaler

1. Angi formålet med behandlingen

- Det skal klart fremgå av avtalen hva som er formålet med behandlingen av personopplysningene.

2. Beskriv hvordan personopplysningene skal behandles

- Det skal tydelig fremgå av avtalen hva databehandler skal gjøre med personopplysningene.
- Databehandler har ikke råderett over personopplysningene, og kan dermed heller ikke behandle disse til egne formål.
- Databehandler skal kun forholde seg til avtalen. Hvis han skal utlevere personopplysninger til andre eksterne parter må dette framgå klart av databehandleravtalen.
- Avtalen må inneholde bestemmelser om hvem som skal kunne få personopplysninger utlevert, og vilkår i tilknytning til dette.

3. Bruk av underleverandør skal reguleres i avtalen

- Hvis databehandler gjør bruk av underleverandører av tjenester, skal dette klart framgå av avtalen mellom databehandler og behandlingsansvarlig.

Minimumskrav til databehandleravtaler

4. Ivareta den registreres rettigheter

- Avtalen kan inneholde en arbeidsfordeling mellom behandlingsansvarlige og databehandler, for eksempel hvem som skal håndtere og behandle henvendelser fra de registrerte.

5. Avtalen må pålegge databehandleren å ha tilfredsstillende informasjonssikkerhet

- Avtalen må klargjøre hva databehandler skal ha på plass av sikringstiltak for å ivareta *konfidensialitet*, *integritet* og *tilgjengelighet*

6. Avtalens varighet må avtales

- Avtalen må inneholde opplysninger om avtalens varighet hva som skal skje med opplysningene etter at avtalen er opphørt

Problemstillinger som må vurderes

- Sikkerhetskopiering / speiling
- Segmentering
- Hvor lagres data? Overføring til tredjeland?
- Tilgangsstyring
- Dokumentasjon
- Sletting
- Bruk til egne formål (Forbedre egne tjenester? Profilering?)
- Underleverandører
- Sikkerhetsrevisjon
  - Påse at databehandler iverksetter tiltak og dekker hele kjeden
  - Alternativt tredjepartsrevisjon – krev å få se rapporten!
- Sikker kommunikasjon - Kryptering

Internasjonalt samarbeid

- Article 29 Working Party (Art. 29 WP), *Opinion 5/2012*
  - Etterlevelse av personverndirektivet

- International Conference of Data Protection and Privacy Commissioners, *Resolution October 2012*
  - Overordnet

- Berlingruppen (the International Working Group on Data Protection in Telecommunications (IWGDPT)), *Sopot Memorandum April 2012*
  - Best Practice - kulepunkter

Aktuelt arbeid i Norge og i EU

- KMDs referansegruppe for policy for bruk av skytjenester i offentlig sektor
  - En policy er ventet ferdig høsten 2015
  - KMD har lansert en rapport fra en interdepartemental gruppe som har sett på hindringer i ulike regelverk (juni 2015)
  - KS har lansert en rapport (en mulighetsstudie) for bruk av nettsky i kommunal sektor (juni 2015)

- Cloud Select Industry Group (C-SIG) on Code of Conduct
  - Mange problemstillinger er avklart. Vi venter på beslutning i Art. 29-gruppen.

- ENISA
  - Cloud Security Guide for SMEs m.m.

Sosiale medier i undervisningen?

Denne veiledningen er utviklet i samarbeid med det svenske Skolverket og fungerer som en sjekkliste for lærere som ønsker å ta i bruk sosiale medier i undervisningen. Denne norske versjonen inneholder det viktigste, ellers kan dere lese mer på de svenske nettsidene, **www.skolverket.se/kollakallan**.

SJEKKLISTE

Personopplysninger

- Hvilke personopplysninger må du oppgi når du registrerer deg for tjenesten?
- Fremgår det i brukervilkår eller personvilkårene hvordan…

Les mer

Stedsinformasjon

- Må du oppgi hvor du befinner deg geografisk for at tjenesten skal fungere?
- Hvis du har oppgitt din geografiske plassering i en tjeneste – går det da…

Les mer

Innhold

- Kan du selv bestemme hvordan innholdet ditt spres? Med innhold menes det du publiserer i sosiale medier. Det kan for eksempel være tekst, bilde, film eller kommentarer…

Mer informasjon

- Skytjenester (veileder)
- Risikovurdering (veileder)
- Databehandleravtale (veileder og mal)
- Skolerapporten

…og masse mer på
www.datatilsynet.no

Takk for oss!

Datatilsynet

postkasse@datatilsynet.no
Telefon: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no

eol@datatilsynet.no
mei@datatilsynet.no | @marthaeike (Twitter)