Störningsjouren

Störningsjouren i Göteborg AB

Styrelsehandling nr 13
Datum: 2023-01-20
Diarienummer: SJ2023-0001

Handläggare: Louise Ternlind

Telefon: 031-773 83 82
E-post: louise.ternlind@storningsjouren.goteborg.se

Årsrapport för dataskyddsarbetet 2022

Informationsärende

Styrelsen Störningsjouren i Göteborg AB

Dataskyddsombudets information till styrelsen samt Årsrapport för dataskyddsarbetet 2022 föreslås antecknas.

Ärendet

Dataskyddsombudets uppgift att övervaka den personuppgiftsansvariges efterlevnad av dataskyddsförordningen 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. De årliga kontrollerna består av tolv fasta kontrollpunkter och en fördjupad kontroll.

För dataskyddsombudet är kontrollarbetet ett sätt att få en bild av vilka risker och/eller brister som eventuellt föreligger inom en verksamhet. Genom kontroller får verksamheten och dataskyddsombudet en nulägesbild av verksamhetens dataskyddsarbete. Kontrollerna ska ses som vägledning och verktyg för verksamhetens fortsatta arbete med dataskydd. Det är sedan upp till varje verksamhet att besluta om hur det interna dataskyddsarbetet ska utformas. I det arbetet är dataskyddsombudet behjälplig med rådgivning utifrån verksamhetens behov och identifierade risker.

Fördjupad kontroll av behörighetsstyrning 2022

Den fördjupade kontrollen har utförts för bolagets behörighetsstyrning i ärendehanteringssystemet Lime.

Bedömning ur ekonomisk dimension

Genom ett dataskyddsarbete som utgår från risker för registrerades fri- och rättigheter minskas även risken för negativa konsekvenser för verksamheten. Konsekvenser kan omfatta bland annat skadestånd, sanktionsavgifter, försämrat varumärke eller minskad tillit för verksamheten.

Bedömning ur ekologisk dimension

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

Bedömning ur social dimension

Det systematiska dataskyddsarbetet och dataskyddsombudets kontrollplan syftar till att säkerställa att verksamheten skyddar enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter, privatliv och personlig integritet.

Samverkan

Ärendet anses inte vara föremål för samverkan.

Bilagor

1. Årsrapport för dataskyddsarbetet 2022

Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Störningsjouren

2022-12-23

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 behörighetsstyrning 2022

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

Dataskyddsombudets övergripande intryck efter kontrollen är att bolaget har god koll på sin behörighetsstyrning i stort och att bolaget genomför flertalet såväl tekniska som organisatoriska åtgärder för att förhindra obehörig åtkomst. I rapporten har dataskyddsombudet haft en anmärkning och har därför lämnat en rekommendation till verksamheten för att ytterligare förbättra sitt arbete.

Rekommendationen avser att bolaget bör säkerställa att det finns en tydlig rutin/instruktion för loggkontroll i systemet. Rutinen bör vara heltäckande och det

bör framgå vad som utgör misstanke om oegentlighet samt när och hur kontroll ska ske utifrån en sådan misstanke.

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 Störningsjourens dataskyddsarbete 2022

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

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

2.4.1 Kontrollpunkt 1: Dataskyddsorganisation

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

Dataskyddsombudets kommentarer:

Bolaget har skattat sig likadant på denna kontrollpunkt som föregående år. Samtliga påståenden har besvarats med alternativet *Ja, det stämmer helt*, vilket innebär att bolaget anser sig ha mycket goda organisatoriska förutsättningar för att kunna bedriva ett effektivt och fungerande dataskyddsarbete. Skattningen indikerar att det inom ramen för kontrollpunkten inte föreligger några risker av betydelse och bolaget arbetar på ett systematiskt vis.

Höga skattningar på denna punkt innebär att det finns tydliga mandat och rapporteringsvägar, att organisationen har de resurser som den behöver, att dataskydd är en naturlig och integrerad del i det dagliga arbetet i alla delar av verksamheten osv. Dataskyddsombudet har inte fått några indikationer som medför en annan bedömning än den som bolaget gör, men har inte heller kontrollerat dataskyddsorganisationen särskilt. Dataskyddsombudet rekommenderar att bolaget fortsätter arbetet med dataskyddsorganisationen för att hålla den effektiv och ändamålsenlig.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Dataskyddsombudets kommentarer:

Bolagets skattning är något högre detta år än föregående. Precis som föregående år hamnar bolagets skattning på nivå 4, vilket indikerar att det inom ramen för kontrollpunkten inte föreligger några risker av betydelse och bolaget arbetar på ett systematiskt vis.

I och med att bolaget har svarat att samtliga påståenden stämmer helt, anser bolaget att arbetet med incidenthantering fungerar het utan anmärkning.

Dataskyddsombudet har under 2022 fått information om tre incidenter. Bolaget uppger också att fler har skett, men att de har varit av mycket ringa allvarlighetsgrad och inte medfört risk för den registrerade.

Likt under ovanstående kontrollpunkt har dataskyddsombudet inte anledning att göra en bedömning, men har inte heller kontrollerat bolagets rutiner för personuppgiftsincidenter särskilt i en fördjupad kontroll.

2.4.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

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

Dataskyddsombudets kommentarer:

Bolagets skattning är marginellt lägre detta år än föregående. Precis som föregående år hamnar bolagets skattning på nivå 4, vilket indikerar att det inom ramen för kontrollpunkten inte föreligger några risker av betydelse och att bolaget arbetar på ett systematiskt vis.

Den marginella försämringen består i att bolaget har angett *Ja, det stämmer bra*, istället för *Ja, det stämmer helt*, när det kommer till att bedöma om andra överenskommelser/avtal (än personuppgiftsbiträdesavtal) behöver upprättas avseende gemensam/annan delad hantering av personuppgifter när en leverantör anlitas eller när samarbeten sker (både externt och inom Göteborgs Stad). Dataskyddsombudet instämmer i att frågan om hur personuppgiftsansvar ska fördelas är svår, kanske särskilt inom ramen för de samarbeten och fördelning av uppdrag inom Göteborgs Stad. Trots detta utläser dataskyddsombudet att bolaget anser sig ha relativt god koll på detta, vilket såklart är positivt. Med hänsyn till svårigheterna anser dataskyddsombudet att årets skattning sannolikt är mer rättvisande än föregående år.

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 skattat sig likadant på denna kontrollpunkt som föregående år. Samtliga påståenden utom ett har besvarats med alternativet *Ja, det stämmer helt*,

vilket innebär att bolaget anser sig bedriva ett mycket gott arbete kopplat till personuppgiftsregistret och man hamnar återigen på nivå 4.

Inte heller på denna kontrollpunkt har dataskyddsombudet anledning att ifrågasätta bolagets skattning, men har inte heller kontrollerat bolagets rutiner kring registret inom ramen för en fördjupad kontroll. Bolagets skattning innebär att registret innehåller bolagets samtliga behandlingar, att behandlingarna innehåller den information som krävs enligt artikel 30 GDPR och att ansvaret för uppdatering av registret är tydlig fördelat. Det anges också att registret uppdateras kontinuerligt samt att bolagets dataskyddsorganisation använder registret som en del i det löpande dataskyddsarbetet.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Bolaget har besvarat samtliga påståenden utom ett med alternativet *Ja, det stämmer helt*, vilket innebär att bolaget anser sig bedriva ett mycket gott arbete kopplat till övergripande strategi för dataskydd och man hamnar återigen på nivå 4.

En av frågorna har besvarats med alternativet *Nej, det stämmer inte bra,* vilket innebär att bolaget sannolikt behöver arbeta med denna fråga. Frågan avser om bolaget säkerställer att det finns rutiner för att efterleva GDPR:s krav vid olika sammankomster och möten, såväl digitala som fysiska. Vid avstämning med bolaget framgår dock att det genomförs en del åtgärder och finns rutiner kopplat till digitala möten via Teams. Det finns också rutiner för fotografering, vid fysiska sammankomster (utifrån hur dataskyddsombudet uppfattar det). Bolaget anger dock att de behöver rutiner för att informera om personuppgiftsbehandling inför och under evenemang och digitala sammankomster. Detta instämmer dataskyddsombudet i.

I övrigt har dataskyddsombudet inget att invända mot bolagets skattning. Det är positivt att bolaget har en strategi för sitt dataskyddsarbete, en policy för informationssäkerhet, aktivt och medvetet arbetar riskbaserat med dataskyddsfrågor, har klassificerat samtliga av sina behandlingar och utför interna kontroller.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

Bolagets skattning detta år gör att bolaget ligger kvar på nivå 4. I och med att samtliga påståenden har besvarats med alternativet *Ja, det stämmer helt*, har bolaget till och med gjort en marginell förbättring jämfört med föregående år.

Bolagets svar på enkäten i denna punkt indikerar att medarbetarna regelbundet utbildas inom dataskydd och att den allmänna kunskapsnivån ger goda förutsättningar för att bedriva dataskyddsarbetet. Dataskyddsombudet har inte fått några indikationer som medför en annan bedömning och det förefaller stämma med skattningen på övriga kontrollpunkter. Höga skattningar på denna punkt innebär exempelvis att i princip alla anställda korrekt ska kunna identifiera en personuppgiftsincident, att vissa roller ska veta hur och när en konsekvensbedömning ska göras och att ansvariga ska ha koll på tillvägagångssätt när registrerade utövar sina rättigheter i förhållande till bolaget. Såvida detta inte stämmer in på bolaget bör arbetet ses över på denna punkt.

2.4.7 Kontrollpunkt 7: Integritetspolicy

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

Dataskyddsombudets kommentarer:

Bolagets skattning detta år ligger fortsatt på en hög nivå (4), men kontrollpunktens medelvärde har sjunkit något jämfört med tidigare år. Bolaget anger detta år att det *stämmer bra* istället för att det *stämmer helt* att verksamhetens integritetspolicy uppfyller kraven på information enligt GDPR.

Efter att ha sett över bolagets externa integritetspolicy på en övergripande nivå anser dataskyddsombudet att årets skattning är mer korrekt än föregående års skattning och att det finns skäl att se till att utövandet av informationsplikten förbättras. För att informationsplikten ska anses vara uppfylld ska det bland annat tydligt framgå ändamål och rättslig grund, hur länge uppgifterna lagras eller vara väldigt tydligt för den registrerade hur lagringstiden bedöms, om personuppgifterna inte samlas in direkt från den registrerade så ska kategorierna av personuppgifter framgå, mottagare ska framgå och så även tydlighet kring tredjelandsöverföring och vad som gäller när det kommer till de registrerades rättigheter.

Även om mycket av ovanstående finns med i policyn så bör bolaget se över exempelvis hur man informerar om lagringstid. Det kan vara okej att hänvisa till kriterierna för hur lagringstiden bedöms om exakt lagringstid inte anges. Den registrerade ska dock, utifrån sin egen situation, i så fall kunna bedöma lagringstiden utifrån kriterierna. Dataskyddsombudet bedömer det som tveksamt om hänvisning till dokumenthanteringsplan som den registrerade inte har tillgång till kan anses tillräckligt. Bolaget bör även se över tydligheten i vissa angivningar

av rättslig grund, särskilt när det anges att behandlingen utförs i enlighet med en rättslig förpliktelse, då det i flera fall är något otydligt. En ordentlig översyn av helheten bör genomföras kontinuerligt, inte minst med hänsyn till den praxis som nu finns kopplat till informationsplikten och som kontinuerligt fortsätter att komma.

2.4.8 Kontrollpunkt 8: E-post och dokumenthantering

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

Dataskyddsombudets kommentarer:

Bolaget ligger enligt sin skattning kvar på nivå 4, men med en marginell försämring av medelvärdet. Enligt skattningen har bolaget koll på sin hantering av personuppgifter i e-post och man har fungerande rutin för gallring och övrig dokumenthantering.

Enligt skattningen är ca 75 % av bolagets personuppgiftsbehandlingar klassificerade i enlighet med stadens styrande dokument och ca 75 % av dessa är kontrollerade för aktualitet det senaste året. Detta är mycket positivt, men bör fortsätta att arbetas med för att uppnå 100 %.

Dataskyddsombudet har ingen anledning att i övrigt göra en annan bedömning än den som bolaget gör, men har heller ännu inte kontrollerat rutinerna inom ramen för en fördjupad kontroll.

2.4.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

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

Dataskyddsombudets kommentarer:

Bolagets skattning är marginellt högre detta år än föregående. Precis som föregående år hamnar bolagets skattning på nivå 4, vilket indikerar att det inom ramen för kontrollpunkten inte föreligger några risker av betydelse och bolaget arbetar på ett systematiskt vis med konsekvensbedömningar.

Bolagets skattning innebär att samtliga efterfrågade rutiner finns på plats; för att identifiera behandlingar med hög risk, inhämta dataskyddsombudets synpunkter

efter utförd tröskelanalys och konsekvensbedömning, genomföra och dokumentera konsekvensbedömningar innan behandlingarna påbörjas, uppdatera konsekvensbedömningar vid förändringar i behandlingen, bedöma risker för de registrerade och för hur beslut inom ramen för konsekvensbedömningen ska fattas och dokumenteras. Bolaget rekommenderas att arbeta vidare med att bedöma om personuppgiftsbehandlingarna som utförs behöver konsekvensbedömas. Även om 75 % av behandlingarna är bedömda, vilket får anses vara en relativt hög andel, bör målsättningen vara att bedöma samtliga. Bolaget anger vidare att konsekvensbedömningar har utförts för cirka 75 % av de behandlingar där det bedöms behövas. Även detta bör bolaget alltså fortsätta arbeta med.

Dataskyddsombudet har involverats i konsekvensbedömningar som berör enbart störningsjouren, men också koncerngemensamma behandlingar, vilka ofta är väl utförda.

2.4.10 Kontrollpunkt 10: IT-projekt och upphandling

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

Dataskyddsombudets kommentarer:

Bolaget ligger kvar på samma nivå (4) som föregående år, enligt sin skattning. Detta innebär alltså att inga risker av betydelse inom ramen för kontrollpunkten och man anser sig arbeta systematiskt med dataskydd kopplat till IT-projekt och upphandling.

Enligt skattningen finns dataskyddsperspektivet med i arbetet med nya IT- och digitaliseringslösningar samt vid utvecklingen av redan befintliga system och tjänster. Vid upphandlingen av nya system/tjänster så tas anpassning till inbyggt dataskydd och dataskydd som standard med i kravställningen. Man har också rutin för att dataskyddsombudet involveras från start i dessa processer.

Dataskyddsombudet har blivit involverat i frågor kring tredjelandsöverföring i samband med avrop från ramavtal och har även blivit involverat i konsekvensbedömningar som berör nya IT-system. Dataskyddsombudet har därför ingen anledning att på det stora hela göra en annan bedömning än den som bolaget har gjort.

2.4.11 Kontrollpunkt 11: IT-system och digitala verktyg

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

Dataskyddsombudets kommentarer:

Bolaget har skattat sitt arbete inom ramen för denna kontrollpunkt marginellt lägre än föregående år, men ligger ändå kvar på nivå 4. Bolagets skattning antyder alltså att man arbetar systematiskt med dataskydd kopplat till IT-system och digitala tjänster och att inga risker av betydelse lär finnas inom ramen för kontrollpunkten.

Bolaget har enligt skattningen, god koll på sin behörighetsstyrning, man har dokumentation över samtliga IT-system och digitala tjänster och sina kommunikationskanaler.

Bolaget har också skattat sig högt på påståendet om att användning av cookies på webbsidor följer kraven i GDPR och att de registrerade får information om behandlingen via verksamhetens integritetspolicy. I bolaget policy anges att enbart nödvändiga cookies för hemsidans funktionalitet samlas in. Nödvändiga cookies kräver inget samtycke enligt lagen för elektronisk kommunikation (2022:482) för att få samlas in (tidigare SFS 2003:389). Det är därför bra att bolaget informerar om att enbart nödvändiga cookies samlas in, men att man inte efterfrågar besöker samtycke.

Vid kontroll av bolagets hemsida framgår att tredjepartsförfrågningar som skulle kunna innebära risk för tredjelandsöverföring förekommer. Bolaget bör utreda detta för att säkerställa att användningen inte bryter mot bestämmelserna i GDPR.

Avseende sociala medier anger bolaget att bolaget har börjat använda plattformen LinkedIn, men att man säkerställer att plattformen används på ett sätt som medför så lite risker som möjligt för de registrerade och för att göra så lite avsteg som möjligt mot Schrems II-domen.

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

Dataskyddsombudets rekommendationer är att upphöra med att behandla personuppgifter i sociala medier i de fall följsamhet mot GDPR inte kan säkerställas. I detta utgår dataskyddsombudet helt ifrån bestämmelserna i GDPR och i den praxis som finns tillgänglig. Även om dataskyddsombudet anser det positivt att bolaget försöker använda plattformen så säkert som möjligt, bör bolaget fortsatt utreda om användningen kan ske på ett sätt som inte strider emot GDPR.

2.4.12 Kontrollpunkt 12: Hantering av registrerades rättigheter

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

Dataskyddsombudets kommentarer:

Bolaget ligger kvar på nivå 4 precis som förra året, men har också gjort en marginell förbättring av medelvärdet eftersom man nu har besvarat samtliga påståendet med *Ja, det stämmer helt.*

Dataskyddsombudet har ingen anledning att göra en annan bedömning än bolaget, men vill likt andra kontrollpunkter som har besvarats på samma sätt, lyfta att någon fördjupad kontroll av bolagets rutiner för hanteringen av de registrerades rättigheter inte har genomförts. Dataskyddsombudet har inte heller involverats i några frågor kopplade till de registrerades rättigheter under 2022.

2.5 Sammanfattande rekommendationer

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

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

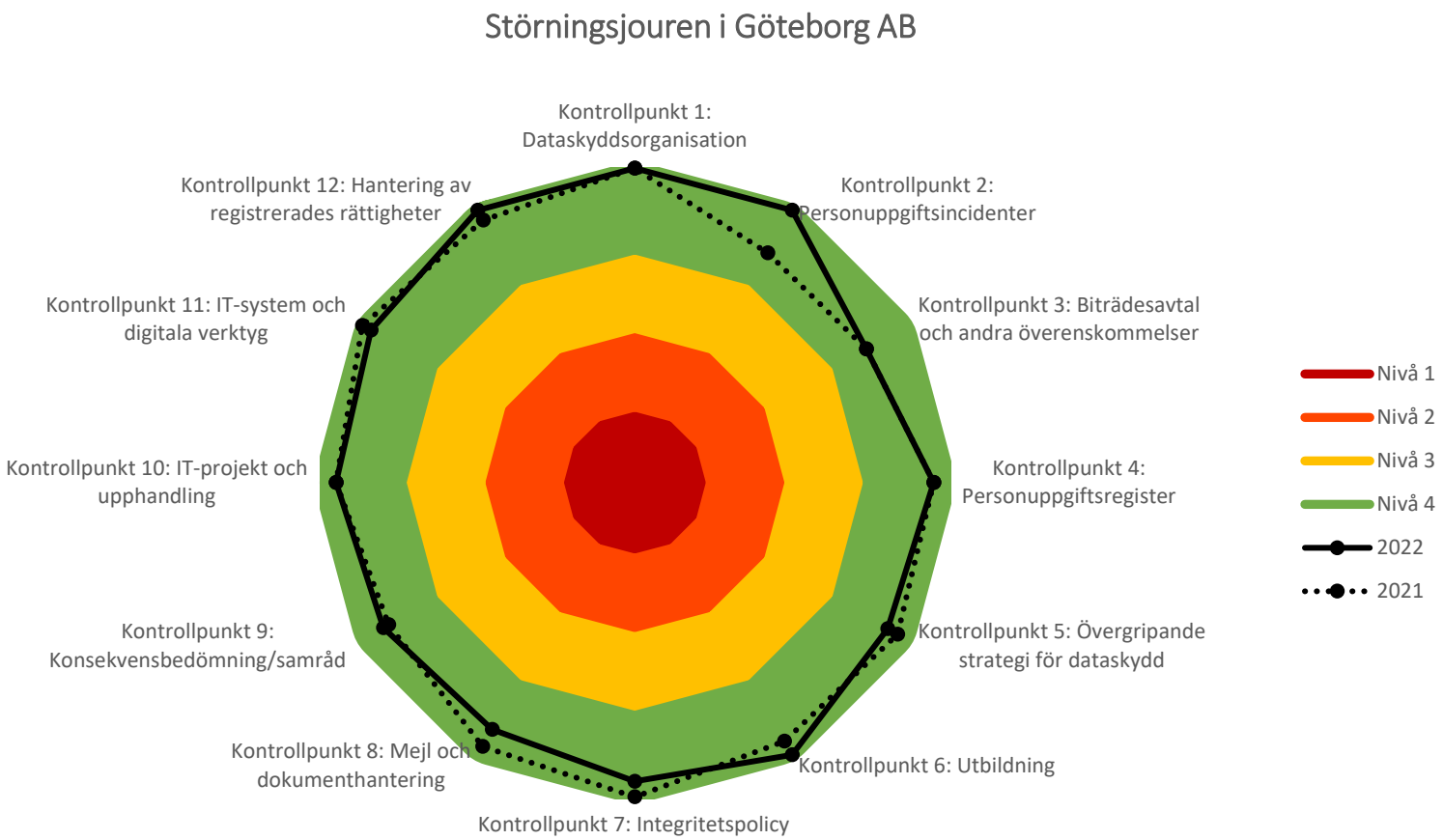
- Kontrollpunkt 7: Integritetspolicy
- Kontrollpunkt 9: Konsekvensbedömning/samråd
- Kontrollpunkt 11: IT-system och digitala verktyg

3 Bilagor

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

Bilaga 2: Fördjupad kontroll 2022 - Behörighetsstyrning

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



Fördjupad kontroll

Kontrollpunkt 11: Behörighetsstyrning Störningsjouren

Bakgrund

Den fördjupade kontrollen av behörighetsstyrning syftar till att se om verksamhetens hantering av personuppgifter är säker och korrekt utifrån både tekniska och organisatoriska åtgärder. Med utgångspunkt i artikel 32.2 GDPR har kontrollen granskat verksamhetens bedömning av lämplig säkerhetsnivå med hänsyn till risker i synnerhet från bland annat obehörig åtkomst till personuppgifter. Därför har fokus legat på behörighetsstyrning och hur det används för att begränsa vilka personuppgifter som medarbetarna får ta del av.

Kontrollen har genomförts i två delar, den första som ett generellt frågeutskick och den andra som ett kompletterande frågeutskick. I kontrollen ingick verksamhetens rutiner för tilldelning av behörigheter och åtkomster i ett särskilt utvalt IT-system, uppföljning av behörigheter samt användning av logg-/åtkomstkontroller.

Iakttagelser från kontrollen

En medarbetare i en verksamhet ska enbart ha tillgång till personuppgifter som är anpassade och begränsade till det som är nödvändigt för att medarbetaren ska kunna utföra sina arbetsuppgifter. För att säkerställa detta bör verksamheten ha rutiner för tilldelning av behörigheter, uppföljning av behörigheter samt hur användningen av logg-/åtkomstkontroller sker.

Kontrollen hos Störningsjouren har gjorts av systemet Lime. I systemet behandlas personuppgifter i form av namn, adress, telefonnummer, lägenhetsnummer, personnummer, uppgifter om hyresbetalningar/betalningsförsummelser, uppgift om boendeform och uppgift om störning i boende. Även uppgift om brottslig verksamhet och hälsouppgifter kan förekomma. Ytterligare personuppgifter kan komma att behandlas om de lämnas in i ett ärende och behöver hanteras i enlighet med bestämmelserna om allmänna handlingar. Bolaget har angett att de inte alltid kan styra vilka uppgifter som inkommer. Dataskyddsombudet har förståelse för detta och inser att full kontroll kanske aldrig kan åstadkommas. Däremot bör bolaget säkerställa att man har gjort vad man kan för att förhindra att personuppgifter som inte är nödvändiga behandlas, genom att exempelvis ha tydliga anvisningar för vad som ska lämnas in i ett ärende och inte. Det är positivt att bolagets handläggare, enligt inkomna svar, har goda kunskaper om nödvändighet av personuppgifter i förhållande till ändamål.

Enligt svaren från bolaget förekommer det personuppgifter tillhörande ca 100 000–200 000 kontraktsinnehavare, samt 66 medarbetare på störningsjouren, ett mindre antal konsulter och ca 570 kontaktpersoner (förvaltare, fastighetsägare). Exakt antal varierar.

Behörighetsstruktur och roller i system

Dataskyddsombudet tolkar bolagets svar som att det finns det sex olika roller i Lime som används av bolaget. Dessa utgörs av rollerna trygghetskonsulent natt, trygghetskonsulent dag, jurist för oriktiga hyresförhållanden, fastighetsjour och kontaktperson, samt en roll

som kallas ledning/verksamhetsstöd/konsult. Bolaget har tillhandahållit en beskrivning av vad de olika rollerna använder Lime till och vilka typer av ärenden de är inne i. Användandet varierar mellan bland annat rapportering kring tillsynsärenden, uppsöka namn och adress till hyresgäster och administration av väktarrapporter. Vissa använder enbart kund- och avtalsregistret och kontaktpersoner har inte tillgång till system utan enbart till den rapportportal där rapporter genererade ur Lime tillhandahålls. De sex olika rollerna kan ha någon av de olika behörigheterna *ägare*, *grupp* eller *övriga*. Behörigheterna innebär följande.

Ägare	Användare som skapat ärende (objekt) får behörighet ägare. Ägare har fördefinierad behörighet på respektive flik i ärendet.
Grupp	Användare kan tillhöra flera grupper men har bara en grupp som default. Ägarens grupp är fördefinierad utifrån roll och verksamhetsdel och har tilldelad behörighet baserat på detta.
Övriga	Fördefinierad behörighet till respektive flik i ärendet för personer utanför gruppen baserat på roll och verksamhetstillhörighet.

Tilldelning av och beslut om behörighet utifrån bedömning

Bolaget anger att VD och ledningsgrupp (verksamhetschefer) har definierat behörighetsbehoven för respektive verksamhetsområde utifrån premissen att anställda ska ha den åtkomst som krävs för att kunna utföra sina arbetsuppgifter. Kontaktpersoners (förvaltare, fastighetsägare) behörighet till rapportportalen beställs av ansvarig beställare på respektive förvaltande bolag. Deras behörigheter (enbart rapportportalen) styrs utifrån vilket bolag de arbetar i och vilket område.

Konsulter (från leverantör/Framtidens IT) tilldelas tidsbegränsade behörigheter vid behov.

Av Göteborgs Stads riktlinje för informationssäkerhet framgår det att det ska finnas dokumenterade regelverk och rutin för registrering och avregistrering av behörigheter och åtkomst och att denna ska vara formellt beslutad. Svaren från bolaget avseende hur tilldelning går till tyder på att det finns ett formellt tillvägagångssätt. Bolagets rutiner förefaller uppfylla kraven i stadens riktlinje och ansvarsskyldigheten i GDPR.

Uppföljning av behörighet

I svaret från bolaget anges att behörigheterna baseras på uppgift om avdelning och befattning i de anställdas AD-konto (katalogtjänst som innehåller uppgifter om användare). Kontroll av medarbetares behörighet gentemot AD-konto görs två gånger per år. Kontaktpersoners behörigheter kontrolleras löpande, men också genom en årlig genomgång av samtliga kontaktpersoner genom avstämning med beställningsansvarig hos respektive förvaltande bolag. Kontrollerna utförs av bolagets behörighetsadministratör/systemförvaltare för Lime.

Konsulters behörigheter är tidsbegränsade och har slutdatum 30 april eller 31 oktober. Uppföljning av behörigheterna och beslut om behörigheten ska förlängas eller inte sker både den 1 maj och 1 november varje år. Behörigheterna kan också begränsas till vissa timmar på dygnet.

Dataskyddsombudet har inget att invända mot ovanstående rutiner, utan de förefaller vara ändamålsenliga. Enligt svaren verkar bolaget arbeta systematiskt med uppföljning av

behörigheter och på så vis säkerställa att tillgång till personuppgifter inte innehas i onödan.

Åtkomstkontroll/kontroll av loggar

Bolaget uppger att bolagets behörighetsadministratör/systemförvaltare för Lime kan ta fram loggar över aktivitet i ärenden/objekt i systemet. Detta görs om misstänkt felaktigt nyttjande föreligger. På fråga om vem som ansvarar för loggarna anges att det är behörighetsadministratör/systemförvaltare. Dataskyddsombudet finner det positivt att det finns möjlighet till kontroll av loggar vid misstanke om felaktigt nyttjande. Däremot anser dataskyddsombudet att ansvaret för uttag och granskning av loggar vid misstanke om oegentligheter bör läggas ”högre upp” i organisationen, alltså att det finns en ansvarig chef för kontrollen. Vid avstämning med bolaget anges att så också sker. Enligt kompletterande information framgår att det alltid är bolagets VD eller verksamhetschef som gör en beställning av loggkontroll. Bolaget anger att beslut om detta ingår i ”chefsskapet” och den delegation som chefer har.

Att ha loggning och rutiner för att kontrollera dessa kan vara en viktig del av säkerheten i systemet för att säkerställa att information och uppgifter inte sprids till obehöriga. Sådana kontroller måste emellertid också ske på ett väl avvägt vis med hänsyn till den personliga integriteten så att anställda inte känner sig övervakade. Eftersom en kontroll kan utgöra en personuppgiftsbehandling måste den också ha ett tydligt och avgränsat ändamål.

Dataskyddsombudet anser att det är positivt att enbart en roll har tillgång till och möjlighet att ta fram loggar. Av bolagets svar framgår inte heller något som föranleder dataskyddsombudet att tro att kontroll av loggar sker utan behov. Eftersom det dock inte specificeras vad som kan föranleda misstanke om felaktigt nyttjande och en rutin för hur loggkontroll ska gå till, rekommenderar dataskyddsombudet att bolaget säkerställer att de har tydliga rutiner för när loggranskning aktualiseras, att det är tydligt vad som utgör misstanke om oegentlighet och förfarandet när en sådan misstanke uppstår. Att ta fram en tydlig rutin säkerställer också transparens och medvetandegör medarbetarna om vad, när och hur loggkontroller kan aktualiseras.

Vid avstämning med bolaget framgår att bolagets medarbetare är vana vid att arbeta med känslig information och att medarbetarna är medvetna om vad de får och inte får göra i systemet. Bolaget har också kompletterat med en riktlinje om jäv, vari framgår att det kan inledas utredning om en misstänkt jävssituation uppstår. Båda dessa omständigheter är såklart positiva. Däremot anser dataskyddsombudet att det inte helt täcker det behov som dataskyddsombudet uppmärksammat om tydlig skriftlig rutin/instruktion för loggkontroll enligt ovan.

Annan lagstiftning/bestämmelser (utöver dataskyddsförordningen) som påverkar behörighetstilldelningen

Störningsjouren har i sitt svar till dataskyddsombudet uppgett att offentlighets- och sekretesslagen, förvaltningslagen (avseende service och tillgänglighet), bestämmelser i avtal med kund, Göteborgs Stads riktlinje för informationssäkerhet och Göteborgs Stads regel för chefers informationssäkerhetsansvar har betydelse för bolagets behörighetstilldelning. Dataskyddsombudet har inget att invända eller tillägga till denna bedömning.

Andra åtgärder för att förhindra obehörig åtkomst

Bolaget har angett ett stort antal ytterligare åtgärder som tillämpas av bolaget och tillsammans med leverantören för att förhindra obehörig åtkomst, inklusive kryptering av datatrafik, lösenord och API-nycklar. All data, inklusive säkerhetskopior, lagras i krypterad form och i separata databaser i egna datahallar med åtkomstkontroll och så vidare. Utöver tekniska åtgärder använder bolaget också organisatoriska åtgärder såsom säkerställande av tillräckliga kunskaper hos personalen om korrekt och säker hantering av personuppgifter och uppgifter som omfattas av sekretess. Utbildning i Lime och i korrekt personuppgiftshantering tillhandahålls innan åtkomst ges och utbildning återkommer årligen. Man säkerställer också att enbart relevanta uppgifter finns i systemet och att man tillämpar såväl automatisk som manuell gallring för att säkerställa principerna om uppgiftsminimering och lagringsminimering i art. 5 GDPR.

Dataskyddsombudet bedömer att bolaget arbetar såväl systematisk som ändamålsenligt med åtgärder för att förhindra obehörig åtkomst och har inget att invända mot bolagets hantering i denna del.

Konsekvensbedömning och risker

Störningsjouren har utfört en konsekvensbedömning på personuppgiftsbehandlingarna i Lime. Konsekvensbedömningen är avstämd med dataskyddsombudet som har lämnat rekommendationer. Dataskyddsombudet tolkar bolagets svar som att konsekvensbedömningen kommer följas upp framöver, vilket dataskyddsombudet finner positivt.

Sammanfattade rekommendationer

- Bolaget rekommenderas säkerställa att det finns en tydlig rutin/instruktion för loggkontroll i systemet. Rutinen bör vara heltäckande och det bör framgå vad som utgör misstanke om oegentlighet samt när och hur kontroll ska ske utifrån en sådan misstanke.

Bilagor

1. Frågor och informationsutskick

Information om fördjupad kontroll 2022

Kontrollpunkt 11: Behörighetsstyrning

För att säkerställa säkerheten och en korrekt personuppgiftshantering inom en verksamhet behöver både tekniska och organisatoriska åtgärder vidtas. Exempel på tekniska säkerhetsåtgärder är att system utformas så att endast behöriga personer kan göra sökningar och att det finns behörighetskontrollsystem. En viktig och effektiv organisatorisk åtgärd i en verksamhet är behörighetsstyrning.

I artikel 32.2 i dataskyddsförordningen ställs krav på att den personuppgiftsansvarige i samband med bedömning av lämplig säkerhetsnivå ska ta särskild hänsyn till risker i synnerhet från bland annat obehörig åtkomst till personuppgifter. Obehörig är den som inte har legitim anledning att ta del av en handling eller uppgift i sin tjänsteutövning. Bestämmelser om sekretess utgör ofta men inte alltid en utgångspunkt för vilka uppgifter som någon får ta del av. Genom en ändamålsenlig behörighetsstyrning kan det säkerställas att ingen obehörig åtkomst sker inom verksamheten. Behörighetsstyrning sker genom att bland annat bedriva ett arbete med att avgöra hur stor tillgång till uppgifter i ett verksamhetssystem som en medarbetare med en viss funktion eller roll ska ha. Det är viktigt att behörigheterna är anpassade och begränsade till det som är nödvändigt och i enlighet med gällande rättslig reglering. Dessutom behöver behörigheterna löpande kontrolleras och följas upp samt att åtkomstkontroller genomförs. En felaktig eller bristfällig behörighetsstyrning kan leda till exempelvis inskränkningar av den enskildes integritet eller personuppgiftsincidenter.

Den fördjupade kontrollen avser undersöka hur behörighetsstyrning används för att begränsa vilka uppgifter som medarbetarna får ta del av. Verksamhetens rutiner för tilldelning av behörigheter och åtkomster i IT-system kommer att granskas. Kontrollen kommer även omfatta verksamhetens uppföljning av medarbetares behörigheter och åtkomst till personuppgifter i IT-system samt om logg-/åtkomstkontroller används för att upptäcka och motverka obehörig åtkomst.

Syftet med den fördjupade kontrollen är att undersöka om medarbetares tillgång till personuppgifter är anpassade och begränsade till det som är nödvändigt för att medarbetaren ska kunna utföra sina arbetsuppgifter, att åtkomstkontroller genomförs och att därmed risken för obehörig åtkomst inom verksamheten minimeras.

Tillvägagångssätt

Den fördjupade kontrollen kommer att genomföras i två delar. I del ett ombeds ni att besvara ett antal frågor samt att skicka in dokumenterade rutiner, styrande dokument eller liknande underlag avseende tilldelning av behörigheter och åtkomst till IT-systemet Lime. I del två kommer uppföljande frågor att ställas.

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

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

Fördjupad kontroll 2022

Kontrollpunkt 11: Behörighetsstyrning (del 1)

Del 1: Ni ombeds besvara frågorna nedan samt skicka in dokumenterade rutiner, styrande dokument eller liknande underlag avseende tilldelning av behörigheter och åtkomst till IT-systemet Lime.

- Beskriv systemets behörighetsstruktur och olika roller i systemet.
- Vilka roller får vilka behörigheter och vad baseras den bedömningen på?
- Vem beslutar om vilka som ska ha vilken behörighet?
- Hur ofta följs behörigheterna upp för att kontrollera att dessa är korrekta och anpassade efter medarbetarens arbetsuppgifter? Vem/vilka ansvarar för det?
- Beskriv hur åtkomstkontroller/kontroll av loggar kan genomföras i systemet.
- När och hur ofta genomförs åtkomstkontroller/kontroll av loggar?
- Vem/vilka ansvarar för åtkomstkontrollerna/kontroll av loggar?
- Finns det annan lagstiftning eller andra bestämmelser, utöver dataskyddsförordningen, som er verksamhet behöver beakta i arbetet med behörighetstilldelning? I så fall, vilken/vilka?
- Vilka andra åtgärder vidtas för att förhindra obehörig åtkomst till personuppgifter i systemet?
- Har verksamheten identifierat några personuppgiftsincidenter kopplat till felaktiga behörigheter?

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

Underlaget ska ha inkommit till dataskyddsombudet **senast den 10 mars 2022.**

Har du frågor, kontakta ditt huvudansvarige dataskyddsombud.

Fördjupad kontroll 2022

Kontrollpunkt 11: Behörighetsstyrning (del 2)

Del 2: Utifrån vad som framkommit i del 1 av den fördjupade kontrollen ombeds ni besvara frågorna nedan.

- Vad är det för personuppgifter som behandlas i systemet Lime?
- Hur många registrerades personuppgifter hanteras i Lime?
- Ange antalet personer som har åtkomst till Lime. Specificera svaret så att det framgår hur många som har behörighet till personuppgifterna både inom och utför organisationen.
- Hur kontrolleras personuppgiftsbiträdets behörigheter i systemet?
- Finns det instruktioner till personuppgiftsbiträdet? Om ja, översänd dessa. Om nej, varför inte?
- Har ni konsekvensbedömt behandlingarna i systemet? Varför/varför inte?
- Har ni identifierat specifika risker kopplat till nuvarande hantering av behörigheter? Varför/varför inte? Beakta såväl risker inifrån organisationen som utanför (ex, intrång) för de registrerades rättigheter.

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

Underlaget ska ha inkommit till dataskyddsombudet **senast den 8 juni 2022.** Dataskyddsombudet kan komma att ställa kompletterande frågor i samband med sammanställande av rapporten och/eller begära visning av systemet. Frågor kan komma att ställas såväl muntligen som skriftligen.

Har du frågor, kontakta dataskyddsenheten.