Styrelsehandling nr 13a
Utfärdat 2024-03-26
Diarienummer 2023-00339

Handläggare
Linda Björk
Telefon:031-773 75 56
E-post: linda.bjork@framtiden.se

.

Årsrapport för dataskyddsarbetet 2023

Informationsärende

Styrelsen Förvaltnings AB Framtiden

Årsrapport för dataskyddsarbetet 2023 antecknas.

Ärendet

Dataskyddsombudets uppgift att övervaka den personuppgiftsansvariges efterlevnad av förordningen regleras i artikel 39 i GDPR. I Göteborgs Stad fullgör dataskyddsenheten på Intraservice uppdraget som dataskyddsombud för förvaltningar och bolag

Dataskyddsombudet ska ge råd, rekommendationer och informera om frågor som rör behandlingar av personuppgifter. Dataskyddsombudet har även i uppdrag att oberoende granska verksamheternas arbete med dataskyddsfrågor för att säkerställa att dataskyddslagstiftningen efterlevs.

Dataskyddsombudet lämnar årligen en rapport om verksamhetens dataskyddsarbete till varje nämnd och bolag i Göteborgs Stad. I rapporten redogör dataskyddsombudet för de iakttagelser som gjorts och det kontrollarbete som genomförts. För 2023 bestod kontrollarbetet av en granskning av fasta kontrollpunkter och i årsrapporten presenteras resultaten från denna tillsammans med dataskyddsombudets bedömning. Årsrapporten innehåller även resultaten från dataskyddsombudets årliga uppföljning av verksamhetens hantering av lämnade rekommendationer från tidigare genomförda kontroller.

Årsrapporten är avsedd att kunna användas som ett stöd för verksamheten i sitt fortsatta arbete med dataskydd. Det är 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.

De rekommendationer som dataskyddsenheten lämnar för 2023 berör områden såsom *Dataskyddsorganisation, Register över personuppgiftsbehandlingar* och *Informationsplikt*. Framtiden har med utgångspunkt i rekommendationerna tagit fram en åtgärdsplan för 2024 som redovisas till styrelsen i ett separat ärende på föreliggande sammanträde.

Ärendet bordlades på styrelsens sammanträde 2024-02-07 för behandling på kommande sammanträde.

Bedömning ur ekonomisk, ekologisk och social dimension

Ärendet är av administrativ karaktär och bolaget har därför inte funnit några särskilda aspekter på frågan utifrån dessa dimensioner.

Samverkan

Ärendet har inte varit föremål för samverkan.

Bilaga

Årsrapport för dataskyddsarbetet 2023

Dataskyddsenheten

Göteborgs Stad

Årsrapport för dataskyddsarbetet 2023

Förvaltnings AB Framtiden

2023-12-19

Innehåll

1 Inledning

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. Rätten till en fredad privat sfär och personlig integritet är grundläggande i ett demokratiskt samhälle och är ett av fundamenten på vilket många andra av våra demokratiska rättigheter vilar. Dataskyddsreglerna styr hur personuppgifter får samlas in, användas och hanteras för att säkerställa att uppgifterna används korrekt och rättvist. Lagstiftningen finns till för att skydda individen från skada och sätter ramarna för hur personuppgifter får behandlas i en alltmer digital värld. Dataskydd handlar i grunden om att skapa ett socialt hållbart samhälle.

1.1 Dataskyddsombud i Göteborgs Stad

I Göteborgs Stad fullgör dataskyddsenheten på Intraservice uppdraget som dataskyddsombud för förvaltningar och bolag. Vad som är dataskyddsombudets uppgifter framgår direkt av lagstiftningen. Dataskyddsombudet ska ge råd, rekommendationer och informera om frågor som rör behandlingar av personuppgifter. Dataskyddsombudet har även i uppdrag att oberoende granska verksamheternas arbete med dataskyddsfrågor för att säkerställa att dataskyddslagstiftningen efterlevs.

Enligt lag ska dataskyddsombudet rapportera till högsta förvaltningsnivå och i Göteborgs Stad innebär det att dataskyddsombudet rapporterar direkt till nämnder och styrelser. Dataskyddsombudet lämnar årligen en rapport om verksamhetens dataskyddsarbete till varje nämnd och bolag i Göteborgs Stad. I rapporten redogör dataskyddsombudet för de iakttagelser som gjorts och det kontrollarbete som genomförts. För 2023 bestod kontrollarbetet av en granskning av fasta kontrollpunkter och i årsrapporten presenteras resultaten från denna tillsammans med dataskyddsombudets bedömning. Årsrapporten innehåller även resultaten från dataskyddsombudets årliga uppföljning av verksamhetens hantering av lämnade rekommendationer från tidigare genomförda kontroller.

Årsrapporten är avsedd att kunna användas som ett stöd för verksamheten i sitt fortsatta arbete med dataskydd. Det är 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.

2 Särskilda iakttagelser 2023

2.1 Stadenövergripande

2.1.1 Förutsättningar för en hållbar digitalisering

Fokus på ny teknik och AI har en enorm potential för att göra våra liv bättre, men den digitala utvecklingen blir inte hållbar utan begränsningar. Utan tydlig styrning i arbetet med digital innovation är risken att det går fort och att man i sin iver att röra sig framåt glömmer att hänsyn behöver tas till den personliga integriteten och att personuppgifter behandlas på ett korrekt sätt. Verksamheter i Göteborgs stad behöver tydligt ha med sig integritetsaspekten vid framtagandet av innovativa och nya lösningar inom till exempel AI. Arbetet med att säkerställa att personuppgifter behandlas enligt reglerna i dataskyddslagstiftningen 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 inom Göteborgs Stad.

Som en stor offentlig aktör har Göteborg som stad att förvalta alla invånare och besökares förtroende. Oavsett om det handlar om elever, vårdnadshavare, brukare inom socialtjänst, eller någon annan kategori av kommuninvånare, så ska man kunna känna sig trygg med att användandet av innovativ teknik sker med respekt för den personliga integriteten och de regelverk som finns för att skydda enskildas personuppgifter. I takt med att tekniken tar en allt större plats i våra liv ökar också riskerna för att spåra och övervaka människor. På det rättsliga området har detta fört med sig att regleringarna på EU-nivå blir fler och alltmer komplexa. För att utvecklingen ska kunna ske på ett långsiktigt hållbart sätt är det nödvändigt att varje verksamhet förstår de regelverk som finns, och varför de finns. Man kan naturligtvis se det som en balansakt, men som dataskyddsombud vill vi vara extra tydliga med att balansen alltid behöver vara lagd till de enskilda registrerades fördel och aldrig får innebära att verksamheter tummar på det regelverk som finns till för att skydda personuppgifter. Verksamheterna behöver följa dataskydds-lagstiftningen på samma sätt som man behöver följa all annan lagstiftning.

Dataskyddsombudet bedömer att det inom Staden finns en felaktig uppfattning om att det är omöjligt att följa GDPR och samtidigt driva den digitala utvecklingen framåt. Det finns också en felaktig uppfattning om att GDPR är en lagstiftning som inte är obligatorisk att följa. Dataskyddsombudet vill därför särskilt lyfta att dessa uppfattningar är problematiska och medför risker i form av att dataskydds-perspektivet förbises i digitaliseringsarbetet. Fokus behöver därför skiftas från att betrakta reglerna i dataskyddslagstiftningen som hinder, till att i stället fokusera på syftet med lagstiftningen och använda den som en grund att utgå från i utvecklingen av innovations- och digitaliseringslösningar. Ett sådant fokus kommer gynna enskilda individer och samtidigt medföra en mer hållbar och rättssäker digitalisering i samhället på lång sikt.

3 Granskning av dataskyddsarbetet 2023

3.1 Kontroll av fasta kontrollpunkter

Under 2023 har dataskyddsombudet kontrollerat verksamhetens dataskyddsarbete utifrån de tolv fasta kontrollpunkterna. Kontrollen har genomförts 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.

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.[1]

Risknivå	Beskrivning	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 bedriver ett systematiskt dataskyddsarbete.	

3.2 Resultat från kontrollen 2023

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. För beskrivning av respektive kontrollpunkt se bilaga 2.

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

3.2.1 Kontrollpunkt 1: Dataskyddsorganisation

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsombudet har inte fått några direkta indikationer som medför en annan bedömning än den som bolaget gör, men har inte heller kontrollerat dataskyddsorganisationen särskilt.

Den kontakt som funnits mellan dataskyddsombudet och bolaget har främst utgjorts av bolagets deltagande vid Framtidenkoncernens gruppmöten inom dataskydd, där representanter för de olika bolagen deltar. Utöver det har bolaget kontaktat dataskyddsombudet gällande en inträffad personuppgiftsincident under året. Dataskyddsombudet har sedan tidigare uppfattat att bolagets dataskyddsorganisation är väl organiserad och upplevt att det finns förutsättningar för att kunna bedriva ett systematiskt dataskyddsarbete.

Under året har dataskyddsombudet fått information om att det sker arbete kopplat till informationssäkerhet och dataskydd på en koncernövergripande nivå via ”Säkerhetsrådet”. Utifrån den information som tillhandahållits förstår dataskyddsombudet det som att ”Säkerhetsrådet” representeras av samtliga bolag inom koncernen och att beslut som påverkar bolagens arbete med dataskydd fattas i rådet. Även om rådet behandlar frågor som gäller koncernens arbete med dataskydd har dataskyddsombudet under året ej involverats eller rådfrågats utifrån detta. Dataskyddsombudet vill därför särskilt lyfta till bolaget, i egenskap av koncernmoderbolag, att det är viktigt att bolaget framåt säkerställer att dataskyddsombudet involveras i det koncernövergripande arbetet som gäller dataskydd. Om dataskyddsombudet involveras av bolagen först efter att beslut har fattats och i ett skede när det enbart handlar om genomförande/implementering blir dataskyddsombudets möjligheter till rådgivning, och enskilda bolags möjligheter att omhänderta dataskyddsombudets rekommendationer begränsade. Det innebär även att bolagen riskerar att inte uppfylla sina skyldigheter att involvera dataskyddsombudet i alla frågor som gäller dataskydd. Bolaget rekommenderas därför att framåt se över hur dataskyddsombudet kan involveras mer aktivt i dataskyddsarbetet inom koncernen. Det innefattar arbetet som bedrivs inom ramen för ”Säkerhetsrådet”, med syftet att säkerställa att bolagen inom koncernen ges förutsättningar för att uppfylla kraven enligt artikel 38.1 i GDPR.

Vidare bedömer dataskyddsombudet att det skulle vara fördelaktigt om dataskyddsombudet framåt kunde arbeta mer koncernövergripande, då många frågor är gemensamma/liknande och koncernen som helhet bedöms ha goda förutsättningar för att kunna samordna dataskyddsarbetet. Dataskyddsombudet uppfattar även att det inom koncernen finns en strävan efter att arbeta gemensamt och enhetligt i de frågor där detta är möjligt, vilket bedöms vara positivt.

3.2.2 Kontrollpunkt 2: Personuppgiftsincidenter

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet delar till stor del verksamhetens bedömning, men gör till skillnad ifrån verksamheten bedömningen att det ändå föreligger risker inom kontrollpunkten.

Den risk dataskyddsombudet identifierat lyftes även till bolaget i årsrapporten för 2022 och avser huruvida det inom bolaget finns tillräckliga rutiner för att upptäcka personuppgiftsincidenter. Även om bolaget har en fungerande metod för att omhänderta de incidenter som den interna dataskyddsorganisationen får kännedom om, är dataskyddsombudets bedömning att antalet incidenter fortfarande ligger på en låg nivå. Som lyftes i årsrapporten 2022 är tröskeln för när en personuppgiftsincident har skett låg och personuppgiftsincidenter kommer ofrånkomligen att inträffa även i organisationer som har mycket väl utvecklade rutiner för att förhindra att personuppgiftsincidenter sker.

Utifrån den identifierade risken rekommenderas bolaget framåt att utvärdera om rutinerna och den allmänna medvetenheten hos medarbetarna ger tillräckligt goda förutsättningar för att identifiera såväl som hantera eventuella personuppgiftsincidenter.

3.2.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsombudet har inte fått några direkta indikationer som medför en annan bedömning än den som bolaget gör, men har inte heller kontrollerat hanteringen särskilt.

De risker som identifierats utifrån bolaget skattning gäller andelen upprättade personuppgiftsbiträdesavtal samt genomförande av efterlevnadskontroller. Gällande upprättade personuppgiftsbiträdesavtal anger bolaget att det har tecknats personuppgiftsbiträdesavtal, inkluderat instruktioner, med samtliga biträden. Detta ser dataskyddsombudet anledning att ifrågasätta utifrån att förvaltningen för Intraservice är en tjänsteleverantör till bolaget och det för de behandlingar som

Intraservice utför ej finns instruktioner framtagna. Bolaget rekommenderas utifrån detta se över dess hantering av biträdesavtal och huruvida svaret överensstämmer med de faktiska omständigheterna.

Ytterligare en iakttagelse som dataskyddsombudet gjort utifrån bolagets skattning är att bolaget anger att det saknas dokumenterade arbetssätt för att kontinuerligt genomföra efterlevnadskontroller av anlitade personuppgiftsbiträden med syftet att säkerställa att dessa uppfyller villkoren enligt biträdesavtalet. Utifrån det ansvar bolaget har vid anlitande av biträden enligt artikel 28 GDPR, den s.k. ”omsorgsplikten”, föreligger här en risk för att verksamheten inte kan uppfylla kraven enligt GDPR. Bolaget har därför ett behov av att säkerställa att personuppgiftsbiträdesavtal regelbundet följs upp och att det då kontrolleras att överenskomna villkor uppfylls. Bolaget rekommenderas se över nuvarande hantering för att kunna bedöma vilka åtgärder som behöver vidtas för att hantera risken.

3.2.4 Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

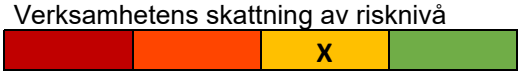
Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet delar inte verksamhetens bedömning, och gör till skillnad ifrån verksamheten bedömningen att det förekommer betydande risker som kräver åtgärder.

Bolaget anger att större delen av bolagets personuppgiftsbehandlingar finns med i behandlingsregistret. Likt 2022 anges att samtliga av dessa behandlingar innehåller den information som ska finnas med enligt artikel 30 i GDPR. Dataskyddsombudet har efter en stickprovskontroll i registret på några av de registrerade behandlingarna kunnat konstatera att skattningen ej stämmer överens med de faktiska omständigheterna, och att den information som anges för respektive behandling ej är tillräcklig utförlig för att uppfylla kraven enligt artikel 30 i GDPR. Utifrån den gjorda kontrollen rekommenderas bolaget göra en helhetsöversyn av behandlingsregistret och den information som finns inlagd. Vid genomgången av årsrapporten med bolaget framgick att bolaget var medvetna om brister i/med nuvarande behandlingsregister och att man framåt avser se över detta inom ramen för ett större arbete kopplat till informationssäkerhet och dataskydd.

Utifrån de av dataskyddsombudet identifierade bristerna rekommenderas bolaget, likt 2022, att framåt prioritera arbetet med att registrerade samtliga personuppgiftsbehandlingar i behandlingsregistret, samt säkerställa att dessa innehåller den information som ska finnas med enligt artikel 30 i GDPR.

3.2.5 Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsombudet har inte fått några direkta indikationer som medför en annan bedömning än den som bolaget gör, men har inte heller kontrollerat den övergripande styrningen särskilt.

Utifrån bolagets egen skattning behöver bolaget framåt arbeta med styrande dokument för behandling av personuppgifter kopplat till användningen av IT-system, mobiler och andra digitala enheter. Bolaget rekommenderas därför se över vilka styrande dokument som finns inom området, och om sådana ej finns upprättade ta fram dessa. Då bolaget angett ett lågt värde för hur stor andel av verksamhetens informationstillgångar som informationsklassificerats rekommenderas bolaget även framåt ta fram en handlingsplan för arbetet med informationsklassning, som ett led i att tillförsäkra rätt nivå av skydd för personuppgifter.

3.2.6 Kontrollpunkt 6: Utbildning

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet har under året inte involverats i någon fråga kopplad till kontrollpunkten, varför ingen övergripande bedömning kan göras i frågan.

Utifrån gjorda iakttagelser kopplat till bolagets hantering av personuppgiftsincidenter bedömer dock dataskyddsombudet att det inom kontrollpunkten kan föreligga risker. Detta utifrån att höga skattningar på denna punkt innebär att i princip alla anställda korrekt ska kunna identifiera en personuppgiftsincident, vilket dataskyddsombudet ställer sig frågande till utifrån det låga antalet rapporterade incidenter under både 2022 och 2023. Med anledning av detta bör bolaget framåt se över ifall den allmänna medvetenheten hos medarbetarna ger tillräckligt goda förutsättningar för att identifiera såväl som hantera eventuella personuppgiftsincidenter.

Vid genomgång av årsrapporten med bolaget framgår att bolaget planerar för att genomföra en utbildningsinsats fokuserad på personuppgiftsincidenter och hantering av dessa under 2024. Under förutsättning att utbildningsinsatsen genomförs bedömer dataskyddsombudet att bolaget bör kunna omhänderta även de rekommendationer som lämnas för kontrollpunkt 2 inom ramen för denna insats.

3.2.7 Kontrollpunkt 7: Informationsplikt

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Resultatet ligger på samma nivå som föregående år. Dataskydds-ombudet delar inte verksamhetens bedömning, och gör till skillnad ifrån verksamheten bedömningen att det förekommer risker som är omfattande och kräver åtgärder.

Dataskyddsombudet genomförde 2022 en fördjupad kontroll med fokus på bolagets integritetspolicy. Baserat på resultatet från denna gjorde dataskyddsombudet då bedömningen att bolagets skattning inom kontrollpunkten ej avspeglade de faktiska omständigheterna och att det fanns brister i informationen. I årsrapporten 2022, samt den fördjupade kontrollen, lämnades därför ett antal rekommendationer. Dessa rekommendationer följs upp under avsnitt 3.3.1 i årsrapporten.

Av bolagets svar på uppföljningen framgår att bolaget under året sett över informationen på hemsidan, och att man avser uppdatera denna efter att bolagets nya behandlingsregister är framtaget. Dataskyddsombudet kan efter en kontroll av informationen på hemsidan se att de rekommendationer som lämnades föregående år ej fullt ut är omhändertagna, vilket hade förväntats utifrån bolagets höga skattning på punkten. Sammantaget gör dataskyddsombudet bedömningen att bolaget behöver utveckla informationen ytterligare för att uppfylla kraven enligt artikel 13 och 14 i GDPR. Dataskyddsombudet rekommenderar att bolaget framåt prioriterar arbetet och framåt vidtar nödvändiga åtgärder för att säkerställa att informationsplikten som helhet uppfylls. I detta arbete är integritetspolicyn en del, och bolaget rekommenderas framåt säkerställa att de rekommendationer som 2022 lämnades kopplat till den specifika informationen i integritetspolicyn omhändertas. Under året har dataskyddsombudet utfört en informationsinsats om informationsplikten och tillhandahållit såväl muntlig information som skriftligt underlag för stadens samtliga verksamheter. Bolaget kan använda sig av underlaget som stöd i arbetet med informationsplikten.

3.2.8 Kontrollpunkt 8: E-post och dokumenthantering

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

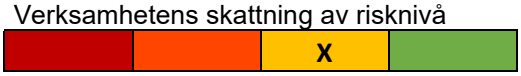
Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga.

Dataskyddsombudet har under året inte involverats i någon fråga kopplad till kontrollpunkten, men kan utifrån bolagets skattning utläsa att det inom kontrollpunkten föreligger risker kopplat till gallring, dokumenthantering och informationsklassificering. Det anges även saknas dokumenterade arbetssätt för hur information i olika informationsklasser ska hanteras och vilka lagringsytor som får användas, samt dokumenterade arbetssätt för hur personuppgifter får hanteras i e-post.

Bolaget rekommenderas framåt se över hur man inom verksamheten kan arbeta med frågorna, med syftet att ge medarbetare förutsättningar för att kunna hantera personuppgifter på rätt sätt och minska risken för att incidenter inträffar. Utifrån de risker som en oreglerad informationshantering innebär rekommenderas bolaget att framåt ta fram en handlingsplan för arbetet med informationsklassning, som ett led i att tillförsäkra rätt nivå av skydd för personuppgifter. Bolaget rekommenderas även ta fram dokumenterade arbetssätt/anvisningar för hur information i olika informationsklasser ska hanteras och vilka lagringsytor som får användas samt för hur personuppgifter får hanteras i e-post.

3.2.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

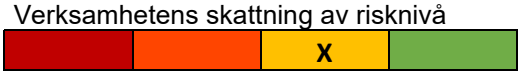
Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsombudet delar till viss del verksamhetens bedömning, men gör till skillnad ifrån verksamheten bedömningen att det inom kontrollpunkten förekommer risker som är omfattande och kräver åtgärder.

Bolaget anger att det finns framtagna konsekvensbedömningar för ca 50% av de personuppgiftsbehandlingar som kräver det. Under året har dataskyddsombudet involverats i arbetet med tre tröskelanalyser och lämnat återkoppling på samtliga. Efter återkopplingen har dataskyddsombudet inte kontaktats av bolaget igen i dessa frågor, och dataskyddsombudet saknar därför kunskap om hur bolaget omhändertagit de rekommendationer som lämnats. Dataskyddsombudet avser följa upp hanteringen under 2024.

Dataskyddsombudet gör, utifrån bolagets egen skattning och gjorda iakttagelser under året, bedömningen att det inom kontrollpunkten föreligger ett stort behov av att fortsätta utveckla arbetet ytterligare. Bolaget rekommenderas inledningsvis fokusera dels på att bedöma befintliga personuppgiftsbehandlingar utifrån höga risker för att få koll på vilka personuppgiftsbehandlingar som kräver att en konsekvensbedömning genomförs, dels på att säkerställa att det införs dokumenterade arbetssätt för att säkerställa att konsekvensbedömningar genomförs innan riskfyllda behandlingar påbörjas. Även om bolaget, utifrån skattningen, också behöver arbeta med att ta fram rutiner för att uppdatera konsekvensbedömningar vid förändringar i behandlingen, för att säkerställa beslutsmandat vid beslut kopplade till konsekvensbedömning och för att inhämta de registrerades rättigheter när det anses lämpligt bedömer dataskyddsombudet att bolaget bör prioritera arbetet med att få en överblick av helheten. Därför behöver bolaget lägga upp en planering för genomförandet och säkerställa att det praktiska arbetet med att ta fram konsekvensbedömningar för de aktuella behandlingarna genomförs. Utöver att involvera dataskyddsombudet, rekommenderas bolaget även att se över möjligheterna för bolaget att samverka med andra bolag med liknande uppdrag inom koncernen i arbetet.

3.2.10 Kontrollpunkt 10: IT-projekt och upphandling

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsombudet har under året inte involverats i någon fråga kopplad till kontrollpunkten, varför ingen övergripande bedömning kan göras i frågan.

Utifrån bolagets egen skattning kan det utläsas att verksamheter har god koll på att dataskyddsperspektivet finns med i arbetet med nya IT- och digitaliseringslösningar och vid utvecklingen av redan befintliga system och tjänster. Bolaget anger även att det kravställs att det finns en anpassning till inbyggt dataskydd och dataskydd som standard vid upphandling av nya system/tjänster.

På frågan om verksamheten har dokumenterade arbetssätt för att involvera dataskyddsombudet från start vid uppstart av nya IT-projekt och/eller införandet av nya tjänster där personuppgifter kommer att hanteras anges att det *stämmer bra*. Dataskyddsombudet ser utifrån bolaget svar anledning att lyfta den risk som identifierades under kontrollpunkt 1 gällande att dataskyddsombudet ej involveras i tillräcklig utsträckning i det interna dataskyddsarbetet. Även om bolaget har dokumenterade arbetssätt som anger att dataskyddsombudet ska involveras, vilket är positivt, är det viktigt att bolaget säkerställer att så även görs. Bolaget rekommenderas framåt se över hur det kan säkerställas att befintliga arbetssätt följs och att dataskyddsombudet involveras i frågorna, särskilt i de fall då bolaget har ett samordningsansvar/uppdrag för implementeringen av nya system på koncernnivå.

3.2.11 Kontrollpunkt 11: IT-system och digitala verktyg

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet delar inte verksamhetens bedömning, och gör till skillnad ifrån verksamheten bedömningen att det förekommer risker som kräver omgående åtgärder.

Utifrån skattningen kan det utläsas att bolaget, likt 2022, fortfarande har behov av att ta fram dokumenterade arbetssätt för att följa upp och kontrollera att användningen av system och tjänster och digitala verktyg används på avsett vis, samt för att säkerställa att dataskyddsperspektivet finns med vid införande och användande av kostnadsfria tjänster såsom gratisappar och sociala medier.

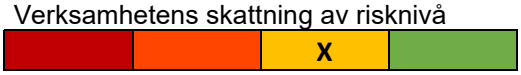
De risker som dataskyddsombudet särskilt identifierat gäller dels användningen av kakor (cookies) på hemsidan, dels användningen av sociala medier. Bolaget anger i skattningen att verksamhetens användning av kakor (cookies) på hemsidor följer kraven enligt GDPR. Dataskyddsombudet genomförde i oktober 2023 en kontroll av bolagets hemsida och kunde då konstatera att flertalet kakor användes på hemsidan, inkluderat kakor för analys/statistik. Bolaget fick information om resultatet av kontrollen från ett dotterbolag (som dataskyddsombudet hade möte med) och vidtog därefter åtgärder för att avaktivera kakorna på hemsidan. Dataskyddsombudet har fått information om att bolaget ej varit medvetna om att kakor användes och att dessa ska ha aktiverats av misstag då det inom bolaget ej bedömts finnas ett behov av att ha kakor på hemsidan. Dataskyddsombudet är positiv till att bolaget snabbt vidtog åtgärder och att det inom bolaget tagits ett aktivt beslut i frågan. Samtidigt visar händelsen hur viktigt det är att ha koll på sina behandlingar och (kopplat rekommendationer för kontrollpunkt 3) betydelsen av att regelbundet genomföra efterlevnadskontroller av anlitade biträden. I det här fallet visade det sig att kakor varit aktiverade på hemsidan sedan mars 2023, vilket innebär att det pågått en omfattande personuppgiftsbehandling utan rättslig grund under en längre period. Dataskyddsombudet bedömer det därtill som osannolikt att detta skulle ha upptäckts av bolaget i det fall dataskyddsombudet ej genomfört kontrollen, vilket i sig är en risk.

Även vid årets genomgång av bolagets kommunikationskanaler noterar dataskyddsombudet att bolaget använder sociala medier (LinkedIn). Trots att förutsättningarna för överföringar till amerikanska leverantörer har ändrats finns flera aspekter att ta hänsyn till än enbart tredjelandsproblematiken. Bolaget rekommenderas bland annat att kartlägga vilka behandlingar och vilka personuppgifter som behandlas av bolaget kopplat till användningen av sociala medier, utreda om profilering sker och identifiera vilka ansvarsförhållanden som råder för de olika behandlingarna. Vidare rekommenderas bolaget att utföra och

dokumenterar noggranna riskanalyser samt se över för vilka behandlingar kopplat till användningen av sociala medier som kräver en konsekvensbedömning.

3.2.12 Kontrollpunkt 12: Hantering av registrerades rättigheter

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. 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.

Skattningen visar att bolaget, likt 2022, behöver arbeta med att säkerställa att det finns en process för att hitta och få tillgång till efterfrågad information vid en begäran om registerutdrag. För att en begäran om registerutdrag ska kunna hanteras på rätt sätt behöver verksamheten säkerställa att den efterfrågade informationen kan lokaliseras genom till exempel sökningar i olika system eller register. Om en verksamhet saknar dokumenterade arbetssätt för hanteringen medför det risker för att en begäran om registerutdrag ej kan hanteras inom utsatt tid. Vidare visar skattningen även att bolaget behöver ta fram dokumenterade arbetssätt för att hantera ett tillbakadragande av samtycke från en registrerad.

3.3 Uppföljning

3.3.1 Uppföljning av rekommendationer lämnade inom ramen för tidigare genomförda kontroller

Dataskyddsombudet har under året följt upp vilka åtgärder som vidtagits avseende tidigare års lämnade rekommendationer av gjorda kontroller.

Kontroll (2022): Integritetspolicy

Verksamheten gavs följande rekommendationer:

- Komplettera med information om att den registrerade kan få ta del av mer information om intresseavvägningsbedömningen i den externa integritetspolicyn för de behandlingar som baseras på berättigat intresse/intresseavvägning enligt art. 6.1 f GDPR.
- Förtydliga rättslig grund för behandlingarna i den information som lämnas till anställda.
- Tydliggör lagringstid för respektive behandling i såväl den externa integritetspolicyn som i informationen till anställda.

- Säkerställ att samtliga behandlingar, där personuppgifterna inte samlas in direkt från den registrerade, kompletteras med information om kategorier av personuppgifter och var personuppgifterna kommer ifrån.
- Förtydliga vad som gäller avseende de registrerades rättigheter och specificera för respektive behandling, primärt i den externa integritetspolicyn. Förtydliga också kring rätten att invända mot en behandling i tillämpliga fall.
- Förtydliga informationen om tredjelandsöverföring i den externa integritetspolicyn och se till att informationen finns även i den information som lämnas till anställda.
- Säkerställ att den externa integritetspolicyn är heltäckande och innehåller alla behandlingar eller säkerställ att information lämnas till de registrerade på annat vis.
- Säkerställ att den externa integritetspolicyn och informationen har ett tydligt språk och inte innehåller bestämningsord såsom ”kan” och liknande.

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten vidtagit ett antal åtgärder utifrån de rekommendationer som dataskyddsombudet lämnat. Bolaget har under året verkställt en första översyn av informationen på den externa hemsidan och anger att delar av informationen kommer komma att förtydligas efter att bolagets nya behandlingsregister är framtaget. Vidare framgår det i uppföljningen att information till medarbetare har utvecklats och att denna nu ges via en ny sida på bolagets intranät. I samband med den nya sidan på intranätet gjordes även en översyn av innehållet, och även denna kommer komma att förtydligas efter att bolagets nya behandlingsregister är framtaget.

Dataskyddsombudet rekommenderar bolaget att under 2024 fokusera på arbetet med informationsplikten, inom vilket integritetspolicyn utgör en del. I samband med detta rekommenderas bolaget fortsatt omhänderta de kvarstående rekommendationerna gällande integritetpolicyn.

Resultatet från uppföljningen visar att verksamheten fortfarande har förbättringsområden inom denna kontroll. Uppföljning kommer därför att ske igen under 2024.

4 Rekommenderade fokusområden 2024

Utifrån höga föreliggande risker för de registrerades fri- och rättigheter har dataskyddsombudet identifierat ett antal områden som verksamheten rekommenderas att särskilt arbeta med under det kommande året. Dessa listas i punktform enligt nedan. Detta är områden som dataskyddsombudet särskilt kommer att följa upp framåt. Uppföljningen kommer ske löpande under det kommande året, i dialog med verksamheten.

Utifrån identifierade risker är dataskyddsombudets sammanfattande rekommendationer till bolaget att under 2024 prioritera följande delar av dataskyddsarbetet:

- Kontrollpunkt 1: Dataskyddsorganisation

Se över hur dataskyddsombudet kan involveras mer aktivt i dataskyddsarbetet inom koncernen, inklusive i det arbete som bedrivs inom ramen för ”Säkerhetsrådet”, med syftet att säkerställa att bolagen inom koncernen ges förutsättningar för att uppfylla kraven enligt artikel 38 i GDPR.

- Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Gör en översyn av befintligt register. Gå igenom hur de dokumenterade behandlingarna är definierade och kontrollera för respektive behandling att informationen uppfyller kraven enligt artikel 30 i GDPR.

- Kontrollpunkt 7: Informationsplikt

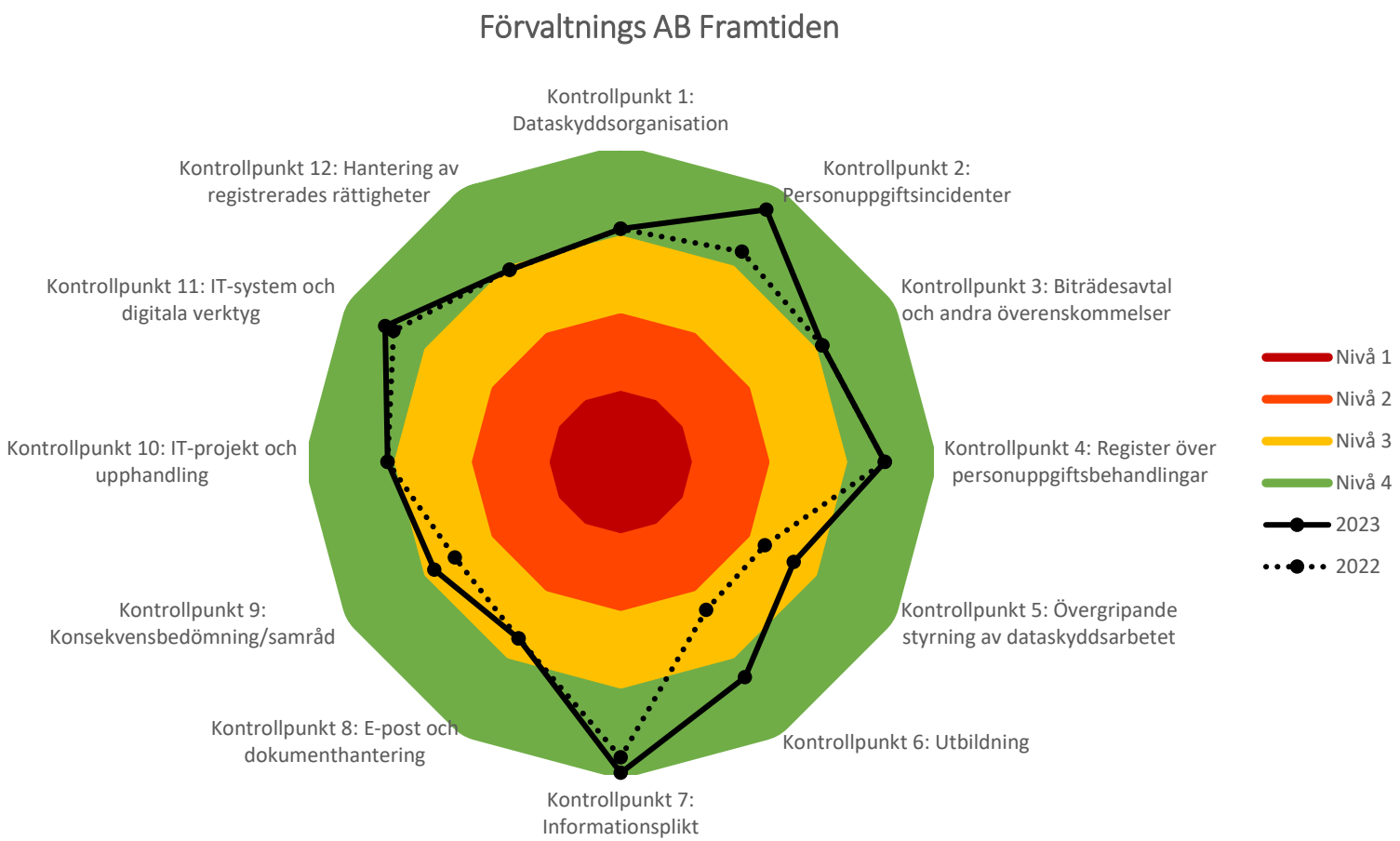
Se över samtliga delar i den information som lämnas till de registrerade och de arbetssätt som tillämpas för att säkerställa att informationsplikten gentemot de registrerade uppfylls. I arbetet behöver de rekommendationer som tidigare lämnats kopplat till den specifika informationen i integritetspolicyn omhändertas.

5 Bilagor

Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2022.

Bilaga 2: Kontrollplan för dataskyddsarbetet 2023–2024.

Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2022.



Göteborgs Stad

Förvaltnings AB Framtiden

Kontrollplan för dataskyddsarbetet 2023–2024

2023-02-06

Innehåll

1 Bakgrund

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 värna om den enskildes rätt till integritet och kontroll över vad som sker med ens personuppgifter. 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 personuppgifter.

Det är varje nämnd och bolaget som är ytterst ansvarig för att dess verksamhet följer dataskyddslagstiftningen. För att stödja stadens nämnder och bolag i arbetet med dataskydd har ett dataskyddsombud utsetts. I Göteborgs Stad fullgör dataskyddsenheten på Intraservice uppdraget som dataskyddsombud. Dataskyddsombudet har särskild sakkunskap i dataskyddslagstiftning och arbetar bland annat för att hålla nämnden/bolaget informerade om hur verksamheten lever upp till dataskyddslagstiftningen. Vad som är dataskydds-ombudets uppgifter framgår direkt av GDPR. En av dessa uppgifter är att övervaka att stadens förvaltningar och bolag följer dataskyddslagstiftningen. När dataskyddsombudet kontrollerar efterlevnaden av dataskyddslagstiftningen sker det bland annat genom att samla in information om hur personuppgifter behandlas inom en verksamhet och genom att kontrollera hur bestämmelser och interna styrdokument som styr dataskyddsarbetet efterlevs.

1.1 Ny utformning av kontrollarbetet

För att ytterligare stärka kvaliteten i verksamheternas dataskyddsarbete kommer dataskyddsombudets kontrollarbete att framgent löpa över tvåårsperioder. Tidigare har kontrollarbetet planerats årsvis, vilket ändras från och med år 2023. För att också underlätta verksamheternas egen planering kommer en ny kontrollplan att skickas ut varje år, som omfattar både innevarande och nästkommande kalenderår.

Kontrollarbetet kommer även fortsättningsvis bestå av tre delar, men frekvensen för den fasta respektive fördjupade kontrollen ändras. Framåt kommer dessa kontroller att ske vartannat år och under 2023 kommer en kontroll av de fasta kontrollpunkterna att genomföras. Genom att alternera den fasta respektive fördjupade kontrollen mellan åren får verksamheterna mer tid till att omhänderta resultaten från kontrollerna, vilket bedöms kunna bidra till ökad kvalitet på vidtagna åtgärder såväl som lagefterlevnad. Detta ligger också i linje med önskemål från flera verksamheter som har signalerat att tätt liggande kontroller gör det svårt att hinna med att arbeta med de lämnade rekommendationerna.

Den nya utformningen innebär även att tid frigörs för dataskyddsombudet, vilken kommer att läggas på att ytterligare stärka arbetet med informations- och utbildningsinsatser för stadens förvaltningar och bolag.

2 Kontrollarbetet 2023–2024

Dataskyddsombudets uppgift att övervaka den personuppgiftsansvariges efterlevnad av dataskyddslagstiftningen görs i Göteborgs stad genom ett antal kontroller. Dessa kontroller specificeras genom denna kontrollplan, som syftar till att informera personuppgiftsansvariga om upplägg och tidplan för kontrollarbetet åren 2023 och 2024. Enligt GDPR ska dataskyddsombudet arbeta utifrån en riskbaserad metod. Riskbedömningen utgår från riskerna för de registrerades fri- och rättigheter. Kontrollplanen utgår från dataskyddsombudets bedömning avseende risker kopplat till personuppgiftsbehandlingar i verksamheten.

Syftet med att arbeta utefter en på förhand fastställd kontrollplan är att det ska bidra till att sätta fokus på verksamhetens dataskyddsarbete och därmed:

1. Säkerställa ett kontinuerligt dataskyddsarbete som skapar förutsättningar för efterlevnad av förordningen.
2. Uppmuntra ett riskbaserat arbetssätt och därigenom minimera risken för lagbrott.
3. Göra dataskyddsarbetet till en integrerad del i verksamhetens informationssäkerhetsarbete.

2.1 Kontrollarbetets delar

Kontrollarbetet består av tre delar som tillsammans syftar till att ge, såväl dataskyddsombud som personuppgiftsansvariga, en överblick över verksamhetens dataskyddsarbete och dess följsamhet gentemot GDPR.

Del	Beskrivning	Frekvens
Fasta kontrollpunkter	En övergripande kontroll av verksamhetens dataskyddsarbete. Verksamheten skattar det interna arbetet i en enkät uppdelad i tolv fasta kontrollpunkter.	Vartannat år fr.o.m. 2023
Fördjupad kontroll	En fördjupad kontroll av en eller flera utvalda verksamhetsspecifika kontrollpunkter.	Vartannat år fr.o.m. 2024
Uppföljning	Uppföljning och bedömning av hur verksamheten omhändertagit lämnande rekommendationer.	Årligen

2.2 Tidplan för kontrollarbetet 2023–2024

I tabellerna nedan anges huvuddragen i kontrollarbetet för åren 2023–2024 för stadens förvaltningar och bolag.

2023	Aktivitet
Januari - april	Årsrapport 2022 presenteras för nämnd/styrelse.
Januari - februari	Kontrollplan för 2023–2024 lämnas till nämnd/bolag.
September	Utskick av enkät för fasta kontrollpunkter.
November - december	Genomgång av innehåll i årsrapport med förvaltning/bolag.
December	Fastställd årsrapport översänds till förvaltning/bolag.

2024	Aktivitet
Januari - april	Årsrapport 2023 presenteras för nämnd/styrelse.
Januari - februari	Kontrollplan för 2024–2025 lämnas till nämnd/bolag.
Augusti - november	Fördjupad kontroll.
November - december	Genomgång av innehåll i årsrapport med förvaltning/bolag.
December	Fastställd årsrapport översänds till förvaltning/bolag.

3 Kontroller

3.1 Fasta kontrollpunkter

De fasta kontrollpunkterna utgår från principerna om inbyggt dataskydd och dataskydd som standard (enligt artikel 25 i GDPR). Verksamhetens följsamhet mot förordningen beror till stor del på hur väl dessa principer har integrerats i ordinarie arbetsprocesser. Att principerna har en central roll i arbetet med dataskydd blir särskilt tydligt i beaktandesats (skäl) 78 i GDPR, som anger att ”skyddet av fysiska personers rättigheter och friheter i samband med behandling av personuppgifter förutsätter att lämpliga tekniska och organisatoriska åtgärder vidtas”, och därtill att den personuppgiftsansvarige, för att kunna visa att förordningen efterlevs, bör anta interna strategier och vidta åtgärder särskilt för att uppfylla principerna om inbyggt dataskydd och dataskydd som standard. Med principerna som utgångspunkt har tolv kontrollpunkter identifierats. Dessa är av både teknisk och organisatorisk karaktär och är gemensamma för alla verksamheter inom Göteborgs Stad.

De fasta kontrollpunkterna kontrolleras genom en enkät som framöver kommer att vara återkommande vartannat år. Enkäten utgår från de tolv kontrollpunkterna där varje punkt innehåller ett antal delfrågor i form av

påståenden och/eller skattningsfrågor. Det är verksamheten som ansvarar för att enkäten fylls i. För att uppskattningarna ska bli så korrekta som möjligt kan det krävas att olika personer från olika delar i verksamheten deltar i arbetet med att fylla i enkäten. Resultaten från enkäten ger en generell ögonblicksbild för respektive kontrollpunkt och kan användas som vägledning för verksamheten i sitt dataskyddsarbete. Syftet är att få till ett långsiktigt och systematiskt arbetssätt som även åskådliggör de förändringar som vidtas över tid.

För beskrivning av de fasta kontrollpunkterna, se bilaga 1.

Fasta kontrollpunkter
1. Dataskyddsorganisation
2. Personuppgiftsincidenter
3. Biträdesavtal och andra överenskommelser
4. Register över personuppgiftsbehandlingar
5. Övergripande styrning av dataskyddsarbetet
6. Utbildning
7. Informationsplikt
8. E-post och dokumenthantering
9. Konsekvensbedömning/samråd
10. IT-projekt och upphandling
11. IT-system och digitala verktyg
12. Hantering av registrerades rättigheter

3.2 Fördjupad kontroll

Den fördjupade kontrollen ska utgå från verksamhetens specifika risker och kommer framöver att genomföras vartannat år. Dataskyddsombudet kommer att fastställa fokusområde för den fördjupade kontrollen i dialog med verksamheten.

Information om fokusområde för 2024 kommer att tillhandahållas nämnd/bolag i kontrollplanen för 2024–2025.

3.3 Uppföljning av genomförda kontroller

Uppföljning av genomförda kontroller görs årligen för att se hur verksamheten har hanterat tidigare lämnade rekommendationer och utvecklat sitt dataskyddsarbete inom varje kontrollpunkt.

4 Rapportering

4.1 Årsrapport

Det är nämnd/bolag som har det yttersta ansvaret för att verksamheten följer dataskyddslagstiftningen och dataskyddsombudet ska enligt lag rapportera om detta till högsta förvaltningsnivå. Därför sammanställer dataskyddsombudet årligen en rapport om verksamhetens dataskyddsarbete. I rapporten redogörs för eventuella risker och brister som dataskyddsombudet har identifierat. I rapporten redogörs också för de råd och rekommendationer som dataskyddsombudet har lämnat. För att möjliggöra en direkt kommunikation mellan dataskyddsombud och personuppgiftsansvarig presenteras årsrapporten för nämnd/styrelse vid sammanträde/möte.

4.2 Särskilt yttrande

Dataskyddsombudet kan i vissa situationer komma att rikta ett särskilt yttrande till högsta ansvarsnivå. En sådan situation kan vara om dataskyddsombudet har identifierat höga risker för de registrerade som kräver omgående åtgärder från ansvarig nämnd/bolag. Det kan också vara om dataskyddsombudet uppmärksammar att det inom verksamheten fattats beslut som är oförenliga med dataskyddslagstiftningen och dataskyddsombudets råd.

5 Kontakt

Eventuella frågor och synpunkter hänvisas i första hand till verksamhetens huvudansvariga kontaktperson inom dataskyddsenheten.

Frågor kan också alltid ställas till dso@intraservice.goteborg.se.

Bilaga 1 - Beskrivning av fasta kontrollpunkter

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.

Kontrollpunkt 2: Personuppgiftsincidenter

Kontrollpunkten avser verksamhetens förutsättningar för att identifiera och hantera personuppgiftincidenter. För att uppfylla ansvarsskyldigheten bör verksamhetens rutin för hanteringen vara dokumenterad. I de fall verksamheten är både personuppgiftsansvarig och personuppgiftsbiträde bör rutinen omfatta båda scenarier. I kontrollpunkten ingår även översyn av verksamhetens rutin för att bedöma incidenter, hantering av eventuell anmälan till tillsynsmyndigheten, samt hur rutinerna tillgängliggörs och kommuniceras inom verksamheten. Även efterlevnad av verksamhetens dokumentationsskyldighet, att alla inträffade personuppgiftsincidenter registreras, innefattas.

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.

Kontrollpunkt 4: Register över personuppgiftsbehandlingar

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 register innefattas.

Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

Kontrollpunkten avser verksamhetens övergripande styrning för att arbeta med dataskydd. Tydlig styrning sätter ramarna för arbetet med dataskydd och främjar ett riskbaserat arbetssätt. Kontrollpunkten innefattar även verksamhetens arbete för att integrera dataskyddsfrågorna i det övriga informationssäkerhetsarbetet, samt hur verksamheten arbetar med egna interna kontroller för att säkerställa att dataskyddslagstiftningen efterlevs.

Kontrollpunkt 6: Utbildning

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

Kontrollpunkt 7: Informationsplikt

Kontrollpunkten avser hur väl verksamheten uppfyller principen om öppenhet och kravet på att lämna information till de registrerade om hur deras person-uppgifter behandlas. Punkten omfattar även hur verksamheten säkerställer att informationen är uppdaterad.

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 dataskyddslagstiftningen. Även verksamhetens rutin för att säkerställa att gallringsrutiner för personuppgifter följs innefattas.

Kontrollpunkt 9: Konsekvensbedömning/samråd

Kontrollpunkten avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras samt genomföra denna. Även verksamhetens rutiner för arbetet med konsekvensbedömningar samt hur dataskyddsombudet involveras i arbetet ingår. Därtill tillkommer verksamhetens rutin för att hantera de risker som identifieras i konsekvensbedömningen, samt hur genomförda konsekvensbedömningar följs upp och hålls aktuella.

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.

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 dataskyddslagstiftningen. Rutin för att säkerställa och kontrollera att dessa system/tjänster uppfyller kraven på dataskydd ingår även.

Kontrollpunkt 12: Hantering av registrerades rättigheter

Kontrollpunkten avser verksamhetens förutsättningar för att hantera de registrerades rättigheter. En förutsättning för att verksamheten ska kunna hantera de registrerades rättigheter är att man har en process och rutiner för arbetet, så att den registrerades personuppgifter enkelt kan lokaliseras vid efterfrågan. Även verksamhetens rutin för att hantera ett tillbakadragande av samtycke ingår i kontrollpunkten.