

Styrelsehandling 7

Utfärdat 2024-02-07

Ärendenummer STJ-2023-00202

Handläggare

Louise Ternlind

Telefon: 031-7738382

E-post: louise.ternlind@storningsjouren.goteborg.se

Årsrapport för dataskyddsarbetet 2023

Informationsärende

Styrelsen Störningsjouren i Göteborg AB

Dataskyddsombudets information till styrelsen samt årsrapport om dataskyddsarbetet 2023 föreslås antecknas.

Sammanfattning

I Göteborgs Stad fullgör dataskyddsenheten på Intraservice uppdraget som dataskyddsombud för förvaltningar och bolag. Dataskyddsombudet har i uppdrag att oberoende granska verksamheternas arbete med dataskyddsfrågor för att säkerställa att dataskyddslagstiftningen efterlevs. Enligt lag ska dataskyddsombudet rapportera till verksamheternas högsta förvaltningsnivå. Dataskyddsombudet lämnar årligen en rapport till varje nämnd och bolag om det kontrollarbete som genomförts och iakttagelser som har gjorts.

I årsrapporten 2023 redogör dataskyddsombudet resultatet av årets granskning av fasta kontrollpunkter samt uppföljning av verksamhetens hantering av lämnade rekommendationer från tidigare genomförda kontroller.

Samverkan

Ärendet anses inte vara föremål för samverkan

Bilagor

1. Årsrapport för dataskyddsarbetet 2023.

Handläggarens namn

Louise Ternlind

Befattning

Dataskyddskontakt

Chefens namn

Sofia Gärdsfors

Befattning

Vd



Årsrapport för dataskyddsarbetet 2023

Störningsjouren i Göteborg AB

2023-12-20

Innehåll

1	Inledning	3
1.1	Dataskyddsbud i Göteborgs Stad	3
2	Särskilda iakttagelser 2023	4
2.1	Stadenövergripande	4
2.1.1	Förutsättningar för en hållbar digitalisering	4
3	Granskning av dataskyddsarbetet 2023.....	5
3.1	Kontroll av fasta kontrollpunkter.....	5
3.2	Resultat från kontrollen 2023	5
3.2.1	Kontrollpunkt 1: Dataskyddsorganisation	6
3.2.2	Kontrollpunkt 2: Personuppgiftsincidenter	6
3.2.3	Kontrollpunkt 3: Biträdesavtal och andra överenskommelser ..	7
3.2.4	Kontrollpunkt 4: Register över personuppgiftsbehandlingar ...	8
3.2.5	Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet	8
3.2.6	Kontrollpunkt 6: Utbildning	9
3.2.7	Kontrollpunkt 7: Informationsplikt	9
3.2.8	Kontrollpunkt 8: E-post och dokumenthantering.....	10
3.2.9	Kontrollpunkt 9: Konsekvensbedömning/samråd	10
3.2.10	Kontrollpunkt 10: IT-projekt och upphandling	11
3.2.11	Kontrollpunkt 11: IT-system och digitala verktyg	11
3.2.12	Kontrollpunkt 12: Hantering av registrerades rättigheter	12
3.3	Uppföljning	12
3.3.1	Uppföljning av rekommendationer lämnade inom ramen för tidigare genomförda kontroller	12
4	Rekommenderade fokusområden 2024	14
5	Bilagor	15

1 Inledning

Dataskyddsförordningen (GDPR) har tillkommit för att särskilt skydda människors rätt till integritet, och för att värna var och ens rätt att få ha kontroll över vad som sker med uppgifter om ens person. Rätten till en fredad privat sfär och personlig integritet är grundläggande i ett demokratiskt samhälle och är ett av fundamenten på vilket många andra av våra demokratiska rättigheter vilar. Dataskyddsreglerna styr hur personuppgifter får samlas in, användas och hanteras för att säkerställa att uppgifterna används korrekt och rättvist. Lagstiftningen finns till för att skydda individen från skada och sätter ramarna för hur personuppgifter får behandlas i en alltmer digital värld. Dataskydd handlar i grunden om att skapa ett socialt hållbart samhälle.

1.1 Dataskyddsombud i Göteborgs Stad

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

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

Årsrapporten är avsedd att kunna användas som ett stöd för verksamheten i sitt fortsatta arbete med dataskydd. Det är upp till varje verksamhet att besluta om hur det interna dataskyddsarbetet ska utformas utifrån verksamhetens förutsättningar för att på bästa sätt kunna hantera identifierade risker.

2 Särskilda iakttagelser 2023

2.1 Stadenövergripande

2.1.1 Förutsättningar för en hållbar digitalisering

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

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

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

3 Granskning av dataskyddsarbetet 2023

3.1 Kontroll av fasta kontrollpunkter

Under 2023 har dataskyddsombudet kontrollerat verksamhetens dataskyddsarbete utifrån de tolv fasta kontrollpunkterna. Kontrollen har genomförts genom en enkät. Enkäten består av tolv punkter ("fasta kontrollpunkter") där varje punkt innehåller ett antal delfrågor i form av påståenden och/eller skattningsfrågor. Enkäten är avsedd att spänna över de viktigaste delarna inom dataskyddsarbetet för att på så sätt fånga in en större bredd av frågor. Metoden syftar till att få till ett långsiktigt och systematiskt arbetssätt som möjliggör uppföljning över tid.

I arbetet används en modell som består av fyra kategorier, vilka representerar fyra olika risknivåer. Verksamheten får utifrån sina svar ett värde som visar vilken risknivå verksamheten befinner sig på inom respektive kontrollpunkt. Genom att arbeta med risknivåer möjliggörs ett riskbaserat arbetssätt för både verksamhet och dataskyddsombud, då resultaten ger en bild av vad verksamheten behöver prioritera i dataskyddsarbetet framåt.¹

Riskenivå	Beskrivning	Färgkod
Nivå 1	Höga risker identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten.	
Nivå 2	Risker identifierade som bedöms vara omfattande och/eller kräver omgående åtgärder.	
Nivå 3	Risker identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga.	
Nivå 4	Inga direkta risker av betydelse identifierade. Indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete.	

3.2 Resultat från kontrollen 2023

I detta avsnitt anges vilken risknivå verksamheten befinner sig inom för respektive kontrollpunkt, baserat på verksamhetens svar på de fasta kontrollpunkterna. Under varje kontrollpunkt presenteras även dataskyddsombudets bedömning gällande verksamhetens risker utifrån de iakttagelser som dataskyddsombudet gjort under året. För beskrivning av respektive kontrollpunkt se bilaga 2.

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

3.2.1 Kontrollpunkt 1: Dataskyddsorganisation

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet har inte fått några indikationer som medför en annan övergripande bedömning än den som bolaget gör, men har inte heller kontrollerat dataskyddsorganisationen särskilt.

I skattningen anger bolaget att det inom verksamheten finns dokumenterade arbetssätt som säkerställer att dataskyddsombudet regelbundet kontaktas för att delta i frågor som rör skyddet av personuppgifter. Dataskyddsombudet kan utifrån den begränsade kontakt som varit mellan bolaget och dataskyddsombudet under året se att det finns en risk i att dataskyddsombudet ej involveras i tillräcklig utsträckning i det interna dataskyddsarbetet. Även om det finns en mognad i frågorna inom bolaget och ett utbyte på koncernnivå behöver bolaget säkerställa att dataskyddsombudet involveras i frågorna. Utifrån det uppmuntras bolaget att framåt se över hur verksamheten kan involvera dataskyddsombudet mer i arbetet med dataskydd, med syftet att säkerställa att bolaget uppfyller kravet enligt artikel 38.1 i GDPR gällande att dataskyddsombudet ska involveras i alla frågor som gäller dataskydd.

3.2.2 Kontrollpunkt 2: Personuppgiftsincidenter

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet har inte fått några direkta indikationer som medför en annan bedömning än den som bolaget gör, men har inte heller kontrollerat hanteringen särskilt.

Vid genomgången av årsrapporten angav bolaget att de incidenter som inträffat under året handlar nästan enbart om felskickade mejl, och att medarbetares kunskaper inom området upplevs ha ökat. Även om bolaget har en fungerande metod för att omhänderta de incidenter som den interna dataskyddsorganisationen får kännedom om, är dataskyddsombudets bedömning att antalet samt typen (utifrån att det nästan uteslutande anges handla om samma typ av incident) av incidenter fortfarande indikerar att det föreligger risker inom kontrollpunkten. Tröskeln för när en personuppgiftsincident har skett är låg och personuppgiftsincidenter kommer ofrånkomligen att inträffa även i organisationer

som har mycket väl utvecklade rutiner för att förhindra att personuppgiftsincidenter sker. Utifrån detta rekommenderas bolaget framåt att utvärdera om rutinerna och den allmänna medvetenheten hos medarbetarna ger tillräckligt goda förutsättningar för att identifiera såväl som hantera eventuella personuppgiftsincidenter.

3.2.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser



Dataskyddsombudets bedömning

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

De risker som identifierats utifrån bolaget skattning gäller andelen upprättade personuppgiftsbiträdesavtal samt genomförande av efterlevnadskontroller. Gällande upprättade personuppgiftsbiträdesavtal anger bolaget att det har tecknats personuppgiftsbiträdesavtal, inkluderat instruktioner, med samtliga biträden. Detta ser dataskyddsombudet anledning till att ifrågasätta utifrån att förvaltningen för Intraservice är en tjänsteleverantör till bolaget och det för de behandlingar som Intraservice utför ej finns instruktioner framtagna. Vid genomgången av årsrapporten angav bolaget dock att skattningen avsåg de biträden som bolaget självt har rådighet över. Dataskyddsombudet vill därför lyfta att bolaget vid kommande kontroller behöver ta hänsyn till samtliga biträdesrelationer för att resultatet inte ska bli missvisande.

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

3.2.4 Kontrollpunkt 4: Register över personuppgiftsbehandlings

Verksamhetens skattning av risknivå



Dataskyddsbudets bedömning

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

Bolaget anger att samtliga av bolagets personuppgiftsbehandlingsregister, och att samtliga av dessa behandlingsregister innehåller den information som ska finnas med enligt artikel 30 i GDPR. Dataskyddsbudet har efter en stickprovskontroll av behandlingsregister i registret kunnat konstatera att skattningen inte stämmer överens med de faktiska omständigheterna, och att den information som anges för respektive behandling ej är tillräcklig utförlig för att uppfylla kraven enligt artikel 30 i GDPR. Utifrån den gjorda kontrollen rekommenderas bolaget göra en helhetsöversyn av behandlingsregistret och den information som finns inlagd. Bolaget rekommenderas se över hur behandlingsregister definierats då det bedöms finnas ett behov av att bryta ner flera av behandlingsregisterna i mindre delar, samt säkerställa att (om bolaget väljer att ange rättslig grund) enbart en rättslig grund finns angiven per behandling. Bolaget behöver även säkerställa att alla personuppgifter som behandlas finns angivna i registret.

Vidare har dataskyddsbudet också kunnat se att informationen i behandlingsregistret och informationen i integritetsinformationen på bolagets hemsida om när bolaget är personuppgiftsansvarig skiljer sig åt. Bolaget behöver säkerställa att informationen som lämnas blir korrekt och, vid behov, utreda ansvarsförhållandena för behandlingsregisterna.

Bolaget rekommenderas prioritera arbetet med att registrera samtliga personuppgiftsbehandlingsregister i behandlingsregistret, samt säkerställa att dessa innehåller den information som ska finnas med enligt artikel 30 i GDPR.

Under året har dataskyddsbudet utfört en informationsinsats om behandlingsregistret och tillhandahållit såväl muntlig information som skriftligt underlag för stadens samtliga verksamheter. Bolaget kan med fördel använda sig av underlaget som stöd i arbetet framåt.

3.2.5 Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet har inte involverats i några frågor kopplat till kontrollpunkten, men har ingen anledning att göra en annan bedömning än den som verksamheten har gjort avseende risknivå.

Bolaget rekommenderas att fortsatt arbeta för att bibehålla de goda förutsättningar som finns enligt skattningen.

3.2.6 Kontrollpunkt 6: Utbildning

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet delar till stor del verksamhetens bedömning. I dialog med verksamheten har dataskyddsombudet informerats om att bolaget försöker integrera dataskydd i andra utbildningar samt att bolaget använder den digitala grundutbildningen i dataskydd.

Även inom verksamheter med låga risker krävs det kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare. Förbättringsåtgärder som dataskyddsombudet har identifierat och som skulle kunna vidtas inom ramen för kontrollpunkten gäller att se över och stärka den allmänna kunskapsnivån inom verksamheten, med syftet att säkerställa att de goda förutsättningarna som finns bibehålls.

3.2.7 Kontrollpunkt 7: Informationsplikt

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

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

För bolagets del lyfte dataskyddsombudet i årsrapporten 2022 att det fanns skäl för bolaget att se över hur utövandet av bolagets informationsplikt kunde förbättras. Exempel på hur detta skulle kunna göras lämnades även i årsrapporten. Efter att ha kontrollerat bolagets nuvarande information på hemsidan gör dataskyddsombudet

bedömningen att de rekommendationer som lämnades 2022 ej har omhändertagits, vilket också bolagets egen skattning indikerar. Utifrån bolagets skattning på frågan om verksamhetens integritetsinformation uppfyller kraven på information enligt GDPR är dataskyddsombudets bedömning att bolaget är medvetna om bristerna i nuvarande integritetsinformation. Viss dialog har även varit mellan dataskyddsombudet och bolaget gällande hur informationen framåt skulle kunna utformas.

Sammantaget bedömer dataskyddsombudet att bolaget behöver göra en översyn av hur informationsplikten hanteras som helhet. I detta arbete är integritetspolicyn en del, och bolaget rekommenderas framåt säkerställa att de rekommendationer som 2022 lämnades kopplat till den specifika informationen i integritetspolicyn omhändertas. En förutsättning för att bolaget ska kunna uppfylla kraven på information är också att behandlingsregistret är fullständigt, och att bolagets ansvar för olika personuppgiftsbehandlingar är utrett (se kontrollpunkt 4).

Under året har dataskyddsombudet utfört en informationsinsats om informationsplikten och tillhandahållit såväl muntlig information som skriftligt underlag för stadens samtliga verksamheter. Bolaget kan använda sig av underlaget som stöd i arbetet med informationsplikten.

3.2.8 Kontrollpunkt 8: E-post och dokumenthantering

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet har inte fått några direkta indikationer som medför en annan bedömning än den som bolaget gör, men har inte heller kontrollerat hanteringen särskilt.

Bolaget rekommenderas att fortsatt arbeta för att bibehålla de goda förutsättningar som finns enligt skattningen.

3.2.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet delar till viss del verksamhetens bedömning, men

gör till skillnad ifrån verksamheten bedömningen att det inom kontrollpunkten förekommer risker som kräver åtgärder.

Bolaget anger, likt 2022, att det finns framtagna konsekvensbedömningar för ca 75 % av de personuppgiftsbehandlingar som kräver det. Utifrån att bolaget bedöms behöva åtgärda nuvarande register över personuppgiftsbehandlingar utifrån bland annat hur behandlingarna hittills har definierats, ser dataskyddsombudet att det föreligger en risk för att de konsekvensbedömningar som hittills genomförts ligger på en för övergripande nivå. Bolaget kommer sannolikt behöva uppdatera befintliga såväl som att ta fram nya konsekvensbedömningar i takt med att behandlingsregistret färdigställs.

Bolaget rekommenderas därför att i takt med att behandlingsregistret uppdateras se över genomförda konsekvensbedömningar och ta fram en handlingsplan för arbetet med att uppdatera och/eller ta fram nya konsekvensbedömningar.

3.2.10 Kontrollpunkt 10: IT-projekt och upphandling

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet har under året inte involverats i några frågor kopplat till kontrollpunkten, men har ingen anledning att göra en annan bedömning än den som verksamheten har gjort avseende risknivå då bolaget tidigare år involverat dataskyddsombudet i det arbete som bedrivits.

Bolaget rekommenderas att fortsatt arbeta för att bibehålla de goda förutsättningar som finns enligt skattningen.

3.2.11 Kontrollpunkt 11: IT-system och digitala verktyg

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

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

Även vid årets genomgång av bolagets kommunikationskanaler noterar dataskyddsombudet att bolaget använder sociala medier (LinkedIn). Trots att förutsättningarna för överföringar till amerikanska leverantörer har ändrats finns

fler aspekter att ta hänsyn till än enbart tredjelandsproblematiken. Bolaget rekommenderas bland annat att kartlägga vilka behandlingar och vilka personuppgifter som behandlas av bolaget kopplat till användningen av sociala medier, utreda om profilering sker och identifiera vilka ansvarsförhållanden som råder för de olika behandlingarna. Vidare rekommenderas bolaget att utföra och dokumentera noggranna riskanalyser samt se över för vilka behandlingar kopplat till användningen av sociala medier som kräver en konsekvensbedömning.

3.2.12 Kontrollpunkt 12: Hantering av registrerades rättigheter

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet har inte fått några direkta indikationer som medför en annan bedömning än den som bolaget gör, men har inte heller kontrollerat hanteringen särskilt.

Den risk som dataskyddsombudet bedömer kan föreligga inom kontrollpunkten är kopplad till bolagets register över personuppgiftsbehandlingar. Utan överblick av alla behandlingar som sker inom verksamheten finns en risk att bolaget missar behandlingar som görs inom verksamheten vid handläggning av registerutdrag.

Bolaget rekommenderas framåt att fortsatt arbeta för att utveckla och bibehålla de goda förutsättningar som finns enligt skattningen, men samtidigt vara medvetna om den risk som föreligger kopplat till ett ofullständigt behandlingsregister.

3.3 Uppföljning

3.3.1 Uppföljning av rekommendationer lämnade inom ramen för tidigare genomförda kontroller

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

Kontroll (2022): Behörighetsstyrning

Verksamheten gavs följande 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.

Kommentarer och rekommendationer:

I uppföljningen anger bolaget att det installerats en "ärendelogg" i systemet som är synligt för alla medarbetare där man direkt ser vem som läst i ärendet och snabbt kan upptäcka eventuella undantag som behöver hanteras. Bolaget bedömer att det faktum att medarbetarna själva kan se loggen i sina ärenden i sig innebär en minskad risk för att man läser i fel ärende. Om man som handläggare bedömer att någon "obehörig" har läst i ett ärende ska närmaste chef kontaktas för att utreda frågan vidare.

Ytterligare åtgärder som vidtagits utifrån rekommendationerna är att det nu i bolagets anvisning för informationshantering framgår:

- att det inte är tillåtet att söka i ärendehanteringssystem eller upplysningstjänst för eget intresse eller av andra behov som inte är förenligt med arbetsuppgifter eller det specifikt angivna ändamålet.
- Information om att loggkontroller görs regelbundet via stickprov samt vid behov så som vid misstanke om oegentlighet, hur misstankar kring oegentligheter ska hanteras, vilka funktioner/roller som ansvarar för genomförandet av kontroller och vilka eventuella konsekvenser agerandet kan få för enskilda.

Uppföljningen visar att verksamheten har vidtagit flera åtgärder i enlighet med de rekommendationer som lämnades 2022. Den rekommendation som dataskyddsombudet bedömer kvarstå gäller att bolaget fortfarande behöver förtydliga vad som utgör misstanke om oegentlighet, särskilt utifrån att bolaget i anvisningen anger att det är en "låg tröskel" för vad som utgör en sådan.

Utifrån att bolaget vidtagit flera åtgärder för att säkerställa behörighetsstyrningen bedömer dataskyddsombudet att fortsatt uppföljning kan ske inom ramen för de fasta kontrollpunkterna, om inget särskilt föranleder att det behöver följas upp separat under 2024.

4 Rekommenderade fokusområden 2024

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

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

- Kontrollpunkt 4: Register över personuppgiftsbehandlingar

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

- Kontrollpunkt 7: Informationsplikt

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

- Kontrollpunkt 9: Konsekvensbedömningar/samråd

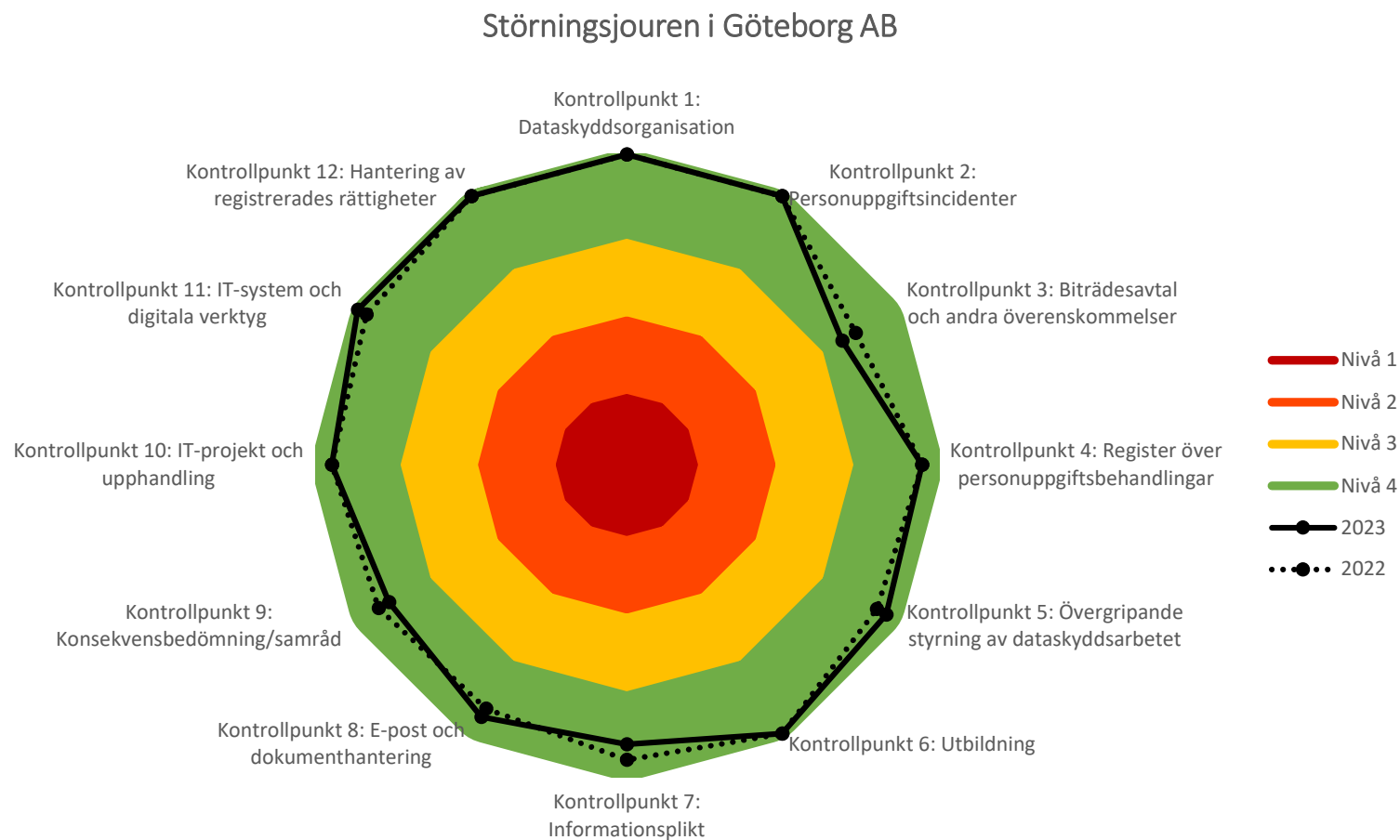
I takt med att behandlingsregistret uppdateras se över genomförda konsekvensbedömningar och ta fram en handlingsplan för hanteringen för arbetet med att uppdatera och/eller ta fram nya konsekvensbedömningar. Fokus för arbetet ska vara på de behandlingar som kan innebära höga risker för de registrerade.

5 Bilagor

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

Bilaga 2: Kontrollplan för dataskyddsarbetet 2023–2024.

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





Störningsjouren i Göteborg AB

Kontrollplan för dataskyddsarbetet 2023–2024

2023-02-06

Innehåll

1	Bakgrund.....	3
1.1	Ny utformning av kontrollarbetet	3
2	Kontrollarbetet 2023–2024	4
2.1	Kontrollarbetets delar.....	4
2.2	Tidplan för kontrollarbetet 2023–2024	5
3	Kontroller	5
3.1	Fasta kontrollpunkter	5
3.2	Fördjupad kontroll.....	6
3.3	Uppföljning av genomförda kontroller	6
4	Rapportering.....	7
4.1	Årsrapport.....	7
4.2	Särskilt yttrande.....	7
5	Kontakt.....	7

1 Bakgrund

Att få ta del av och hantera andra människors personliga uppgifter på ett sådant sätt som kommunala förvaltningar och bolag gör innebär att förvalta ett stort förtroende. Dataskyddsförordningen (GDPR) har tillkommit för att särskilt värna om den enskildes rätt till integritet och kontroll över vad som sker med ens personuppgifter. Att förvaltningar och bolag hanterar personuppgifter i enlighet med gällande lag bör vara en självklarhet i syfte att visa omsorg om det förtroende som givits den som har att hantera personuppgifter.

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

1.1 Ny utformning av kontrollarbetet

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

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

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

2 Kontrollarbetet 2023–2024

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

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

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

2.1 Kontrollarbetets delar

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

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

2.2 Tidplan för kontrollarbetet 2023–2024

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

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

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

3 Kontroller

3.1 Fasta kontrollpunkter

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

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

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

För beskrivning av de fasta kontrollpunkterna, se bilaga 1.

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

3.2 Fördjupad kontroll

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

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

3.3 Uppföljning av genomförda kontroller

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

4 Rapportering

4.1 Årsrapport

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

4.2 Särskilt yttrande

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

5 Kontakt

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

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

Bilaga 1 - Beskrivning av fasta kontrollpunkter

Kontrollpunkt 1: Dataskyddsorganisation

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

Kontrollpunkt 2: Personuppgiftsincidenter

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

Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

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

Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Kontrollpunkten avser verksamhetens efterlevnad av skyldigheten att systematiskt dokumentera alla personuppgiftsbehandlingar i form av ett register. Även verksamhetens arbete med, och rutin för, att säkerställa ett uppdaterat och heltäckande register innefattas.

Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

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

Kontrollpunkt 6: Utbildning

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

Kontrollpunkt 7: Informationsplikt

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

Kontrollpunkt 8: E-post och dokumenthantering

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

Kontrollpunkt 9: Konsekvensbedömning/samråd

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

Kontrollpunkt 10: IT-projekt och upphandling

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

Kontrollpunkt 11: IT-system och digitala verktyg

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

Kontrollpunkt 12: Hantering av registrerades rättigheter

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