GDPR i praksis, sett fra en teknisk bedömmer

Anders Bergman
IT-bedömmer NA og SWEDAC
Greenfinger AB

Lov om behandling av personopplysninger (personopplysningsloven)

LOV-2018-06-15-38

Hva er viktig for akkrediterte organisasjoner, og hva har skjedd i Sverige etter introduksjonen 25/5 2018?

Hva vil NA fokusere på på IT-revisjoner?

- NA er IKKE tilsynsmyndighet for GDPR
- Akkrediterte virksamheter må etterkomme alle gjeldende lover og forskrifter, ikke bare GDPR
- Fokus vil være på systematisk (informasjonssikkerhets-)arbeid i virksomheten med hensyn til etterkommelse av GDPR
- Informasjonsklassifisering, risikostyring og avviksstyring er de viktigste områdene
- Databehandlingsavtaler med leverandører

Noen viktige artikler i GDPR

- **GDPR artikkel 3**
  GDPR bør brukes av enhver organisasjon som behandler data fra EU-registrerte
- **GDPR artikkel 37-39**
  Utnevnelse av en kvalifisert databeskyttelsesansvarlig (DPO) (om nødvendig)
- **GDPR artikkel 35**
  Forpliktelse til å gjennomføre risikoanalyser og konsekvensvurderinger
- **GDPR artikkel 5, 89**
  - Personlige data må samles inn for spesifiserte, eksplisitte og legitime formål og ikke viderebehandles på en måte som er uforenlig med disse formålene. - -
  - Personlige data må være tilstrekkelig, relevant og begrenset til de som er nødvendige;
  - Hvor personopplysninger skal arkiveres, f.eks. for forskning og statistiske formål bør personvernrisikoen behandles ved hjelp av egnede kontroller som pseudonymisering og dataminimalisering når det er mulig

Forts. Noen viktige artikler i GDPR

- **GDPR artikkel 17**
  Lagringsbegrensning (data skal ikke holdes lenger enn det er nødvendig); Rett til å slette ("rett til å bli glemt"), inkludert tilbaketrekking av samtykke;
- **GDPR Recital nr. 39**
  Integritet og konfidensialitet, passende sikkerhet for personopplysningene (inkludert beskyttelse mot uautorisert eller ulovlig behandling og utilsiktet tap, ødeleggelse eller skade)
- **GDPR artikkel 33-34**
  Krav til håndtering av avvik/databrudd

Konklusjon

- Sørg for at organisasjonens informasjonssikkerhetsarbeid inkluderer personvern og beskyttelse av personopplysninger, pseudonymisera eller anonymisera hvis mulig.
- Hvis databeskyttelsesansvarlig (DPO) er utnevnt innenfor den akkrediterte virksomheten, må være en dokumentert rolle med stillingsbeskrivelse
- Risikoanalyse av informasjonshåndtering må gjennomføres med hensyn til teknologi, organisasjon og personlig integritet. Identifiserte risikoer må dokumenteres og avhjelpes
- Prosedyrer må utvikles for å sikre at personrelatert informasjon som er registrert i bedriftens IT-system minimeres, og det behandles bare ut fra spesifisert formål

Konklusjon, forts.

- Databehandlingsavtaler (med IT-tjenesteleverandører) skal brukes til kommunikasjon og lagring av personopplysninger som sikrer at informasjonen: - håndteres på en måte som overskrider informasjonens klassifisering / forretningsbehov.
- Aktivt samtykke til personlig databehandling skal dokumenteres, og samtykke skal tilbakekalles i relevante tilfeller
- Når man anskaffer nye IT-systemer / IT-funksjoner, må kravet om "Privacy by design and default" overveies.
- Mye er fortsatt uklart når det gjelder tolkning av lovverket,
  Vennligst les anbefalingene fra artikkel 29-gruppen:
  http://ec.europa.eu/newsroom/article29/news-overview.cfm
- Ha en nær dialog med ansvarlige personer for juridik/lov og informasjonssikkerhet i organisasjonene dine, og følg instruksjonene de gir.....

Erfaringer fra Sverige etter 25/5

- Noen ganger vanskelig å bestemme hvilken organisasjon som er PUA og PUB
- Få forespørsler om registerutdrag og stadig avtagende
- De fleste organisasjoner gir bare metadata ved den første forespørselen
- Relativt få rapporterte hendelser i løpet av den første måneden, men nå stadig økende antall
- Tilsynsmyndigheten *Datainspektionen* oppfordrer underretningen om mindre kritiske hendelser for å få et godt bilde av hva som skjer i organisasjonene
- Den vanligste hendelsen er at e-post sendes til feil person, og at sensitive personlige data sendes ukryptert via e-post
- Den nest vanligste hendelsen er tapt eller stjålet mobiltelefoner, lesplater og bærbare PC-er
- Mange spørsmål om håndtering av bilder og filmer….
- Rutiner for håndtering av personopplysninger blir stadig større spørsmål
- Stor fokus på systematisk informasjonssikkerhetsarbeid

Takk for din oppmerksomhet!

Anders Bergman
IT-bedömmer för NA och SWEDAC
anders@greenfinger.se