Utbildningsförvaltningens rutin för hantering av personuppgiftsincidenter

Dokumentnamn: Utbildningsförvaltningens rutin för hantering av personuppgiftsincidenter			
Beslutad av: Avdelningschef administration och ekonomi	Gäller för: Utbildningsförvaltningen	Diarienummer: 0206/21	Datum och paragraf för beslutet: 2023-03-15
Dokumentsort: Rutin	Giltighetstid: Tillsvidare	Senast reviderad: 2026-03-20 (korr)	Dokumentansvarig: Informationssäkerhetssamordnare
Bilagor: [Bilagor]			

Innehåll

Definitioner

Nedan är en lista över några av de definitioner som används i detta dokument:

Integritetsskyddsmyndigheten (IMY):	Integritetsskyddsmyndigheten, tidigare Datainspektionen är en svensk statlig förvaltningsmyndighet (tillsynsmyndighet) som har till uppgift att verka för att människor skyddas mot att deras personliga integritet kränks genom behandling av personuppgifter.
Dataskyddsförordningen	Dataskyddsförordningen, General Data Protection Regulation, GDPR, är en europeisk förordning med syftet att stärka och harmonisera skyddet för levande, fysiska personer inom Europeiska unionen vid hantering av personuppgifter.
Personuppgift	Varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.
Personuppgiftsansvarig	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamål och medlen för behandlingen av personuppgifter.
Personuppgiftsbiträde	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.
Personuppgiftsincident	En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats
Registrerad	Fysisk person vars personuppgifter behandlas.

Inledning

Syftet med denna rutin

Syftet med denna rutin är att skapa ett systematiskt och strukturerat sätt att hantera och rapportera personuppgiftsincidenter enligt kraven i dataskyddsförordningen (GDPR).

Vem omfattas av rutinen

Denna rutin gäller tills vidare för samtliga anställda på utbildningsförvaltningen.

Bakgrund

Den 25 maj 2018 trädde dataskyddsförordningen (GDPR) i kraft och ersatte därmed personuppgiftslagen (PUL). Dataskyddsförordningen gäller för alla länder i EU.

Med införandet av dataskyddsförordningen är myndigheter, organisationer och företag skyldiga att rapportera och anmäla personuppgiftsincidenter till tillsynsmyndigheten Integritetsskyddsmyndigheten.

För att utbildningsförvaltningen ska kunna leva upp till kraven i gällande dataskyddslagstiftning samt för att skydda de registrerades rättigheter och minska incidentens påverkan är det viktigt att det finns utarbetade och strukturerade arbetssätt och rutiner för hur en sådan incident ska hanteras. Detta för att möjliggöra en snabb och korrekt hantering av personuppgiftsincidenter.

Koppling till andra styrande dokument

Denna rutin är framarbetad med utgångspunkt från följande överordnade styrande dokument:

- Göteborgs Stads Riktlinje för Informationssäkerhet.

Personuppgiftsincident

En personuppgiftsincident är en säkerhetsincident som innefattar oavsiktlig eller avsiktlig förstöring, förlust, ändring eller spridning av personuppgifter som kan innebära risker för de registrerades rättigheter och friheter. Exempel på personuppgiftsincidenter kan vara följande:

a) En obehörig person får tillgång till personuppgifter, till exempel genom att personuppgifter skickas till fel mottagare via e-post
b) En obehörig person får tillgång till personuppgifter genom att komma över ett lösenord och sedan logga in i ett system där personuppgifter hanteras t.ex Personec, PMO eller IST
c) Datorer som innehåller personuppgifter förloras eller blir stulna
d) En dator blir infekterad med skadlig kod och det medför att en obehörig person kan komma åt personuppgifter
e) Personuppgifter blir ändrade av någon som inte har tillstånd till det

f) Personuppgifter är inte tillgängliga för den som behöver dem, vilket leder till negativa effekter för den registrerade

Rapportering av svagheter gällande personuppgiftsskydd

Alla anställda, leverantörer och inhyrd personal som har tillgång till de personuppgifter som utbildningsförvaltningen förfogar över är skyldiga att notera och rapportera alla misstänkta organisatoriska svagheter (t.ex. bristfälliga rutiner) eller tekniska svagheter (t.ex. skadlig kod i datorn) som berör personuppgiftsskydd. På detta sätt kan eventuella brister och svagheter förutses och förebyggas innan de orsakar problem.

Intern rapportering av personuppgiftsincidenter

Personuppgiftsincidenter ska rapporteras så snabbt som möjligt till närmaste chef eller dataskyddskontakterna på utbildningsförvaltningen. Om dataskyddskontakterna ska rapportera incidenten vidare till Integritetsskyddsmyndigheten måste detta göras inom 72 timmar från att den upptäcktes och det är därför viktigt att de informeras i tid.

Alla anställda, leverantörer och inhyrd personal ska få information om sitt ansvar att rapportera personuppgiftsincidenter så snabbt som möjligt.

En incidentrapport ska innehålla följande information och när dataskyddskontakten informeras om incidenten bör så mycket av detta som möjligt finnas med i informationen som lämnas. Om allt inte är känt bör dataskyddskontakten informeras om det man vet och sedan uppdateras löpande medan incidenten utreds vidare.

a) Vilken typ av incident som inträffat,
b) När den inträffat och när den upptäcktes (datum och klockslag),
c) Vilka kategorier av registrerade som kan komma att påverkas,
d) Hur många registrerade som berörs,
e) Vilka konsekvenser incidenten kan få,
f) Vilka åtgärder som vidtagits för att motverka eventuella negativa konsekvenser och när dessa genomförts (datum och klockslag).

Kontaktuppgifter till utbildningsförvaltningens dataskyddskontakt:

E-post dataskydd@educ.goteborg.se

Personuppgiftsincidenter hos personuppgiftsbiträden

Om det inträffar en personuppgiftsincident där ett personuppgiftsbiträde bär ansvaret ska incidenten utredas av biträdet och ett underlag ska lämnas till utbildningsförvaltningen. Detta regleras i de personuppgiftsbiträdesavtal som upprättas med förvaltningens biträden.

För att göra det möjligt för personuppgiftsbiträden att informera utbildningsförvaltningen om personuppgiftsincidenter ska alla personuppgiftsbiträden få information om vilka som är dataskyddskontakter på utbildningsförvaltningen samt få kontaktuppgifter till dessa.

Utredning och hantering av personuppgiftsincidenter

Personuppgiftsincidenter ska hanteras av dataskyddskontakterna på utbildningsförvaltningen.

Inkomna anmälningar om incidenter ska utredas och en bedömning ska göras om huruvida det inträffade är att betrakta som en personuppgiftsincident.

Vid bedömning av personuppgiftsincident för utbildningsförvaltningen som personuppgiftsansvarig gäller följande:

a) Bedömning ska ske kring allvarlighetsgrad av konsekvenserna och sannolikheten av att detta inträffar och enskilda personer drabbas.
b) Bedömning av om anmälan till Integritetsskyddsmyndigheten behöver genomföras ska ske.
c) Bedömning av om information om de registrerade behöver informeras om incidenten.

Resultaten av utredningar och beslut ska dokumenteras och sparas.

Rapportering av personuppgiftsincidenter till Integritetsskyddsmyndigheten

En personuppgiftsincident ska anmälas till Integritetsskyddsmyndigheten inom 72 timmar om det är troligt att incidenten medför en risk för de registrerade. Anmälan ska ske inom denna tidsram även om alla detaljer inte är utredda ännu.

En anmälan av personuppgiftsincident till Integritetsskyddsmyndigheten ska som minst innefatta följande:

g) Vilken typ av incident som inträffat,
h) Vilka kategorier av registrerade som kan komma att beröras,
i) Hur många registrerade som berörs,
j) Vilka konsekvenser incidenten kan få,
k) Vilka åtgärder man vidtagit för att motverka eventuella negativa konsekvenser.

Anmälan av personuppgiftsincidenter till Integritetsskyddsmyndigheten ska utföras av dataskyddskontakter på beslut av avdelningschef. Dataskyddsombudet ska informeras om alla incidenter som anmäls till Integritetsskyddsmyndigheten.

För anmälan ska e-tjänst som finns på Integritetsskyddsmyndighetens hemsida användas: www.imy.se

Alla personuppgiftsincidenter, inklusive tillhörande dokumentation ska diarieföras.

Information till de registrerade

Information ska delges de registrerade om bedömning gjorts att personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter, särskilt om det finns ett behov av att mildra en omedelbar risk för skador.

Den information som delges ska som minst innefatta följande:

a) Klar och tydlig beskrivning av orsaken bakom personuppgiftsincidenten.
b) Namn och kontaktuppgifter till dataskyddsombudet och dataskyddskontakter, eller till annan kontakt som kan svara på frågor.
c) Beskrivning av de sannolika konsekvenserna av personuppgiftsincidenten.
d) Beskrivning av vad utbildningsförvaltningen har gjort, eller kommer göra, för att hantera personuppgiftsincidenten.
e) I förkommande fall: Beskrivning av vad utbildningsförvaltningen har gjort för att mildra eventuella negativa effekter.

Den registrerade kan kontaktas om ovan information via mail, telefonsamtal eller vanligt brev och det är dataskyddskontakten som ansvarar för att den registrerade kontaktas. Den information som delges den registrerade ska alltid diarieföras. Om information lämnas via telefon, ska en tjänsteanteckning skrivas.

All information som har gått ut, t.ex. via e-post, vanligt brev eller telefonsamtal i form av tjänsteanteckningar ska diarieföras.

Att lära av personuppgiftsincidenter

Information och kunskaper baserade på analyser av hanterade personuppgiftsincidenter ska användas för att minimera sannolikheten eller påverkan av framtida incidenter.

Den information som erhålls från utvärderingen av personuppgiftsincidenter ska användas för att identifiera återkommande incidenter eller incidenter med stor påverkan.