sydnärkes utbildningsförbund

Tjänsteskrivelse

2018-05-17

Riktlinjer för Dataskydd vid hantering av personuppgifter

Bakgrund

Från och med den 25 maj 2018 gäller EUs dataskyddsförordning (2016/679) för hantering av personuppgifter. Förordningen ersätter personuppgiftslagen, PuL (1998:204).
Förordningen är direkt tillämplig, vilket innebär att den inte behöver implementeras i svensk rätt, med svensk lag.

Syfte

Riktlinjen har som syfte att göra policyn konkret – den ger vägledning i hur hantering av personuppgifter skall ske inom Sydnärkes Utbildningsförbund. Riktlinjen är antagen av förbundsdirektionen och gäller från och med 2018-05-25. Riktlinjen följer gällande lagstiftning och kan komma att justeras vid förändringar av gällande rätt.

Omfattning

Riktlinjen gäller för Sydnärkes Utbildningsförbund.
Riktlinjen avser hantering av personuppgifter som helt eller delvis företas på automatisk väg samt på annan än automatisk behandling av personuppgifter som ingår eller kommer att ingå i ett register.
Register definieras här som en strukturerad samling uppgifter som är tillgängliga för sökning eller sammanställda enligt särskilda kriterier.

Tillämpningsområde

Förordningen ska tillämpas på all hantering av personuppgifter som helt eller delvis företas på automatisk väg samt på annan än automatisk behandling av personuppgifter som ingår eller kommer att ingå i ett register.
Register definieras här som en strukturerad samling uppgifter som är tillgängliga för sökning eller sammanställda enligt särskilda kriterier.

Personuppgiftsansvar

Sydnärkes Utbildningsförbund är personuppgiftsansvariga.
Ansvaret innebär en yttersta skyldighet att se till att gällande lagstiftning följs genom att bl.a:

- Fastställa ändamål och syfte med behandling av personuppgifter, innan behandling påbörjas
- Utse Dataskyddsombud med rätt förutsättningar att kunna genomföra sitt uppdrag
- Säkerställa att det finns tekniska och organisatoriska förutsättningar att behandla personuppgifter med nödvändig säkerhet
- Kunna visa att kraven i lagstiftningen är uppfyllda genom noggrann dokumentation och verifierande tester
- Föra register över behandlingar av personuppgifter

Laglig behandling av personuppgifter

Dataskyddsförordningen säger att personuppgifter endast får behandlas om det finns laglig grund för behandlingen. Den lagliga grunden skall alltid fastställas innan behandling påbörjas. Fastställ laglig grund för behandling utifrån något av följande:

- Samtycke – skall vara informerat, frivilligt och specifikt samt kunna visas
- Behandlingen är nödvändig för att fullgöra ett avtal
- Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som den personuppgiftsansvarige har
- Behandlingen är nödvändig för att skydda ett grundläggande intresse för den registrerade eller annan fysisk person
- Behandlingen är nödvändig för att utföra uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning

Sydnärkes Utbildningsförbund har därför etablerat arbetsrutin för behandling av personuppgifter:

Innan behandling av personuppgifter inom Sydnärkes Utbildningsförbund påbörjas krävs följande*:*

1. Identifiera ändamål och syfte med behandlingen – varför skall personuppgifterna behandlas.
2. Undersök syfte med behandlingen i förhållande till redan befintliga register – det skall ej finnas flera olika register som behandlar personuppgifter i samma syfte.
3. Dokumentera ändamål och syfte samt under hur lång tid behandlingen beräknas pågå, det vill säga hur lång tidsfristen är till radering av personuppgifterna som skall behandlas.
4. Fastställ rättslig grund.
5. Inhämta samtycke vid behov.
6. Säkerställ att behandlingen sker i enlighet med de grundläggande principerna i GDPR-lagstiftningen och i enlighet med denna policy och riktlinje.
7. Vid behov, rådgör med Dataskyddsombudet.
8. Klassificera personuppgifterna utifrån informationssäkerhetsnivå och genomför riskanalys av den planerade behandlingen. Dataskyddsombudet ska involveras i riskanalysen.
9. Samråd med tillsynsmyndighet avseende fall där hög risk föreligger och som inte kan åtgärdas inför behandling av personuppgifter.
10. Säkerställ att det finns implementerat tillräckliga tekniska och organisatoriska säkerhetsåtgärder baserat på genomförd informationssäkerhetsklassning och resultat från riskanalys. Med tillräckliga organisatoriska säkerhetsåtgärder avses här också att bemanna samtliga roller i organisationen som bidrar till en säker hantering av personuppgifter, t.ex. systemägare, informationsägare, systemförvaltare, tillse att de individer som bemannar respektive roll har tillräckliga förutsättningar och kompetens för att utföra sina uppdrag samt förankra med varje individ att de tar ägarskap för rollen.
11. Klargör om, och i så fall vilken, kommunikation med den registrerade som är nödvändig.
12. Upprätta personuppgiftsbiträdesavtal vid behov.
13. Verifiera att Dataskyddsombudet godkänner behandlingen.
14. Anteckna ny behandling av personuppgifter i registerförteckningen.

Säkerhet

Behandling av personuppgifter får ske om lämplig teknisk och organisatorisk säkerhet vidtagits för behandlingen. Säkerheten ska baseras på genomförda informationssäkerhetsklassningar och riskanalyser.

Säkerhet grundläggs av:

- att säkerställandet av personuppgiftshanteringen ska finnas med redan från den initiala

planeringen för systeminförande och systemförvaltning samt övrig planering av behandling av personuppgifter och då täcka såväl tekniska som organisatoriska åtgärder.
• använda åtgärder som uppgiftsminimering, lagringsminimering, fritextfältsminimering och åtkomstbegränsning.
• säkerställa att Sydnärkes Utbildningsförbund har en grundsäkerhetsnivå för informationssäkerhet samt där så är möjligt använda åtgärder som pseudonymisering, anonymisering eller kryptering.
• säkerställa att Sydnärkes Utbildningsförbund vidmakthåller en säkerhetsnivå för informationssäkerhet avseende särskilda personuppgifters konfidentialitet och riktighet vilket för elektronisk hantering bl.a. innebär att använda kryptering samt stark autentisering.

Införande och tillämpning av rutiner för att:

• Kontinuerligt testa, undersöka och visa på effektiviteten av införda säkerhetsåtgärder.
• Anmäla en personuppgiftsincident till tillsynsmyndighet.
• Om behov uppstår kunna informera berörda registrerade om incidenter.
• Om behov uppstår kunna involvera och rådgöra med Dataskyddsombudet.

Personuppgiftsbiträde

Den som behandlar personuppgifter på uppdrag av annan personuppgiftsansvarig blir personuppgiftsbiträde i förhållande till den personuppgiftsansvarige. Vid anlitandet av ett personuppgiftsbiträde ska Sydnärkes Utbildningsförbund säkerställa att personuppgiftsbiträdet kan ge tillräckliga garantier om att upprätthålla lämplig teknisk och organisatorisk säkerhet i enlighet med gällande rätt.

Samtliga val att anlita personuppgiftsbiträden och vilka personuppgiftsbiträden som anlitas för verksamhet inom Sydnärkes Utbildningsförbund skall ske efter noggrant arbete enligt förbundets processer för förstudie av systeminförande och systemförvaltning. Detta säkerställer att förbundsledningen som har personuppgiftsansvaret vid var tid har kontroll på organisationens behandling av personuppgifter.

Personuppgiftsbiträdesavtal

Personuppgiftsbiträdets behandling av personuppgifter ska regleras av personuppgiftsbiträdesavtal mellan biträdet och Sydnärkes Utbildningsförbund i förbundets roll som Personuppgiftsansvarig.

I avtalet ska anges:
• Vem som är personuppgiftsansvarig respektive personuppgiftsbiträde
• Vad behandlingen avser, dess varaktighet, art, ändamål, typ av personuppgifter samt kategori av registrerade
• Den personuppgiftsansvariges skyldigheter och rättigheter
• Att biträdet endast får behandla personuppgifter i enlighet med den ansvariges instruktion
• Att biträdet iakttar nödvändig konfidentialitet och tystnadsplikt
• Att biträdet vidtar alla lämpliga tekniska och organisatoriska åtgärder för att säkerställa adekvat skydd för personuppgifterna samt att detta kan visas genom att ge personuppgiftsansvarige tillgång till vederbörlig information
• Att biträdet ska bistå den ansvarige i att uppfylla sina förpliktelser enligt förordningen
• Att biträdet inte får anlita underleverantör för behandling av den ansvariges personuppgifter utan den ansvariges skriftliga medgivande till detta. Om biträdet anlitar underleverantör ska personuppgiftsbiträdesavtal upprättas även mellan dessa parter

• Reglering om inom vilken tid radering eller överflyttning av personuppgifter sker vid avtals upphörande.
• Reglering om servicenivåer och tidsfrist för systemstöd och felavhjälpning.
• Att biträdet inte får lämna ut personuppgifter på annan myndighets begäran utan att informera personuppgiftsansvarige.

Register över behandling

Sydnärkes Utbildningsförbund skall i sin roll som Personuppgiftsansvarig föra ett register över behandling av personuppgifter som utförs under dess ansvar.

Registret ska minst innehålla:

• Namn och kontaktuppgifter till den Personuppgiftsansvarige samt Dataskyddsombudet
• Ändamålet med behandlingen
• Laglig grund
• Kategori av registrerade, personuppgifter samt behandlingar
• Mottagare av personuppgifter, i förekommande fall
• Eventuell överföring till tredje land med tillhörande säkerhetsåtgärder
• Tidsfrist för radering
• Beskrivning av tekniska och organisatoriska säkerhetsåtgärder för behandlingen
• Systemägare
• Systemförvaltare