Styrelsehandling nr. 7
Utfärdat 2023-02-28
Diarienummer 2023–0058

Handläggare
Tullan Nilsson
Telefon:0707-616621
E-post: tullan.nilsson@framtiden.se

.

Årsrapport för dataskyddsarbetet 2022

Informationsärende

Styrelsen Förvaltnings AB Framtiden

Årsrapport för dataskyddsarbetet 2022 antecknas.

Ärendet

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.

Från december 2021 har Förvaltnings AB Framtiden hela Göteborgs Stads dataskyddsenhet som dataskyddsombud. Tidigare fanns en utpekad tjänsteperson som bolagets ombud.

Kontrollerna är 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 bild av hur de faktiskt ligger till i sitt dataskyddsarbete. Kartläggningen kan sedan användas som stöd för verksamhetens fortsatta arbete med dataskydd.

Årsrapporten innehåller dels en uppföljning av bolagets egen skattning av det interna dataskyddsarbetet som görs genom en enkät bestående av tolv punkter (”fasta kontrollpunkter”) där varje punkt innehåller ett antal delfrågor i form av påståenden och/eller skattningsfrågor. Årsrapporten innehåller också en uppföljning av den fördjupade kontroll som dataskyddsombudet gjort av bolagets *integritetspolicy*, såväl den externa på bolagets hemsida, som den interna information som lämnas till anställda.

Årets rekommendationer från dataskyddsenheten berör områden såsom *Övergripande strategi för dataskydd, Utbildning, Mejl- och dokumenthantering* samt *Konsekvensbedömningar/samråd*. Framtiden gör bedömningen att detta kommer att leda till vissa åtgärder för verksamheten. Vidtagna åtgärder kommer att redovisas till styrelsen under året. Dessutom kan nämnas att Framtiden, under året, har rekryterat en informationssäkerhetsstrateg i syfte att arbeta mer strategiskt och långsiktigt med informationssäkerhet och dataskydd. Konkreta åtgärder för att exempelvis tillgodose medarbetarnas behov av utbildning och en översyn av bolagets *integritetspolicy* har redan genomförts.

Ärendet bordlades på Förvaltnings AB Framtidens styrelsesammanträde 2023-02-08.

Bedömning ur ekonomisk dimension

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

Bedömning ur ekologisk dimension

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

Bedömning ur social dimension

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

Samverkan

Ärendet har inte varit föremål för samverkan.

Bilaga

Årsrapport för dataskyddsarbetet 2022

Dataskyddsenheten

Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Förvaltnings AB Framtiden

2022-12-22

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, såväl den externa på bolagets hemsida, som den interna information som lämnas till anställda. 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 behov av avseende rättslig grund, lagringstid, tredjelandsöverföring och vad som gäller för respektive behandling när det kommer till de registrerades rättigheter. Dataskyddsombudet rekommenderar också att bolaget säkerställer att den externa integritetspolicyn är heltäckande eller

att information om andra behandlingar lämnas på annat vis i samband med att behandlingen påbörjas.

För att uppfylla kravet om ett klart och tydligt språk lämnas även en rekommendation om språklig översyn.

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 Förvaltnings AB Framtidens 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

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

verksamhetens risker utifrån de iakttagelser som dataskyddsombudet gjort under året.

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:

Bolaget har skattat sig till samma nivå som föregående år avseende dataskyddsorganisation. Resultatet indikerar att det kan förekomma risker som bör åtgärdas, men ej bedöms vara brådskande, omfattande eller allvarliga. Resultatet ligger väldigt nära nivå 4, vilket indikerar att dataskyddsorganisationen fungerar väl och att det finns ett systematiskt tänk kring dataskyddsorganisationen.

Dataskyddsombudet har inte någon anledning att ifrågasätta bolagets skattning i stort. Dataskyddsorganisationen framstår vara väl organiserad och det verkar finnas förutsättningar att bedriva ett systematiskt dataskyddsarbete. Dataskyddsombudet anser det positivt att det inom koncernen har anställts en person som särskilt ansvarar för samordningen av dataskyddsarbetet mellan bolagen och att man strävar efter att arbeta gemensamt och enhetligt. På så vis kan man också utnyttja varandras kompetenser och kontinuerligt driva arbetet framåt.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Dataskyddsombudets kommentarer:

Bolagets skattning på denna kontrollpunkt ligger kvar på samma nivå som föregående år. Resultatet indikerar att det inom ramen för kontrollpunkten inte har identifierats några direkta risker av betydelse och att verksamheten bedriver ett systematiskt och välfungerande arbete kring personuppgiftsincidenter.

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” och indikerar att den aktuella verksamheten dels har goda rutiner för att upptäcka incidenter och att medarbetare är medvetna om vad som utgör en incident och hur de ska rapportera den.

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 på denna kontrollpunkt ligger kvar på samma nivå som föregående år. Resultatet indikerar att det förekommer risker som bör åtgärdas, men som ej bedöms vara brådskande, omfattande eller allvarliga. Resultatet ligger väldigt nära nivå 4, vilket indikerar att ett gott arbete sammantaget bedrivs inom ramen för kontrollpunkten. Det är mycket bra att det förefaller finnas biträdesavtal tecknade för samtliga personuppgiftsbiträdesrelationer.

På frågan om bolaget har rutiner för att kontinuerligt genomföra efterlevnadskontroller av anlitade personuppgiftsbiträden i syfte att säkerställa att dessa uppfyller villkoren i biträdesavtalet, har dock bolaget svarat att det inte stämmer. Då efterlevandskontroller är en viktig del i att uppfylla ansvarsprincipen i dataskyddsförordningen bör bolaget införa rutiner för detta.

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:

Bolaget har enligt skattningen ett betydligt bättre resultat på denna kontrollpunkt jämfört med föregående år och ligger nu på nivå 4, vilket indikerar att det inom ramen för kontrollpunkten inte har identifierats några direkta risker av betydelse

samt att bolaget bedriver ett systematiskt och välfungerande arbete kring sitt personuppgiftsregister.

Enligt skattningen har bolaget blivit bättre på att dels använda registret som en del i det löpande dataskyddsarbetet och dels avseende rutiner för vem som ansvarar för att uppdatera registret. Bolaget har också förbättrat sig när det kommer till antalet behandlingar som registrerats i registret och att de innehåller den information som de ska innehålla enligt art. 30 GDPR. Dataskyddsombudet vill dock belysa att bolaget har angett att cirka 75% av bolagets behandlingar finns registrerade i registret och att cirka 75% av dessa innehåller den information som ska finnas med enligt art. 30 GDPR. I och med att allt annat än att 100% av en personuppgiftsansvarigs behandlingar finns registrerade i registret och att 100% av dessa innehåller den information som art. 30 GDPR säger, inte är förenligt med lagstiftningen, rekommenderar därför dataskyddsombudet att detta arbete fortsatt prioriteras. Vid avstämning med bolaget har dock angivits att närmare 100% av bolagets behandlingar finns med i registret, vilket dataskyddsombudet finner positivt.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Bolagets skattning på denna kontrollpunkt ligger kvar på samma nivå som föregående år. Resultatet indikerar att det förekommer risker som bör åtgärdas, men som ej bedöms vara brådskande, omfattande eller allvarliga. Skattningen ligger dock väldigt nära nivå 2, vilket innebär att det inom ramen för kontrollpunkten skulle kunna finnas risker som behöver åtgärdas skyndsamt.

Bolaget behöver, enligt skattningen, arbeta vidare med värderingen (konfidentialitet, riktighet, och tillgänglighet) av sina informationstillgångar utifrån stadens styrande dokument. Detta då bolaget angett att detta enbart är gjort för cirka 25% av bolagets informationstillgångar. Bolaget behöver även ta fram en informationssäkerhetspolicy, rutiner för att efterleva kraven enligt GDPR vid fysiska och digitala sammankomster och säkerställa att eventuella styrande dokument hålls uppdaterade. Bolaget behöver även utföra intern kontroll för att säkerställa följsamhet till GDPR.

Vid avstämning med bolaget framgår att bolaget avser upprätta ett ledningssystem för informationssäkerhet och dataskydd. Detta för att förbättra och systematisera arbetet.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

Bolagets skattning på denna kontrollpunkt ligger kvar på samma nivå som föregående år. Resultatet indikerar att det förekommer risker som bör åtgärdas, men som ej bedöms vara brådskande, omfattande eller allvarliga. Skattningen ligger dock väldigt nära nivå 2, vilket innebär att det inom ramen för kontrollpunkten skulle kunna finnas risker som behöver åtgärdas skyndsamt.

Enligt skattningen behöver bolaget kartlägga medarbetarnas utbildningsbehov, se till att medarbetarna får delta i utbildningar samt följa upp och bibehålla kunskapsnivån. Vid avstämning med bolaget framgår att bolaget avser att arbeta med frågan framöver och lägga upp en plan för det.

Trots den låga skattningen i övrigt anger bolaget att medarbetarna verkar ha goda kunskaper om dataskydd, vilket får anses positivt.

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 på denna kontrollpunkt ligger kvar på samma nivå som föregående år, men med en marginell förbättring av medelvärdet. Skattningen indikerar att det inte föreligger några direkta risker av betydelse.

Bolagets interna och externa integritetspolicy har varit föremål för den fördjupade kontrollen 2022, vilken har påvisat behov av förbättringar. Även om det finns rutiner för att uppdatera policyn och att det finns information till registrerade, så innebär resultatet av den fördjupade kontrollen att dataskyddsombudet inte instämmer med det övergripande resultatet av skattningen. Se avsnitt 2.2.1 och bilaga 2.

2.4.8 Kontrollpunkt 8: Mejl och dokumenthantering

Kontrollpunkten avser verksamhetens rutiner för mejl 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:

Bolagets skattning innebär en mycket stor förbättring jämfört med föregående år. Bolaget hamnar nu på nivå 3 i stället för nivå 2, vilket indikerar att det finns risker inom ramen för kontrollpunkten, men de bedöms inte vara brådskande, omfattande eller allvarliga.

Framför allt anger bolaget nu att klassificeringen av bolagets personuppgiftsbehandlingar i enlighet med stadens styrande dokument är aktuell (även om skattningen också visar att det föreligger behov av att fortsätta skatta sina behandlingar), men också att bolaget nu har som rutin att informera de registrerade om hur deras personuppgifter behandlas direkt via länk till integritetspolicyn i medarbetarnas e-postsignaturer.

Dataskyddsombudet bedömer dock att bolaget bör arbeta med denna kontrollpunkt då flera av frågorna har besvarats med alternativet *Nej, det stämmer inte bra.* Bolaget behöver säkerställa att gallring sker och att information till anställda om gallring och dokumenthantering ges. Bolaget behöver också fortsätta klassificera personuppgiftsbehandlingar och ta fram anvisningar för hur olika informationsklasser ska hanteras. Bolaget bör även ta fram rutiner för hantering av känsliga eller extra skyddsvärda personuppgifter i e-post.

Vid avstämning med bolaget framgår att bolaget förväntar sig att även denna kontrollpunkt kommer gynnas av det ledningssystem för informationssäkerhet och dataskydd som bolaget kommer införa.

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 innebär att det övergripande resultatet på kontrollpunkten har försämrats något överlag, men man ligger kvar på samma nivå (3) som föregående år.

Skattningen visar att det fortsatt föreligger behov av arbete inom ramen för kontrollpunkten. Bolaget behöver fortsatt bedöma om konsekvensbedömningar bör genomföras och i förekommande fall genomföra dem innan personuppgiftsbehandlingen påbörjas. Bolaget behöver även rutiner för att uppdatera konsekvensbedömningar vid förändringar i behandlingen, för att säkerställa beslutsmandat vid beslut kopplade till konsekvensbedömning, följa upp de åtgärder som enligt konsekvensbedömningen behöver vidtas för att behandlingen ska kunna inledas och för att inhämta de registrerades rättigheter när det anses lämpligt.

Skattningen visar dock också på positiv utveckling eftersom det anges att bolaget alltid inhämtar råd från dataskyddsombudet i samband med att en konsekvensbedömning genomförs samt att bolaget förbättrats avseende pågående arbete med konsekvensbedömningar för behandlingar där hög risk föreligger. I sammanhanget vill dataskyddsombudet lyfta att det inte är valbart att inhämta råd från dataskyddsombudet i samband med att en konsekvensbedömning genomförs. Detta är en skyldighet för den personuppgiftsansvarige i enlighet med artikel 35.2 GDPR. Konsekvensbedömningar som genomförts utan avstämning med dataskyddsombudet anses därför inte som färdigställda.

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:

Bolagets skattning på denna kontrollpunkt ligger kvar på samma nivå som föregående år. Resultatet indikerar att det förekommer risker som bör åtgärdas, men som ej bedöms vara brådskande, omfattande eller allvarliga. Resultatet ligger mycket nära nivå 4 och bolaget verkar enligt skattningen ha 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 de kravställer att det finns en anpassning till inbyggt dataskydd och dataskydd som standard vid upphandling av nya system/tjänster.

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:

Bolagets skattning på denna kontrollpunkt ligger kvar på samma nivå som föregående år (4), vilket indikerar att det inte föreligger några direkta risker av betydelse. Enligt skattningen behöver bolaget dock arbeta med att följa upp och kontrollera att användningen av system och tjänster och digitala verktyg används på avsätt vis, samt säkerställa att dataskyddsperspektivet finns med vid införande och användande av kostnadsfria tjänster såsom gratisappar och sociala medier.

Bolaget har skattat sig högt avseende användningen av cookies och informationen om dessa till de registrerade. Vid avstämning med bolaget framgår att bolaget helt avbrutit sin användning av cookies. Då det fortsatt finns information om bolagets användning av cookies i bolagets integritetspolicy bör bolaget ändra denna så den överensstämmer med vad som faktiskt sker. Dataskyddsombudet har inte kunnat kontrollera bolagets cookies då de verktyg som finns tillgängliga för detta inte kan läsa av bolagets hemsida på grund av för många omdirigeringar.
Dataskyddsombudet rekommenderar därför att bolaget säkerställer att all cookieanvändning är borttagen samt att det inte föreligger risk för överföring av personuppgifter till tredjeland på grund av tredjepartsförfrågningar.
Dataskyddsombudet lyfter detta då det vid kontroll av dotterbolagens hemsidor i flera fall föreligger sådan risk.

Avseende sociala medier anger bolaget att de använder plattformen LinkedIn, men att det utförts analys av användningen efter att Schrems II-domen kom.

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 utifrån den praxis som finns tillgänglig. Även om dataskyddsombudet anser det positivt att bolaget har genomfört en analys av användningen, bör bolaget vidta ytterligare åtgärder för att följsamhet mot förordningen ska kunna säkerställas vid användningen av LinkedIn.

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:

Bolagets skattning på denna kontrollpunkt ligger kvar på samma nivå som föregående år (3). Resultatet indikerar att det förekommer risker som bör åtgärdas, men som ej bedöms vara brådskande, omfattande eller allvarliga. Resultatet ligger mycket nära nivå 4 och bolaget verkar enligt skattningen ha relativt god koll på hanteringen av de registrerades rättigheter. Enligt skattningen behöver bolaget dock säkerställa att det finns en process för att hitta och få tillgång till efterfrågad information vid en begäran om registerutdrag. Om den rättsliga grunden samtycke används för någon av bolagets behandlingar behöver det även finnas rutiner för att hantera ett tillbakadragande av samtycket från den registrerade (detta är en rättighet som den registrerade har).

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 rekommendationerna under följande kontrollpunkter.

- Kontrollpunkt 5: Övergripande strategi för dataskydd
- Kontrollpunkt 6: Utbildning
- Kontrollpunkt 8: Mejl- och dokumenthantering
- Kontrollpunkt 9: Konsekvensbedömning/samråd

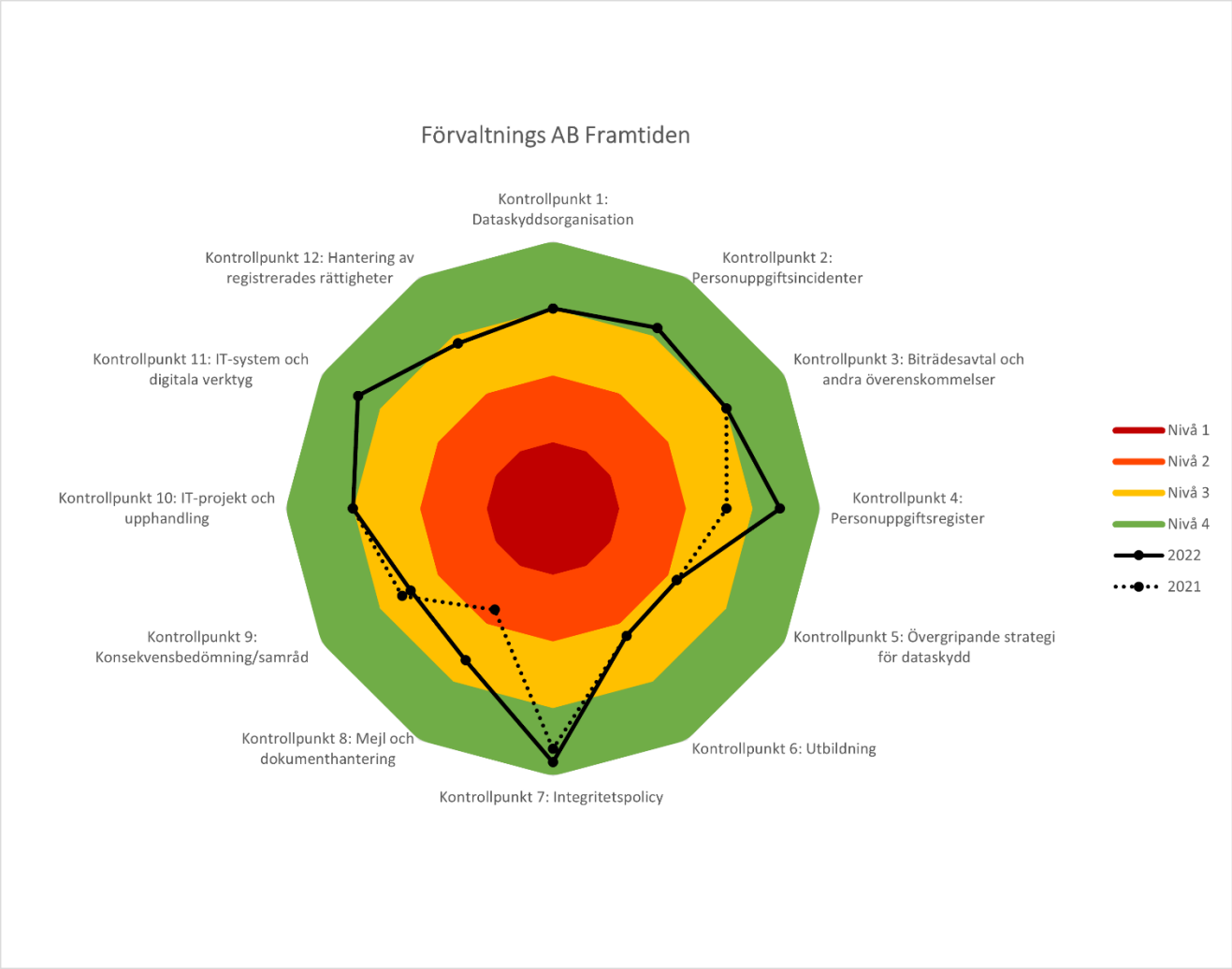
3 Bilagor

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 genomförts i två delar där del ett har bestått av ett generellt frågeutskick samt begäran om kopior på den information som ges till registrerade. Del två har bestått av ett kompletterande frågeutskick. Den information som samlas i ett dokument och tillhandahålls registrerade kan ha olika namn. Förvaltnings AB Framtiden kallar inte sina dokument för policy, men dataskyddsombudet använder detta ord genomgående i kontrollen av förståelseskäl.

lakttagelser 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.

Dataskyddsombudets rekommendationer

Generellt

Förvaltnings AB Framtiden har till dataskyddsombudet skickat in dokument i form av den externa integritetspolicyn, information om personuppgiftsbehandling till anställda som lämnas i samband med anställningsavtal samt information om personuppgiftsbehandling till anställda som finns i bolagets personalhandbok.

Information som ska tillhandahållas

Vilken information som ska ges till de registrerade beror på hur den personuppgiftsansvarige har samlat in personuppgifterna. Om personuppgifterna kommer direkt från den registrerade behöver det t.ex. inte lämnas information om vilka kategorier av personuppgifter som behandlingen gäller vilket det annars behöver informeras om när uppgifter kommer från någon annan än den registrerade själv.

Aktuella behandlingar, ändamål och rättslig grund

Förvaltnings AB Framtidens externa integritetspolicy inleds med att redogöra för vilka registrerade som policyn riktar sig till, nämligen ”intressenter”, ”leverantör eller affärspartner” och ”webbplatsbesökare”. Informationen i policyn är sedan uppdelad utifrån dessa kategorier och för respektive kategori framgår vid vilka tillfällen som bolaget kan komma att samla in personuppgifter om en registrerad och vad som gäller avseende ändamål och rättslig grund. Bolaget kompletterar även med information om två ytterligare situationer som bolaget kan komma att behandla personuppgifter – nämligen vid handläggning av rättsliga anspråk och vid åtgärder för att säkerställa säkerhet och skydd för bolagets medarbetare. Majoriteten av behandlingarna baseras på den rättsliga grunden berättigat intresse/intresseavvägning enligt art. 6.1 f GDPR, men ett par baseras på den rättsliga grunden avtal enligt art. 6.1 b GDPR.

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 anser dataskyddsombudet att bolaget gör. Av artikel 29-gruppens vägledning om öppenhet, framgår dock 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 intresseavvägningsbedömningen i integritetspolicyn.

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

Avseende den information som lämnas till anställda i samband med anställningsavtalet framgår när och för vilka ändamål som behandling av personuppgifter aktualiseras. Däremot vore det bra om det förtydligades vilken rättslig grund som avses, även om det går att göra vissa tolkningar om man har kunskaper om dataskyddsförordningen.

Lagring

I den externa integritetspolicyn 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 bolagets dokumenthanteringsplan fastställer.

Liknande generell information framgår i den information som lämnas internt till anställda (även om det specificeras ytterligare lite grann när det kommer till gallring av personuppgifter avseende anställningar som upphör).

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. Med hänsyn till att såväl den externa som den interna (till anställda) integritetspolicyn inte innehåller särskilt många behandlingar, bör det inte vara omöjligt för bolaget att tydligare ange lagringstid för respektive behandling. Dataskyddsombudet rekommenderar därför att dessa kompletteras med denna information för respektive behandling.[3]

Kategorier av personuppgifter

Avseende den externa integritetspolicyn noterar dataskyddsombudet att all insamling av personuppgifter som bolaget gör, inte sker direkt via den registrerade. Detta innebär, som anges ovan, att bolaget i de fall som personuppgifterna inte samlas in av den registrerade, behöver ange vilka kategorier av personuppgifter som bolaget behandlar och var uppgifterna kommer ifrån. Avseende kontaktuppgifter till anhöriga till personer som är anställda på bolaget, anges såväl vem personuppgifterna samlas in ifrån, som att det är just kontaktuppgifter som avses (dock inte i vilken form). Dataskyddsombudet rekommenderar att bolaget säkerställer att samtliga behandlingar, där personuppgifterna inte samlas in direkt från den registrerade, kompletteras med information om kategorier av personuppgifter och var personuppgifterna kommer ifrån.

[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).

Den information som lämnas till anställda innehåller uppgift om vilka kategorier av personuppgifter.

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 externa integritetspolicy 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.

Informationen till anställda är bättre utformad än den externa policyn när det kommer till de registrerades rättigheter. Däremot anges att den registrerade kan kontakta dataskyddsombudet om denna ville utnyttja sin rätt till registerutdrag. Detta är en felaktig skrivning då detta ska hanteras inom bolaget och inte är en uppgift som dataskyddsombudet ansvarar för. Dataskyddsombudet har inte heller tillgång till bolagets system och liknande för att kunna sammanställa den information som krävs för ett registerutdrag.

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.

Information om tredjelandsöverföring saknas helt i den information som lämnas till anställda, vilket dataskyddsombudet rekommenderar att bolaget åtgärdar.

Övrigt

Slutligen vill dataskyddsombudet lyfta att det saknas behandlingar i åtminstone den externa integritetspolicyn. Detta framgår av bolagets svar på frågan om integritetspolicyn omfattar information om samtliga personuppgiftsbehandlingar som personuppgiftsansvarig utför och är skyldiga att informera om. På fråga om information om de behandlingar som saknas lämnas på annat vis och om inte, varför så inte sker, har angetts att bolaget kontinuerligt arbetar med att identifiera nya och tidigare okända personuppgiftsbehandlingar samt att även om bolaget anser sig ha täckt in merparten av

[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).

de nuvarande behandlingarna i bolagets information till de registrerade kan det inte uteslutas att det finns behov av uppdateringar. 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 på annat vis.

Det kan vara okej att inte ha en heltäckande integritetspolicy. I de fall en personuppgiftsansvarig har väldigt många personuppgiftsbehandlingar så kan det till och med vara så att det inte är lämpligt att samla alla dessa i en integritetspolicy. En förutsättning för att detta ska vara okej är dock att all information som ska lämnas enligt art. 13-14 GDPR, lämnas till de registrerade på annat vis. Bolaget har inte angett att så sker, varför dataskyddsombudet rekommenderar att bolaget antingen uppdaterar sin integritetspolicy så att den är heltäckande eller säkerställer att information lämnas till de registrerade på annat vis. Om fler behandlingar läggs till i integritetspolicyn bör bolaget utveckla tillämpningen av en skiktad metod där den enskilde, beroende vem denne är, snabbt kan finna den information som är relevant för denne.[5]

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 informationen.

Förvaltnings AB Framtidens externa integritetspolicy finns tillgänglig på bolagets hemsida. Redan på förstasidan uppmärksammas den registrerade på var denne kan läsa den fullständiga integritetspolicyn och behöver enbart klicka två gånger 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". Bolaget uppmanar även sina medarbetare att länka till integritetspolicyn i sin e-postsignatur. Dataskyddsombudet anser att det är positivt att den registrerade får information om personuppgiftsbehandlingen vid första kontakt med bolaget.

Informationen till anställda lämnas i samband med att den anställde får del av och skriver under sitt anställningsavtal och finns dessutom tillgänglig i personalhandboken, vilket dataskyddsombudet anser är ett klokt tillvägagångssätt.

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 rekommenderar att bolaget ser över både den interna och den externa policyn i de delar då bestämningsord förekommer, bland annat när det kommer till skrivningarna om när personuppgifter kan komma att behandlas, för vilka ändamål de

[5] Artikel 29-arbetsgruppen, *Riktlinjer om öppenhet enligt förordning (EU) 2016/679*, WP260rev.01, senast granskade och antagna den 11 april 2018, s. 19ff.

behandlas och med vilka personuppgifter delas, då där förekommer ord som ”kan” exempelvis.

Rutin för uppdatering

Bolaget anger att översyn och uppdatering av dokumenten sker årligen och utförs av bolagets utsedda dataskyddskontakt samt HR-chef i samråd med utsedd dataskyddskontakt när det kommer till behandling av anställdas personuppgifter. Dataskyddsombudet ser positivt på denna rutin.

Sammanfattade 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.

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.

Fördjupad kontroll 2022

Kontrollpunkt 7: Integritetspolicy (del 2)

Uppföljande frågor att besvara om Framtidens integritetspolicy samt informationen tillhandahållen genom 1) ”Bilaga till anställningsavtal – Så här behandlar vi dina personuppgifter” och 2) ”Personalhandbok för Förvaltnings AB Framtiden”.

1. Omfattar de integritetspolicys/den information som har skickats in/hänvisats till **samtliga** personuppgiftsbehandlingar som personuppgiftsansvarig utför och är skyldiga att informera om?
2. Om de integritetspolicys/den information som skickats in/hänvisats till inte är heltäckande, får de registrerade information om behandlingen/behandlingarna på annat sätt?
    a. Om ja, beskriv hur och ange den information som ges.
    b. Om nej, ange förklaring till varför information inte ges.

Obs! Det är mycket viktigt att frågorna besvaras av eller i samråd med rätt befattningar inom förvaltningen för att resultatet ska bli korrekt. Säkerställ även en lämplig förankring av svaren inom organisationen innan de översänds till dataskyddsombudet.

Svar ska ha inkommit till dataskyddsombudet **senast den 8 juli 2022.** Dataskyddsombudet kan komma att ställa kompletterande frågor i samband med sammanställande av rapporten.

Har ni frågor, kontakta ert huvudansvariga dataskyddsombud.