Utbildningsnämnden, Stockholms stad
Utbildningsförvaltningen
Box 22049
104 22 Stockholm

Tillsyn

Datainspektionen har beslutat att granska er personuppgiftsbehandling och har inlett ett tillsynsärende. Ni behöver därför svara på våra frågor.

Varför granskar Datainspektionen er verksamhet?

Utbildningsnämnden i Stockholms stad har den 3 december 2018 och den 3 april 2019 inkommit med anmälningar om personuppgiftsincidenter till Datainspektionen (ert dnr 1.4.2- 9883/2018 respektive ert dnr 1.4.2- 2771/2019) avseende obehörig åtkomst av elevuppgifter.

Datainspektionen har beslutat att granska behörighetsstyrningen för åtkomsten till personuppgifter inom ramen för *skolpliktsbevakningen* samt *barn och elevregistret (nedan uppgiftssamlingarna)* hos utbildningsnämnden i Stockholms stad. Datainspektionen granskar även skyldigheten att informera de registrerade avseende de ovannämnda incidenterna.

Våra frågor

Datainspektionen vill att ni svarar på följande frågor:

1. Är utbildningsnämnden i Stockholms stad (ni) personuppgiftsansvarig för de personuppgiftsbehandlingar som har skett inom ramen för *de aktuella uppgiftssamlingarna* enligt de ovannämnda incidenterna? Om ni anser att ni inte är personuppgiftsansvarig, uppge vem den personuppgiftsansvarige är samt varför ni anser det?

Om ni anser att ni är personuppgiftsansvarig för personuppgiftsbehandlingar som har skett i *de aktuella uppgiftssamlingarna* vänligen svara på följande.

2 Beskriv personuppgiftsbehandlingen inom ramen för *de aktuella uppgiftssamlingarna*? Om behandlingarna sker i en del av ett system, ange namnet på systemet samt i vilken del av systemet behandlingarna sker.

3 Vilka personuppgifter behandlas inom ramen för *de aktuella uppgiftssamlingarna*? Ange även vilka kategorier av uppgifter som behandlas såsom om känsliga personuppgifter behandlas och vilka uppgifter det rör. Se definitionen av känsliga personuppgifter nedan under Övriga upplysningar.

4 Vilka grupper av registrerade finns inom ramen för *uppgiftssamlingarna*? Beskriv om det exempelvis finns barn i vilka åldrar och om det finns utsatta personer med skyddad identitet.

5 Hur många antal registrerade finns det inom ramen för *uppgiftssamlingarna*? Hur många av dessa är elever? Hur många har skyddad identitet? Hur många av dem som har skyddad identitet är barn?

6 Har ni gjort en risk- och sårbarhetsanalys gällande hanteringen av personuppgifter inom ramen för *de aktuella uppgiftssamlingarna*? Om ja, när är den genomförd och vad resulterade den i?

7 Hur sker tilldelning av behörigheter och vilka typer av behörigheter har ni inom ramen för *uppgiftssamlingarna*?

8 Vilka bedömningar ligger till grund för tilldelningen av behörigheterna?

9 Vilka faktiska åtkomstmöjligheter ger de olika tilldelade behörigheterna i *de aktuella uppgiftssamlingarna*?

10 Finns det en policy, rutiner eller instruktioner för hur behörigheterna får användas i *uppgiftssamlingarna*? Var eller hur kan den anställde ta del av dessa?

11 Dokumenterar ni vilka användare som haft elektronisk tillgång till personuppgifter genom behandlingshistorik (loggar) i *de aktuella uppgiftssamlingarna*? Beskriv hur logguppföljningen sker.

12 Genomför ni systematiska och återkommande kontroller av loggarna för att se om någon obehörig åtkomst till uppgifterna förekommit? Beskriv dessa rutiner. Finns det rutiner för åtkomstkontroll på förekommen anledning?

13 På vilket sätt säkerställer ni behörighetsstyrningen vid uppdatering och testning av de aktuella delarna av systemet?

Enligt de inkomna anmälningarna om personuppgiftsincidenter har obehörig åtkomst inträffat inom ramen för *skolpliktsbevakningen* samt i *barn och elevregistret*. Svara på följande frågor gällande de inträffade incidenterna:

14 Beskriv de inträffade incidenterna i respektive anmälan utförligt.

15 När inträffade respektive incident? Om ni inte kan uppge när förklara vad detta beror på. Beskriv även utförligt när incidenterna upptäcktes.

16 Vad har föranlett de inträffade incidenterna? Beskriv detta i detalj.

17 Är det samma eller olika orsaker som ligger till grund för incidenterna? Är det de organisatoriska eller de tekniska åtgärderna som har brustit? Beskriv på vilket sätt.

18 Hur många registrerade har påverkats av respektive incident samt på vilket sätt?

19 Har incidenterna omfattat uppgifter om personer som lever med skyddad identitet? Om ja, ange antalet registrerade som påverkats av respektive incident? Vad har respektive incident inneburit för dessa registrerade? Vad har varje incident inneburit för de övriga registrerade? Beskriv konsekvenserna av incidenterna.

20 Enligt anmälningarna har incidenterna inneburit obehörig åtkomst internt eller externt. Lämna en detaljerad redogörelse om den obehöriga åtkomsten. Hur många har *tagit del* av informationen som de saknade behörighet till? Hur många har haft *möjlighet* att ta del av uppgifter som de saknade behörighet till? Svara även på sistnämnda frågor avseende barn med skyddad identitet.

21 Har ni åtgärdat incidenterna? Beskriv i detalj på vilket sätt.

22 Har ni undanröjt eller minimerat risken för en liknande incident? Hur har ni gjort detta?

23 Har ni lämnat information till de registrerade om incidenterna? Om inte, ange i detalj orsaken till att ni inte informerat de registrerade. Ange även vilken bestämmelse i dataskyddsförordningen (GDPR)[1] ni har tillämpat.

Övriga upplysningar

Personuppgiftsansvarig är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter (artikel 4.7 i dataskyddsförordningen).

Personuppgifter är enligt artikel 4.1 i dataskyddsförordningen varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), 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 onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Behandling av särskilda kategorier av personuppgifter (känsliga personuppgifter) är enligt artikel 9.1 i dataskyddsförordningen behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Ert svar

Svara skriftligt till Datainspektionen **senast den 12 augusti 2019.**

---

[1] Europaparlamentets och rådets förordning (EU) 2016/79 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG.

Förutsatt att svaret inte innehåller några känsliga eller integritetskänsliga personuppgifter eller uppgifter som kan omfattas av sekretess, kan ni e-posta det till arendehandlaggning@datainspektionen.se och DI-2019-7024.

Om ni utöver svaren på våra frågor vill hänvisa till ytterligare information eller handlingar så ange detta och vad ni vill visa med dem men skicka inte in handlingar som går utöver det angivna syftet med tillsynen.

Måste ni svara Datainspektionen?

Ja, Datainspektionen är tillsynsmyndighet enligt dataskyddsförordningen, GDPR. Det innebär att vi får begära att ni lämnar all information som Datainspektionen behöver för att vi ska kunna fullgöra våra uppgifter som tillsynsmyndighet.[2]

Vad händer sen?

När Datainspektionen är färdig med granskningen kommer ni att få ett beslut. Där kommer ni att få besked om eventuella brister i ert dataskydd och om ni måste vidta några korrigerande åtgärder. Datainspektionen kan exempelvis påföra administrativa sanktionsavgifter enligt dataskyddförordningen.[3]

Om ni har frågor kontakta:
Salomeh Fanaei, telefon 08-657 61 45
Ranja Bunni, telefon 08-657 61 46
Alli Abdulla, telefon 08-657 61 66
Registrator, telefon 08-657 61 31

Med vänlig hälsning

Salli Fanaei, 2019-06-24 (Det här är en elektronisk signatur)

---

[2] Artikel 58.1 i dataskyddsförordningen.

[3] Artikel 58.2 och artikel 83-84 i dataskyddsförordningen.

Kopia till:

Dataskyddsombudet Johan Adolfsson,
dataskyddsombud.utbildning@stockholm.se

Information om Datainspektionens behandling av personuppgifter
https://www.datainspektionen.se/om-oss/information-om-hur-datainspektionen-behandlar-personuppgifter/