Strategisamling 14.-15. jan 2016 Sikkerhet

- EUs GDPR – Ny personvern forordning
- Sikkerhetskurs – E-læring
- Policy og Rutiner

Ny personvernlov - forordning

GDPR trer i kraft i mars 2016 og kommunene skal være «compliant» innen mars 2018.

Overnasjonal lov som vil erstatte Personopplysningsloven (POL)
Overgangstid 2 år (dvs. virksomheter MÅ kunne dokumentere etterlevelse inn mars 2018)

GDPR – omfattende og mer konkrete krav til personvern

- 11 kapitler, 15 seksjoner og 91 artikler (paragrafer)
- Gjelder for alle virksomheter som behandler PII* om EU
- På noen få områder vil nasjonal (sær-)lovgivning gjelde (helsesektoren, forskning, nasjonal sikkerhet..)

Ny personvernlov - forordning

Hovedpunkter i den nye Personvern Forordningen:

- Mer omfattende regelverk enn dagens Personopplysningslov
- Økt krav til oversikt, kontroll og dokumentasjon
- Krav til «privacy-by-design» må etableres i nye prosjekter
- Tjenesteleverandører vil få økt ansvar/risiko
- Norske virksomheter MÅ starte arbeidet asap
- Databehandleres (utvidede ansvar & risiko) som kan medføre sanksjoner
- Databehandlere som må ansette / innleie av kompetente Personvernombud / Data Privacy Officers
- Virksomheter som driver nettbaserte tjenester / leveranser har en rekke nye krav til bl.a.
  - Økt krav og innhold til informasjonsplikten
  - Privacy-by-design
  - Bruk og kontroll av underleverandører
  - ..mm

Ny personvernlov - forordning

HVILKE MULIGHETER / KONSEKVENSER KAN DETTE MEDFØRE?

- Strengere krav til etablering og oppfølging av eget internkontrollsystem for personvern
- Økt fokus på risikobasert behandling og dokumentasjon, av personopplysninger
- Krav til «privacy by design» samt «security by default» i nye digitale tjenester
- Stiller større krav til avklaring, dokumentasjon og kontroll i forholdet mellom behandlingsansvarlig og databehandler
- Økt krav til personvernkompetanse og –ressurser i de fleste virksomheter hvor PII inngår i kjernevirksomheten
- Bøtesatsene og sanksjoner ved personvernavvik / -lovbrudd vil øke betydelig – vil svi økonomisk!
- M.m…

Ny personvernlov - forordning

HVILKE MULIGHETER / KONSEKVENSER KAN DETTE MEDFØRE?

- Strengere krav til etablering og oppfølging av eget internkontrollsystem for personvern
- Økt fokus på risikobasert behandling og dokumentasjon, av personopplysninger
- Krav til «privacy by design» samt «security by default» i nye digitale tjenester
- Stiller større krav til avklaring, dokumentasjon og kontroll i forholdet mellom behandlingsansvarlig og databehandler
- Økt krav til personvernkompetanse og –ressurser i de fleste virksomheter hvor PII inngår i kjernevirksomheten
- Bøtesatsene og sanksjoner ved personvernavvik / -lovbrudd vil øke betydelig – vil svi økonomisk!
- M.m…

Privacy by Design

Privacy by Design:

- Privacy by Design er en tilnærming til systemutvikling som tar personvernhensyn gjennom hele prosessen. Tar hensyn til menneskelige verdier i materiale gjennom hele prosessen.

- Individets rettigheter:

Personvernombud

… er en ressursperson som styrker virksomhetens kunnskap og kompetanse om personvern. Personvernombudsordningen er en frivillig ordning administrert av Datatilsynet.

Personvernombudets og virksomhetens plikter

1. Den som virksomheten har utnevnt til personvernombud skal være egnet til, på en uavhengig måte, å vurdere om *behandlingsansvarlig* overholder reglene i personopplysningsloven.
2. Personvernombudet skal
   a. påse at behandlinger av personopplysninger blir meldt til ombudet, og at meldingene inneholder korrekte og tilstrekkelige opplysninger,
   b. føre en systematisk og offentlig tilgjengelig fortegnelse over behandlingene,
   c. påse at behandlingsansvarlig har et system for *internkontroll* som tilfredsstiller personopplysningslovens § 14, jf. personopplysningsforskriftens kapittel 3,

Personvernombud

d. bistå de registrerte med å ivareta deres rettigheter etter reglene om behandling av personopplysninger,
e. påpeke brudd på personopplysningsloven overfor behandlingsansvarlig,
f. gi Datatilsynet opplysninger dersom tilsynet ber om det, herunder foreta undersøkelser i konkrete saker,
g. holde seg orientert om utviklingen innen personvern, og
h. gi råd og veiledning til behandlingsansvarlig om behandling av personopplysninger og reglene for dette.

Etablering av personvernombud fritar ikke virksomheten fra dennes ansvar for at reglene i personopplysningsloven overholdes.

Virksomheten skal informere Datatilsynet dersom avtalen om personvernombud opphører, eller virksomheten endrer personvernombud.

GDPR- paragrafer - noen utvalgte

Artikkel 26– Databehandler
Artikkel 27– Behandling av PII hos behandlingsansvarlig eller hos databehandler
Artikkel 28 – Dokumentasjon
Artikkel 29– Samarbeid med tilsynsmyndighet(er)
Artikkel 30 – Sikkerhet ifbm prosessering av personopplysninger
Artikkel 31 – Varsling til tilsynsmyndighet ved personvernbrudd
Artikkel 32 – Varsling til «den registrerte» som er berørt av personvernbruddet
Artikkel 33 – Risikovurdering (inkl. Privacy Impact Assessments)
Artikkel 34 – Forhåndsgodkjenning (konsesjon) fra tilsynsmyndighet
Artikkel 35 – Data Privacy Officer (DPO)
Artikkel 38 – God praksis (Codes of conducts)
Artikkel 39 – Sertifisering
Artikkel 42 – Overføring av personopplysninger til land utenfor EU
Artikkel 77 – Rett til kompensasjon og ansvarliggjøring
Artikkel 79 – Administrative sanksjoner

Artikkel 79 – Administrative sanksjoner

Sanksjoner – nasjonale tilsynsmyndigheter skal ha makt til å pålegge sanksjoner som er effektive, forholdsmessige og avskrekkende.

Sanksjoner kan inkludere praktiske tiltak – behandlingsansvarlig og/eller databehandler(e) kan bli pålagt til å gjennomføre konkrete tiltak, stoppe behandling, sletting av opplysninger, kreve dokumentert etterlevelse innen frist, pålagt jevnlige revisjoner (eksterne), mm

Mulige type sanksjonsnivåer – vil være avhengig av flere faktorer som bl.a.; type personvernbrudd, bevisst / ikke bevisst handling, omfang (antall berørte, varighet, type opplysninger, etc.), tidligere hendelser, mm.:

- Skriftlig advarsel, årlig personvern revisjon, bøter og evt. fengsel
- Bøter opp til 250 000 Euro eller opptil 0,5% av årlig omsetning
- Bøter opp til 500 000 Euro eller opptil 1 % av årlig omsetning
- Bøter opp til 1 000 000 Euro eller opptil 2-5 % av årlig omsetning

GDPR – Hva betyr det for oss

- Personvern
- Individets rettigheter
- Dokumentasjon
- Privacy by Design
- Personvernombud
- Sanksjoner

Compliant?

IKTNH kjører et prosjekt på GDPR. Vi ønsker å bli Compliant så snart som mulig:

- Status ihht eksisterende Personopplysningslov (POL)
  - Identifisere personvernnivå / - status
  - Identifisere forbedringsområder som er grunnleggende / kritisk
- Introduksjon av den nye GDPR
  - Avklare og prioritere relevante GDPR-krav:
    - Som enten er; (ikke) relevante krav, nye krav, strengere krav, mer detaljert krav, økte plikter & ansvar, mm.
- Avklaringer av lovkrav i nytt regelverk som er relevant for IKTNH og virksomheten
- Etablering av en overordnet handlingsplan
  - Vurdere, prioritere og konkretisere hvordan sikre etterlevelse iht GDPR*

Strategisamling

Sikkerhetskurs:
https://nordhordland.knowledgeportal.no/#/carousel

TLA – Policy og Rutiner:
http://iktnh.custompublish.com/iktnh-og-kommunane.365284.nn.html

Policy og Rutiner

1. Overordnet Sikkerhetspolicy
    a. IKTNH sikkerhetspolicy
2. Ansettelsessikkerhetspolicy
3. Brukersikkerhetspolicy
4. Fysisksikkerhetspolicy
5. Informasjonssikkerhetspolicy
6. Policy for behandling av helse og personopplysninger
7. Teknologisk sikkerhetspolicy
8. Tilgangskontrollpolicy
9. Rutiner
    a. Brukerregistrering
    b. Endringshåndtering
    c. Hendelseshåndtering
    d. Logghåndtering
    e. Sikkerhetsrevisjon
    f. Utstyr med helse – og personopplysninger

Sikkerhetsnivå 4

- Dagens sikkerhetsnivå 4 er ikke lengre en sikkerhetsnivå 4 løsning.
  - Kravene til sikkerhetsnivå 4 har økt.

- Det må investeres i ny løsning

- IKTNH investerer i løsningen for sikkersone
- Kommunene kjøper inn etter behov:
  - Kortlesere
  - Klientlisenser
  - Kort

- I ny PC avtale så har vi inkludert tastatur med kortlesere. Vil være tilgjengelig fra april.