

Krav til informasjonssikkerhet

DRI1010 – forelesning 16.03.2016

Jon B. Holden – jobe@holden.no

Dagens tema: Informasjonssikkerhet og eforvaltningsforskriften

- Hva er informasjonssikkerhet?
 - Hvem skal sikre?
 - Hva skal sikres, mot hva?
 - Hvor sikkert?
 - Hvordan?
- Krav til informasjonssikkerhet og internkontroll etter pol
- Eforvaltningsforskriften

Direktivet

- Behandlingsikkerhed, artikel 17:
 - 1. Medlemsstaterne fastsætter bestemmelser om, at den **registeransvarlige** skal iværksætte de **fornødne tekniske og organisatoriske foranstaltninger** til at beskytte personoplysninger **mod hændelig eller ulovlig tilintetgørelse, mod hændeligt tab, mod forringelse, ubeføjet udbredelse eller ikke-autoriseret adgang**, navnlig hvis behandlingen omfatter fremsendelser af oplysninger i et net, samt mod enhver anden form for **ulovlig behandling**.
 - <http://eur-lex.europa.eu/legal-content/DA/ALL/?uri=CELEX:31995L0046#texte>

Forordningen

- Artikel 30 (utkast, [omforent avtale](#))
 - 1. Under hensyn til det aktuelle tekniske niveau og gennemførelsesomkostningerne og i betragtning af den pågældende behandlings karakter, omfang, kontekst og formål og **risikoen** af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder træffer den **dataansvarlige og databehandleren passende tekniske og organisatoriske foranstaltninger** for at sikre et **sikkerhedsniveau**, der passer til disse risici, herunder bl.a. i det **nødvendige** omfang:
 - ...
 - 1a. Ved vurderingen af et passende sikkerhedsniveau tages der navnlig hensyn til de **risici**, som behandling af oplysninger udgør, navnlig ved **hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse** af eller **adgang** til personoplysninger, der er videregivet, opbevaret eller på anden måde behandlet.

Sikkerhet - hva skal beskyttes?

- Informasjonssikkerhet (def. ISO 27001, 3.4)
 - Bevare konfidensialitet, integritet og tilgjengelighet. Dessuten kan andre egenskaper, som autensitet, ansvarlighet, uavviselighet og pålitelighet, omfattes.
- Konfidensialitet
 - Vern mot uautorisert innsyn
- Integritet
 - Vern mot uautorisert endring/tap
- Tilgjengelighet
 - Tilgjengelig på behov

Informasjonssikkerhet i media

Spionerte på Telenor-sjefer, tømte all e-post og datafiler - Aftenposten - Mozilla Firefox
www.aftenposten.no/nyheter/Spionerte-pa
Verden Norge Osloby
-DN, 13.03.13

Problemer med innlogging i Altinn er løst - Aftenposten - Mozilla Firefox
www.aftenposten.no/okonomi/Problemer-med-f
Verden Norge Osloby Øk
God turmat

Norge ikke godt nok sikra - Nasjonal sikkerhetsmyndighet
https://www.nsm.st
Sikkerhetsbloggen Arb
Aktuelt
Mediebrief fra NSM
Nytt fra NSM
NSM i media

Nye problemer for Altinn: Brukere fikk tilgang til andres Altinn-kontoer - VG Nett - Mozilla Firefox
www.vg.no/nyheter/innenriks/artikkel.php?artid=10101534
Google

Nye problemer for Altinn: Brukere fikk tilgang til andres Altinn-kontoer
** Feilen rettet opp onsdag morgen
** Altinn-direktør: Sterkt beklagelig

altinn
Forklaring - Min meldingsboks
Velg periode: Søkk på tittel

FIKK FEIL KONTO: VG har vært i kontakt med en mann som hevder han tirsdag kveld kom inn på profilen til en for ham helt ukjent mann. Foto: Skjermdump Altinn
Publisert 19.03.13 - 23:11, endret 20.03.13 - 06:49 (VG NETT)
Av [Tim Peters](#) og [Geir Arne Kippemes](#)

Hovedsaken nå
[Les hele saken](#)

(VG Nett) En teknisk feil sørget for at flere personer tirsdag ble logget på som en helt annen.
VG fikk tirsdag kveld det første tipset fra en bruker som hadde logget seg på med BankID, og kom inn på en for ham helt ukjent person.

- Jeg har ingen kjennskap til ham. Det så ut som jeg hadde fri tilgang til informasjonen hans, men jeg valgte å ikke snoke for mye, forteller mannen - som tok en printscreen av det som møtte ham hos Altinn.

- Jeg logget ut og inn igjen, og var da på min egen profil igjen, forteller han

igland GARASJEN
BESTILL I MARS -20%
FRA MODUL TIL MONTERT
BESTILL GARASJE NÅ I MARS OG FÅ 20% RABATT PÅ GRUNNPRISEN.
Husk: Hos oss får du gratis hjelp til standard byggeskred for garasje!

Finn: altinn
Neste Forrige Marker tekst Skjll mellom store/små bokstaver

Aftenposten

Aftenposten

Nasjonale

VG

Informasjonssikkerhet i media

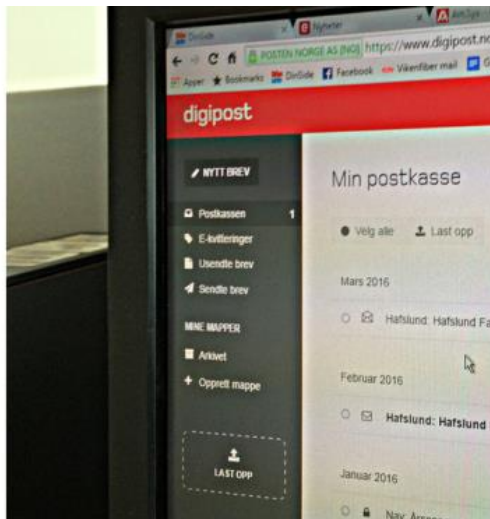
Norge Siste nytt Dokumentar Klima

Ny rapport: All kommunene

Mangler eller feil i pasienters helseinformasjon ut for tidlig. Dette er noen av funnene i e-Helsetilsynet.



SKRIVES UT TIDLIGERE FRA SYKEHUS: Fastleger helsestatus og behov for hjelp når pasienter skrives ut. FOTO: JUNGE, HEIKO / NTB SCANPIX



SIKRERE: Både e-Boks og Digipost tilfredsstiller kravene, men Digipost har høyest sikkerhetsnivå. (Foto: TORE NESET)

- Digipost er sikrere

24

Det mener sikkerhetseksperter Per Thorsheim.

Dinside Onsdag denne uka gjorde Dinside en sammenligning mellom de to digitalpostkassene Digipost og e-Boks. av Tore Neset



Publisert: Torsdag 10. mars 2016 kl 17:00



Tirsdag offentliggjorde Helsetilsynet Norge etter at samarbeidsreformer

Informasjonssikkerhet, pol § 13

- **§ 13. Informasjonssikkerhet**
- Den behandlingsansvarlige og databehandleren skal gjennom **planlagte og systematiske** tiltak sørge for **tilfredsstillende informasjonssikkerhet** med hensyn til **konfidensialitet, integritet og tilgjengelighet** ved behandling av personopplysninger.
- For å oppnå tilfredsstillende informasjonssikkerhet skal den behandlingsansvarlige og databehandleren **dokumentere** informasjonssystemet og sikkerhetstiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernemnda.
- En behandlingsansvarlig som lar **andre** få tilgang til personopplysninger, **f.eks. en databehandler eller andre som utfører oppdrag** i tilknytning til informasjonssystemet, skal **påse at disse oppfyller kravene** i første og annet ledd.
- Kongen kan gi **forskrift** om informasjonssikkerhet ved behandling av personopplysninger, herunder nærmere regler om organisatoriske og tekniske sikkerhetstiltak.

Internkontroll, pol § 14

- **§ 14. Internkontroll**
- Den behandlingsansvarlige skal etablere og holde vedlike **planlagte og systematiske** tiltak **som er nødvendige** for å oppfylle kravene i eller i medhold av denne loven, herunder sikre personopplysningenes **kvalitet**.
- Den behandlingsansvarlige skal **dokumentere** tiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernemnda.
- Kongen kan gi **forskrift** med nærmere regler om internkontroll.

Personopplysningslovens krav

- Hva skal sikres?
 - Vern av konfidensialitet, integritet og tilgjengelighet for personopplysninger, pof § 2-1
- Hvem skal sikre?
 - Den behandlingsansvarlige og databehandleren, § 13
- Hvor sikkert?
 - Tilfredsstillende, jf. § 13 = forholdsmessig, pof [§ 2-1](#)
 - Risikovurdering, jf. pof § 2-4
 - Behandlingsansvarlig avgjør nivå, ev. Datatilsynet, jf. pof § 2-2

Personopplysningslovens krav (forts.)

- Hvordan sikre?
 - Systematisk, dokumentert arbeid
 - Bl.a. sikkerhetsmål, -strategi, revisjoner (§§2-3 – 2-5), 5 års lagring §2-16 mfl
 - Organisatoriske, tekniske tiltak
 - Eks. pof §§ 2-11 – 2-13 pålegger tiltak *hvis nødvendig*
 - Følge opp databehandlere ("påse", pol § 13 tredje ledd)

Risikovurdering - prioritering av tiltak

- Mange metoder
- Veiledning fra [Datatilsynet](#) og [Difi](#)
 - Kartlegge opplysningstyper
 - Identifisere uønskede hendelser
 - Vurdere konsekvenser og sannsynligheter
 - Innplassering i risikomatrise
 - Valg av tiltak

Aksepttabell

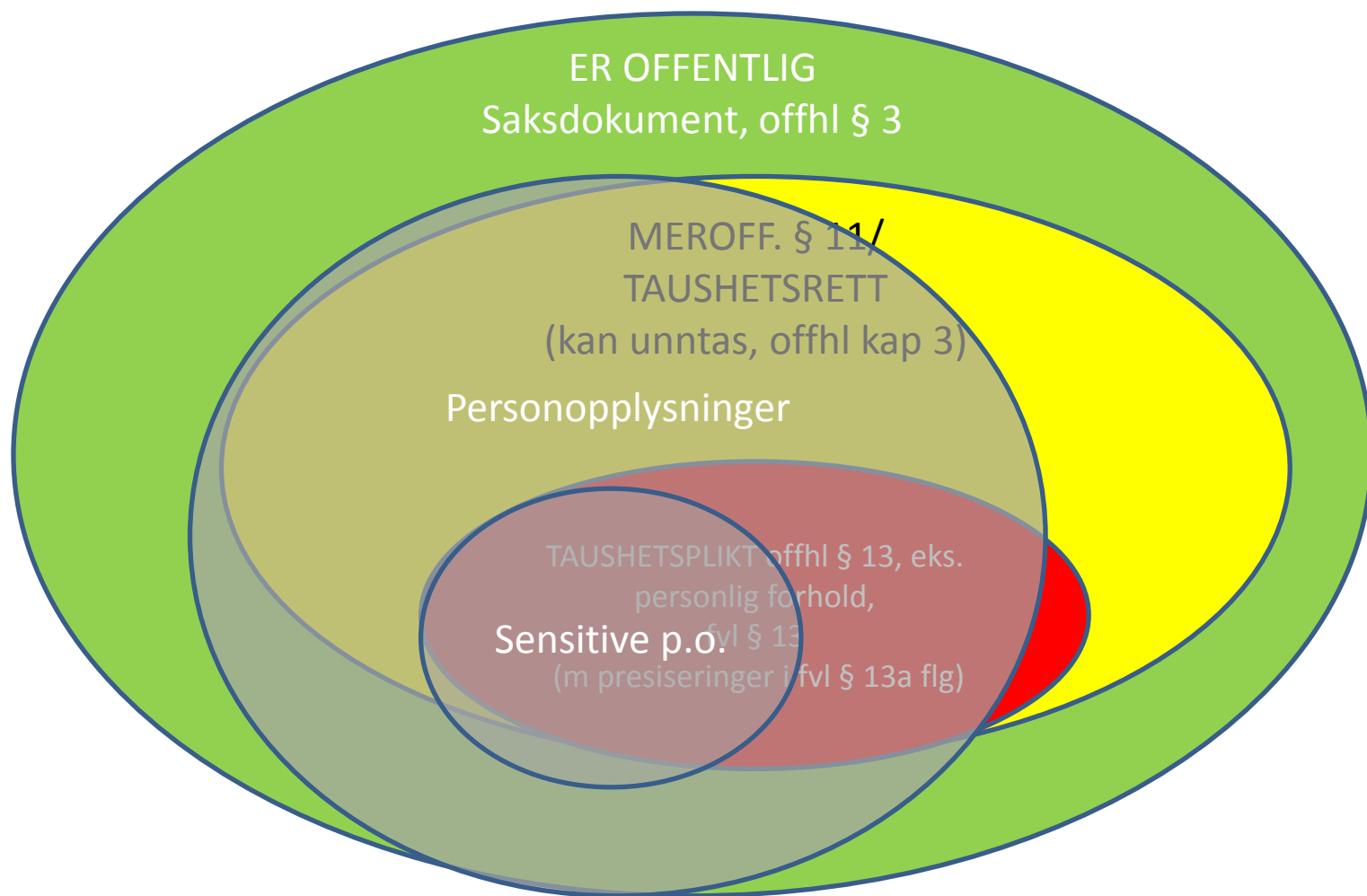
		Konsekvens			
		Liten/ ubetydelig(1)	Moderat/ mindre alvorlig (2)	Stor/ alvorlig (3)	Katastrofal/Svært alvorlig (4)
Sannsynlighet	Svært høy (4)		Ref: 11		
	Høy (3)	Ref: 9		Ref: 2, 32	
	Moderat (2)		Ref: 5, 25	Ref: 1, 6, 10, 12, 13 16	
	Lav (1)	Ref: 4, 14, 15, 17, 21, 22, 23, 24, 28, 30, 31	Ref: 3, 8	Ref: 7, 18, 20, 29	Ref: 19, 26, 27
		Lav risiko	Middels risiko		

High risk (Høy risiko) is indicated on the right side of the table, corresponding to the top two rows (Svært høy and Høy). Medium risk (Middels risiko) is indicated on the right side of the table, corresponding to the bottom two rows (Moderat and Lav).

Kartlegging

- Konfidensialitet - innsynsvern
 - Uvedkommendes bruk/innsyn
 - Taushetsplikt vs. offentlighet
- Integritet - endringsvern
 - Betydning for vedtak, avgjørelser
- Tilgjengelighet - tilgangsværn
 - Tidskritisk?

Kartlegging - konfidensialitet



Identifisere og analysere hendelser

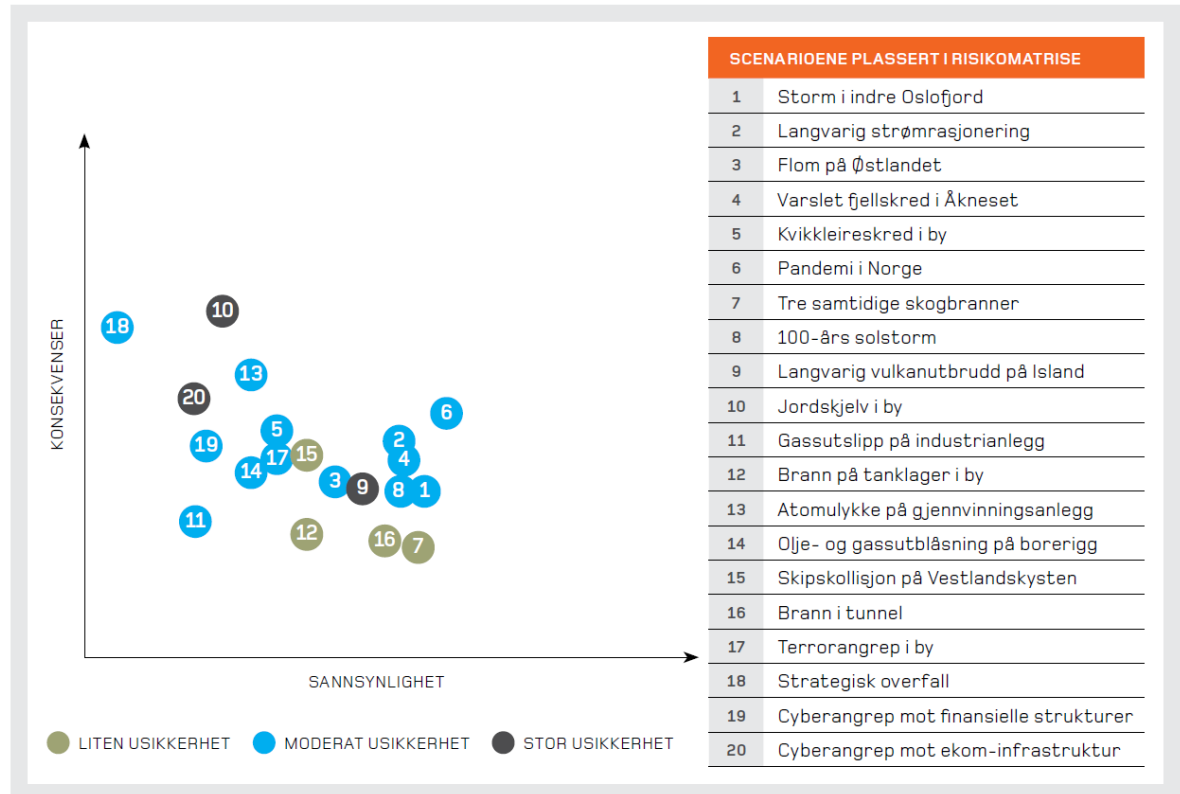
- Identifisere uønskede hendelser
 - Villedte og uaktsomme handlinger, hendelige uhell og naturfenomener
- Vurdere konsekvenser for hendelsene
- Vurdere sannsynlighet for hendelsene
- = Risiko

Risikomatrise

- Risiko: sannsynlighet
konsekvens
- Akseptabelt risiko
fastsettes
- Konsekvenser
- Sannsynlighet vurderes
– Letthet, motivasjon,
kapasitet, frekvens
- Eksempler: [Bok om
Nasjonalt risiko
2014](#) (s205)

Akseptabel risiko:	1-3
Evalueres	4-6
Uakseptabel risiko:	8-16

De analyserte scenarioene plassert i risikomatrise – med angitt usikkerhet



FIGUR 22. Nasjonalt risikobilde – samlet risikomatrise viser vurdert risiko (sannsynlighet, konsekvens og usikkerhet) knyttet til de konkrete alvorlige scenarioene som er analysert.

Eksempler på sikkerhetstiltak

- Krav til innlogging
 - Passord, MinID, BankID, smartkort, biometri (fingeravtrykk, ansiktsgeometri), etc
- Tilgangsstyring (need-to-know vs. need-to-hide)
- Krav til logging, gjennomgang av logger
- Backup, reserveløsninger
- Kryptering, tempest-vern, forsvarlig sletting
- Sikkerhetstesting (innbruddstest)
- Revisjon, pof § 13

Hendelser – K, I, T; tilsiktet/utilsiktet

Altinn Direktoratet for forvaltning og IKT

OFFENTLIGE ANSKAFFELSER

28 Jan 2014 10:24:42 3 Days 19:2

Home Configuration

AA59 NO PLA

XXF NO PLA

NO PLA

NO PLA

NO PLA

NO PLA

Et slikt skjermbilde møtte Stangvik da han fant siden h

Kamera so på gamleve åpent ute p

Dersom du visste nettdressen, kunne som krysset svenskegrensen på Fylkes

Arild Færaas

Oppdatert: 23. mar. 2014 19:20



Skole Huawei er hoffeverandør av b... (Jørgenrud)

PST adv:

– Vi har ikke nasjonal ko

Mandag 10. februar 2014 kl. Av Norsk Telegrambyrå

Politiets sikkerhetstjeneste myndighetene ikke har god norske telekommnetet, hvor er dypt inne i utbyggingen.

– Det er et problem at sels ikke har sikkerhetssamarb seksjonssjef Erik Hauglanc

Han sikter til det kinesiske som har fått oppdraget mer deler av nettet nordmenn b elektronisk kommunikasjor han nå advarselen PST, No Sikkerhetsmyndighet (NSN Etterretningstjenesten kom

– Som andre lands sikkerh bekymret for at vi ikke har vårt eget ekomnett. Vi men man sørge for å ha et sikke det landet som den aktører



STOPPET OPP: 17-åringen hacket en rekke av landets største nettsider. DNB alene varslet millioensaksimål i etterkant.

Hacker (17) slipper å betale 400.000 kr

■ Må jobbe 150 timer

Skoleelev fra Bergen parkere en rekke av landets største nettsider, men trenger ikke å betale erstatning.

Frode Buanes, Guro Valland, Audun Hageskal

Publisert: 26 feb. 2015 18:43 Oppdatert: 26 feb. 2015 18:50

Lagre i leselisten



I juli i fjor ble en 17-åring i Åsane pågrepet og siktet for å ha gjennomført omfattende dataangrep mot flere av Norges største bedrifter.

Nå er han dømt til samfunnsstraff i 150 timer for ungeringen. Det var BA som

FAKTA

- DDoS er en forkortelse for «Distributed Denial of Service», eller tjenestenektangrep på norsk. Det er ikke det samme som et hackerangrep.
- Tjenestenektangrep har til hensikt å hindre tilgangen til tjenestene på et nettsted. Hackerangrep har på sin side som regel til hensikt å ødelegge systemer eller innhente sensitive opplysninger.
- Tjenestenektangrep gjennomføres ved at angriperen eller angriperne sender enorme mengder henvendelser til et

Andre regelverk med krav til informasjonssikkerhet

- eforvaltningsforskriften, § 15 m.fl.
- Taushetspliktsbestemmelser
 - [Forvaltningsloven §13](#), [lignl §3-13](#)
 - [Sikkerhetsloven](#) & [informasjonssikkerhetsforskriften](#), [objektsikkerhetsforskriften](#)
 - [Beskyttelsesinstruksen](#) (kun statsforvaltningen)
- [Internkontrollkrav](#)
- Særregulering
 - Helseregisterloven, ikt-forskriften

Forvaltningsloven § 13 flg

- **hindre** at andre får adgang eller kjennskap... § 13
- forsvarlig oppbevaring, § 13c annet ledd
- informerte medarbeidere, § 13c første ledd

Kort om sikkerhetsloven

- Formål, jf. § 1
 - ”motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser...”
- Gradering, § 11 – STRENGT HEMMELIG/ HEMMELIG/ KONFIDENSIELT/ BEGRENSET
 - Skade hvis informasjonen kommer på avveie (ref. § 1)
- Streng need-to-know, § 12
- NSM-godkjenning av informasjonssystemer, § 13, m.v.
- Forskrifter
 - Informasjonssikkerhetsforskrift m.v. med detaljerte sikringsregler
 - [Objektsikkerhetsforskriften](#)

Kort om beskyttelsesinstruksen

- Instruks for statsforvaltningen
- Gradering (§ 2)
 - STRENGT FORTROLIG eller FORTROLIG
- Vurderingstema (§ 4)– skade/betydelig skade mht.
 - offentlige interesser, en bedrift, en institusjon eller en enkeltperson at dokumentets innhold blir kjent for uvedkommende
- Konsekvenser
 - Strengt need-to-know-prinsipp, § 7 – personlig ansvar
- Elektronisk behandling ”så langt det passer” ihht. deler av [informasjonssikkerhetsforskriften](#) etter sikkerhetsloven, jf. § 12

Eforvaltningsforskriften

- Opprinnelig fra 2002
- Viktige endringer 2014 – digitalt førstevalg
- Hjemlet i forvaltningsloven [§ 15a](#) (og esignl)
- Formål, [§ 1](#):
 - **sikker og effektiv bruk** av elektronisk kommunikasjon med og i forvaltningen
 - **forutsigbarhet**, fleksibilitet, samordning av løsninger
 - enhver på en **enkel måte** kan utøve sine rettigheter og oppfylle sine plikter i forhold til det offentlige

efvf og informasjonssikkerhet

- Overordnet krav til **internkontroll** på informasjonssikkerhetsområdet, [§ 15](#)
 - Basert på anerkjente standarder for styringssystem for informasjonssikkerhet
 - Mål og strategier, ref. pof § 2-3
 - Omfang basert på **risiko**, ref. pof [§ 3-1](#)
 - Fortrinnsvis helhetlig styringssystem
- Publikums digitale kommunikasjon med forvaltningen
 - Kan skje uten bruk av sikkerhetstjenester, med mindre det kreves, § 4
 - Organet må tilby eller peke på løsninger, § 4 nr 4
 - Regulering av innkommende taushetsbelagte opplysninger fra publikum, § 5
- Efvf kap 4-6 – regulering av sertifikater og private nøkler

Efvf § 15

- § 15. *Internkontroll på informasjonssikkerhetsområdet (utdrag: annet og tredje ledd)*
 - Forvaltningsorganet skal ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på **anerkjente standarder** for styringssystem for informasjonssikkerhet. Internkontrollen **bør** være en **integreert del** av virksomhetens helhetlige styringssystem. Det organet departementet peker ut skal gi **anbefalinger** på området.
 - Omfang og innretning på internkontrollen skal være **tilpasset risiko**.
- Veiledning: internkontroll.infosikkerhet.difi.no

Digital kommunikasjon til innbyggerne

- Digitale **meldinger** til innbyggerne
 - Kan sendes, [efvf § 8](#)
 - Strengere krav til enkeltvedtak og andre viktige meldinger
 - Egnede informasjonssystem (hovedregel)
 - Varsel, gjentatt varsel
 - Logging av innsyn
 - Innbygger kan reservere seg mot å få viktige meldinger, § 9
- Digital **kontaktinformasjon** til innbyggerne
 - Kan lagres, efvf § 31
 - Opprettes med opplysninger fra ID-porten, § 38
 - Kan brukes i forvaltningen, varsling § 29

- Spørsmål?