Göteborgs Stad

Grundskoleförvaltningens rutin för hantering av personuppgiftsincidenter

Dokumentnamn: Grundskoleförvaltningens rutin för hantering av personuppgiftsincidenter			
Beslutad av: Avdelningschef, Avdelningen för styrning och ledning	Gäller för: Grundskoleförvaltningen	Diarienummer: [Nummer]	Datum och paragraf för beslutet: [Text]
Dokumentsort: Rutin	Giltighetstid: Tillsvidare	Senast reviderad: 2022-11-11	Dokumentansvarig: Informationssäkerhetssamordnare
Bilagor: [Bilagor]			

Innehåll

Inledning

Syftet med denna rutin

Syftet med denna rutin är att underlätta en effektiv och korrekt hantering av personuppgiftsincidenter enligt dataskyddsförordningens krav.

Vem omfattas av rutinen

Denna rutin gäller tillsvidare för grundskoleförvaltningens anställda.

Bakgrund

Grundskoleförvaltningens anställda har ett ansvar att notera och rapportera misstänkta organisatoriska eller tekniska svagheter som rör hanteringen av personuppgifter. På detta sätt kan problem förutses och förebyggas innan de orsakar allvarligare incidenter.

Skulle en så kallad personuppgiftsincident inträffa har grundskoleförvaltningen enligt dataskyddsförordningen (GDPR), artikel 33-34, en skyldighet att utreda denna och i förekommande fall anmäla den till Integritetsskyddsmyndigheten (IMY). Att personuppgiftsincidenter hanteras på ett korrekt sätt är viktigt. Långsam eller felaktig hantering kan påverka allmänhetens tilltro till organisationen och dessutom leda till sanktionsavgifter.

I den här rutinen kan du läsa mer om hur grundskoleförvaltningen arbetar med personuppgiftsincidenter. Information och kunskap baserad på en analys av hanterade personuppgiftsincidenter ska användas för att minimera sannolikheten för och påverkan av framtida incidenter och är på så sätt en viktig del i förvaltningens kontinuerliga informationssäkerhetsarbete.

Koppling till andra styrande dokument

Göteborgs Stads riktlinje för informationssäkerhet

Stödjande dokument

- Göteborgs Stad riktlinje för informationssäkerhet
- ISO/IEC 27001
- Ledningssystem för informationssäkerhet (LIS)
- Europaparlamentets och rådets förordning (EU) nr 2016/679

Vad är en personuppgiftsincident?

En personuppgiftsincident är en säkerhetsincident som rör hanteringen av personuppgifter. En personuppgiftsincident har inträffat om personuppgifter, oavsiktligt eller avsiktligt, har

- förstörts eller förlorats,

- ändrats eller
- kommit obehöriga till del.

Exempel på personuppgiftsincidenter kan vara

- post och e-post med personuppgifter som skickats till fel mottagare,
- stöld eller förlust av datorer som innehåller personuppgifter,
- obehörig åtkomst till personuppgifter i verksamhetssystem såsom IST, Vklass, Personec eller PMO till följd av tekniska fel, bristande rutiner eller röjda lösenord,
- skadlig kod (virus) som möjliggjort obehörig åtkomst till personuppgifter,
- personuppgifter som blir ändrade av någon som inte har tillstånd till det eller
- personuppgifter som inte är tillgängliga för den som behöver dem, vilket leder till negativa effekter för den registrerade.

Rapportering av personuppgiftsincidenter

Grundskoleförvaltningens anställda har ett ansvar att rapportera personuppgiftsincidenter så snabbt som möjligt. Personuppgiftsincidenter ska rapporteras till grundskoleförvaltningens informationssäkerhetssamordnare.

Förvaltningens informationssäkerhetssamordnare ansvarar för utredningen av incidenten och att denna dokumenteras i grundskoleförvaltningens diarium. Grundskoleförvaltningens informationssäkerhetssamordnare har att bedöma

- om den inträffade incidenten har medfört en risk för den/de registrerades fri- och rättigheter,
- om incidenten ska anmälan till Datainspektionen och
- om den/de registrerade ska informeras.

Personuppgiftsbiträdets ansvar

Grundskoleförvaltningens personuppgiftsbiträden är på samma sätt som förvaltningens anställda skyldighet att rapportera personuppgiftsincidenter. Den praktiska hanteringen ska regleras i personuppgiftsbiträdesavtalet. Personuppgiftsbiträdet ansvarar för att utreda inträffade incidenter och lämna ett underlag för bedömning till grundskoleförvaltningen i de fall personuppgiftsbiträdet bär ansvaret för en inträffad incident. Grundskoleförvaltningens informationssäkerhetssamordnare har därefter att bedöma incidenten enligt ovan.

Anmälan av personuppgiftsincidenter till Integritetsskyddsmyndigheten (IMY)

Om det är troligt att personuppgiftsincidenten har medfört eller kommer att medföra en risk för den/de registrerades fri- och rättigheter ska incidenten anmälas till IMY. Anmälan ska ske inom 72 timmar från det att incidenten kom till grundskoleförvaltningens kännedom, även om inte alla detaljer är utredda ännu. En anmälan till IMY ska

- beskriva personuppgiftsincidenten,
- förmedla kontaktuppgifter till dataskyddsombud och förvaltningens kontaktperson i ärende,
- beskriva de sannolika konsekvenserna av incidenten, och
- beskriva de åtgärder som den personuppgiftsansvarige har vidtagit.

Beslut om att anmäla en personuppgiftsincident till IMY fattas enligt grundskolenämndens delegationsordning, nummer 11.1.11, av förvaltningens informationssäkerhetssamordnare. Anmälan görs genom en digital blankett på IMYs hemsida och dokumenteras därefter i grundskoleförvaltningens diarium. Det fattade delegationsbeslutet ska även anmälas till grundskolenämnden.

Information till de registrerade

Gör förvaltningens informationssäkerhetssamordnare bedömningen att personuppgiftsincidenten sannolikt leder till en hög risk för registrerades fri- och rättigheter ska den/de som berörs av incidenten, direkt och utan onödigt dröjsmål, informeras. Informationen ska innehålla uppgifter om

- orsaken bakom personuppgiftsincidenten,
- namn och kontaktuppgifter till dataskyddsombudet och informationssäkerhetssamordnare,
- de sannolika konsekvenserna av personuppgiftsincidenten,
- vad grundskoleförvaltningen har gjort, eller kommer göra, för att hantera personuppgiftsincidenten
- och, i förekommande fall, vad grundskoleförvaltningen har gjort för att mildra negativa effekter.