Direktoratet for e-helse

GDPR – Hva er det og hva er nytt?

Presentasjon fra GDPR-prosjektet hos Direktoratet for e-helse

Bakgrunn

- General Data Protection Regulation (GDPR) ble formelt vedtatt av EU i april 2016
- GDPR trer i kraft to år etter at den er vedtatt i EU (25.mai 2018)
- Formål:
  - Felles regelverk for personvern i Europa
  - Styrke den europeiske borgers rettigheter
  - Styrke tilliten til digitale tjenester

Forholdet til nasjonal lovgivning

- EU-medlemstatene
  - Direkte gjeldende i EU-land og erstatter nasjonal lovgivning
  - GDPR begrenser medlemslandenes mulighet for «nasjonale» bestemmelser

- EØS-land
  - GDPR er EØS-relevant og må dermed inntas som vedlegg i EØS-avtalen
  - Nye personvernregler i Norge fra mai 2018

Definisjoner

- **Personopplysninger**
  - enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»)

- **Den registrerte (identifiserbar fysisk person)**
  - en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en online-identifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet

- **Behandling**
  - enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring

Definisjoner forts.

- **Databehandlingsansvarlig (DBA)**
  - den fysiske eller juridiske person, offentlige myndighet, byrå eller ethvert annet organ
  - som alene eller sammen med andre bestemmer
  - formålet med behandlingen og hvilke virkemidler som skal benyttes

- **Databehandler**
  - den fysiske eller juridiske person, offentlige myndighet, byrå eller ethvert annet organ
  - som behandler personopplysninger på vegne av en behandlingsansvarlig

Prinsippene for vern av personopplysninger – GDPR art. 5

- Lovlighet, rettferdighet og gjennomsiktighet
  - Personopplysninger skal behandles på en lovlig, rettferdig og gjennomsiktig måte med hensyn til den registrerte
  - Strengere dokumentasjonskrav
- Formålsbegrensning
  - Personopplysninger skal samles inn for spesifikke formål og ikke viderebehandles på en måte som er uforenlig med disse formålene
- Dataminimering
  - Personopplysninger skal være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for
- Riktighet
  - Personopplysninger skal være korrekte og om nødvendig oppdaterte
- Lagringsbegrensning
  - Personopplysninger skal lagres kun i perioder der de er nødvendige for formålene
- Integritet og fortrolighet
  - Personopplysninger skal behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysninger

Hva er nytt i forordningen?

- Styrking av den registrertes rettigheter
- Flere plikter for databehandleransvarlig og databehandler
- Nye krav til samtykke
- Krav til innebygd personvern og personvern som standardinnstilling
- Krav til vurdering av personvernkonsekvenser
- Strengere krav til avvikshåndtering
- Strengere sanksjoner

Styrking av den registrertes rettigheter

- Informasjon
  - Utvidet informasjon plikt: nye informasjon elementer i art. 13 og art. 14
- Innsyn
  - Utvidet innsyn: detaljerte krav i art. 15
- Korrigering
  - Korrigering må skje uten ugrunnet opphold
- Sletting
  - Sletting må skje uten ugrunnet opphold
  - Plikt for DBA som har offentliggjort opplysninger til å informere andre DBA som behandler personopplysningene

Styrking av den registrertes rettigheter forts.

- Begrensning
  - Retten til å kreve at behandlingen av personopplysningene begrenses
    - den registrerte bestrider at opplysningene er korrekte
    - behandlingen er ulovlig og den registrerte ikke ønsker at opplysninger skal slettes
  - DBA har plikt til å informere om begrensning av behandling av personopplysninger til alle som har mottatt personopplysningene

- Dataportabilitet
  - Retten til å ta med seg sine opplysninger fra en virksomhet til en annen
  - Gjelder kun for opplysninger som den registrerte selv har gitt til DBA
  - Gjelder kun når behandling av personopplysninger skjer på bakgrunn av et samtykke eller en kontrakt

Styrking av den registrertes rettigheter forts.

- Automatiserte avgjørelser inkl. profilering
  - Gjelder for avgjørelser som utelukkende er basert på automatisert behandling som har rettsvirkning for eller på tilsvarende måte betydelig påvirker den registrerte
  - Hovedregelen er at slike avgjørelser er forbudt
  - Automatiserte avgjørelser er kun tillatt dersom de:
    - er nødvendige for å inngå eller gjennomføre en avtale med de registrerte
    - er hjemlet i lov som samtidig gir tilfredsstillende garantier for personvernet til de registrerte
    - er basert på eksplisitt og gyldig samtykke
  - DBA har plikt til å gi informasjon om
    - at automatiserte avgjørelser finner sted
    - den underliggende logikken
    - betydningen og de forventede konsekvensene av en slik behandling for den registrerte

Styrking av den registrertes rettigheter forts.

- Innsigelse
  - Retten til å motsette seg behandling av personopplysninger dersom
    - opplysningene behandles fordi det er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet etter forordningen art. 6 (1) (e)
    - opplysningene behandles med grunnlag i en interesseavveining etter art. 6 (1) (f)
    - formålet med behandlingen er direkte markedsføring (uavhengig av hva behandlingsgrunnlaget er)
  - DBA har plikt til å informere eksplisitt om retten til å motsette seg
  - DBA skal ikke lenger behandle personopplysningene men mindre
    - det foreligger tvingende, berettigede grunner for behandlingen som går foran den enkeltes personvern og rettigheter, eller
    - behandlingen er nødvendig for å ivareta et rettskrav

Plikter for databehandlingsansvarlig og databehandler

- Nye krav til innhold i databehandleravtale
- Strengere krav til oversikt av personopplysninger
- Sikre informasjonssikkerhet
  - DBA og DB må gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet i forhold til risikoen
- Oppnevne personvernombud i visse tilfeller

Plikter for databehandlingsansvarlig

- Internkontrollsystem
  - Egnede tekniske og organisatoriske tiltak, med utvidet fokus
  - Tiltak skal gjennomgås på nytt og skal oppdateres ved behov
- Innebygd personvern og personvern som standardinnstilling
- Bruke databehandler som gir tilstrekkelig garanti for ivaretakelse av personvernet
- Sende avviksmelding til Datatilsynet
  - Krav til innhold og tidsfrister
- Gjennomføre personvernkonsekvensvurderinger
- Forhåndsdrøftinger med Datatilsynet

Selvstendige plikter for databehandler

- Hjelpe DBA med etterlevelse av forordningen
- Søke forhåndsgodkjenning fra DBA ved bruk av underleverandører
- Behandle personopplysninger kun basert på avtale med DBA
  - Krav til innhold i databehandleravtale
    - Tilstrekkelig garanti for ivaretakelse av personvernet
- Dokumentere behandling av personopplysninger som foretas for hver enkelt DBA

Samtykke

- Krav til samtykke:
  - frivillig
  - uttrykkelig
  - informert
  - utvetydig
- Inaktivitet/passivitet er ikke lovlig samtykke
- Samtykkeskjema må være klart, konsist og ikke unødvendig forstyrrende for bruken av tjenesten
- Tilbaketrekking av samtykke skal være like enkelt som å avgi samtykke

Innebygd personvern og personvern som standardinnstilling

- DBA har plikt til å følge prinsippene for innebygd personvern og personvern som standardinnstilling
  - Ta hensyn til personvernet i alle utviklingsfasene av et system

- Omfatter både organisatoriske og tekniske tiltak

- Det minst personverninngripende alternativet skal brukes som standard

Vurdering av personvernkonsekvenser

- Vurdering av personvernkonsekvenser blir obligatorisk for behandlingen som kan medføre en høy risiko for den registrerte
  - For eksempel behandling av sensitive personopplysninger (helseopplysninger) i stort omfang
  - For å kartlegge typer, omfang og grad av risiko
  - Det må gjøres før behandlingen starter

Avvikshåndtering

- DBA har en varslingsplikt ved brudd på personopplysningssikkerheten
  - Krav til innhold i art. 33(3)

- DBA skal holde oversikt og dokumentere alle sikkerhetsbrudd

- Melding til Datatilsynet:
  - uten ugrunnet opphold og senest 72 timer etter at de ble kjent med bruddet
  - eventuelt forsinkelse må begrunnes

- DBA skal underrette den registrerte:
  - uten ugrunnet opphold dersom det er sannsynlig at bruddet vil medføre en høy risiko for den registrertes grunnleggende rettigheter

Sanksjoner

Gradert tilnærming

- Brudd på databehandlingsansvarliges og databehandlers plikter
  - 10 mill EUR eller 2% av omsetting på verdensbasis
- Brudd på prinsipper og rettigheter
  - 20 mill EUR eller 4% av omsetting på verdensbasis
- Alvorlige feil og mangler, herunder manglende overholdelse av pålegg
  - 20 mill EUR eller 4% av omsetting på verdensbasis