Göteborgs Stad

Årsrapport för dataskyddsarbetet 2021

Higab AB

2021-12-23

Innehåll

1 Dataskyddsarbetet ... 3

1.1 Att förvalta ett förtroende ... 3

1.2 Dataskyddsenhetens gemensamma arbete ... 3

2 Kontrollarbetet ... 4

2.1 Ett systematiskt arbete ... 4

2.2 Rättsutveckling som påverkat kontrollarbetet under året ... 4

2.2.1 Tredjelandsöverföringar (överföringar till länder utanför EU/EES) ... 4

2.2.2 Rätt beslutsnivå ... 5

2.2.3 Kommungemensamma interna tjänster ... 6

2.3 Årets kontrollarbete ... 6

2.3.1 Fördjupad kontroll ... 6

2.3.2 Fasta kontrollpunkter ... 7

2.4 Resultat av fasta kontrollpunkter för Higab AB ... 8

2.4.1 Kontrollpunkt 1: Dataskyddsorganisation ... 8

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter ... 8

2.4.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser ... 8

2.4.4 Kontrollpunkt 4: Personuppgiftsregister ... 9

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd ... 9

2.4.6 Kontrollpunkt 6: Utbildning ... 10

2.4.7 Kontrollpunkt 7: Integritetspolicy ... 10

2.4.8 Kontrollpunkt 8: Mejl och dokumenthantering ... 10

2.4.9 Kontrollpunkt 9: Konsekvensbedömning/samråd ... 11

2.4.10 Kontrollpunkt 10: IT-projekt och upphandling ... 11

2.4.11 Kontrollpunkt 11: IT-system och digitala verktyg ... 12

2.4.12 Kontrollpunkt 12: Hantering av registrerades rättigheter ... 12

2.5 Uppföljning ... 12

2.5.1 Uppföljning av genomförda kontroller 2018 - 2020 ... 12

2.5.2 Uppföljning av genomförd kontroll 2021 ... 13

2.6 Sammanfattande rekommendationer ... 13

3 Bilagor ... 14

3.1 Bilaga 1: Diagram över resultat av fasta kontrollpunkter, i jämförelse med Göteborgs Stads genomsnitt. ... 14

1 Dataskyddsarbetet

1.1 Att förvalta ett förtroende

Att få ta del av och hantera andra människors personliga uppgifter innebär att förvalta ett stort förtroende. Dataskyddsförordningen 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. Lagen har höga sanktionsavgifter, men det är inte därför det är viktigt att lagen följs. Att personuppgifter hanteras lagenligt bör snarare vara en självklarhet i syfte att visa omsorg om det förtroende som givits den som har att hantera uppgifterna.

Enligt lagstiftningen har dataskyddsombudet bland annat till uppgift att ge råd och information till den personuppgiftsansvarige i dataskyddsfrågor. Dataskyddsombudet har även till uppgift att övervaka efterlevnaden av dataskyddsförordningen hos personuppgiftsansvariga.

Dataskyddsombudet ska enligt lagstiftningen rapportera till högsta förvaltningsledning dvs. styrelse eller nämnd. Detta för att den högsta ledningen ska få den information som behövs för att kunna bedöma vilka prioriteringar som ska göras och vilka risker som organisationen är beredd att ta. Dataskyddsombudet fattar inte beslut åt verksamheten. Ytterst vilar ansvaret för att verksamheterna följer lagen på nämnd/styrelse. De råd och rekommendation som ges av dataskyddsombudet syftar till att ge ledningen underlag för att kunna fatta väl underbyggda beslut.

1.2 Dataskyddsenhetens gemensamma arbete

Dataskyddsenheten har under det gångna året regelbundet skickat ut nyhetsbrev innehållandes omvärldsbevakning och information från enheten. Däremellan har enheten även informerat verksamheterna om förändringar i lagstiftning och praxis.

Enheten har också tillgängliggjort en digital grundutbildning som alla stadens bolag och förvaltningar har fått tillgång till, och som fritt kan användas av verksamheterna. Det har även arrangerats ett flertal lärarledda utbildningar, bland annat en grundutbildning och en utbildning riktad till yrkesgruppen kommunikatörer. Genom att hålla utbildningarna digitalt har flera hundra personer inom stadens verksamheter haft möjlighet att delta. Då intresset varit stort kommer dataskyddsenheten fortsätta anordna utbildningar inom olika ämnesområden.

För att skapa möjligheter för samarbete och erfarenhetsutbyte i dataskyddsfrågor har enheten under året anordnat två nätverksträffar för stadens dataskyddskontakter. Teman för nätverksträffarna har anpassats utefter de frågor enheten identifierat att många av stadens verksamheter arbetar med.

2 Kontrollarbetet

2.1 Ett systematiskt arbete

Dataskyddsenheten har under året tagit fram gemensamma rutiner för kontrollarbetet, med syfte att skapa ett enhetligt, transparent och systematiskt arbetssätt för Göteborgs Stads verksamheter. Kontrollerna följer en årsplan, nedan kallad ”Kontrollplan”.

Kontrollplanen skickades ut i januari 2021, med en redogörelse för planerade kontroller under året samt relevanta tidpunkter. Kontrollplanen redogjorde dels för två fördjupade kontroller, som valdes ut efter verksamhetens riskområden, dels återkommande fasta kontrollpunkter som årligen kommer att stämmas av för att se var verksamheten befinner sig i sitt dataskyddsarbete. Av kontrollplanen framgick också att en uppföljning kommer att ske av tidigare lämnade rekommendationer.

Under första halvåret har dataskyddsombudet genomfört de fördjupade kontrollerna. Under andra halvåret har dataskyddsombudet genomfört en kontroll av de fasta kontrollpunkterna samt gjort en uppföljning av tidigare lämnade rekommendationer i tidigare utförda kontroller.

2.2 Rättsutveckling som påverkat kontrollarbetet under året

Rättsutvecklingen under året har föranlett dataskyddsombudet att särskilt uppmärksamma behandlingen av personuppgifter som påverkats av nya rättsfall och rekommendationer. Ett antal händelser har också gjort att enheten har haft anledning att analysera stadens struktur rörande kommungemensamma interna tjänster.

2.2.1 Tredjelandsöverföringar (överföringar till länder utanför EU/EES)

I juli 2020 kom en dom från EU-domstolen kallad Schrems II-domen. Frågan i målet var om det avtal som fanns mellan EU och USA gav tillräckligt skydd för personuppgifter för att dessa lagligen skulle få överföras till USA. Frågeställningen i sig var väckt med anledning av den omfattande datainsamling som amerikansk lagstiftning möjliggör för amerikanska säkerhetsorgan av icke-amerikanska medborgares uppgifter. Rättsfallet rörde bulkinsamling av data ”in transit” men

frågan är principiellt intressant eftersom i princip alla verksamheter som faller under amerikansk jurisdiktion kan förmås överlämna annans data, även i de fall denna finns utanför USA. Domstolen ogiltigförklarade avtalet och fastslog att det kan krävas omfattande säkerhetsåtgärder för att kunna överföra uppgifter till USA eller andra länder med liknande lagstiftning. Skyddsåtgärderna behövde i princip omöjliggöra för utländska myndigheter att kunna få del av uppgifterna, genom exempelvis kryptering eller anonymisering. Domen har fått stor påverkan, och sedan den kom har därför frågan om tredjelandsöverföringar varit ständigt aktuell. Under året har också några vägledningar publicerats av Europeiska dataskyddsstyrelsen, EDPB, ett organ där samtliga länders tillsynsmyndigheter samverkar. Domen har inneburit att en översyn av aktuella personuppgiftsbehandlingar har behövt ske för att ta reda på om någon överföring sker till USA eller i vissa fall även annat land. Begreppet överföring är dessutom brett och inkluderar även att ge någon i USA åtkomst till uppgifter, även när uppgifterna befinner sig inom EU. Domstolen har uppmanat tillsynsmyndigheterna i respektive land att börja agera i frågan.

Kommentarer och rekommendationer

Om denna översyn ännu inte genomförts rekommenderar dataskyddsombudet att detta arbete prioriteras, så verksamheten får en tydlig riskbild och kan vidta åtgärder eller fatta nödvändiga beslut.

2.2.2 Rätt beslutsnivå

Frågan om tredjelandsöverföringar har varit omfattande och har berört såväl användningen av olika system (M365, Google) som sociala medier, cookies, osv. Frågan är komplex eftersom stora investeringar gjorts under den tid som avtalet mellan EU och USA var i kraft och förutsättningarna nu ändrats. Det har också förelegat en osäkerhet om USA tänker ändra sin lagstiftning, om leverantörerna kommer att skapa nya koncernkonstellationer eller om nya förhandlingar mellan EU och USA kan leda till ett nytt avtal (vilket idag endast är möjligt om amerikansk lagstiftning först ändras). Mer än ett år har dock passerat sedan domen kom och några nya lösningar för att kunna överföra personuppgifter till USA i klartext finns fortfarande inte. Det innebär att det idag i de flesta fall saknas lagliga möjligheter för överföring av personuppgifter till USA. Om en verksamhet väljer att fortsätta att behandla personuppgifter utan att ha säkerställt en laglig överföring så innebär detta ett accepterande av risk för förtroendeskada, skadestånd och sanktionsavgift. Ett accepterande skulle även kunna förstås som att man medvetet väljer att bryta mot gällande lagstiftning och riskera de registrerades fri- och rättigheter.

Kommentarer och rekommendationer

Nämnd/styrelse är ansvarig för att verksamheten följer lagen. Nämnd/styrelse rekommenderas att säkerställa att beslut som innebär en avvikelse från gällande dataskyddslagstiftning fattas på behörig nivå.

2.2.3 Kommungemensamma interna tjänster

De kommungemensamma interna tjänsterna erbjuds och levereras idag av Intraservice. Vad som utgör en kommungemensam intern tjänst beslutas av stadsdirektören, på delegation av kommunstyrelsen, efter samråd med förvaltnings- och bolagsledningar.

Enligt stadens styrande dokument så är det för många av stadens verksamheter obligatoriskt att använda tjänsterna. I vissa fall pekar styrande dokument ut exakt vilket system som utgörs av tjänsten, tex. M365, medan det i andra fall endast anges typ av tjänst. Intraservice roll innebär att upphandla och/eller teckna avtal med en underleverantör för stadens räkning. I styrande dokument anges att Intraservice ska betraktas som leverantör och därmed ett personuppgiftsbiträde (dvs. någon som behandlar personuppgifter för annans räkning) åt stadens bolag och förvaltningar.

Den personuppgiftsansvarige är den som bestämmer ändamål och medel med en behandling. I normala fall är det respektive bolag och nämnd som är personuppgiftsansvarig för de personuppgiftsbehandlingar som sker inom verksamheten. När det kommer till stadens kommungemensamma interna tjänster blir detta dock ofta problematiskt eftersom verksamheterna ibland inte har någon möjlighet att påverka vissa av de ändamål och medel för behandlingar som sker inom dessa tjänster. Utifrån detta uppstår frågor om vilket ansvar som Intraservice och kommunstyrelsen har för dessa tjänster, samt hur stadens struktur för kommungemensamma interna tjänster påverkar fördelningen av personuppgiftsansvaret för de behandlingar där dessa tjänster används. Oaktat vad som anges i styrande dokument skulle utgångspunkten, vid en rättslig prövning, vara vem som faktiskt hade rådighet att besluta om ändamål och medel.

Kommentarer och rekommendationer

Utifrån ett ansvarsperspektiv, då sanktionsavgifter i normalfallet riktas mot den som är personuppgiftsansvarig, rekommenderar dataskyddsombudet att bolaget säkerställer att de har tillgång till komplett och aktuell information om de kommungemensamma interna tjänster som används i bolaget och att eventuell tredjelandsöverföring i tjänsterna är laglig. Då det är Intraservice som är personuppgiftbiträde för de kommungemensamma interna tjänsterna så är det Intraservice som på anmodan ska tillse att denna information ges till bolaget.

2.3 Årets kontrollarbete

2.3.1 Fördjupad kontroll

Den fördjupade kontrollen har bestått av IT-system och digitala verktyg. Kontrollen har genomförts under våren och resultatet har kommunicerats i maj 2021.

Dataskyddsombudet har i rapporten avseende den fördjupade kontrollen haft några rekommendationer till verksamheten vilka har följts upp under punkten 2.5.2.

2.3.2 Fasta kontrollpunkter

För att ge verksamheten en bild av hur långt man har kommit i det systematiska dataskyddsarbetet har dataskyddsenheten tagit fram en enkät utifrån de fasta kontrollpunkterna. Enkäten är avsedd att spänna över de viktigaste delarna inom dataskyddsarbetet för att på så sätt fånga in en större bredd av frågor. Enkäten består av tolv punkter där varje punkt innehåller ett antal delfrågor i form av påståenden och/eller skattningsfrågor. Verksamheten har fått besvara frågorna utifrån aktuellt läge inom verksamheten.

I arbetet används en modell som består av fyra kategorier, vilka representerar fyra olika mognadsnivåer. Verksamheten har utifrån svaren på den enkät som skickats ut från dataskyddsenheten fått ett värde som indikerar vilken mognadsnivå verksamheten befinner sig på inom respektive kontrollpunkt. Genom att arbeta med förbättringsområden möjliggörs ett riskbaserat arbetssätt för både verksamhet och dataskyddsombud, då resultaten ger en bild av vad verksamheten kan behöva prioritera i dataskyddsarbetet framåt.[1]

Resultaten från enkäten ger en generell ögonblicksbild för respektive kontrollpunkt. Enkäten kommer att upprepas kommande år. Avsikten med detta arbetssätt är att både att få en bild av nuläget och att kunna åskådliggöra de förändringar som vidtas över tid. Enkäten har ej främst för avsikt att peka ut brister utan ska ses som en vägledning för verksamheten och ett verktyg för att identifiera relevanta prioriteringar. Syftet är att få till ett långsiktigt och systematiskt arbetssätt som möjliggör uppföljning över tid.

Beskrivning av mognadsnivåer

Mognadsnivåer	Färgkod
Nivå 1. Bolaget har självskattat sig lågt på flertalet av de ingående komponenterna i kontrollpunkten. Kan indikera att kontrollpunkten är ett prioriterat förbättringsområde avseende dataskydd.	
Nivå 2. Bolaget har självskattat sig lågt på flera punkter av de ingående komponenterna i kontrollpunkten. Kan indikera att flera prioriterade förbättringar finns inom kontrollpunkten avseende dataskydd.	
Nivå 3. Bolaget har självskattat sig lågt på några av de ingående komponenterna i kontrollpunkten. Kan indikera att ett mindre antal prioriterade förbättringar finns inom kontrollpunkten avseende dataskydd.	
Nivå 4. Bolaget har självskattat sig högt på flera av de ingående komponenterna i kontrollpunkten. Kan indikera att det finns få eller inga prioriterade förbättringar inom kontrollpunkten avseende dataskydd.	

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

2.4 Resultat av fasta kontrollpunkter för Higab AB

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.

Kommentarer och rekommendationer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig utifrån frågornas formulering i kontrollpunkten. Bolagets dataskyddsombud kommer att tillsammans med verksamheten göra en djupare analys av kontrollpunktens ingående komponenter för att bedöma eventuella förbättringsområden gällande dataskydd.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Kommentarer och rekommendationer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig utifrån frågornas formulering i kontrollpunkten. Bolagets dataskyddsombud kommer att tillsammans med verksamheten göra en djupare analys av kontrollpunktens ingående komponenter för att bedöma eventuella förbättringsområden gällande dataskydd.

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.

Kommentarer och rekommendationer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig utifrån frågornas formulering i kontrollpunkten. Bolagets dataskyddsombud kommer att tillsammans med verksamheten göra en djupare analys av kontrollpunktens ingående komponenter för att bedöma eventuella förbättringsområden gällande dataskydd.

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.

Kommentarer och rekommendationer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig utifrån frågornas formulering i kontrollpunkten. Bolagets dataskyddsombud kommer att tillsammans med verksamheten göra en djupare analys av kontrollpunktens ingående komponenter för att bedöma eventuella förbättringsområden gällande dataskydd.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Kommentarer och rekommendationer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig utifrån frågornas formulering i kontrollpunkten. Bolagets dataskyddsombud kommer att tillsammans med verksamheten göra en djupare analys av kontrollpunktens ingående komponenter för att bedöma eventuella förbättringsområden gällande dataskydd.

2.4.6 Kontrollpunkt 6: Utbildning

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

Kommentarer och rekommendationer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig utifrån frågornas formulering i kontrollpunkten. Bolagets dataskyddsombud kommer att tillsammans med verksamheten göra en djupare analys av kontrollpunktens ingående komponenter för att bedöma eventuella förbättringsområden gällande dataskydd.

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.

Kommentarer och rekommendationer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig utifrån frågornas formulering i kontrollpunkten. Bolagets dataskyddsombud kommer att tillsammans med verksamheten göra en djupare analys av kontrollpunktens ingående komponenter för att bedöma eventuella förbättringsområden gällande dataskydd.

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.

Kommentarer och rekommendationer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig utifrån frågornas formulering i kontrollpunkten. Bolagets dataskyddsombud kommer att tillsammans med verksamheten göra en djupare analys av kontrollpunktens ingående komponenter för att bedöma eventuella förbättringsområden gällande dataskydd.

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.

Kommentarer och rekommendationer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig utifrån frågornas formulering i kontrollpunkten. Bolagets dataskyddsombud kommer att tillsammans med verksamheten göra en djupare analys av kontrollpunktens ingående komponenter för att bedöma eventuella förbättringsområden gällande dataskydd.

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.

Kommentarer och rekommendationer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig utifrån frågornas formulering i kontrollpunkten. Bolagets dataskyddsombud kommer att tillsammans med verksamheten göra en djupare analys av kontrollpunktens ingående komponenter för att bedöma eventuella förbättringsområden gällande dataskydd.

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.

Kommentarer och rekommendationer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig utifrån frågornas formulering i kontrollpunkten. Bolagets dataskyddsombud kommer att tillsammans med verksamheten göra en djupare analys av kontrollpunktens ingående komponenter för att bedöma eventuella förbättringsområden gällande dataskydd.

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.

Kommentarer och rekommendationer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig utifrån frågornas formulering i kontrollpunkten. Bolagets dataskyddsombud kommer att tillsammans med verksamheten göra en djupare analys av kontrollpunktens ingående komponenter för att bedöma eventuella förbättringsområden gällande dataskydd.

2.5 Uppföljning

2.5.1 Uppföljning av genomförda kontroller 2018 - 2020

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

Kontroll 1 (2018): Organisatoriska förutsättningar för dataskyddsarbetet.

Verksamheten gavs följande rekommendationer:

Utifrån den sårbarhet som utgörs av att dataskyddsarbetet centreras kring en person (dataskyddskontakten) rekommenderar dataskyddsombudet bolaget att utöka bemanningen och skapa en större dataskyddsorganisation.

Kommentarer och rekommendationer:

Bolaget genomför en omorganisation som innebär en förändring av bolagets dataskyddsorganisation. Dataskyddsombudet har fått förfrågan om att delta i de delar av omorganisationen som rör dataskydd vilket dataskyddsombudet ser som väldigt positivt. Uppföljning kommer att ske under 2022.

2.5.2 Uppföljning av genomförd kontroll 2021

Verksamheten har fått en kort enkät med frågor om åtgärder har vidtagits med anledning av dataskyddsombudets lämnade rekommendationer för den genomförda kontrollen under våren 2021.

Kontroll 1 (2021): IT-system och digitala verktyg

Verksamheten gavs följande rekommendationer:

De förbättringar som bolaget kan vidta är att dokumentera informationsklassningen av behandling/IT-system så att det framgår hur bolaget har kommit fram till respektive nivå utifrån konfidentialitet, riktighet och tillgänglighet.

Ytterligare förbättringsområde är att införa regelbundna dokumenterade riskanalyser utifrån informationssäkerhet/dataskydd. Då bolaget har bedömt granskade IT-system som verksamhetskritiska är det extra viktigt att informationssäkerhetsrisker hanteras i bolagets övergripande riskhanteringsprocess.

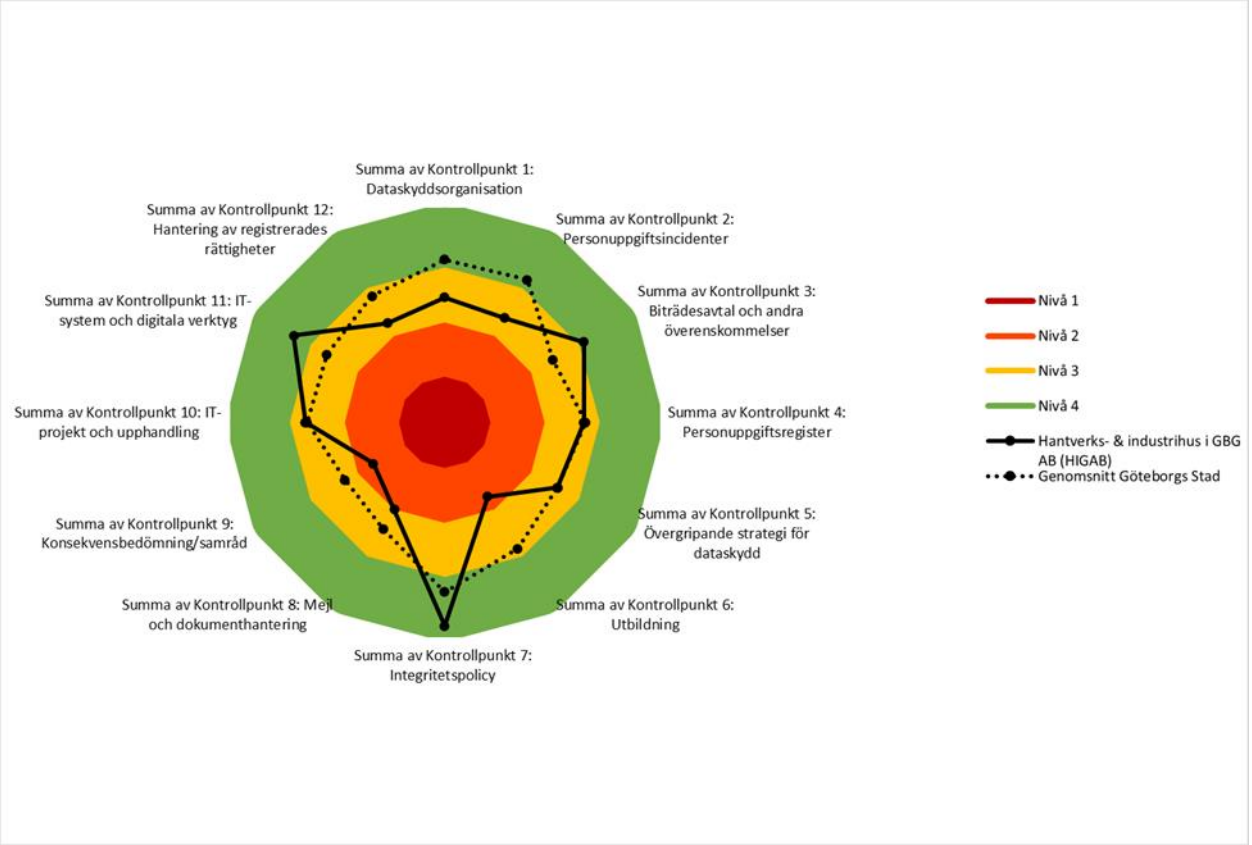
Kommentarer och rekommendationer:
Bolaget kommer fortsätta arbetet med dessa frågor under 2022. Rutin är upprättad för att identifiera kritiska informationstillgångar. Dataskyddsombudet kommer att följa upp arbetet under 2022.

2.6 Sammanfattande rekommendationer

För att på ett praktiskt plan kunna identifiera vad verksamheten behöver arbeta med inom ramen för respektive kontrollpunkt behövs en mer 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.

3 Bilagor

3.1 Bilaga 1: Diagram över resultat av fasta kontrollpunkter, i jämförelse med Göteborgs Stads genomsnitt.



Göteborgs Stad

Higab AB

Kontrollplan för dataskyddsarbetet 2022

2022-01-21

Innehåll

1 Bakgrund ... 3

1.1 Dataskyddsförordningen ... 3

1.1.1 Personuppgiftsansvarig ... 3

1.1.2 Dataskyddsombud ... 3

2 Kontrollplan för dataskyddsarbetet 2022 ... 4

2.1 Syfte och mål ... 4

2.2 Ett riskbaserat arbetssätt ... 4

2.3 Upplägg ... 4

2.3.1 Verksamhetsspecifika förutsättningar ... 5

2.4 Tidplan för kontroller 2022 ... 5

3 Kontrollpunkter ... 5

3.1 Fasta kontrollpunkter ... 5

3.1.1 Beskrivning av fasta kontrollpunkter ... 7

3.2 Fördjupad kontroll 2022 ... 9

4 Uppföljning ... 9

4.1 Uppföljning av lämnade rekommendationer ... 9

4.1.1 Uppföljning av hittills genomförda kontroller ... 10

5 Rapportering till nämnd/styrelse ... 10

5.1 Delårsrapportering ... 10

5.2 Årsrapport ... 10

5.3 Särskilt yttrande till högsta ledning ... 10

5.4 Beslutanderätten i dataskyddsfrågor ... 11

6 Kontakt ... 11

1 Bakgrund

1.1 Dataskyddsförordningen

Dataskyddsförordningen (GDPR) trädde i kraft den 25 maj 2018 och är en EU-förordning med syfte att skydda fysiska personers grundläggande fri- och rättigheter, att garantera ett likvärdigt skydd samt att säkerställa det fria flödet av personuppgifter inom unionen. Förordningen kompletteras av dataskyddslagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning. Dessa samspelar även med annan speciallagstiftning.

Dataskyddsförordningen ställer höga krav på organisationers behandling av enskildas personuppgifter. Utöver att insamlingen av personuppgifterna ska vara tillåten, måste den personuppgiftsansvarige dessutom hantera dessa uppgifter på ett korrekt sätt. Detta ska ske med respekt för den enskildes integritet och genom att vidta lämpliga säkerhetsåtgärder.

Efterlevnaden av lagstiftningen övervakas av Integritetsskyddsmyndigheten och överträdelser kan bland annat leda till sanktionsavgifter eller skadestånd.

1.1.1 Personuppgiftsansvarig

En personuppgiftsansvarig kan vara en fysisk person eller juridisk person, en offentlig myndighet, institution eller ett annat organ. Varje förvaltning med egen nämnd räknas som en egen offentlig myndighet. Varje enskild nämnd eller styrelse är ytterst ansvarig för att organisationen behandlar personuppgifter i enlighet med gällande regelverk. För att följa dataskyddsarbetet och hålla nämnden/styrelsen informerad bör, enligt dataskyddsförordningen, ett dataskyddsombud, med särskild sakkunskap om dataskyddslagstiftning och praxis, utses för att bistå den ansvarige med att övervaka den interna efterlevnaden av förordningen.

1.1.2 Dataskyddsombud

Dataskyddsombudet ska ge råd och information till den personuppgiftsansvarige samt övervaka efterlevnaden av dataskyddsförordningen och annan relevant dataskyddslagstiftning. Det innebär bland annat att kontrollera hur den personuppgiftsansvarige behandlar personuppgifter, att bestämmelser och interna styrdokument följs samt att ge råd och stöd vid konsekvensbedömningar. Dataskyddsombudet ska enligt dataskyddsförordningen utföra sitt arbete på ett oberoende sätt gentemot den som är personuppgiftsansvarig och får inte instrueras av denne i hur arbetet ska utföras. Dataskyddsombudet är inte heller ansvarig för att lagstiftningen efterlevs.

Dataskyddsombudet är även kontaktperson för de registrerade och tillsynsmyndigheten. Dataskyddsenheten kommer under 2022 att bli dataskyddsombud för förvaltningar och bolag i Göteborgs Stad.

2 Kontrollplan för dataskyddsarbetet 2022

2.1 Syfte och mål

Dataskyddsombudets uppgift att övervaka den personuppgiftsansvariges efterlevnad av förordningen regleras i artikel 39 GDPR. En del av denna övervakning innebär att dataskyddsombudet genomför kontroller av dataskyddsarbetet inom den personuppgiftsansvariges organisation. Dessa kontroller specificeras genom denna kontrollplan som syftar till att informera personuppgiftsansvariga om tidplan och särskilda fokusområden för kontrollarbetet år 2022.

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

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

2.2 Ett riskbaserat arbetssätt

Enligt dataskyddsregelverket ska dataskyddsombudet arbeta utifrån en riskbaserad metod. Kontrollplanen utgår därför ifrån dataskyddsombudets bedömning avseende risker kopplat till verksamhetens personuppgiftsbehandlingar.

Riskbedömningen utgår ifrån riskerna för de registrerades fri- och rättigheter. Det tas även hänsyn till potentiella konsekvenser för verksamheten. Både till risken för ekonomisk skada (exempelvis skadestånd och sanktionsavgifter), samt till risken för förtroendeskada (så som exempelvis försämrat varumärke och minskad tillit). Genom ett systematiskt och proaktivt dataskyddsarbete kan risken för att drabbas av någon av dessa följder minimeras.

2.3 Upplägg

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

a) Den första delen består av fasta kontrollpunkter där varje punkt bedöms årligen. Bedömningen görs genom löpande kontroller, genom deltagande i verksamhetens arbete och i förekommande fall utifrån given information.

Genom att ha en årlig uppföljning av de fasta kontrollpunkterna kommer varje personuppgiftsansvarig kunna följa utvecklingen av dataskyddsarbetet inom verksamheten över tid.

b) Den andra delen är en fördjupad kontroll av en eller flera utvalda verksamhetsspecifika kontrollpunkter.

c) Den tredje delen är en uppföljning och bedömning av hur verksamheten hanterat tidigare lämnande rekommendationer.

Kontrollarbetets olika delar kommer sammanställas och presenteras i årsrapporten för nämnd/styrelse.

2.3.1 Verksamhetsspecifika förutsättningar

Dataskyddsombudets arbete kommer att bedrivas utifrån verksamhetens specifika förutsättningar. Identifierade aktiviteter kan därför komma att justeras utifrån händelser som inträffar i verksamheterna eller i omvärlden.

2.4 Tidplan för kontroller 2022

Månad	Aktivitet
Januari	Kontrollplan för året lämnas till nämnd/styrelse Årsrapport presenteras för nämnd/styrelse (januari/februari)
Februari - april	Fördjupad kontroll av utvalda verksamhetsspecifika kontrollpunkter genomförs
Maj - juni	Fördjupad kontroll slutförs och delårsrapport lämnas till verksamheten *(rapportering inför nämnd/styrelse sker vid behov)*
September - november	Uppföljning av tidigare lämnade rekommendationer Kontroll av fasta kontrollpunkter
December	Årsrapport lämnas till verksamheten

3 Kontrollpunkter

3.1 Fasta kontrollpunkter

De fasta kontrollpunkternas omfattning utgår från principerna om inbyggt dataskydd och dataskydd som standard (enligt artikel 25 GDPR). Verksamhetens följsamhet mot förordningen beror till stor del på hur väl dessa principer har integrerats i verksamhetens ordinarie processer. Att principerna har en central roll i arbetet med dataskydd blir särskilt tydligt i beaktandesats

(skäl) 78 GDPR, som anger att ”skyddet av fysiska personers rättigheter och friheter i samband med behandling av personuppgifter förutsätter att lämpliga tekniska och organisatoriska åtgärder vidtas”, och därtill att den personuppgiftsansvarige, för att kunna visa att förordningen efterlevs, bör anta interna strategier och vidta åtgärder särskilt för att uppfylla principerna om inbyggt dataskydd och dataskydd som standard.

Med principerna som utgångspunkt har tolv kontrollpunkter identifierats. Dessa är av både teknisk och organisatorisk karaktär och är gemensamma för alla verksamheter inom Göteborgs Stad. De punkter som fastställts utgör en del av fundamentet i lagstiftningen. Syftet med arbetssättet är att tillsammans hitta strategier, rutiner och arbetssätt så att kontrollerna över tid kommer att kräva mindre och mindre arbete.

De fasta kontrollpunkterna kontrolleras genom en enkät som kommer att vara återkommande varje år. Enkäten utgår ifrån de tolv kontrollpunkterna där varje punkt innehåller ett antal delfrågor i form av påståenden och/eller skattningsfrågor. Det är verksamheten som ansvarar för att enkäten fylls i. För att uppskattningarna ska bli så korrekta som möjligt kan det krävas att olika personer från olika delar i verksamheten deltar i att fylla i enkäten.

Resultaten från enkäten ger en generell ögonblicksbild för respektive kontrollpunkt. Avsikten med detta arbetssätt är att både att få en bild av nuläget och att kunna åskådliggöra de förändringar som vidtas över tid. Enkäten har ej främst för avsikt att peka ut brister utan ska ses som en vägledning för verksamheten och ett verktyg för att identifiera relevanta prioriteringar. Syftet är att få till ett långsiktigt och systematiskt arbetssätt som möjliggör uppföljning över tid.

Kontrollpunkter
1. Dataskyddsorganisation
2. Personuppgiftsincidenter
3. Biträdesavtal och andra överenskommelser
4. Personuppgiftsregister
5. Övergripande strategi för dataskydd
6. Utbildning
7. Integritetspolicy
8. Mejl- och dokumenthantering
9. Konsekvensbedömning/samråd
10. IT-projekt och upphandling
11. IT-system och digitala verktyg
12. Hantering av registrerades rättigheter

3.1.1 Beskrivning av fasta kontrollpunkter

Kontrollpunkt 1: Dataskyddsorganisation

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

Kontrollpunkt 2: Personuppgiftsincidenter

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

Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

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

Kontrollpunkt 4: 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.

Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd. En verksamhetsspecifik strategi som anger ramarna för arbetet med dataskydd kan både främja ett riskbaserat arbetssätt och bidra till en kontinuitet i dataskyddsarbetet.

Kontrollpunkten innefattar även verksamhetens strategi för att integrera dataskyddsfrågorna i det övriga informationssäkerhetsarbetet, samt hur verksamheten arbetar med egna interna kontroller för att säkerställa att dataskyddsförordningen efterlevs.

Kontrollpunkt 6: Utbildning

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

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.

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.

Kontrollpunkt 9: Konsekvensbedömning/samråd

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

Kontrollpunkt 10: IT-projekt och upphandling

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

Kontrollpunkt 11: IT-system och digitala verktyg

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

Kontrollpunkt 12: Hantering av registrerades rättigheter

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

3.2 Fördjupad kontroll 2022

Den fördjupade kontrollen utgår från verksamhetens specifika risker. För verksamhetsåret har följande punkt/punkter fastställts:

Fokusområde: Biträdesavtal och andra överenskommelser

Den personuppgiftsansvarige är ansvarig för all behandling som utförs å dennes vägnar. En personuppgiftsansvarig som anlitar ett personuppgiftsbiträde att utföra personuppgiftsbehandlingar för sin räkning är alltså fortfarande personuppgiftsansvarig och kan inte avsäga sig de skyldigheter som följer av detta ansvar. Det är således av stor vikt att personuppgiftsansvariga har överblick över sina anlitade personuppgiftsbiträden och att de uppfyller de kvalitetskrav och krav vid anlitande av underbiträden som uppställs i dataskyddsförordningen.

Förordningen kräver också att förhållandet mellan den personuppgiftsansvarige och personuppgiftsbiträdet regleras genom avtal (eller annan rättsakt) och det är den personuppgiftsansvarige som är ansvarig för att ett sådant avtal upprättas. Förordningen uppställer även vissa krav på vad ett sådant avtal ska innehålla.

Denna fördjupade kontroll syftar till att undersöka vilka personuppgiftsbiträden som behandlar personuppgifter för Higabs räkning och ifall dessa förhållanden är reglerade genom adekvata avtal. För att skapa en överblick över den personuppgiftsansvariges övergripande arbete med personuppgiftsbiträden inkluderar kontrollen även en undersökning av vilka rutiner och arbetssätt som den personuppgiftsansvarige har vid anlitande av personuppgiftsbiträden.

4 Uppföljning

4.1 Uppföljning av lämnade rekommendationer

I dataskyddsförordningen anges att dataskyddsombudet ska rapportera direkt till den personuppgiftsansvariges eller personuppgiftsbiträdets högsta förvaltningsnivå, för att säkerställa att högsta ledningen är medveten om dataskyddsombudets råd och rekommendationer. Detta är grunden för ett proaktivt arbetssätt och utgör en trygghet för nämnd/styrelse som uppmärksammas på status och observerade brister i dataskyddsarbetet. Det är då också av vikt för nämnd/styrelse att veta hur eventuella rekommendationer/brister omhändertagits. Dataskyddsombudet kommer därför årligen att följa upp hanteringen av de rekommendationer som lämnats till verksamheten och rapportera detta i årsrapporten.

4.1.1 Uppföljning av hittills genomförda kontroller

Sedan dataskyddsförordningen trädde i kraft i maj 2018 har dataskyddsombudet genomfört ett antal kontroller för er verksamhet. För det fall att rekommendationer för tidigare kontroller kvarstår genomförs en särskild uppföljning. I annat fall kommer kontrollerna att följas upp inom ramen för de fasta kontrollpunkterna.

5 Rapportering till nämnd/styrelse

5.1 Delårsrapportering

I juni månad kommer respektive nämnd/styrelse att få en delårsrapport för dataskyddsarbetet av dataskyddsombudet. Fokus för delsårsrapporteringen är den verksamhetsspecifika fördjupade kontrollen som genomförs under våren.

Genom en delårsrapportering säkerställs att personuppgiftsansvarig nämnd/styrelse hålls informerad om dataskyddsombudets observationer av verksamhetens personuppgiftshantering. Formen för rapporteringen anpassas efter dataskyddsombudets bedömning av verksamhetens behov.

5.2 Årsrapport

Verksamhetens dataskyddsarbete kommer att sammanställas i en skriftlig årsrapport till nämnd/styrelse. Årsrapporten kommer innehålla information om verksamhetens samarbete med dataskyddsombudet, genomförda kontroller, lämnade rekommendationer samt en övergripande bedömning av status på verksamhetens personuppgiftshantering utifrån fasta kontrollpunkter.

För att möjliggöra en direkt kommunikation mellan dataskyddsombud och personuppgiftsansvarig nämnd/styrelse ska årsrapporten presenteras i möte med nämnd/styrelse.

5.3 Särskilt yttrande till högsta ledning

Om det skulle uppstå situationer där den ansvarige fattar beslut som är oförenliga med den allmänna dataskyddsförordningen och dataskyddsombudets råd, till exempel om en allvarlig brist kvarstår och inte åtgärdas, har dataskyddsombudet möjlighet att klargöra sin avvikande ståndpunkt genom ett yttrande riktat till högsta förvaltningsnivå och till dem som fattar besluten.

5.4 Beslutanderätten i dataskyddsfrågor

Beslutanderätten i dataskyddsfrågor ligger alltid på den personuppgiftsansvarige och aldrig på dataskyddsombudet. Dataskyddsombudet är en specialist med en rådgivande roll och är en resurs som, på ett oberoende sätt, fokuserar på dataskyddsfrågorna i verksamheten och på det sättet bistår den personuppgiftsansvarige med bedömningar och råd. Om nämnden/styrelsen väljer att inte följa dataskyddsombudets rekommendationer ska skälen till detta motiveras och dokumenteras i enlighet med god praxis samt för att uppfylla ansvarsskyldigheten. Detta är även viktigt för det fall frågan senare skulle bli föremål för tillsyn.

6 Kontakt

Eventuella frågor och synpunkter hänvisas i första hand till er kontaktperson. Frågor kan också alltid ställas till dso@intraservice.goteborg.se.