26 oktober 2023

Stab

Dataskyddsgruppen

Kristina Augustsson

Gryaab AB, Box 8984, 402 74 Göteborg, 031-64 74 00, gryaab.se

Åtgärdsplan dataskyddsarbetet 2023-2025

Med detta ärende informeras styrelsen om de åtgärder bolaget har planerat för ett förstärkt dataskydd.

Gryaabs dataskyddsombud har lämnat en årsrapport för 2022 avseende bolagets dataskyddsarbete. Styrelsen fick årsrapporten som information på styrelsemötet i februari 2023. Årsrapporten innehåller dels en uppföljning av bolagets egen skattning av det interna dataskyddsarbetet och dels en uppföljning av den fördjupade kontroll av behörighetsstyrning som dataskyddsombudet gjort.

I årsrapporten lämnades ett antal kommentarer och rekommendationer (nedan rekommendationer) till bolaget. En del rekommendationer har redan omhändertagits och återstående rekommendationer kommer att åtgärdas enligt en åtgärdsplan som sträcker sig över perioden 2023-2025.

Av bilaga 1 framgår de rekommendationer som dataskyddsombudet lämnat i årsrapporten för 2022 och åtgärder för dataskyddsarbetet 2023-2025.

Bilaga 1

Åtgärdsplan för förstärkt dataskydd 2023-2025

Kontrollpunkt	Rekommendation	Åtgärder	Status
1.Dataskyddsorganisation	Dataskyddsombudet har inget att invända mot bolagets skattning gällande den interna dataskyddsorganisationen. Det finns dock utmaningar i att två av tre inom dataskyddsorganisationen är nya i rollerna som dataskyddskontakt. Det är därför extra viktigt att bolaget lyfter dataskyddsfrågor även på en högre nivå samt att det finns dokumenterade rutiner som kan omhändertas av de som är nya. Eftersom arbetet har fungerat bra hittills ser dataskyddsombudet inga hinder i att de nya dataskyddskontakterna kan upprätthålla det goda interna arbetet. Bolaget behöver arbeta med att integrera dataskyddet i det dagliga arbetet i alla delar av verksamheten samt fastställa vilka befattningar/roller inom bolaget som har utpekat ansvar och mandat att fatta beslut i olika dataskyddsfrågor.	Gryaab ser över dataskyddsorganisationen och säkerställer att det finns tillräckliga resurser för att hålla dataskyddsarbetet på en ändamålsenlig nivå. Gryaab ska ta fram rutin gällande ansvar och vilka befattningar som har mandat att fatta beslut i dataskyddsfrågor.	Pågår

Kontrollpunkt	Rekommendation	Åtgärder	Status
2. Personuppgiftsincidenter	Bolagets skattning inom kontrollpunkten indikerar att inga större risker föreligger men att arbete ändock kvarstår med personuppgiftsincidenter. Dataskyddsombudet har tidigare granskat bolagets hantering av incidenter och de rekommenderade åtgärderna har vidtagits, därför har dataskyddsombudet inga invändningar mot skattningen. Enligt uppgift har bolaget dokumenterat inträffade personuppgiftsincidenter under 2022 och ingen har behövt anmälas till tillsynsmyndigheten. DSO rekommenderar att verksamheten regelbundet informerar i den egna organisationen om vad en incident är för att säkerställa att rutinerna är kända och följs. Samtidigt bör inträffade incidenter följas upp så verksamheten för att identifiera återkommande incidenter och kunna sätta in åtgärder i förebyggande syfte.	Gryaab ska ta fram en rutin för personuppgiftsincidenter och informera personalen om den.	Planerad

Kontrollpunkt	Rekommendation	Åtgärder	Status
3. Biträdesavtal och andra överenskommelser	Bolagets svar indikerar att stora risker fortfarande finns kopplat till bolagets arbete med biträdesavtal och andra överenskommelser. Årets skattning är något sämre än förra året trots att dataskyddsombudet granskade kontrollpunkten förra året där bolaget uppgav att alla åtgärder vidtagits. Dataskyddsombudet kopplar resultatet till att dataskyddsorganisationen ändrats och de nya dataskyddskontakterna är osäkra på vilka rutiner som finns inom bolaget. Bolaget behöver ta fram rutiner för att kontinuerligt genomföra efterlevnadskontroller, bedöma om andra överenskommelser/avtal behövs utifrån omständigheterna samt kunna bedöma hela kedjan av underbiträden. Dataskyddsombudets rekommendation är att bolaget bör se över vilka biträdessituationer som föreligger och ta fram biträdesavtal där det behövs om sådana saknas. Verksamheten rekommenderas säkerställa att rutiner och åtgärder som vidtogs efter fördjupade kontrollen finns tillgängliga och är uppdaterade.	Gryaab har gjort om sina inköpsrutiner så att dataskyddsgruppen involveras innan en upphandling/inköp som kan innebära att någon annan behandlar våra personuppgifter. Gryaab har uppdaterat sin rutin avseende PUB-avtal. Gryaabs medarbetare ska informeras om rutinerna. Gryaab ska ta fram en ny mall för PUB-avtal. Gryaab ska teckna PUB-avtal i alla nya biträdessituationer.	Inköpsrutinen är klar. Rutinen avseende PUB-avtal är uppdaterad. Övriga punkter är planerade.

Kontrollpunkt	Rekommendation	Åtgärder	Status
4. Personuppgiftsregister	Bolaget skattning skiljer sig något åt från förra året, men beror troligtvis på den nya dataskyddsorganisationen. Dataskyddsombudet har förståelse för att nya arbetssätt tar tid innan de sätter sig. Ett komplett och aktuellt register kan vara ett hjälpmedel för dataskyddsarbetet, vilket bolaget bör sträva efter. Dataskyddsombudet rekommendation är att verksamheten ser över, uppdaterar och använder registret kontinuerligt för att ha bra koll internt på personuppgiftsbehandlingarna. Eftersom bolaget uppger att det saknas dokumenterad ansvarsfördelning över vem/vilka som ansvarar för uppdatering av behandlingar i registerförteckningen i motsats till vad som uppgavs vid förra årets fördjupade kontroll, är rekommendationen att bolaget försöker reda ut huruvida en sådan rutin finns. Bolaget bör även säkerställa och förtydliga vem/vilka inom verksamheten som ansvarar för kontinuerlig uppdatering av registret.	Gryaab har uppdaterat sin rutin angående behandlingsregister. Gryaab ska se över och uppdatera sitt behandlingsregister. Gryaab ska informera sin personal om dataskydd för säkerställa att alla personuppgiftsbehandlingar registreras.	Rutinen angående behandlingsregister är klar. Övriga åtgärder är planerade.

5. Övergripande strategi för dataskydd	Bolagets skattning på kontrollpunkten kopplat till övergripande strategi för dataskydd indikerar att en del risker föreligger i arbetet. Bolaget uppger att det i stort sett saknas en övergripande strategi för dataskydd och att inget systematiskt arbete med att integrera dataskyddsfrågorna i det övriga informationssäkerhetsarbetet föreligger. Dataskyddsombudet bedömer att även detta är kopplat till den nya dataskyddsorganisationen. Bolaget behöver också identifiera och värdera informationstillgångar utifrån behovet av konfidentialitet, riktighet och tillgänglighet i enlighet med stadens styrande dokument inom informationssäkerhet. Verksamheten rekommenderas att se till att säkra egna styrande dokument som berör behandling av personuppgifter samt säkra att de är kända och följs, vilket inkluderar egna regelbundna efterlevnadskontroller av dessa. Rutiner för hantering av personuppgifter vid anordnande av fysiska och digitala sammankomster är särskilt viktiga för bolaget att ta fram, bland annat eftersom bolaget enligt sin hemsida erbjuder skolklasser att besöka bolagets anläggningar. Enligt uppgift från bolaget behandlas dock inga uppgifter om barn då endast lärare kontaktas vid skolklassbesök.Verksamheten rekommenderas att ta fram en övergripande strategi för dataskydd som utgår ifrån ett riskbaserat arbetssätt.	Gryaab ser över dataskyddsorganisationen och säkerställer att det finns tillräckliga resurser för att hålla dataskyddsarbetet på en ändamålsenlig nivå. Gryaab har integrerat dataskydd och informationssäkerhet som riskanalyser i bolagets löpande riskarbete. Gryaab ska ta fram ett årshjul för de delar av dataskyddsarbetet som är av återkommande och uppföljande karaktär. Gryaab ska ta fram rutiner för hantering av personuppgifter vid anordnade av fysiska och digitala sammankomster. Gryaab ska säkerställa följsamhet mot Göteborgs Stads riktlinje för informationssäkerhet och informationsklassificera all information som skapas och hanteras.	Gryaab har integrerat dataskydd och informationssäkerhet i bolagets riskarbete. Övriga åtgärder är pågående eller planerade.

Kontrollpunkt	Rekommendation	Åtgärder	Status
6. Utbildning	Dataskyddsombudet instämmer i bolagets bedömning. Olika befattningar i verksamheten kan kräva olika utbildningsinsatser varför en kartläggning av behovet är viktigt. Dataskyddsombudet rekommenderar att bolaget regelbundet utreder behovet av utbildningsinsatser, dokumenterar och använder olika typer av informationsinsatser för att säkerställa att man upprätthåller en god kunskap i dataskyddsfrågor.	Gryaab ska ta fram ett utbildningspaket gällande dataskydd och informationssäkerhet. Vissa av utbildningsinsatserna ska tas in i årshjulet för dataskyddsarbetet som är av löpande och återkommande karaktär.	Vissa utbildningsinsatser pågår och övriga är planerade.
7. Integritetspolicy	Bolagets skattning innebär att det inte föreligger några risker kopplat till integritetspolicyn. Bolaget rekommenderas att uppdatera informationen med jämna mellanrum för att säkerställa att den uppfyller kraven enligt GDPR. Dataskyddsombudet har inte granskat bolagets integritetspolicy i detalj, men en efter en snabb överflygning kan dataskyddsombudet konstatera att integritetspolicyn inte beskriver några behandlingar i detalj. Dataskyddsombudet rekommenderar att bolaget ser över policyn och säkerställer att information lämnas på annat sätt, om policyn inte är ämnad att vara heltäckande.	Gryaab ska se över sin integritetspolicy och säkerställa att den uppfyller kraven i GDPR.	Planerad

Kontrollpunkt	Rekommendation	Åtgärder	Status
8. Mejl och dokumenthantering	Bolagets skattning är lägre jämfört med föregående år och dataskyddsombudet instämmer i bedömningen att det föreligger en del risker kopplat till kontrollpunkten. En uppdaterad dokumenthanteringsplan med gallringsrutiner är en förutsättning för att bolaget ska kunna säkerställa principen om lagringsminimering enligt GPDR. Bolaget är osäkra på hur stor andel av bolagets personuppgiftsbehandlingar som har informationsklassificerats utifrån stadens riktlinje för informationssäkerhet, och kan inte svara på om informationen är aktuell och har kontrollerats det senaste året. Bolaget saknar också anvisningar för hur information i olika informationsklasser ska hanteras och vilka lagringsytor som får användas. Dataskyddsombudet rekommenderar att bolaget ser över och åtgärdar detta. Bolaget rekommenderades förra året att åtgärda sina rutiner för hantering av personuppgifter i e-post och eftersom skattning fortfarande är låg kvarstår denna rekommendation. Rutiner för hantering av personuppgifter i e-post rekommenderades bolaget åtgärda förra året, och eftersom skattningen fortfarande är låg kvarstår den rekommendationen.	Gryaab ska uppdatera sin dokumenthanteringsplan med gallringsrutiner. Gryaab ska säkerställa följsamhet mot Göteborgs Stads riktlinje för informationssäkerhet och informationsklassificera all information som skapas och hanteras. Gryaab ska ta fram rutin för hantering av e-post och annan molnhantering och informera personalen om den. Gryaab ska säkerställa att allmänheten får information om hur bolaget hanterar handlingar och personuppgifter när man mailar Gryaab och via hemsidan (integritetspolicyn).	Planerade

Kontrollpunkt	Rekommendation	Åtgärder	Status
9. Konsekvensbedömning /Samråd	Bolagets skattning på kontrollpunkten visar att det finns en del risker kopplat till arbetet med konsekvensbedömningar som behöver åtgärdas. Dataskyddsombudet instämmer i den bedömningen eftersom så vitt dataskyddsombudet vet har bolaget hittills enbart genomfört en regelrätt konsekvensbedömning. Dataskyddsombudets bedömning är dock att det troligtvis finns fler behandlingar som kräver konsekvensbedömningar. Dataskyddsombudet bedömer att i den mån bolaget framöver kommer införa nya behandlingar som kan innebära stora risker för de registrerade behöver verksamheten öka sin kunskap kopplat till konsekvensbedömningar. Efter att bolaget har identifierat och registrerat de behandlingar som redan utförs, bör bolaget också se över riskerna kopplat till dessa. Dataskyddsombudet är behjälpligt vid bedömningar och ska involveras i konsekvensbedömningar. Eftersom konsekvensbedömningsarbetet är ett sätt för bolaget att hantera de risker som föreligger med behandlingar och är en del i strategin för övergripande dataskydd, är dataskyddsombudets rekommendation att bolaget tar fram ett arbetssätt för att säkerställa efterlevnaden av GDPR.	Gryaab har gjort om sina inköpsrutiner så att dataskyddsgruppen involveras innan en upphandling/inköp som kan innebära att någon annan behandlar våra personuppgifter. Gryaab genomför tröskel- och konsekvensbedömningar på nya behandlingar och involverar dataskyddsombudet i dessa. Gryaab ska ta fram en rutin för när tröskel- och konsekvensbedömningar och samråd ska göras, hur det ska dokumenteras och hur bolaget säkerställer att bedömningarna uppdateras vid ändringar i behandlingen.	Inköpsrutinen är klar. Tröskel- och konsekvensbedömningar sker på nya behandlingar. Övriga åtgärder är planerade.

Kontrollpunkt	Rekommendation	Åtgärder	Status
10. IT-projekt och upphandling	Bolagets skattning på kontrollfrågan visar att inga större risker föreligger. Eftersom dataskyddsombudet inte blivit involverad i några IT-projekt eller upphandlingar under året, saknas insyn i hur verksamheten arbetar i dessa frågor. Dataskyddsombudet vill påminna bolaget om att dataskyddsombudet ska involveras i alla frågor som rör dataskydd från start. Dataskyddsombudet vill dock lyfta, i och med att kunskapen om dataskydd generellt behöver höjas inom verksamheten, att det finns risker att dataskyddsperspektivet missas vid uppstart av IT-projekt och initierande av upphandlingar. Inbyggt dataskydd och dataskydd som standard behöver tas med i kravställningen för att säkerställa efterlevnad vid upphandlingsfasen och senare.	Gryaab har gjort om sina inköpsrutiner så att dataskyddsgruppen involveras innan en upphandling/inköp som kan innebära att någon annan behandlar våra personuppgifter. Medarbetarna ska informeras om rutinen.	Inköpsrutinen är klar. Övriga åtgärder är planerade.

Kontrollpunkt	Rekommendation	Åtgärder	Status
11. IT-system och digitala verktyg	Bolaget har skattat sitt arbete blandat på kontrollpunkten kopplat till IT-system och digitala verktyg. Kopplat till behörigheter har detta berörts i den fördjupade kontrollen och behandlas inte ytterligare här. Bolaget uppger att det saknas rutiner för att systematiskt kunna följa upp och kontrollera att användning av system och/eller andra digitala verktyg följer antagna rutiner/riktlinjer/policyer. Som ett led i ett systematiskt arbetssätt kan dataskyddsombudet komma att följa upp lämnade rekommendationer och bolagets arbete under 2023.	Gryaab ska ta fram rutiner för hur bolaget ska följa upp system och digitala verktyg utifrån GDPR. Uppföljningen ska inkluderas i årshjulet för dataskyddsarbetet.	Planerad
12. Hantering av registrerades rättigheter	Bolagets skattning på kontrollfrågan visar att inga större risker föreligger. Dataskyddsombudet har inte blivit involverad i några frågor gällande registrerades rättigheter under året och saknar därför inblick i hur arbetet med att säkerställa dessa fungerar inom bolaget. Medvetenheten gällande registrerades rättigheter är kopplat till den generella kunskapen om dataskydd och kan alltid höjas. Bolaget uppger att det finns en rutin för tillbakadragande av samtycke. Verksamheten rekommenderas att ta fram en process för att kunna ta fram efterfrågad information vid registerutdrag.	Gryaab ska ta fram en rutin för att ta fram efterfrågad information vid ett registerutdrag.	Planerad

Kontrollpunkt	Rekommendation	Åtgärder	Status
Fördjupad kontroll	Definiera vad som kan utgöra ett larm som generar att loggar kontrolleras för att undvika övervakning av anställda.	Gryaab har definierat vid vilka situationer larm kan generera att loggar kontrolleras.	Klart
Fördjupad kontroll	Kontrollera behörigheter även vid ändring av anställning inom bolaget för att förhindra att medarbetare kommer åt uppgifter de inte behöver vid en ny/ändrad anställning.	Gryaab kommer påbörja ett arbete med informationssäkerhet under Q1 2024 och kommer då ta fram rutiner för behörighetsstyrning.	Planerad
Fördjupad kontroll	Kontinuerligt se över de behandlingar som sker i systemet för att ha koll på de risker som förekommer, och i de fall det krävs, genomföra tröskelanalys och/eller konsekvensbedömning.	Se kontrollpunkt 9 som berör samma frågor.	Se kontrollpunkt 9 som berör samma frågor.