Styrelsehandling nr: 6
Datum för styrelsemöte: 230119
Diarienummer: EH2023-0001

Handläggare: Erik Windt-Wallenberg
Telefon: 031-707 70 22
E-post: erik.windt.wallenberg@egnahemsbolaget.se

Årsrapport dataskyddsarbete 2022

Informationsärende

Styrelsen för Göteborgs Egnahems AB

Årsrapport dataskyddsarbete 2022 antecknas.

Sammanfattning

Dataskyddsenheten på Intraservice är Göteborgs Stads dataskyddsombud. Dataskyddsombudets viktigaste uppgift är att övervaka att stadens förvaltningar och bolag följer dataskyddslagstiftningen. Dataskyddsombudet har också till uppgift att ge råd och information till förvaltningar och bolag i dataskyddsfrågor.

Det är styrelsen som har det yttersta ansvaret för att verksamheten följer dataskyddslagstiftningen.

Under verksamhetsåret 2022 har en fördjupad kontroll at bolagets integritetspolicy genomförts. Dataskyddsombudet har lämnat ett antal rekommendationer till verksamheten för att förbättra sin integritetspolicy och säkerställa följsamhet mot GDPR.

Utifrån identifierade risker rekommenderar dataskyddsombudet att bolaget under 2023 prioriterar följande delar av dataskyddsarbetet:

- Integritetspolicy
- E-post och dokumenthantering
- Konsekvensbedömning/samråd
- IT-system och digitala verktyg

Bedömning ur ekonomisk dimension

Bolaget har inte funnit några aspekter på frågan utifrån denna dimension.

Bedömning ur ekologisk dimension

Bolaget har inte funnit några aspekter på frågan utifrån denna dimension.

Bedömning ur social dimension

Bolaget har inte funnit några aspekter på frågan utifrån denna dimension.

Samverkan

Ärendet har inte varit föremål för samverkan.

Bilagor

1. Årsrapport dataskyddsarbetet 2022 Egnahem

Ärendet

Dataskyddsombudets årsrapport av bolagets dataskyddsarbete för verksamhetsåret 2022.

Beskrivning av ärendet

Arbetet med att säkerställa att personuppgifter behandlas i enlighet med reglerna i GDPR behöver genomsyra arbetet inom de kommunala verksamheterna på alla olika plan. I det framåtsyftande arbetet är GDPR ett viktigt redskap för att kunna säkerställa en digitalisering som håller över tid.

Dataskyddsenheten på Intraservice är Göteborgs Stads dataskyddsombud. Dataskyddsombudets viktigaste uppgift är att övervaka att stadens förvaltningar och bolag följer dataskyddslagstiftningen. Dataskyddsombudet har också till uppgift att ge råd och information till förvaltningar och bolag i dataskyddsfrågor.

Det är styrelsen som har det yttersta ansvaret för att verksamheten följer dataskyddslagstiftningen.

Under verksamhetsåret 2022 har en fördjupad kontroll av bolagets integritetspolicy genomförts. Dataskyddsombudet har lämnat ett antal rekommendationer till verksamheten för att förbättra sin integritetspolicy och säkerställa följsamhet mot GDPR.

Utifrån identifierade risker rekommenderar dataskyddsombudet att bolaget under 2023 prioriterar följande delar av dataskyddsarbetet:

- Integritetspolicy
- E-post och dokumenthantering
- Konsekvensbedömning/samråd
- IT-system och digitala verktyg

Rekommendationerna avser bland annat ett behov av förtydliganden kring lagringstid, tredjelandsöverföring och vad som gäller för respektive behandling när det kommer till de registrerades rättigheter. Dataskyddsombudet rekommenderar att bolaget säkerställer att policyn är heltäckande. Bolaget behöver även säkerställa att det finns rutiner och utpekat ansvar för att hålla policyn uppdaterad.

Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Göteborgs Egnahems AB (Egnahemsbolaget)

2022-12-29

Innehåll

1 Dataskydd i kommunal verksamhet

Att få ta del av och hantera andra människors personliga uppgifter på ett sådant sätt som kommunala förvaltningar och bolag gör innebär att förvalta ett stort förtroende. Dataskyddsförordningen (GDPR) har tillkommit för att särskilt skydda människors rätt till integritet, och för att värna var och ens rätt att få ha kontroll över vad som sker med uppgifter om ens person. Att förvaltningar och bolag hanterar personuppgifter i enlighet med gällande lag bör vara en självklarhet i syfte att visa omsorg om det förtroende som givits den som har att hantera uppgifterna.

Arbetet med att säkerställa att personuppgifter behandlas enligt reglerna i GDPR behöver genomsyra arbetet inom de kommunala verksamheterna på alla olika plan. Det gäller allt från rutiner och processer för det dagliga arbetet, till arbetet med innovations- och digitaliseringslösningar för framtidens arbetssätt på förvaltningar och bolag inom Göteborgs Stad. I det framåtsyftande arbetet är GDPR ett viktigt redskap för att kunna säkerställa en digitalisering som håller över tid.

1.1 Göteborgs Stads dataskyddsombud

Dataskyddsenheten på Intraservice är Göteborgs Stads dataskyddsombud. Vad som är dataskyddsombudets uppgifter framgår direkt av lagstiftningen i GDPR.[1] Dataskyddsombudets viktigaste uppgift är att övervaka att stadens förvaltningar och bolag följer dataskyddslagstiftningen. Detta sker bland annat genom att samla in information om hur personuppgifter behandlas och genom att kontrollera hur bestämmelser och interna styrdokument som styr dataskyddsarbetet efterlevs.

Dataskyddsombudet har också till uppgift att ge råd och information till förvaltningar och bolag i dataskyddsfrågor. Detta sker genom att dataskyddsombudet är behjälplig när frågor rörande behandlingen av personuppgifter uppkommer hos verksamheterna. Dataskyddsombudet erbjuder också regelbundet utbildningar för stadens medarbetare. Rådgivning ges även till förvaltningar och bolag när dessa genomför konsekvensbedömningar, vilket är en skyldighet som följer av GDPR. Efter att ha identifierat ett särskilt behov av stöd i arbetet med konsekvensbedömningar, har dataskyddsenheten under 2022 tagit fram mallar och mallstöd för det arbetet.

Det är nämnd/styrelse som har det yttersta ansvaret för att verksamheterna följer dataskyddslagstiftningen och dataskyddsombudet ska enligt lag rapportera om detta till högsta förvaltningsnivå.[2] Dataskyddsombudet har inte mandat att fatta beslut åt verksamheterna. Det är i stället genom råd och rekommendationer som dataskyddsombudet bistår verksamheterna med underlag för att dessa själva ska kunna fatta väl underbyggda beslut.

[1] Artikel 39 i GDPR
[2] Artikel 38.3 i GDPR

2 Granskning av dataskyddsarbetet 2022

2.1 Dataskyddsombudets kontrollfunktion

Dataskyddsombudets uppgift att övervaka den personuppgiftsansvariges efterlevnad av förordningen regleras i artikel 39 i GDPR. I Göteborgs Stad innebär en del av denna övervakning att dataskyddsombudet genomför kontroller av dataskyddsarbetet inom den personuppgiftsansvariges organisation.

Enligt dataskyddsregelverket ska dataskyddsombudet arbeta utifrån en riskbaserad metod som utgår från risker för de registrerades fri- och rättigheter. Genom att utgå från en sådan metod minskas risken för negativa konsekvenser även för verksamheten själv. Sådana konsekvenser kan omfatta bland annat skadestånd, sanktionsavgifter, försämrat varumärke eller minskad tillit för verksamheten.

För dataskyddsombudet är kontrollarbetet ett sätt att få en bild av vilka risker och/eller brister som eventuellt föreligger inom en verksamhet. Genom kontroller kan dataskyddsombudet kartlägga verksamhetens dataskyddsarbete, och därigenom hjälpa verksamheten att få en nulägesbild av hur de faktiskt ligger till i sitt dataskyddsarbete. Denna kartläggning kan sedan användas som ett stöd för verksamheten i sitt fortsatta arbete med dataskydd. Kontrollarbetets syfte är inte främst att peka ut brister utan ska ses som en vägledning för verksamheten och ett verktyg för att identifiera relevanta prioriteringar. Det är sedan upp till varje verksamhet att besluta om hur det interna dataskyddsarbetet ska utformas utifrån verksamhetens förutsättningar för att på bästa sätt kunna hantera identifierade risker. I det arbetet är dataskyddsombudet behjälplig med rådgivning utifrån verksamhetens behov och de risker som identifierats.

2.2 Fördjupad kontroll

2.2.1 Kontroll av integritetspolicy 2022

Den fördjupade kontrollen har utförts för bolagets integritetspolicy. Resultatet av kontrollen presenteras i sin helhet i bilaga 2.

Dataskyddsombudet har i rapporten avseende den fördjupade kontrollen haft vissa anmärkningar och har därför lämnat ett antal rekommendationer till verksamheten för att förbättra sin integritetspolicy och säkerställa följsamhet mot GDPR.

Rekommendationerna avser bland annat ett behov av förtydligande kring lagringstid, kring tredjelandsöverföring och vad som gäller för respektive behandling när det kommer till de registrerades rättigheter. Dataskyddsombudet rekommenderar också att bolaget säkerställer att policyn är heltäckande eller att information om andra behandlingar lämnas på annat vis i samband med att

behandlingen påbörjas. Bolaget bör även säkerställa att det finns rutiner och utpekat ansvar för att hålla policyn uppdaterad.

2.3 Årlig kontroll av dataskyddsarbetet

Verksamhetens interna dataskyddsarbete följs årligen upp genom en enkät. Enkäten består av tolv punkter (”fasta kontrollpunkter”) där varje punkt innehåller ett antal delfrågor i form av påståenden och/eller skattningsfrågor. Enkäten är avsedd att spänna över de viktigaste delarna inom dataskyddsarbetet för att på så sätt fånga in en större bredd av frågor. Metoden syftar till att få till ett långsiktigt och systematiskt arbetssätt som möjliggör uppföljning över tid.

2.3.1 Metod och risknivåer

I arbetet används en modell som består av fyra kategorier, vilka representerar fyra olika risknivåer. Verksamheten får utifrån sina svar ett värde som visar vilken risknivå verksamheten befinner sig på inom respektive kontrollpunkt. Genom att arbeta med risknivåer möjliggörs ett riskbaserat arbetssätt för både verksamhet och dataskyddsombud, då resultaten ger en bild av vad verksamheten behöver prioritera i dataskyddsarbetet framåt.[3]

Beskrivning av risknivåer

Risknivåer	Färgkod
Nivå 1. Höga risker identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten.	
Nivå 2. Risker identifierade som bedöms vara omfattande och/eller kräver omgående åtgärder.	
Nivå 3. Risker identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga.	
Nivå 4. Inga direkta risker av betydelse identifierade. Indikerar att verksamheten har ett systematiskt dataskyddsarbete.	

2.4 Egnahemsbolagets dataskyddsarbete 2022

I detta avsnitt anges vilken risknivå verksamheten befinner sig inom för respektive kontrollpunkt, baserat på verksamhetens svar på de fasta kontrollpunkterna. Under varje kontrollpunkt presenteras även dataskyddsombudets bedömning gällande verksamhetens risker utifrån de iakttagelser som dataskyddsombudet gjort under året.

[3] I arbetet med enkäten har dataskyddsenheten utgått från Myndigheten för samhällsskydd och beredskaps (MSB) uppföljningsstruktur för den offentliga förvaltningens systematiska informationssäkerhetsarbete.

2.4.1 Kontrollpunkt 1: Dataskyddsorganisation

Kontrollpunkten avser verksamhetens organisatoriska förutsättningar för att kunna bedriva ett kontinuerligt dataskyddsarbete, och omfattar bland annat verksamhetens dataskyddsorganisation, definierade ansvarsområden och rapporteringsvägar för involverade funktioner samt tillhandahållna resurser för arbetet.

Dataskyddsombudets kommentarer:

Bolagets skattning ligger kvar på ungefär samma nivå som föregående år, men med en förbättring av medelvärdet. En förbättring kan ses avseende att bolaget nu angivit att den interna organisationen för dataskydd har tillräckligt med resurser för att kunna bedriva ett systematiskt dataskyddsarbete. Skattningen indikerar att det inom ramen för kontrollpunkten har identifierats risker som bör åtgärdas, men som ej bedöms vara brådskande, omfattande eller allvarliga. Resultatet ligger precis på gränsen till nivå 4.

Det är positivt att det inom bolaget, enligt skattningen, finns goda förutsättningar att bedriva ett gott arbete med dataskyddsfrågor och att ansvar, mandat och rapporteringsvägar är tydligt angivna. Det är också positivt att det anges att dataskyddsombudet regelbundet kontaktas för att delta i frågor som rör skyddet av personuppgifter.

Dataskyddsombudet har ingen anledning att göra en annan bedömning än bolaget, men har inte involverats i några särskilda frågor kring dataskyddsarbetet under 2022 och har inte heller kontrollerat dataskyddsorganisationen inom ramen för en fördjupad kontroll. Vid avstämning med bolaget i december 2022 framgår också att dataskyddsorganisationen med fördel kan utökas till att omfatta fler personer. En dataskyddsorganisation som består av en eller ett mycket litet antal personer medför sårbarhet. Det kan exempelvis bli svårt att hantera incidenter inom den lagstadgade tiden, eller att säkerställa kontinuitet vid personalförändringar. Detta är även viktigt i mindre bolag.

Vidare har bolaget också haft svårt att besvara dataskyddsombudets frågor kring den fördjupade kontrollen i tid och har trots förlängd svarstid inte besvarat samtliga frågor.

Med hänsyn till ovanstående rekommenderar dataskyddsombudet att bolaget kontinuerligt utvärderar om dataskyddsorganisationen är ändamålsenlig.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

Kontrollpunkten avser verksamhetens förutsättningar och rutiner för att identifiera och hantera personuppgiftincidenter.

Dataskyddsombudets kommentarer:

Bolagets skattning är något högre detta år jämfört med föregående och man ligger nu på nivå 4. Skattningen indikerar att det inom ramen för kontrollpunkten inte finns några risker av betydelse och bolaget anser att de arbetar systematiskt med personuppgiftsincidenter. Jämfört med förra året anges nu att det finns en rutin för när och hur information till de registrerade ska tillhandahållas, vilket dataskyddsombudet finner positivt.

Det enda dataskyddsombudet vill lyfta under denna kontrollpunkt är att bolaget bör se över om man verkligen har tillräckliga rutiner för att upptäcka personuppgiftsincidenter. Detta då bolaget under 2022 enbart har haft en personuppgiftsincident. Med hänsyn till att tröskeln för när en personuppgiftsincident har skett är låg och att personuppgiftsincidenter förekommer även i organisationer som har mycket väl utvecklade rutiner för att förhindra att personuppgiftsincidenter sker, bedömer dataskyddsombudet det som osannolikt att enbart en incident har skett under 2022. Det kan snarare vara så att ett visst antal incidenter är ett slags ”friskhetstecken” som indikerar att den aktuella verksamheten har goda rutiner för att upptäcka incidenter och att medarbetare är medvetna om vad som utgör en incident och hur de ska rapportera den. Mot denna bakgrund rekommenderas bolaget att utvärdera om rutinerna och den allmänna medvetenheten hos medarbetarna ger tillräckligt goda förutsättningar för att hantera eventuella incidenter.

2.4.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Kontrollpunkten avser verksamhetens dokumentation av biträdesavtal och andra överenskommelser gällande dataskydd, och förutsätter att verksamheten har identifierat samt registrerat personuppgiftsbiträden i personuppgiftsregistret. Även verksamhetens rutiner för uppdatering och uppföljning av tecknade biträdesavtal innefattas.

Dataskyddsombudets kommentarer:

Bolagets skattning är något lägre på denna kontrollpunkt jämfört med tidigare år, men bolaget ligger kvar på nivå 3. Sammantaget indikerar skattningen att det inom ramen för kontrollpunkten har identifierats risker som bör åtgärdas, men som ej bedöms vara brådskande, omfattande eller allvarliga.

Enligt skattningen behöver bolaget säkerställa att det finns rutiner för att kontinuerligt genomföra efterlevnadskontroller av anlitade personuppgiftsbiträden. Enligt skattningen finns det också rutiner för att bedöma om andra överenskommelser/avtal behöver upprättas avseende gemensam eller annan delad hantering av personuppgifter när en leverantör anlitas, eller när samarbeten sker. Med hänsyn till att det, enligt skattningen, har tecknats personuppgiftsbiträdesavtal

med cirka 75% av de som har bedömts utgöra personuppgiftsbiträden till bolaget, bör bolaget fortsätta att teckna dessa så att man når en nivå på 100%.

2.4.4 Kontrollpunkt 4: Personuppgiftsregister

Kontrollpunkten avser verksamhetens efterlevnad av skyldigheten att systematiskt dokumentera alla personuppgiftsbehandlingar i form av ett register. Även verksamhetens arbete med, och rutin för, att säkerställa ett uppdaterat och heltäckande personuppgiftsregister innefattas.

Dataskyddsombudets kommentarer:

Bolagets skattning visar på en förbättring inom ramen för kontrollpunkten, men bolaget ligger kvar på nivå 3 över lag. Sammantaget indikerar skattningen att det inom ramen för kontrollpunkten har identifierats risker som bör åtgärdas, men som ej bedöms vara brådskande, omfattande eller allvarliga.

Det är positivt att bolaget har förbättrat sig avseende andelen av bolagets behandlingar i registret som uppfyller kraven på information enligt artikel 30 i GDPR. Eftersom cirka 75% av bolagets behandlingar uppskattas finnas med i registret bör bolaget fortsätta arbeta med detta. Detta eftersom det är ett krav enligt artikel 30 i GDPR att den personuppgiftsansvariges samtliga behandlingar finns upptagna i registret, med fullständig information. Bolaget rekommenderas även säkerställa att det finns rutiner för att uppdatera registret vid tillkomna eller förändrade personuppgiftsbehandlingar. Dataskyddsombudet rekommenderar också att bolaget integrerar personuppgiftsregistret som en del i det löpande dataskyddsarbetet. Att centrera sitt dataskyddsarbete runt ett fullständigt och uppdaterat register förenklar dataskyddsarbetet i övrigt, såsom vid konsekvensbedömningar och liknande.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Bolagets skattning innebär en förbättring från föregående års skattning på denna kontrollpunkt och bolaget ligger nu på nivå 3. Sammantaget indikerar skattningen att det inom ramen för kontrollpunkten har identifierats risker som bör åtgärdas, men som ej bedöms vara brådskande, omfattande eller allvarliga.

Med hänsyn till hur flera av frågorna har besvarats bedömer dataskyddsombudet dock att det förefaller finnas risker inom ramen för kontrollpunkten som bör

hanteras. Bland annat bör det finnas skäl för bolaget att upprätta en informationssäkerhetspolicy. Detta för att säkerställa att det finns övergripande principer för hur personuppgifter i exempelvis IT-system, datorer och mobila enheter ska hanteras inom organisationen. Bolaget bör även aktivt och medvetet anta ett riskbaserat arbetssätt och genomföra interna kontroller för att säkerställa följsamhet till GDPR. Skattningen visar också att bolaget bör säkerställa att det finns rutiner för att efterleva GDPR:s krav vid olika sammankomster, såväl digitala som fysiska. Bolagets informationstillgångar behöver också klassificeras utifrån *Konfidentialitet, Riktighet* och *Tillgänglighet* i enlighet med stadens styrande dokument. Bolaget har angett att så har gjorts för cirka 50% av bolagets informationstillgångar.

2.4.6 Kontrollpunkt 6: Utbildning

Kontrollpunkten avser verksamhetens arbete med att utbilda och upprätthålla kunskapsnivån i dataskyddsfrågor hos anställda.

Dataskyddsombudets kommentarer:

Bolagets skattning är något lägre detta år än föregående, men ligger kvar på samma övergripande nivå (3). Sammantaget indikerar skattningen att det inom ramen för kontrollpunkten har identifierats risker som bör åtgärdas, men som ej bedöms vara brådskande, omfattande eller allvarliga.

Det är positivt att bolaget anger att kunskapsnivån bland medarbetarna är god och att man möjliggör för medarbetare att delta i utbildningar. Enligt skattningen behöver bolaget ta fram rutiner för att följa upp och säkerställa att medarbetarnas kunskapsnivå bibehålls. Inför att utbildningsinsatser planeras bör bolaget även kartlägga vilken nivå av dataskyddskunskaper som olika befattningar bör ha och sedan utbilda därefter. Dataskyddsenheten har flera utbildningar som är tillgängliga för förvaltningar och bolag inom Göteborgs Stad. Enheten kan också bistå med specifik utbildning för en särskild grupp om ett sådant behov identifieras hos bolaget.

2.4.7 Kontrollpunkt 7: Integritetspolicy

Kontrollpunkten avser verksamhetens utformning samt tillhandahållande av dess integritetspolicy till registrerade (både internt och externt). Även verksamhetens rutin för att upprätthålla en aktuell integritetspolicy omfattas.

Dataskyddsombudets kommentarer:

Bolagets skattning detta år ligger på nivå (4), vilket innebär en förbättring från föregående år. Enligt skattningen uppfyller bolagets integritetspolicy kraven på

information. Det finns, enligt skattningen, även rutiner för att informera medarbetare om behandlingen av deras personuppgifter och för att uppdatera integritetspolicyn vid behov. Bolaget behöver, enligt skattningen, säkerställa att de registrerade på ett enkelt sätt kan nå integritetspolicyn via bolagets samtliga digitala kanaler.

Med tanke på de observationer som dataskyddsombudet gjort i inom ramen för den fördjupade kontrollen av integritetspolicyn, instämmer dataskyddsombudet inte i bolagets höga skattningar under denna kontrollpunkt. Som framgår i den fördjupade kontrollen förekommer brister i integritetspolicyn. Bolaget har heller inte besvarat dataskyddsombudets frågor om rutiner för uppdatering av policyn.

2.4.8 Kontrollpunkt 8: E-post och dokumenthantering

Kontrollpunkten avser verksamhetens rutiner för e-post och dokumenthantering. I detta är en aktuell och fastställd dokumenthanteringsplan med gallringsbeslut en förutsättning för att verksamheten ska kunna säkra följsamhet gentemot dataskyddsförordningen. Även verksamhetens rutin för att säkerställa att gallringsrutiner för personuppgifter följs innefattas.

Dataskyddsombudets kommentarer:

Bolaget har ett lägre resultat på denna kontrollpunkt jämfört med föregående år och hamnar på nivå 1 (dock nära nivå 2). Skattningen indikerar att det finns höga risker identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten.

Enligt skattningen saknar bolaget dokumenthanteringsplan och rutiner för att kontrollera att gallring sker i enligt med gällande gallringsbeslut. Det saknas också rutiner för att informera medarbetare om dokumenthantering och gallring kopplat till GDPR. Bolaget har inte heller rutiner för hur olika informationsklasser enligt stadens styrande dokument ska hanteras eller rutiner för behandling av känsliga eller extra skyddsvärda personuppgifter i e-post. Bolaget informerar inte heller de registrerade direkt vid kontakt med bolaget (exempelvis genom autosvar med länk till integritetspolicy) om hur deras personuppgifter behandlas.

Enligt skattningen har cirka 0% av bolagets personuppgiftsbehandlingar klassificerats utifrån *Konfidentialitet*, *Riktighet* och *Tillgänglighet* i enlighet med stadens riktlinjer.

Vid avstämning med bolaget framgår att det finns ett behov av att se över just hur olika informationsklasser får hanteras, särskilt eftersom ett stort antal av bolagets handlingar hanteras lagras i Sharepoint (som också används som diarium). Dataskyddsombudet finner det positivt att bolaget inom en snar framtid kommer att använda ett nytt system (som tillhandahålls hela staden) för diarieföring.

Sammantaget bedömer dataskyddsombudet att det finns höga risker inom ramen för kontrollpunkten och rekommenderar att det skyndsamt vidtas åtgärder.

2.4.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

Kontrollpunkten avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras, samt rutiner kopplat till detta.

Dataskyddsombudets kommentarer:

Bolagets skattning är lägre på denna kontrollpunkt än föregående år, men det övergripande resultatet ligger kvar på nivå 2, vilket innebär att det inom ramen för kontrollpunkten finns risker som behöver åtgärdas inom en snar framtid.

Resultatet av skattningen på de 14 frågorna under kontrollpunkten är splittrat. Detta då det förvisso anges att några rutiner finns på plats, men att flera efterfrågade rutiner saknas. Enligt bolaget finns det rutiner för att bedöma risker för de registrerade inom ramen för en konsekvensbedömning och för att inhämta dataskyddsombudets synpunkter efter utförd tröskelanalys. Övriga efterfrågade rutiner saknas och bolaget anger även att enbart cirka 25% av bolagets behandlingar har kontrollerats utifrån höga risker och att för cirka 0 % av de behandlingar där det bedöms behövas en konsekvensbedömning har sådana genomförts. Bolaget har också angett att de inte kan besvara frågan om de kontinuerligt inhämtar dataskyddsombudets råd vid konsekvensbedömningar.

Vid avstämning med bolaget framgår att bolaget nu genomför sin första konsekvensbedömning. Den koncerngemensamma resursen inom dataskydd bistår bolaget i detta arbete.

Med hänsyn till vad som framgår ovan och vid avstämning med bolaget, rekommenderar dataskyddsombudet att arbetet med denna kontrollpunkt prioriteras.

2.4.10 Kontrollpunkt 10: IT-projekt och upphandling

Kontrollpunkten avser verksamhetens organisation och rutiner för hantering av dataskyddsfrågor inom IT-projekt och upphandling. I detta ingår till exempel hur verksamheten integrerar dataskyddsfrågor i arbetet med upphandling av nya, samt utvecklingen av, befintliga system och tjänster.

Dataskyddsombudets kommentarer:

Bolaget har skattat sig betydligt sämre på denna kontrollpunkt än föregående år. Det innebär att man landar på nivå 2 (dock nära nivå tre). Resultatet indikerar att

det inom ramen för kontrollpunkten finns risker identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder.

Det som drar ned resultatet är frågorna om kravställning vid upphandling för dataskydd som standard och inbyggt dataskydd, som bolaget inte har kunnat besvara. I övrigt anger bolaget att de säkerställer att dataskyddsperspektivet finns med i arbetet med nya IT- och digitaliseringslösningar samt vid utvecklingen av redan befintliga system och tjänster. Bolaget anger också att dataskyddsombudet involveras från start i dessa processer.

Dataskyddsombudet rekommenderar att bolaget säkerställer att det vid kravställning säkerställs att inbyggt dataskydd och dataskydd som standard finns med som krav. Dataskyddsombudet har inte involverats i frågor relaterade till kontrollpunkten under 2022.

2.4.11 Kontrollpunkt 11: IT-system och digitala verktyg

Kontrollpunkten avser verksamhetens rutiner för att säkerställa att verksamhetens personuppgiftshantering inom ramen för IT-system och digitala verktyg är förenlig med dataskyddsförordningen. Rutin för att säkerställa och kontrollera att dessa system/tjänster uppfyller kraven på dataskydd ingår även.

Dataskyddsombudets kommentarer:

Bolaget har skattat sitt arbete inom ramen för denna kontrollpunkt något högre än föregående år, men ligger ändå kvar på nivå 3. Sammantaget indikerar skattningen att det inom ramen för kontrollpunkten har identifierats risker som bör åtgärdas, men som ej bedöms vara brådskande, omfattande eller allvarliga.

Bolaget behöver, enligt skattningen, utföra kontroller för att säkerställa att medarbetares behörigheter till IT-system är korrekta och utföra kontroller så att IT-system och digitala verktyg används på rätt sätt. Därför är det även nödvändigt att verksamheten ser till att informera medarbetarna om korrekt användning av systemen/verktygen.

Vid avstämning med bolaget framgår att bolaget genomför kontroller av anställdas behörigheter löpande när någon byter tjänst eller avslutar sin anställning. Även årlig översyn av samtliga behörigheter görs. Detta finner dataskyddsombudet vara positivt.

Enligt bolagets skattning beaktas dataskyddsperspektivet vid införandet och användandet av kostnadsfria tjänster, såsom gratisappar och sociala medier. Avseende sociala medier framgår att bolaget använder såväl LinkedIn som Facebook och Instagram. Vid avstämning med bolaget framgår att det pågår en koncerngemensam översyn av de sociala medierna, inte minst med hänsyn till domen i Schrems II-målet.

I Schrems II-domen (juli 2020) förtydligade EU-domstolen vad som gäller för överföringar av personuppgifter till länder utanför EU/EES, så kallade tredjelandsöverföringar. Domen sade, i breda drag, att det skydd för personuppgifter som finns i USA inte är likvärdigt med det som finns i EU/EES, varför den personuppgiftsansvarige antingen måste vidta extra skyddsåtgärder eller avbryta behandlingen. I Schrems II-domen prövades särskilt Facebook, men även andra sociala medier såsom Instagram, Youtube och LinkedIn är exempel på sociala medier som överför personuppgifter till USA.

Dataskyddsombudets rekommendationer är att upphöra med att behandla personuppgifter i sociala medier i de fall följsamhet mot GDPR inte kan säkerställas. I detta utgår dataskyddsombudet helt ifrån bestämmelserna i GDPR och i den praxis som finns tillgänglig. Även om dataskyddsombudet anser det positivt att bolaget tillsammans med koncernen genomför en analys av användningen, bör bolaget vidta ytterligare åtgärder för att säkerställa att bolaget inte bryter mot förordningen vid användningen av Facebook, Instagram och LinkedIn. Dataskyddsombudet noterar att det förekommer behandling av personuppgifter, bland annat i form av bilder på personer, i bolagets sociala medier.

Bolaget har vidare skattat sig högt på påståendet om att användning av cookies på webbsidor följer kraven i GDPR och att de registrerade får information om behandlingen. Enligt information på bolagets hemsida samlas både så kallade nödvändiga cookies, som icke nödvändiga cookies in. För att få samla in nödvändiga cookies krävs inget samtycke enligt lagen (2022:482) om elektronisk kommunikation (tidigare SFS 2003:389). Det krävs däremot för icke nödvändiga cookies, såsom statistikcookies. Det ska vara lika lätt att tacka nej till insamlingen av icke-nödvändiga cookies som att tacka ja till dem. Bolagets cookie-ruta är bristfällig med hänsyn till detta. Det går inte att tacka nej till insamlingen direkt via cookie-rutan, vilket inte är förenligt med gällande lagstiftning.

Utöver bristande samtyckesinsamling, framgår av såväl bolagets information på hemsidan, som vid kontroll, att bolaget använder sig av Google Analytics för statistikinsamling och tredjepartscookies för annonsering via Facebook. Båda dessa användningar är problematiska, inte minst utifrån aspekten om olovlig tredjelandsöverföring. Vid kontroll framgår även att ett stort antal tredjepartsförfrågningar finns via bolagets hemsida. Flera av dessa innebär också risk för tredjelandsöverföring.

Avseende Google Analytics finns det tillsynsbeslut från tillsynsmyndigheter i Europa som fastställer att användningen inte är förenlig med lagstiftningen. Bolaget bör skyndsamt se över denna användning samt övriga cookies eller tredjepartsförfrågningar.

2.4.12 Kontrollpunkt 12: Hantering av registrerades rättigheter

Kontrollpunkten avser verksamhetens förutsättningar och rutiner för att hantera de registrerades rättigheter, till exempel registerutdrag eller radering.

Dataskyddsombudets kommentarer:

Bolaget ligger enligt skattningen på nivå 3, vilket innebär att det finns risker inom ramen för kontrollpunkten, men dessa bedöms ej som brådskande, omfattande eller allvarliga.

Dataskyddsombudet bedömer att det finns risker inom kontrollpunkten som behöver omhändertas. Bolaget uppger att det saknas rutiner för att hantera ett tillbakadraget samtycke från en registrerad, för att hantera registerutdrag och för att söka upp relevant information till ett registerutdrag inom bolaget. Rätten till registerutdrag är en grundläggande rättighet för de registrerade i GDPR och det är viktigt att bolaget har möjlighet att hantera dessa och säkerställa att de är rättvisande (att samtlig information har kunnat hittas och lämnas ut). Eftersom bolaget använder samtycke som rättslig grund för några av sina behandlingar är det också viktigt att det finns rutiner för att kunna hantera ett tillbakadraget samtycke. Den registrerade har nämligen rätt att när som helst dra tillbaka sitt samtycke och bolaget får då inte lov att fortsätta att behandla den registrerades personuppgifter.

2.5 Sammanfattande rekommendationer

För att på ett praktiskt plan kunna identifiera vad verksamheten behöver arbeta med inom ramen för respektive kontrollpunkt behövs en noggrann genomgång av enkätresultaten. I detta rekommenderas verksamheten att samråda med dataskyddsombudet för att se hur arbetet framåt bör utformas och vilka delar som bör prioriteras utifrån verksamhetens risker. Även för verksamheter med låga risker krävs kontinuerliga insatser för att denna risknivå ska bibehållas.

Utifrån identifierade risker rekommenderar dataskyddsombudet att bolaget under 2023 prioriterar följande delar av dataskyddsarbetet:

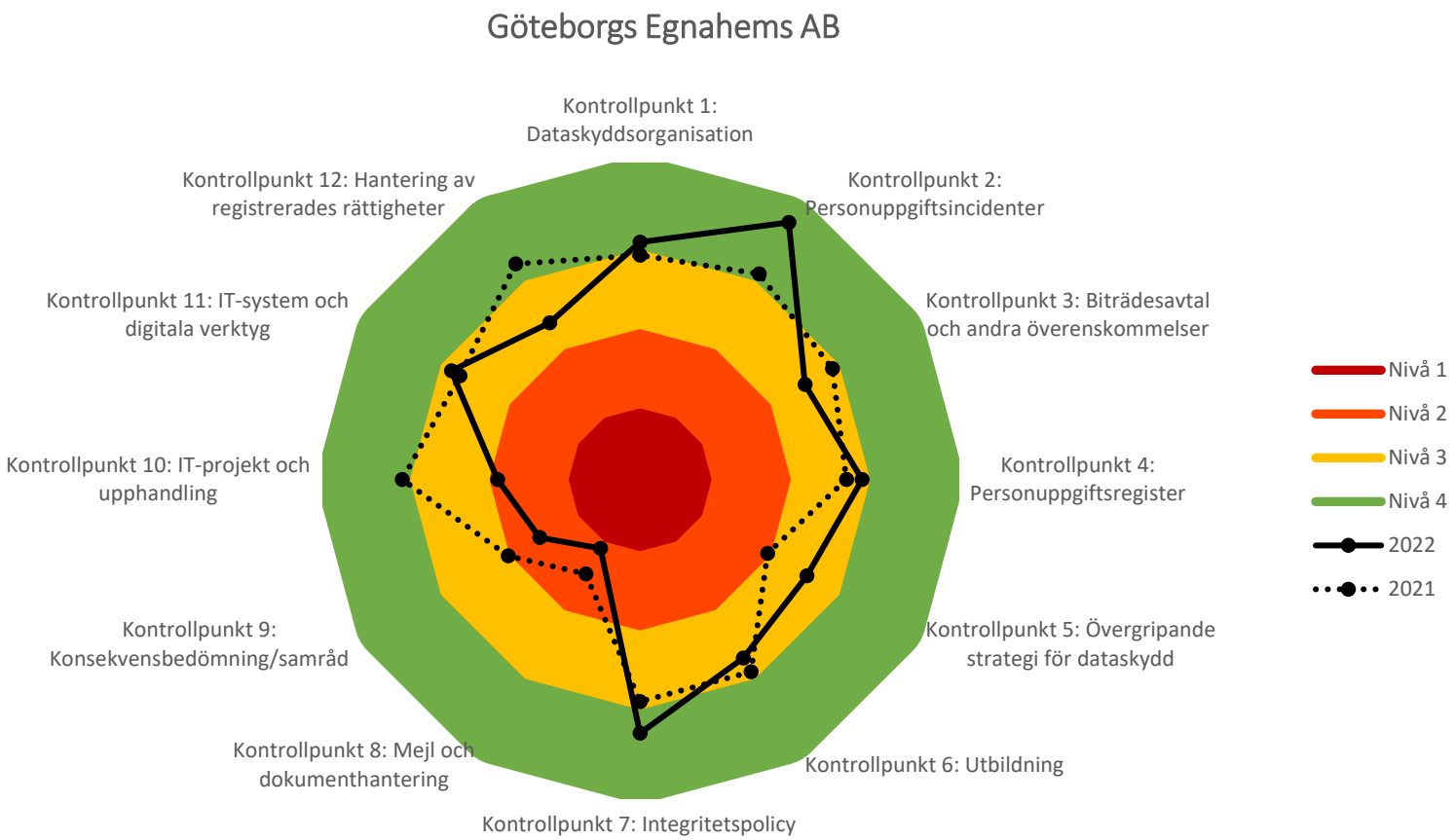
- Kontrollpunkt 7: Integritetspolicy.
- Kontrollpunkt 8: E-post och dokumenthantering
- Kontrollpunkt 9: Konsekvensbedömning/samråd
- Kontrollpunkt 11: IT-system och digitala verktyg

3 Bilagor

Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2021.

Bilaga 2: Fördjupad kontroll 2022 - Integritetspolicy.

Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2021.



Fördjupad kontroll

Kontrollpunkt 7: Integritetspolicy

Bakgrund

Dataskyddsförordningen innehåller ett antal rättigheter för den registrerade, alltså den vars personuppgifter behandlas. En av dessa rättigheter är rätten till information, vilket innebär att registrerade har rätt att få information från myndigheter och bolag om hur dessa behandlar personuppgifterna som samlas in. Denna information ska som regel ges både när uppgifterna samlas in och på begäran från den registrerade. Utifrån kraven i dataskyddsförordningen ska informationen vara lättillgänglig och tillhandahållas kostnadsfritt i skriftlig form, samt vara utformad med ett klart och tydligt språk.

Ett sätt för en verksamhet att uppfylla kravet på information till registrerade är att tillhandahålla en integritetspolicy. Integritetspolicyns syfte blir då att informera registrerade om verksamhetens behandling av personuppgifter i enlighet med de krav som ställs i dataskyddsförordningen. För att integritetspolicyn ska kunna anses bidra till att en verksamhet uppfyller dess ansvarsskyldighet krävs det att policyn är utformad så att den motsvarar de krav som ställs i förordningen.

I den aktuella kontrollen har det alltså skett en granskning av verksamhetens integritetspolicy, med fokus på utformning och tillhandahållande till registrerade (både internt och externt). Även verksamhetens rutiner för att arbeta med integritetspolicyn och säkerställa att den hålls uppdaterad ingår i kontrollen. Kontrollen har bestått av ett generellt frågeutskick samt begäran om kopior på den information som ges till registrerade.

Iakttagelser från kontrollen

Rättslig reglering och vägledning

Kravet på att ge registrerade information om behandlingen av deras personuppgifter har sin grund i artikel 5 dataskyddsförordningen (GDPR) där det anges att ”uppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade”. Vidare och mer specifika krav om hur informationen ska tillhandahållas samt vilken information som ska tillhandahållas framgår av artiklarna 12–14 GDPR. Hur dessa artiklar i sin tur ska tolkas framgår av artikel 29-gruppens vägledning om öppenhet[1] och är utgångspunkten i dataskyddsombudets kontroll och rekommendationer.

[1] Artikel 29-arbetsgruppen, *Riktlinjer om öppenhet enligt förordning (EU) 2016/*679, WP260rev.01, senast granskade och antagna den 11 april 2018.

Dataskyddsombudets rekommendationer

Generellt

Den aktuella kontrollen skickades ut den 1 mars 2022, med sista svarsdatum satt till 17 mars. När bolaget inte återkommit med svar i maj månad tog dataskyddsombudet kontakt och efterfrågade bolagets svar. Bolaget svarade då att svar skulle ges inom den närmsta veckan. När svaren följande vecka fortfarande inte tillhandahållits tog dataskyddsombudet återigen kontakt för att efterfråga bolagets svar, samt fråga om bolaget behövde förlänga svarstiden ytterligare och informera om att det i så fall skulle kunna innebära att bolaget enbart får en grundläggande kontroll i år (då tid inte skulle finnas tid för en uppföljande ”del 2” av kontrollen). Bolaget svarade då att man önskade förlänga svarstiden och deadline sattes till 30 juni.

Den 30 juni skickade bolaget in ett dokument, policy för personuppgiftsbehandling, som svar på frågorna i kontrollen. Svar på frågorna gällande att bifoga länkar till policyn, hur informationen tillhandahålls anställda eller vilka rutiner som finns för att säkerställa att policyn hålls uppdaterad besvarades ej av bolaget. Det framgick inte heller om bolaget tillhandahåller någon ytterligare information till anställda på annat sätt än via policyn.

I samband med att dokumentet översändes uppgav bolaget att man under våren arbetat med att uppdatera styrande och stödjande dokument, och att det aktuella dokumentet var under revidering. Inskickad version uppdaterades senast 2020-05-14.

Bolaget skickade in en ny version av sin integritetspolicy efter muntlig avstämning av kontrollen i december 2022, men utifrån vad dataskyddsombudet kan utläsa verkar det inte ha gjorts några större ändringar i den uppdaterade policyn. Primärt kontaktuppgifter till bolaget, dataskyddsombudet och tillsynsmyndigheten har ändrats. Dataskyddsombudet gör därför bedömningen att nedan rekommendationer fortsatt är aktuella för bolaget.

Aktuella behandlingar, ändamål och rättslig grund

Bolagets policy för personuppgiftshantering inleds med att redogöra för de sex olika kategorier av registrerade som policyn riktar sig till. Informationen i policyn är sedan uppdelad utifrån dessa kategorier och för respektive framgår vid vilka tillfällen som bolaget kan komma att samla in personuppgifter om en registrerad och vad som gäller avseende ändamål och rättslig grund. Behandlingarna baseras på någon av de rättsliga grunderna samtycke, avtal eller berättigat intresse/intresseavvägning.

Då bolaget har valt en övergripande beskrivning av personuppgiftsbehandlingarna finns endast ett fåtal behandlingar beskrivna mer utförligt. För de angivna behandlingarna finns ett ändamål och rättslig grund angiven. Utifrån den begränsade mängd behandlingar som anges ställer sig dataskyddsombudet dock frågande till huruvida bolaget kan anses uppfylla sin informationsplikt, detta då samtliga behandlingar sannolikt inte anges. Ett tydligt exempel som dataskyddsombudet ser är att det inte finns någon information om behandlingen av personuppgifter när någon kontaktar bolaget via e-post eller annat vis. Det är dock oklart om bolagets integritetspolicy avser att vara heltäckande för bolagets samtliga personuppgiftsbehandlingar. Det är möjligt att inte ha en heltäckande policy om bolaget säkerställer att den registrerade får information om en behandling som inte ingår i

policyn på annat vis. Om bolaget strävar efter att integritetspolicyn ska vara heltäckande, rekommenderas bolaget göra en översyn av befintliga personuppgiftsbehandlingar och komplettera integritetspolicyn med den information som saknas för att bolaget ska kunna bedömas uppfylla sin informationsplikt. Om bolaget inte ämnar att integritetspolicyn ska vara heltäckande bör bolaget säkerställa att de registrerade får information om de behandlingar som inte ingår på annat vis.

När behandling sker i enlighet med berättigat intresse/intresseavvägning framgår av art. 13.1 d och 14.2 b GDPR att den personuppgiftsansvarige ska ange vilka berättigade intressen som avses. Detta görs för vissa behandlingar, men inte samtliga. Av artikel 29-gruppens vägledning om öppenhet, framgår också att ”best practice” är att även informera om den bakomliggande bedömningen kring intresseavvägningen i integritetspolicyn. Enligt vägledningen bör den personuppgiftsansvarige åtminstone alltid informera om att den registrerade kan få ta del av mer information om bedömningen om denne så önskar.[2] Dataskyddsombudet rekommenderar därför att bolaget åtminstone kompletterar med information om att den registrerade kan få ta del av mer information om de gjorda intresseavvägningsbedömningarna i integritetspolicyn.

Lagring

I policyn specificeras lagringstiden särskilt när det kommer till kontaktpersoner hos leverantörer där det framgår att personuppgifterna sparas så länge den registrerade är kontaktperson och ett år därefter. Även för webbloggar anges lagringstiden särskilt (30 dagar). För övriga behandlingar anges lagringstid samlat och då enbart genom att ange att personuppgifterna enbart behandlas så länge som det är nödvändigt med hänsyn till ändamålet, men också så länge som anges i bolagets dokumenthanteringsplan.

Generellt kan sägas att det inte är tillräckligt att informera om att personuppgifterna bevaras så länge som är nödvändigt för de berättigade ändamålen med behandlingen. Däremot kan det vara okej att i stället för specifik lagringstid ange de kriterier som bestämmer lagringstiden. Om så görs behöver kriterierna anges på ett sådant sätt att den registrerade, utifrån sin egen situation, kan bedöma lagringstiden för särskilda uppgifter/ändamål. Dataskyddsombudet anser det mycket tveksamt om hänvisning till dokumenthanteringsplanen kan anses utgöra tillräckligt med information för att den registrerade själv ska kunna bedöma lagringstiden. Dataskyddsombudet rekommenderar därför att bolaget kompletterar med denna information för respektive behandling.[3]

Mottagare

När det kommer till mottagare av personuppgifter så har bolaget angett att personuppgifter kan komma att delas med leverantörer, företag, andra personuppgiftsansvariga, försäkringsbolag och myndigheter. Dataskyddsombudet anser att det är positivt att bolaget har specificerat att personuppgifter kan delas med

[2] Artikel 29-arbetsgruppen, *Riktlinjer om öppenhet enligt förordning (EU) 2016/679*, WP260rev.01, senast granskade och antagna den 11 april 2018, s. 38 (bilaga).
[3] Artikel 13.2 a och 14.2 a GDPR, samt artikel 29-arbetsgruppen, *Riktlinjer om öppenhet enligt förordning (EU) 2016/679*, WP260rev.01, senast granskade och antagna den 11 april 2018, s. 38 (bilaga).

exempelvis försäkringsbolag och myndigheter. Dataskyddsombudet rekommenderar att bolaget ser över om det är möjligt och lämpligt att specificera mottagare ytterligare.

Registrerades rättigheter

Avseende de registrerades rättigheter så framgår det av vägledningen att informationen om dessa rättigheter bör vara specifik för behandlingen i fråga och innehålla en sammanfattning av vad rättigheten innebär, hur den registrerade kan gå till väga för att utöva den och vilka begränsningar som rättigheten eventuellt omfattas av. Rätten att invända mot behandlingen (i de fall rättigheten är tillämplig) måste kommuniceras till den enskilde senast vid den första kontakten. Informationen om rätten att invända ska redovisas klart och tydligt och åtskilt från annan information.[4]

Bolagets policy anger enbart vilka rättigheter den registrerade kan kontakta bolaget för att utnyttja. Rättigheterna är inte beskrivna eller specificerade för respektive behandling. Dataskyddsombudet rekommenderar att detta åtgärdas. Med hänsyn till att flera av behandlingarna baseras på den rättsliga grunden berättigat intresse/intresseavvägning och den registrerade därmed har rätt att invända mot behandlingen, bör denna rättighet tydliggöras i integritetspolicyn.

Överföring till tredjeland

Avseende överföring till tredjeland anger bolagets externa integritetspolicy att bolaget strävar efter att alltid behandla personuppgifterna inom EU/EES. Dataskyddsombudet rekommenderar att informationen tydliggörs. Antingen behandlar bolaget personuppgifterna inom EU/EES och kan ange att så sker eller så gör bolaget inte det och då ska information i enlighet med art. 13.1 f och 14.1 f GDPR lämnas.

Lättillgänglig form

Kravet på att informationen ska vara lättillgänglig innebär att de registrerade inte ska behöva leta reda på informationen. Det ska vara direkt uppenbart för dem var och hur de kan få åtkomst till den.

Egnahemsbolagets integritetspolicy finns tillgänglig på bolagets hemsida. På förstasidan uppmärksammas den registrerade på var denne kan läsa den fullständiga integritetspolicyn och behöver enbart klicka en gång för att komma till den fullständiga policyn. Detta är i enlighet med vägledningen som säger att information aldrig ska vara mer än "två klick bort".

Utifrån underlaget som bolaget skickat in är det oklart hur och när anställda informeras om behandlingen av deras personuppgifter eller om så enbart sker via informationen på hemsidan. Det är också oklart om bolaget har andra kommunikationskanaler eller om information för vissa behandlingar ges på annat sätt.

[4] Artikel 29-arbetsgruppen, *Riktlinjer om öppenhet enligt förordning (EU) 2016/679*, WP260rev.01, senast granskade och antagna den 11 april 2018, s. 40f (bilaga).

Klart och tydligt språk

Kravet om ett klart och tydligt språk innebär att informationen bör ges på ett så enkelt sätt som möjligt och att komplicerade meningar och språkstrukturer bör undvikas. Informationen bör vara konkret och exakt, och den bör inte vara abstrakt eller tvetydig eller kunna tolkas på olika sätt. Framför allt bör syftena med och de rättsliga grunderna för behandlingen av personuppgifterna vara tydliga. Bestämningsord som “får”, “kan”, “viss”, “ofta” och “eventuellt” bör undvikas, om man inte kan visa varför sådant språk är nödvändigt. Språket bör inte vara överdrivet formalistiskt, tekniskt eller specialiserat.

Dataskyddsombudet har inte några större synpunkter på bolagets användning av bestämningsord då de förekommer i mycket liten omfattning. Däremot anges på några ställen ord som ”med mera”, vilket inte anses vara tillräckligt tydligt.

Rutin för uppdatering

Bolaget har inte besvarat dataskyddsombudets frågor om rutiner och ansvar för att uppdatera policyn vid behov. Om sådana rutiner inte finns rekommenderar dataskyddsombudet att det införs. Praxis utvecklas kontinuerligt på detta område, vilket gör att kraven för att en personuppgiftsansvarig ska anses uppfylla sin informationsplikt ständigt förtydligas.

Sammanfattade rekommendationer

- Om bolaget strävar efter att integritetspolicyn ska vara heltäckande, rekommenderas bolaget göra en översyn av befintliga personuppgiftsbehandlingar och komplettera integritetspolicyn med den information som saknas för att bolaget ska kunna bedömas uppfylla sin informationsplikt.
- Om bolaget inte ämnar att integritetspolicyn ska vara heltäckande bör bolaget säkerställa att de registrerade får information om de behandlingar som inte ingår i policyn på annat vis.
- Tydliggör lagringstid för respektive behandling.
- Komplettera med information om att den registrerade kan få ta del av mer information om intresseavvägningsbedömningen i policyn för de behandlingar som baseras på berättigat intresse/intresseavvägning enligt art. 6.1 f GDPR.
- Förtydliga vad som gäller avseende de registrerades rättigheter och specificera för respektive behandling.
- Förtydliga informationen om tredjelandsöverföring i policyn.
- Säkerställ att det finns rutiner och utpekat ansvar för att kontinuerligt uppdatera policyn vid behov.

Bilagor

- Frågor och informationsutskick

Information om fördjupad kontroll 2022

Kontrollpunkt 7: Integritetspolicy

Dataskyddsförordningen innehåller ett antal rättigheter för den registrerade, alltså den vars personuppgifter behandlas. En av dessa rättigheter är rätten till information, vilket innebär att registrerade har rätt att få information från myndigheter och andra verksamheter om hur dessa behandlar personuppgifterna som samlas in. Denna information ska som regel ges både när uppgifterna samlas in och på begäran från den registrerade. Utifrån kraven i dataskyddsförordningen ska informationen vara lättillgänglig och tillhandahållas kostnadsfritt i skriftlig form, samt vara utformad med ett klart och tydligt språk.

Ett sätt för en verksamhet att uppfylla kravet på information till registrerade är att tillhandahålla en integritetspolicy. Integritetspolicyns syfte blir då att informera registrerade om verksamhetens behandling av personuppgifter i enlighet med de krav som ställs i dataskyddsförordningen. För att integritetspolicyn ska kunna anses bidra till att en verksamhet uppfyller dess ansvarsskyldighet krävs det att policyn är utformad så att den motsvarar de krav som ställs i förordningen.

Granskningen avser kontrollera verksamhetens integritetspolicy, med fokus på utformning och tillhandahållande till registrerade (både internt och externt). Även verksamhetens rutiner för att arbeta med integritetspolicyn och säkerställa att den hålls uppdaterad ingår i kontrollen.

Tillvägagångssätt

Den fördjupade kontrollen kommer att genomföras i två delar. I del ett ombeds ni att skicka in dokumenterade integritetspolicys, rutiner samt besvara ett antal frågor. I del två kommer uppföljande frågor att ställas.

Dataskyddsombudet kommer sedan att sammanställa underlaget i en delårsrapport som lämnas till er i juni.

Fördjupad kontroll 2022

Kontrollpunkt 7: Integritetspolicy (del 1)

Dokumentation för er att skicka in till dataskyddsombudet:

1. Extern integritetspolicy (den policy som används för att informera medborgarna – kunder, besökare etc. – om de personuppgiftsbehandlingar som ni utför. Om ni har flera olika policys ombeds ni skicka in samtliga.)
    a. Skicka även med länkar till var informationen går att hitta så att dataskyddsombudet kan kontrollera tillgängligheten.
2. Intern integritetspolicy (den policy som används för att informera anställda/konsulter etc. om de personuppgiftsbehandlingar som ni utför. Om ni har flera olika policys ombeds ni skicka in samtliga.)
    a. Beskriv hur och när anställda/konsulter etc. får ta del av informationen.

Övrigt:

1. Har ni rutiner för att säkerställa att informationen i era integritetspolicys hålls uppdaterad?
    a. Om ja, beskriv rutinerna eller bifoga underlag där dessa framgår.
    b. Vem/vilken roll ansvarar för uppdateringen?

Underlaget ska ha inkommit till dataskyddsombudet **senast den 8 mars 2021.**

Har du frågor, kontakta ditt huvudansvariga dataskyddsombud.