Betydningen av GDPR i UH-sektoren og Sekretariatets arbeid

Tommy Tranvik

Sekretariatet for informasjonssikkerhet i UH-sektoren

Informasjonssikkerhet og personvern

- Fire oppfatninger om sammenhengen

1. Informasjonssikkerhet og personvern er det samme
2. ***Informasjonssikkerhet og personvern er motsetninger***
3. ***Personvern er mer enn informasjonssikkerhet***
4. ***Informasjonssikkerhet er mer enn personvern***

UNINETT

Overordnet sammenlikning

- GDPR og dagens regelverk (lov og forskrift)
  - Mye «gjenbruk» og (relativt) lite helt nytt
  - Mer ordrik og omfattende
  - Forenkling og av-byråkratisering?

- Overholdes dagens regelverk?
  - «Ja, stort sett» – god kontroll på fristen
  - «Nei, i begrenset grad» – hastverk for å nå fristen
  - «Kjenner ikke dagens regler» – greier ikke fristen

UNINETT

Informasjonssikkerhet

- «Gjenbruk»
  - Ledelsessystem for informasjonssikkerhet
- Nyheter
  - Definisjon – det vanlige pluss «robusthet»
  - Grunnkrav – konfidensialitet og integritet (helt nytt)
  - Varslingsreglene – «De registrerte» og Datatilsynet (delvis nytt)

Sekretariatet for informasjonssikkerhet

- Fokus på reglene om informasjonssikkerhet (eller som berører informasjonssikkerhet)
  - Veileder om regler som helt eller delvis handler om informasjonssikkerhet
  - Oppdatering av veileder for ledelsessystem
  - Sjekkliste for databehandleravtaler
  - Møter med institusjonene
- Institusjonsnivå
  - Status for ledelsessystemet for informasjonssikkerhet
  - Identifisere og lukke avvik, jf. veilederne ovenfor
- Liknende fremgangsmåte mht. andre regler i GDPR
  - Gjennomgang med system- eller tjenesteeiere
  - Særlig fokus på opplysningsoversikt, grunnkrav, hjemmel, rettigheter og databehandlere
  - Dokumentasjon (protokoll)

UNINETT

De viktigste «nyhetene»

- Avvikling av melde- og konsesjonsplikten (helt nytt)
- Krav til «internkontroll» og dokumentasjon (delvis nytt)
- Innebygd personvern (mye nytt)
- Krav til personvernkonsekvensutredning og drøftelser (helt nytt)
- Krav til personvernrådgiver (delvis nytt)
- Databehandleres ansvar (delvis nytt)
- Samordning mellom datatilsynsmyndigheter (mye nytt)
- Sanksjoner (delvis nytt)

Helt eller delvis «gjenbruk»

- Formål
- Virkeområde og definisjoner (noe nytt)
- Grunnkravene (noen endringer)
- Lovlig grunnlag (mindre endringer)
- De fleste rettighetene (enkelte nye)
- Krav til informasjonssikkerhet (noe nytt)
- Bruk av databehandlere og avtaler (mer utfyllende)
- Overføring til tredjeland (mer utfyllende, liberalisering)