Etterlevelse av personvernforordningen (GDPR) sett opp mot ISO 15189 – hva er nytt/viktig?

Anders Bergman

Greenfinger AB

Lov om behandling av personopplysninger (personopplysningsloven)

LOV-2018-06-15-38

Hva betyr dette for akkrediterte aktiviteter, og hva har skjedd i Sverige etter introduksjonen 25/5 2018?

General Date Protection Regulation (GDPR) vs. ISO 15189 tolket av European Accreditation (EA)

- Dokumenter er utviklet for å avklare hvordan kravene til GDPR er relatert til kravene i ISO 15189: 2012
- Beskriver hvilke aktiviteter de akkrediterte organisasjonene må gjennomføre for å oppfylle kravene
- Beskriver også hvilke dokumenter de akkrediterte organisasjonene kan trenge for å fullføre 15189-styringssystemet med.

GDPR artikkel 3

GDPR bør brukes av enhver organisasjon som behandler data fra EU-registrerte.

TILTAK

- Laboratoriestyring skal ha ordninger som er knyttet til personvern og beskyttelse av folks personlige opplysninger, spesielt følsomme datamaskiner.

TILLEGGSDOKUMENTASJON

- Ikke nødvendig

GDPR artikkel 37-39

Utnevnelse av en kvalifisert databeskyttelsesansvarlig (DPO) (om nødvendig)

TILTAK

- DPOs skal utnevnes når det gjelder: (a) offentlige myndigheter, (b) organisasjoner som engasjerer seg i systematisk overvåking, eller (c) organisasjoner som engasjerer seg i omfattende behandling av sensitive personopplysninger.

TILLEGGSDOKUMENTASJON

- Rollebeskrivelse av DPO hvis en slik DPO er nødvendig.

GDPR artikkel 35

Forpliktelse til å gjennomføre risikoanalyser og konsekvensvurderinger

TILTAK

- Personvernrelaterte risikoer bør inkluderes i selskapsrisikoregistre sammen med ulike andre risikoer.

TILLEGGSDOKUMENTASJON

- Analyse av virkningen av behandling av person-opplysninger for fysiske personer.

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.

TILTAK

- Laboratoriums prosesser pluss programmer, systemer og nettverk skal tilstrekkelig sikre personlig informasjon, og krever en omfattende serie av teknologiske, prosessmessige, fysiske og andre kontroller, med utgangspunkt i en vurdering av de tilknyttede informasjons-risikoen.

TILLEGGSDOKUMENTASJON

- Sikkerhetspolicyer som sikrer riktig sikkerhet for personopplysningene, inkludert beskyttelse mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade ved hjelp av passende tekniske eller organisatoriske tiltak

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;

TILTAK

- Datalagringspolicy (Data retention policies)

TILLEGGSDOKUMENTASJON

- Ikke nødvendig, hvis retningslinjer for datalagring implementeres

GDPR Recital nr. 39

Integritet og konfidensialitet, passende sikkerhet for personopplysningene (inkludert beskyttelse mot uautorisert eller ulovlig behandling og utilsiktet tap, ødeleggelse eller skade)

TILTAK

- Dataoverføring og datadeling
- Databehandlingsavtaler
- Sikkerhetspolicy

TILLEGGSDOKUMENTASJON

- Sikkerhetspolicyer som sikrer riktig sikkerhet for personopplysningene, inkludert beskyttelse mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade ved hjelp av passende tekniske eller organisatoriske tiltak

GDPR artikkel 33-34

Krav til håndtering avvik/databrudd

TILTAK

- Prosedyre for avvikshåndtering bør omfatte: - Beskrivelse av arten, antall registrerte personer, de sannsynlige konsekvensene, tiltak som er truffet eller foreslått for å rette opp avviket/bruddet.
- Skal vurderes at det er en stram tidsfrist på 72 timer for melding av avvik til Datatilsynet.

TILLEGGSDOKUMENTASJON

- Databruddprotokoller og prosedyrer for avvikshåndtering som må implementeres likevel under ISO 15189

GDPR artikkel 7-9, nr. 161, nr. 33

Gyldig samtykke er nødvendig (inkludert prosess av barns data). Samtykke kan bli trukket tilbake når som helst.

TILTAK

- Det er et krav om å be om informert samtykke til behandling (ellers stopp!) Og å kunne demonstrere dette.
- Prosedyrer må være på plass for dette, og registreringer som viser at samtykket må være beskyttet og beholdt.
- For å samtykke til deltakelse i vitenskapelig forskningsaktivitet i kliniske studier, bør de relevante bestemmelsene i forordning (EU) nr. 526/2014 gjelde.

TILLEGGSDOKUMENTASJON

- Samtykker
- Implementert datalagringspolicy

Konklusjon

- Sørg for at organisasjonens informasjonssikkerhetsarbeid inkluderer personvern og beskyttelse av personopplysninger, pseudonymisera hvis mulig.
- Hvis databeskyttelsesansvarlig (DPO) er utnevnt innenfor den akkrediterte virksomheten, må det være en dokumentert rolle og arbeidsbeskrivelse
- Risikoanalyse av informasjonshåndtering skal gjennomføres med hensyn til teknologi, organisasjon og personlig integritet. Risikoer må dokumenteres og klare å minimere risikoen for bevisst (forbrytelser) eller utilsiktet skade på eller tap av data
- Rutiner bør gjøres for å sikre at personrelatert informasjon som er registrert i bedriftens IT-system minimeres, og det behandles bare ut fra det oppgitte formålet

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 - Kun lagret så lenge det er nødvendig i samsvar med gjeldende lover, forskrifter og proprietære merknader - i relevante tilfeller kan det slettes på forespørsel fra virksomheten.
- Rutiner bør gis for rapportering og håndtering av avvik
- Aktivt samtykke til personlig databehandling skal dokumenteres, samtykke skal tilbakekalles i relevante tilfeller
- Når man anskaffer nye IT-systemer / IT-funksjoner, bør 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 juridisk og informasjonssikkerhet i organisasjonene dine, og følg instruksjonene de gir.....

Erfaringer fra Sverige etter 25/5

- 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
- 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, noen spørsmål?

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