Riktlinjer för personuppgiftsbehandling

Dnr 58-2020

Jämtlands
Gymnasieförbund

Dnr 58-2020

Fastställd i direktionen 2020-05-25 § 18

1 Inledning

Enligt Dataskyddsförordningens artikel 5.2 om ansvarsskyldighet ska den personuppgiftsansvarige kunna visa att principerna för behandling av personuppgifter efterlevs. Datainspektionen rekommenderar att det ska finnas interna riktlinjer för arbetet med dataskydd.

Följande riktlinjer beskriver hur förbundet arbetar för att säkerställa de registrerades rättigheter. Jämtlands Gymnasieförbund behandlar en stor mängd personuppgifter i många olika syften i det dagliga arbetet med elever och personal och i kontakter med externa företag och myndigheter. Utgångspunkten är att det ska vara "lätt att göra rätt". Riktlinjerna ska tillsammans med Dokumenthanteringsplan och Arkivreglemente säkerställa en rättssäker myndighetsutövning med avseende på systematik, organisation, kunskap och teknik.

2 Begrepp

Begreppsanvändningen i dessa riktlinjer utgår från Dataskyddsförordningen. Ett enhetligt språk underlättar kommunikationen och är grundläggande för en rättssäker myndighetsutövning. Centrala begrepp presenteras i tabell 1.

Tabell 1

Personuppgift	Varje upplysning om en identifierbar nu levande fysisk person. Även bilder och ljudinspelningar.
Behandling	Åtgärd som innebär att personuppgifter behandlas, till exempel registrering och lagring.
Personuppgiftsansvarig	Den person eller organisation som bestämmer ändamålen och medlen för behandlingen.
Personuppgiftsbiträde	Den som behandlar personuppgifter för den personuppgiftsansvariges räkning.
Dataskyddsombud	Person utsedd av den personuppgiftsansvarige att ha en rådgivande och övervakande funktion i dataskyddsarbetet.
Grundläggande dataskyddsprinciper	Grundläggande principer som ska gälla när personuppgifter behandlas.
Rättslig grund	Villkor som ska uppfyllas för att behandling av personuppgifter ska vara laglig.
Särskilda kategorier av personuppgifter	Personuppgifter som är känsliga och som bara får behandlas under vissa förutsättningar.
Särskilt skyddsvärda personuppgifter	Personuppgifter som inte är känsliga men som ska behandlas med restriktivitet.

3 Åtgärder för att skydda personuppgifter

I det följande beskrivs på vilket sätt Jämtlands Gymnasieförbund arbetar för att skydda personuppgifter och för att följa Dataskyddsförordningens krav i övrigt med avseende på organisation, teknik och systematik.

3.1 Organisation

Alla som på olika sätt hanterar personuppgifter inom ramen för sin tjänsteutövning ska på ett enkelt sätt ska kunna få information om hur en arbetsuppgift ska utföras så att de registrerades rättigheter tillvaratas. Anställda som ofta hanterar personuppgifter ska ha relevanta kunskaper om dataskydd och vara väl förtrogna med de rutiner som finns i förbundet med avseende på personuppgiftshantering.

Personuppgiftsansvarig för Jämtlands Gymnasieförbund är direktionen. Förbundet har även ett antal personuppgiftsbiträden i form av systemägare och systemleverantörer samt företag och organisationer som hanterar personuppgifter för förbundets räkning. Särskilda personuppgiftsbiträdesavtal ska finnas som reglerar hur personuppgifterna får behandlas.

Förbundet kan i vissa fall använda läromedel som kräver att elever och lärare registrerar personuppgifter hos externa systemleverantörer med eget personuppgiftsansvar. Användaren lämnar då ett personligt samtycke till behandlingen i samband med registreringen. Jämtlands gymnasieförbund har i dessa fall inget ansvar för behandlingen av personuppgifter och kan heller inte kontrollera eller följa upp om leverantören följer dataskyddsprinciperna i GDPR. Innan läromedel används, som kräver registrering hos extern leverantör med eget personuppgiftsansvar, ska en riskanalys göras för att säkerställa så långt det är möjligt att personuppgifterna skyddas med adekvata skyddsåtgärder. Riskanalysen ska göras på samma sätt som när förbundet har eget personuppgiftsansvar. Endast sådana system får användas, där leverantören kan visa att personuppgifterna skyddas och att de i övrigt följer bestämmelserna i GDPR. Läs mer om riskanalys i avsnitt 3.8.

Förbundet hanterar personuppgifter framför allt utifrån den rättsliga grunden allmänt intresse. Det är den rättsliga grund som är vanligast förekommande på skolans område. Behandling sker även med andra rättsliga grunder såsom samtycke, avtal och rättslig förpliktelse. Känsliga personuppgifter behandlas bland annat i elevhälsoverksamheten, viss personaladministration och i arbetet med att utreda diskriminering och kränkande behandling. Personnummer ska exponeras så lite som möjligt och användas endast för behandlingar som ställer krav på säker identifiering.

3.2 Registerförteckning

Dataskyddsförordningen anger att den personuppgiftsansvarige ska föra ett register över behandling som utförs under dess ansvar. Jämtlands Gymnasieförbund har upprättat ett register i digital form i ett särskilt registerverktyg som tillhandahålls av Draftit AB. I registret finns en detaljerad beskrivning av alla behandlingar av personuppgifter som görs i förbundet. En översikt över de personuppgiftsbehandlingar som är registrerade finns på förbundets intranät.

3.3 Rutiner

I registerförteckningen framgår vilka register (system) som används för olika typer av personuppgiftsbehandling samt om det förekommer någon hantering i ostrukturerat material såsom e-post, blanketter och textfiler. Rutinbeskrivningar för personuppgiftsbehandling görs tillgängliga på förbundets intranät. På intranätet finns även en förteckning över vilka blanketter som används för personuppgiftsbehandling.

3.4 Kompetens och utbildning

Anställda som hanterar personuppgifter inom ramen för sin tjänsteutövning ska känna till innehållet i riktlinjerna för personuppgiftsbehandling. De ska även ha en inblick i Dataskyddsförordningen och en grundläggande förståelse för intentionerna i denna. Vid varje läsårsstart görs en inventering av vilka utbildningsinsatser som behövs för att säkerställa de registrerades rättigheter. Utifrån de behov som identifieras planeras lämpliga utbildningsinsatser. Det kan handla om interna fortbildningar med utgångspunkt i förbundets egna rutiner för dataskyddsarbetet eller externa kurser för att öka kunskapen inom ett specifikt område.

3.5 Information till registrerade

Dataskyddsförordningen anger att den personuppgiftsansvarige ska informera de registrerade om att deras personuppgifter behandlas. I informationsskyldigheten ingår en rad uppgifter, bland annat ändamålet och den rättsliga grunden för behandlingen samt kontaktuppgifter till dataskyddsombudet.

Jämtlands Gymnasieförbund har sammanställt ett informationsmaterial som beskriver hur förbundet arbetar med personuppgiftsbehandling. Informationen utgår från Dataskyddsförordningens artikel 13–20 om information och tillgång till personuppgifter. Informationen är publicerad på förbundets webbplats. På blanketter och formulär som används för att behandla personuppgifter hänvisas till denna informationstext liksom i all utgående e-post som lämnas förbundets e-postserver. Informationen är också tillgänglig via länkar från Dexter och via intranätet. Nya elever ska vid varje läsårsstart
informeras om förbundets arbete med dataskydd.

3.6 Registerutdrag

Enligt Dataskyddsförordningens artikel 15 har den registrerade rätt att få tillgång till de personuppgifter som behandlas av den personuppgiftsansvarige. Ett registerutdrag kan begäras ut från förbundskansliet. Information om hur den registrerade ska gå till väga för att begära registerutdrag finns på förbundets webbplats.

3.7 Incidentrapportering

En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av personuppgifter. Det kan även handla om obehörig åtkomst till personuppgifter genom intrång eller obehörigt röjande. Personuppgifts-incidenter ska anmälas till Datainspektionen inom 72 timmar. Rutiner för incident-rapportering finns på förbundets intranät.

3.8 Teknik

Jämtlands Gymnasieförbund behandlar personuppgifter i många olika digitala system, bland annat för administration, kommunikation och i undervisningen. Personuppgifter som behandlas med hjälp av digital teknik ska ha en lämplig säkerhetsnivå med avseende på risker med behandlingen, vilken typ av uppgifter som behandlas, tillgängliga tekniska lösningar och kostnader. Vid införandet av nya IT-system ska en riskanalys alltid genomföras. Om riskanalysen visar att en personuppgiftsbehandling innebär hög risk för de registrerade ska en konsekvensbedömning göras enligt Dataskyddsförordningens artikel 35. Konsekvensbedömningen ska ligga till grund för beslut om skyddsåtgärder för att säkerställa att personuppgifter skyddas från att förstöras eller ändras eller att obehöriga kommer åt uppgifterna. Skyddsåtgärderna dokumenteras i registerförteckningen. Register som tillåter personuppgiftsbehandling i fritext ska särskilt uppmärksammas. Riktlinjer för hur fritext får utformas finns på intranätet.

Även personuppgiftsbehandling i ostrukturerad form, till exempel i textfiler som lagras digitalt eller i e-postmeddelanden ställer höga krav på säkerhet. Känsliga personuppgifter ska inte behandlas i e-post eller i de molntjänster som används i förbundet.

3.9 Systematiskt kvalitetsarbete

Kvalitetsarbetet med avseende på dataskydd sker på övergripande förbundsnivå. För att säkerställa en hög skyddsnivå för de registrerade görs varje år i samband med läsårsstart en översyn för att säkerställa att rutiner och ansvarsområden är aktuella och uppdaterade. Arbetet följer en särskild checklista. Det är förbundssekreteraren som ansvarar för att översynen genomförs. Checklistan finns på intranätet.