Granskning av Sektor Välfärds dataskyddsarbete 2021

Adrian Vinsa

Dataskyddsombud

Agenda

- Uppföljning av registerförteckning, 2019
- Uppföljning av personuppgiftsansvarigs systematiska arbete med personuppgiftsincidenter, 2020
- Granskning av personuppgiftsansvarigs information om personuppgiftshandlingar till anställda
- Granskning av konsekvensbedömningar avseende dataskydd
- Ambitionsnivå

Uppföljning av registerförteckning, 2019

Personuppgiftsansvarig ska föra ett register över sina personuppgiftsbehandlingar som utförts under dess ansvar.

- Vissa krav: Ändamål, kategorier av registrerade, kategorier av personuppgifter, lagringstid, tredjelandsöverföring, kategorier av mottagare, säkerhetsåtgärder
- Ansvarsprincipen
- Koppling till övrigt dataskyddsarbete, informationskrav, registerutdrag
- Transparant, flexibel och förvaltningsbar

Uppföljning av registerförteckning, 2019

Bedömning:

Alla tre nämnder har idag en registerförteckning tillskillnad från tidigare år.

Frångått dokumentering av system och lagringsytor till verksamhetsprocesser.

Frångått dokumentering i Excel till DraftIT Records.

Inaktuell information om ansvarig för behandlingen.

Saknar rutin för kontinuerlig uppdatering av registerförteckning.

Rekommendation:

Inför rutin för kontinuerlig översyn av registerförteckningen.

Uppföljning av personuppgiftsansvarigs systematiska arbete med personuppgiftsincidenter, 2020

Personuppgiftsansvarig ska **dokumentera**, anmäla till tillsynsmyndighet inom 72 timmar, informera registrerade och **vidta åtgärder** för att minimera risker.

- En personuppgiftsincident kan vara alltifrån en hackerattack där stora mängder personuppgifter blivit stulna till något så enkelt som att någon tappar bort en mobiltelefon eller skickar e-post till fel mottagare.
- Under pandemin har antalet anmälningar till IMY i Sverige sjunkit.
- En metod för att förhindra framtida personuppgiftsincidenter.

Uppföljning av personuppgiftsansvarigs systematiska arbete med personuppgiftsincidenter, 2020

Bedömning:

Flertalet incidenter hanteras inom tidsramen om 72 timmar tillskillnad från tidigare år.

Kunskapshöjande insatser fortfarande nödvändigt för att öka möjligheterna att identifiera incidenter.

Möjlighet att se över sättet man anmäler incidenter.

Rekommendation:

- Genomför kunskapshöjande insatser för anställda med målet att öka kännedom om dataskydd bland anställda.

Granskning av personuppgiftsansvarigs information om personuppgiftsbehandlingar till anställda

Personuppgiftsansvarig ska informera registrerade om vilka personuppgifter organisationen behandlar om dem.

- Arbetsgivare behandlar anställdas personuppgifter för att fullfölja åtaganden utifrån arbetsrätten samt andra lagar och regler som styr verksamheten.
- Inte alltid enkelt att avgöra i vilken utsträckning anställda är medvetna om personuppgiftsbehandlingar. Första steg är framtagande av rutiner och information.
- Uppfylla principen om korrekthet, öppenhet och laglighet.

Granskning av personuppgiftsansvarigs information om personuppgiftshandlingar till anställda

Bedömning: Personaladministration

Information i samband med anställningsavtal

2-lager information men hänvisning till olika källor

Överväg hur anställda tillgodogör sig information om verksamheten och anpassa information om personuppgiftsbehandling därefter.

Svårt att informera om i samband med signering av anställningsavtal.

Rekommendation:

Komplettera information om personuppgiftsbehandling vid personaladministration till anställda.

Granskning av personuppgiftsansvarigs information om personuppgiftshandlingar till anställda

Bedömning: Passagesystem

Information i samband med uthämtning av tagg på kvitto

Generella regler istället för information utifrån ett dataskyddsperspektiv.

Ändamål med behandling är att hindra obehöriga tillträde till lokalen.

Rekommendation:

Genomför översyn över hur anställda informeras om personuppgiftsbehandlingen i passagesystem.

Granskning av personuppgiftsansvarigs information om personuppgiftshandlingar till anställda

Bedömning: Övervakning av anställdas datorer

Rätt till skydd för sin kommunikation och privatliv gäller även vid arbetsplatsen.

Rätt vid stark misstanke om brott.

Krav på information att det kan ske.

Kan implementeras tillsammans med en rutin om hur arbetstagare ska använda e-post, lagringsmiljöer, övriga IT-verktyg.

Rekommendation:

Fastställ rutin över hur anställda får använda sig av arbetsgivarens datorer och e-post samt informera anställda om rutin.

Granskning av personuppgiftsansvarigs information om personuppgiftshandlingar till anställda

Bedömning: Övervakning av IT-system

Nödvändigt utifrån ett informationssäkerhetsperspektiv och dataskyddsperspektiv.

Framgår i *Rutin för loggkontroll* för systemen Treserva och NPÖ att det är en förebyggande åtgärd om användare har kunskap om loggkontroller.

Framgår inte hur det information faktiskt sker.

Anställda kan förväntas i viss utsträckning genom sin profession ha kunskap om detta eller att chefer informerar.

Rekommendation:

Komplettera rutin för loggkontroll med att klargöra hur information lämnas till användare.

Granskning av konsekvensbedömning avseende dataskydd

Personuppgiftsansvarig ska genomföra en konsekvensbedömning när en behandling sannolikt leder till hög risk för de registrerade. Bedömning av sannolikhet görs genom att granska behandlingen utifrån IMY:s förteckning när konsekvensbedömning ska genomföras och 9 kriterier.

- Bedömning görs av ansvarig för informationen/systemet, verksamhetssakunniga, jurister, systemförvaltare, dataskyddssamordnare och dataskyddsombud.
- Kan leda till högra säkerhetskrav, minimering av information som behandlas eller förändring av ändamål m.m.
- IMY är ofta inte tillfredsställd med genomförd bedömning vid förhandssamråd.
- DSO har mall och metod för konsekvensbedömning om inte PUA utvecklat egen.
- Uppfylla ansvarsprincipen

Granskning av konsekvensbedömning avseende dataskydd

Bedömning:

Flertalet konsekvensbedömningar genomförda och pågående.

System med behandlingar som kräver konsekvensbedömning är Tieto och Treserva som alla nämnder använder. Utöver innehåller Canvas behandlingar som kräver konsekvensbedömningar.

Uppfyller kriterierna: Omfattande i relation till verksamheten, känsliga personuppgifter, behandlar information om människor i beroendeställning eller utsatt position, samt använder ny teknik eller nya organisatoriska lösningar.

Alla personuppgiftsbehandlingar kräver en tröskelanalys.

Rekommendation:

Komplettera registerförteckning över personuppgiftsbehandlingar utifrån om de uppfyller kriterierna eller inte för när en konsekvensbedömning ska genomföras.

Genomför konsekvensbedömning över identifierade personuppgiftsbehandlingar som uppfyller kraven för när konsekvensbedömning ska genomföras.

Ambitionsnivå

Mognadsgrad	Beskrivning
Initial	Åtgärder vidtas huvudsakligen händelsestyrt. Mycket arbete med att släcka bränder.
Repeterbar	Grundelement och grundläggande processer finns på plats, liksom de mest väsentliga styrdokumenten, t.ex. intern integritetspolicy.
Definierad	Organisationen använder bästa praxis, standarder och har genomför kontroller om organisationen följer riktlinjer etc.
Strukturerad (kontrollerad)	Mätetal används för att förbättra organisationen över tid. Rapportering sker på ett strukturerat och väldefinierat sätt. Besluten utförs enligt definierade processer.
Optimerad	Organisationen är ett självspelande piano.

Ambitionsnivå

- Fastställ ambitionsnivå.
- Fastställ åtgärdsplan med vilka rekommendation PUA ämnar följa och när de kommer åtgärdas.
- Återkoppling till DSO.