Göteborgs Stad

Genomgång årsrapport 2023

Gårdstensbostäder AB 2023-12-08

Elin Olsson & Carolin Lee, Dataskyddsenheten

Resultat fasta kontrollpunkter

Kontrollpunkt 1: Dataskyddsorganisation

- Dataskyddsombudet har inte fått några direkta indikationer som medför en annan bedömning än den som bolaget gör, men har inte heller kontrollerat dataskyddsorganisationen särskilt.

Kommentar

- DSO ej involverats i några verksamhetsspecifika frågor. Risk att DSO ej involveras i tillräcklig utsträckning.

Fråga

- Personalförändringar under 2022 – följt upp den interna dataskyddsorganisationen mot bakgrund av detta?

Rekommendationer

- Se över hur verksamheten kan involvera dataskyddsombudet mer i arbetet med dataskydd.

Kontrollpunkt 2: Personuppgiftsincidenter

- Dataskyddsombudet har under året inte involverats i någon fråga kopplad till kontrollpunkten, varför ingen särskild bedömning kan göras i frågan.

Kommentar

- Lyfte i samband med årsrapporten 2022 risker kopplade till om det fanns tillräckliga rutiner för att upptäcka personuppgiftsincidenter.

Fråga

- Antal incidenter under 2023?

Rekommendationer

- Utvärdera om rutinerna och den allmänna medvetenheten hos medarbetare ger tillräckligt goda förutsättningar för att identifiera såväl som hantera eventuella personuppgiftsincidenter.

Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

- Dataskyddsombudet har under året inte involverats i någon fråga kopplad till kontrollpunkten, varför ingen särskild bedömning kan göras i frågan.

Kommentar

- Tecknat avtal med samtliga biträden.
  - Avtal tecknat med stadens interna tjänsteleverantörer?

Rekommendationer

- Se över hantering av biträdesavtal.

Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Göteborgs Stad

- Dataskyddsombudet delar till viss del bolagets bedömning, men kan utifrån nuvarande register över behandlingar se att det inom kontrollpunkten föreligger risker som behöver åtgärdas.

Kommentar

- Bolaget anger att samtliga behandlingar finns upptagna i behandlingsregistret och all information finns med.

- Vid stickprov:
  - Angivna behandlingar i vissa fall ej att betrakta som personuppgiftsbehandling.
  - Informationen inte alltid tillräcklig utförlig för att uppfylla kraven i GDPR.

Rekommendationer

- Prioritera arbetet med behandlingsregistret. Se över hur behandlingarna är avgränsade.

- Gör en översyn av helheten. Säkerställ att samtliga registrerade behandlingar innehåller den information som ska finnas med enligt GDPR.

Kontrollpunkt 5: Övergripande styrning av dataskyddsfrågor

- Dataskyddsombudet har inte involverats i några frågor kopplat till kontrollpunkten, men har ingen anledning att göra en annan bedömning än den som verksamheten har gjort avseende risknivå. Bolaget rekommenderas därför att fortsatt arbeta för att bibehålla och utveckla de goda förutsättningar som finns inom kontrollpunkten.

Kontrollpunkt 6: Utbildning

- Dataskyddsombudet har under året inte involverats i någon fråga kopplad till kontrollpunkten, varför ingen särskild bedömning kan göras i frågan.

Kommentar

- Ej kartlagt vilken nivå av dataskyddskunskap som olika befattningars arbete kräver och planerar utbildnings- och informationsinsatser utifrån identifierade behov.
  - Skiljer sig från år 2022.

- Risker kopplat till lågt antal personuppgiftsincidenter.

Rekommendationer

- För att kunna rikta insatser och fånga upp de med störst behov är det viktigt att bolaget ser över hanteringen.

- Se över ifall den allmänna medvetenheten hos medarbetarna ger tillräckligt goda förutsättningar för att identifiera såväl som hantera eventuella personuppgiftsincidenter.

Kontrollpunkt 7: Informationsplikt

- Dataskyddsombudet delar till viss del verksamhetens bedömning, men gör till skillnad ifrån verksamheten bedömningen att det inom kontrollpunkten förekommer risker som är omfattande och kräver omgående åtgärder.

Kommentar

- Extern integritetspolicy uppfyller inte kraven på information. Rekommendationerna från årsrapport 2022 ej omhändertagna.

- Utifrån skattning:
  - Saknas rutiner för att kontinuerligt se över och uppdatera integritetsinformationen.

  - Registrerade kan inte på enkelt sätt kan nå bolagets integritetsinformation från de digitala kanaler som verksamheter använder.

Rekommendationer

- Gör en ordentlig översyn av hur informationsplikten hanteras som helhet. I detta arbete är integritetspolicyn en del.

- Säkerställ att de rekommendationer som 2022 lämnades kopplat till den specifika informationen omhändertas.

Kontrollpunkt 8: E-post och dokumenthantering

- Dataskyddsombudet har under året inte involverats i någon fråga kopplad till kontrollpunkten, men kan utifrån bolagets skattning utläsa att det inom kontrollpunkten föreligger risker.

Kommentar

- Risker kopplat till hur verksamheten informerar de registrerade direkt i samband med upprättande av kontakt om hur deras personuppgifter hanteras
- Saknas dokumenterade arbetssätt för hur personuppgifter får hanteras i e-post.

Rekommendationer

- Lägg in länk till integritetsinformation i e-postsignatur.
- Ta fram dokumenterade arbetssätt för hur personuppgifter får hanteras i e-post

Kontrollpunkt 9: Konsekvensbedömning/samråd

- Dataskyddsombudet delar inte verksamhetens bedömning, och gör till skillnad ifrån verksamheten bedömningen att det förekommer risker som är omfattande och kräver omgående åtgärder.

Kommentar

- Genomfört KB för 75 % av behandlingar som kräver det. DSO ej involverats.

Rekommendationer

- Bedöma befintliga personuppgiftsbehandlingar utifrån höga risker för att få överblick om KB krävs.
- Gör en planering för genomförandet och säkerställa att KB genomförs.
- Involvera DSO.
- Samverka med andra bolag med liknande uppdrag inom koncernen.

Kontrollpunkt 10: IT-projekt och upphandling

- Dataskyddsombudet har under året inte involverats i någon fråga kopplad till kontrollpunkten, varför ingen övergripande bedömning kan göras i frågan.

Kommentar

- Har dokumenterade arbetssätt för att involvera DSO vid uppstart av nya IT-projekt och/eller införandet av nya tjänster.
  - Risker kopplade till att DSO inte involveras.

Rekommendationer

- Säkerställ att befintliga arbetssätt följs och att dataskyddsombudet involveras i arbetet från start.

Kontrollpunkt 11: IT-system och digitala verktyg

- Dataskyddsombudet delar inte verksamhetens bedömning, och gör till skillnad ifrån verksamheten bedömningen att det förekommer risker som är omfattande och kräver omgående åtgärder.

Kommentar

- Cookie-hantering.
  - Samtycke
  - Information

- Sociala medier.

Rekommendationer

- Säkerställa att användningen är förenligt med kraven i både GDPR och LEK.

- Kartlägg och dokumentera behandlingar, utred om profilering sker, identifiera ansvarsförhållanden. Utför och dokumentera riskanalyser, bedöm om konsekvensbedömningar krävs.

Kontrollpunkt 12: Hantering av registrerades rättigheter

- Dataskyddsombudet har inte fått några direkta indikationer som medför en annan bedömning än den som bolaget gör, men har inte heller kontrollerat bolagets hantering särskilt.

Kommentar

- Saknas dokumenterade arbetssätt för att hantera ett tillbakadragande av samtycke.
  - Lägre skattning jmf med år 2022?

Rekommendationer

- Se över så att det inom verksamheten finns förutsättningar för att kunna hantera ett tillbakadragande av samtycke från en registrerad.

Frågor för diskussion

- Vilka fokusområden ser ni inför 2024?

Göteborgs Stad

Kontakt

Elin Olsson
elin.olsson@intraservice.goteborg.se
Intraservice, Göteborgs Stad

Carolin Lee
carolin.lee@intraservice.goteborg.se
Intraservice, Göteborgs Stad