Göteborgs Stad

Tjänsteutlåtande
Utfärdat 2024-01-31
Diarienummer 0006/23

Handläggare
Gustaf Sjöstedt, Mathias Henriksson
Telefon: 031-365 00 00 (växel)
E-post: fornamn.efternamn@arbvux.goteborg.se

Information från nämndens dataskyddsombud om årsrapport för dataskyddsarbetet 2023

Förslag till beslut

Nämnden för arbetsmarknad och vuxenutbildning antecknar informationen till protokollet.

Sammanfattning

Nämnden för arbetsmarknad och vuxenutbildning är enligt nämndens reglemente personuppgiftsansvarig för de behandlingar av personuppgifter som sker i verksamheten. Dataskyddsombudets roll är att ge råd och information till den personuppgiftsansvarige. I uppdraget ingår även att följa upp att den personuppgiftsansvarige följer dataskyddslagstiftningen. Dataskyddsombudet driver eller utför dock inte själva arbetet med dataskydd, utan detta arbete utförs av förvaltningens egna medarbetare.

I det här ärendet informerar nämndens dataskyddsombud om förvaltningens dataskyddsarbete under 2023, inklusive de kontroller som dataskyddsombudet genomfört under året samt uppföljning av dessa. De rekommendationer som dataskyddsombudet lämnat kommer tas om hand i förvaltningens fortsatta utvecklingsarbete inom dataskyddsområdet.

Bedömning ur ekonomisk dimension

I Sverige är Integritetsskyddsmyndigheten ansvarig tillsynsmyndighet för att gällande dataskyddslagstiftning följs. Integritetsskyddsmyndigheten har ytterst getts rätt att besluta om sanktionsavgifter när reglerna inte följs. Hur hög sanktionsavgiften blir beror dels på vilken bestämmelse överträdelsen gäller, dels på omständigheterna i det enskilda fallet. Integritetsskyddsmyndigheten ska bland annat att titta på hur allvarlig överträdelsen är, hur stor skada som skett, om det är fråga om känsliga personuppgifter och om överträdelsen är avsiktlig.

Bedömning ur ekologisk dimension

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

Bedömning ur social dimension

Dataskyddslagstiftningen är till för att skydda grundläggande rättigheter och friheter, särskilt enskildas rätt till skydd av sina personuppgifter. Grunden till enskildas integritetsskydd har även stöd i Europakonventionen, EU:s stadga om de grundläggande rättigheterna och den svenska regeringsformen.

Som kommunal myndighet har arbetsmarknad och vuxenutbildning generellt rätt att hantera enskildas personuppgifter om det är nödvändigt för att utföra vårt myndighetsuppdrag, förutsatt att dataskyddsförordningens grundläggande principer i övrigt följs.

Bilagor

1. Årsrapport för dataskyddsarbetet 2023, 2022-12-21

Ärendet

I det här ärendet informerar nämndens dataskyddsombud om förvaltningens dataskyddsarbete under 2023.

Beskrivning av ärendet

Dataskyddsförordningen ställer krav på att bland annat alla myndigheter och andra offentliga organ ska ha ett dataskyddsombud. Dataskyddsombudets roll är att ge råd och information till den personuppgiftsansvarige. I uppdraget ingår även att följa upp att den personuppgiftsansvarige följer dataskyddslagstiftningen genom att till exempel utföra kontroller på området. Däremot driver eller utför dataskyddsombudet inte själva arbetet med dataskydd, utan detta arbete utförs av förvaltningens egna medarbetare. I Göteborgs Stad är dataskyddsombuden organisatoriskt placerade på förvaltningen för Intraservice.

Enligt dataskyddsförordningen är personuppgiftsansvarig den som bestämmer för vilka ändamål uppgifter ska behandlas och hur behandlingen ska gå till. Nämnden är enligt kommunfullmäktiges beslutade reglemente personuppgiftsansvarig för de behandlingar av personuppgifter som sker i dess verksamhet. Med rollen som personuppgiftsansvarig följer en lång rad administrativa och säkerhetsmässiga krav för att uppfylla lagstiftningen på området.

Årsrapport för dataskyddsarbetet 2023

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.

Utifrån den uppföljning av tolv fasta kontrollpunkter som presenteras i årsrapporten rekommenderar dataskyddsombudet att förvaltningen bör fokusera på områdena konsekvensbedömningar/samråd samt IT-system och digitala verktyg inom dataskyddsarbetet 2024.

Dataskyddsombudet har under året även följt upp vilka åtgärder som förvaltningen genomfört utifrån tidigare års lämnade rekommendationer, vilket visar att samtliga rekommendationer är omhändertagna.

Förvaltningens bedömning

Bilaga 1 till årsrapporten visar resultat av fasta kontrollpunkter 2023 jämfört med 2022, där det framgår att förvaltningens dataskyddsarbete generellt utvecklats positivt sedan senaste motsvarande uppföljning.

De rekommendationer som dataskyddsombudet lämnat i årsrapporten kommer tas om hand i förvaltningens fortsatta utvecklingsarbete inom området.

Andreas Lökholm
Förvaltningsdirektör

Daniel Falkemo
Vik. HR- och kanslichef

Göteborgs Stad

Årsrapport för dataskyddsarbetet 2023

Nämnden för arbetsmarknad och vuxenutbildning

2023-12-21

Innehåll

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 dataskydds-lagstiftningen 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 dataskydds-perspektivet 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]

Risknivå	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 delar verksamhetens bedömning och anser att verksamheten har ett systematiskt arbete inom kontrollpunkten och inga risker av betydelse föreligger.

Förvaltningen rekommenderas därför att fortsatt arbeta för att bibehålla de goda förutsättningar som finns enligt skattningen. Förvaltningen har även muntligen framfört att det kommer att ske en omorganisation under 2024. Dataskyddsombudet rekommenderar därför förvaltningen att kontinuerligt under 2024 utvärdera den interna organisationen för att säkerställa att den har rätt förutsättningar för att bedriva ett effektivt dataskyddsarbete.

Dataskyddsombudet ser även att förvaltningen i större utsträckning bör involvera sitt dataskyddsombud. Dataskyddsombudets uppfattning är att det är flera områden där dataskyddsombudet inte har involverats under året, vilket även framgår inom vissa kontrollpunkter nedan.

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 delar verksamhetens bedömning och anser att verksamheten har ett systematiskt arbete inom kontrollpunkten.

Även inom verksamheter med låga risker krävs det kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare.

Dataskyddsombudet har under året endast involverats vid ett fåtal av förvaltningens personuppgiftsincidenter. Dataskyddsombudet rekommenderar därför förvaltningen att involvera dataskyddsombudet i de fall då det föreligger osäkerhet kring en personuppgiftsincident.

Av förvaltningens skattning framgår det att ca 50 % av förvaltningens personuppgiftsincidenter rapporteras inom 72 timmar till Integritetskyddsmyndigheten (IMY). Dataskyddsombudet rekommenderar därför

förvaltningen att se över rutinerna för anmälan till IMY i samband med en personuppgiftsincident och identifiera varför vissa anmälningar inte kommer in i tid.

3.2.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

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. Dataskyddsombudet gör dock till skillnad ifrån verksamheten bedömningen att det ändå föreligger risker inom kontrollpunkten.

Dataskyddsombudet har identifierat följande riskområden där verksamheten behöver vidta åtgärder:

Förra året rekommenderade dataskyddsombudet att förvaltningen börjar följa upp tidigare tecknade biträdesavtal. Dataskyddsombudet känner inte till att det arbetet har påbörjats eller så har dataskyddsombudet inte varit involverat i frågan. Under årets självskattning har förvaltningen även skattat ett lägre värde vad gäller uppföljning av biträdesavtal varför detta torde utgöra en reell risk. Dataskyddsombudet rekommenderar därför förvaltningen att under kommande år fokusera på uppföljning och efterlevnadskontroller av sina biträdesavtal.

Vidare anger förvaltningen att personuppgiftsbiträdesavtal har tecknats med hundraprocent av de biträden som har anlitas av förvaltningen. Dataskyddsombudet ställer sig frågande till detta eftersom personuppgiftsansvaret kopplat till stadens interna tjänsteleverantörer inte har utretts. Efter muntlig avstämning med förvaltningen har det framkommit att avtal/överenskommelser inte har tecknats med stadens interna tjänsteleverantör. Förvaltningens bedömning är dock att avtal har tecknats i mer än 75% av fallen. Eftersom avtal inte har tecknats med de interna tjänsteleverantörerna och att det är ett krav att reglera hanteringen av personuppgiftsuppgifter med biträdet rekommenderas förvaltningen att föra dialog med stadens tjänsteleverantörer för att säkerställa att sådana upprättas.

3.2.4 Kontrollpunkt 4: Register över personuppgiftsbehandlingar

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 verksamhetens bedömning och anser att verksamheten har ett systematiskt arbete inom kontrollpunkten och inga risker av betydelse föreligger.

Även inom verksamheter med låga risker krävs det kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare.

Dataskyddsombudet har efter stickprov noterat att vissa behandlingar saknas i förvaltningens behandlingsregister, till exempel behandlingen för visselblåsfunktion. Dataskyddsombudet har även noterat att informationen inte alltid är helt korrekt. Eftersom behandlingsregistret är ett levande dokument rekommenderar dataskyddsombudet förvaltningen att fortsatt se över behandlingsregistret och säkerställa att det kontinuerligt uppdateras.

3.2.5 Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsombudet delar verksamhetens bedömning om att det finns risker som behöver åtgärdas, men gör precis som verksamheten bedömningen att de inte är omfattande, brådskande eller allvarliga.

Trots detta finns det ändå områden där verksamheten behöver genomföra åtgärder:

Dataskyddsperspektivet måste komma in i god tid vid frågor som innebär nya eller förändrade behandlingar så att dessa frågor omhändertas innan behandlingen påbörjas. Dataskyddsombudet har vid ett tillfälle under hösten lämnat rekommendationer på en tröskelanalys där behandlingen redan hade genomförts. För att risker med behandlingen ska kunna identifieras och säkerhetsåtgärder ska kunna vidtas är det viktigt att dataskyddsperspektivet finns med från början. Förvaltningen rekommenderas därför att vid nya eller förändrade behandlingar ha som rutin att inkludera sin dataskyddsorganisation samt involvera sitt dataskyddsombud i ett tidigare skede.

Förvaltningen har (liksom förra året) skattat sig något lägre vad gäller att ha rutiner för att säkerställa dataskyddet vid fysiska och digitala sammankomster/möten och vad gäller interna följsamhetskontroller. Dataskyddsombudets rekommendationer från förra året gäller därför fortsatt. Förvaltningen rekommenderas ser över hur det arbetas med dataskydd vid fysiska och digitala sammankomster samt ta fram

rutiner där detta saknas. Förvaltningen rekommenderas också att se över hur interna kontroller kan genomföras för att följa upp hur förvaltningen efterföljer GDPR. Detta är en viktig del av arbetet eftersom det annars är svårt att veta om framtagna rutiner och arbetssätt får önskad effekt.

3.2.6 Kontrollpunkt 6: Utbildning

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga.

Dataskyddsombudet delar verksamhetens bedömning om att det finns risker som behöver åtgärdas, men gör precis som verksamheten bedömningen att de inte är omfattande, brådskande eller allvarliga.

Trots detta finns det ändå områden där verksamheten behöver genomföra åtgärder:

Förvaltningen rekommenderas att fortsatt utbilda medarbetare för att öka och/eller bibehålla deras kunskapsnivå. Dataskyddsombudet rekommenderar också, i likhet med föregående år, att förvaltningen genomför en kartläggning av olika befattningars utbildningsbehov och undersöker var olika utbildningsinsatser kan behöva fokuseras.

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 verksamhetens bedömning och anser att verksamheten har ett systematiskt arbete inom kontrollpunkten och inga risker av betydelse föreligger.

Även inom verksamheter med låga risker krävs det kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare.

Förbättringsåtgärder som dataskyddsombudet identifierat kan vidtas inom ramen för kontrollpunkten gäller bland annat att säkerställa att de registrerade får rätt information i enlighet med art. 13 och 14 i GDPR. Integritetpolicyn på förvaltningens hemsida är inte heltäckande. Dataskyddsombudet är medveten om att information vid vissa behandlingar tillhandahålls på annat sätt till de registrerade. Det är dock viktigt att förvaltningen säkerställer att rätt information

ges vid samtliga av förvaltningens behandlingar. Dataskyddsombudet rekommenderar även förvaltningen att fortsatt arbeta med att uppdatera och justera integritetspolicyn.

3.2.8 Kontrollpunkt 8: E-post och dokumenthantering

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsombudet delar till viss del verksamhetens bedömning, men gör till skillnad ifrån verksamheten bedömningen att det inom kontrollpunkten förekommer risker som är omfattande och kräver åtgärder.

I samband med en personuppgiftincident under sommaren framgick det att förvaltningen saknar rutiner för hur skyddsvärda och känsliga personuppgifter får hanteras i e-post. Detta är även någonting som förvaltningen är medvetna om då förvaltningen har skattat sig lägre på denna punkt. Dataskyddsombudet rekommenderar därför förvaltningen att omgående ta fram rutiner kring hanteringen av e-post eftersom det kan innebära stora risker för de registrerade.

Dataskyddsombudet rekommenderar även (liksom föregående år) att förvaltningen säkerställer att rutiner kopplat till gallring finns på plats och efterlevs, eftersom principerna om uppgifts- och lagringsminimering är en viktig del av GDPR. Förvaltningen behöver också arbeta med sin informationsklassning samt ta fram rutiner för hur olika klasser får hanteras och var de får sparas/lagras. Detta är även någonting som förvaltningen själv har identifierat utifrån sin skattning.

3.2.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga.

Dataskyddsombudet delar till viss del verksamhetens bedömning, men gör till skillnad ifrån verksamheten bedömningen att det inom kontrollpunkten förekommer risker som är omfattande och kräver omgående åtgärder.

Dataskyddsombudets uppfattning är att förvaltningen har många pågående behandlingar där förvaltningen inte har gjort någon konsekvensbedömning trots att behandlingen kan innebära stora risker för de registrerade. Förvaltningens skattning torde indikera på att förvaltningen gör samma bedömning. I likhet med föregående

års enkätsvar har förvaltningen genomfört konsekvensbedömningar för ca 25 % av de behandlingar som förvaltningen utför och som har höga risker. Det anges inte heller att det i någon större utsträckning finns en planering för genomförandet av de konsekvensbedömningar där detta krävs.

Liksom föregående år, trots att förvaltningens placering inom risknivå tre, ser dataskyddsombudet att det här finns risker som omgående behöver åtgärdas. Dessa utgörs både av risker för de registrerade eftersom behandlingar där deras personuppgifter ingår inte har bedömts och risker för förvaltningen som vid en eventuell tillsyn kan få sanktionsavgifter. Förvaltningen har efter muntlig avstämning angett att ett arbete med att identifiera behandlingar med höga risker har påbörjats. Dataskyddsombudet rekommenderar förvaltningen att fortsatt identifiera behandlingar med höga risker och ta fram en handlingsplan för när arbetet med konsekvensbedömningar ska påbörjas och under vilken tidsperiod som arbetet förväntas fortlöpa. Dataskyddsombudet rekommenderar förvaltningen att prioritera detta arbete.

3.2.10 Kontrollpunkt 10: IT-projekt och upphandling

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsombudet delar verksamhetens bedömning om att det finns risker som behöver åtgärdas, men gör precis som verksamheten bedömningen att de inte är omfattande, brådskande eller allvarliga.

Trots detta finns det ändå områden där verksamheten behöver genomföra åtgärder:

Förvaltningen har skattat ett lägre värde på frågan om verksamheten har dokumenterade arbetssätt, vid införandet av nya digitaliseringslösningar, för att genomföra en risk-/behovsanalys med syftet att säkerställa att den nya lösningen uppfyller grundläggande principer enligt GDPR.

Dataskyddsombudet har inte blivit involverat i något projekt och/eller upphandling under året. Dataskyddsombudets uppfattning är att förvaltningen inom detta område (samt även generellt) är mycket självgående i dataskyddsfrågor, vilket är övervägande positivt. Dataskyddsombudet rekommenderar dock förvaltningen att rådgöra med dataskyddsombudet för att kunna identifiera potentiella risker för de registrerade. Dataskyddsombudet rekommenderar även förvaltningen att ta kontakt med dataskyddsombudet i ett tidigare skede så att dataskyddsperspektivet blir en del av hela processen. Förvaltningen bör därför se över sin arbetsprocess i denna del.

3.2.11 Kontrollpunkt 11: IT-system och digitala verktyg

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder. Dataskyddsombudet har under året inte involverats i någon fråga kopplad till kontrollpunkten, varför ingen särskild bedömning kan göras i frågan.

Utifrån förvaltningen egen skattning kan dock dataskyddsombudet utläsa att förvaltningens skattning är något lägre än förgående år vilket indikerar att verksamheten inte aktivt arbetar med frågor kopplat till kontrollpunkten. Förvaltningen har även angett en lägre skattning på samtliga frågor under kontrollpunkten. Vid muntlig avstämning kan förvaltningen inte riktigt besvara vad som är anledning till att skattningen är så låg inom kontrollpunkten. Dataskyddsombudet rekommenderar därför förvaltningen att se över frågorna under kontrollpunkten i stort. Dataskyddsombudet ser även att föregående års rekommendationer därmed kvarstår i sin helhet:

Förvaltningen rekommenderas att ta fram rutiner som säkerställer att tilldelning av behörigheter och åtkomst är begränsat till det som är nödvändigt. Förvaltningen rekommenderas också ta fram rutiner som säkerställer att behörigheter och åtkomster följs upp regelbundet. För att säkerställa att de IT-system och digitala verktyg som införs lever upp till kraven i förordningen rekommenderas förvaltningen också att ta fram en anskaffningsprocess. Förvaltningen bör även ta fram målgruppsanpassad information om hur personuppgifter behandlas i de digitala verktyg och IT-system som används. Det bör också finnas dokumenterat vilka IT-system och digitala verktyg som används inom förvaltningen.

Förvaltningen rekommenderas slutligen att säkerställa användningen av cookies på de hemsidor som förvaltningen ansvarar för. När det gäller användningen av cookies har dataskyddsombudet sedan tidigare tagit fram ett informationsmaterial som tillhandahållits stadens verksamheter. Informationsmaterialet redogör för gällande lagkrav och innehåller exempel på hur en cookieruta kan utformas. Förvaltningen rekommenderas utgå från detta i arbetet.

3.2.12 Kontrollpunkt 12: Hantering av registrerades rättigheter

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga.

Dataskyddsombudet delar verksamhetens bedömning om att det finns risker som behöver åtgärdas, men gör precis som verksamheten bedömningen att de inte är omfattande, brådskande eller allvarliga. Trots detta finns det ändå områden där verksamheten behöver genomföra åtgärder.

Det har uppkommit situationer under året där registrerade har utövat sina rättigheter gentemot förvaltningen och där dataskyddsombudets bedömning är att förvaltningen har hanterat begäran på ett bra sätt. Det framgår dock av förvaltningens skattning ett lägre värde vad gäller kunskapen hos medarbetarna kring de registrerades rättigheter. Dataskyddsombudet rekommenderar förvaltningen att under kommande år följa utvecklingen kring medarbetarnas kunskap inom dataskydd. Dataskyddombudet rekommenderar även förvaltningen att utveckla nuvarande rutin, så att förvaltningen säkerställer att arbetet sker på ett enhetligt sätt samt att arbetet inte blir för personberoende.

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): Kontroll av behörighetsstyrning

Verksamheten gavs följande rekommendationer kopplat till systemet Alvis:

- Ta fram rutin för tilldelning och ändring av behörigheter
- Ta fram rutin för regelbunden uppföljning av tilldelade behörigheter
- Ta fram rutin för regelbunden åtkomstkontroll/kontroll av loggar
- Upphöra med informationsutbytet genom direktåtkomst i Alvis för socialtjänsten i enlighet med tidigare rekommendationer lämnade 2022-10-07
- Utreda Arbetsförmedlingens direktåtkomst i Alvis med utgångspunkt från rekommendationer lämnade 2022-10-07

Kommentarer och rekommendationer:

Den skriftliga uppföljningen samt muntlig information från dataskyddskontakterna visar att verksamheten har vidtagit åtgärder i enlighet med samtliga rekommendationer. Fortsatt uppföljning kommer ske inom ramen för de fasta kontrollpunkterna om inget särskilt föranleder att det behöver följas upp separat.

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 nämnden att under 2024 prioritera följande delar av dataskyddsarbetet:

- Kontrollpunkt 9: Konsekvensbedömningar/samråd

Dataskyddsombudet rekommenderar förvaltningen att arbeta med att genomföra konsekvensbedömningar för de behandlingar som innebär höga risker och/eller där det krävs enligt IMY:s riktlinjer. Förvaltningen rekommenderas även att ta fram en handlingsplan för när arbetet ska påbörjas och under vilken tidsperiod som arbetet planeras fortlöpa.

- Kontrollpunkt 11: IT-system och digitala verktyg

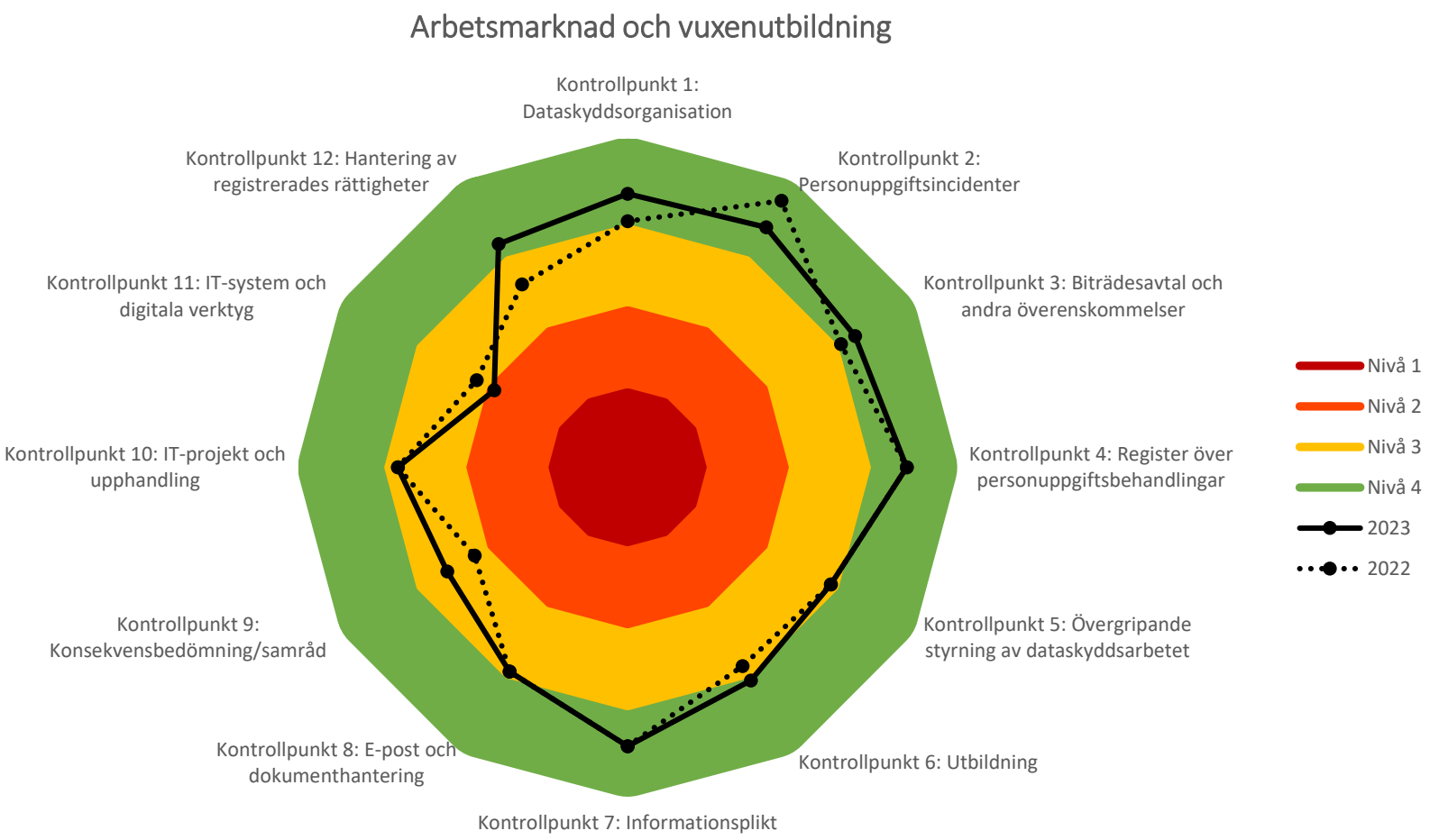
Dataskyddsombudet rekommenderar förvaltningen att i stort arbeta med frågorna under kontrollpunkten för att förvaltningen ska få en bättre överblick över hur förvaltningen rent praktiskt arbetar med frågorna samt säkerställa att dataskyddsperspektivet är en del av detta.

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.



Göteborgs Stad

Förvaltningen för arbetsmarknad och vuxenutbildning

Kontrollplan för dataskyddsarbetet 2023–2024

2023-02-06

Innehåll

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 dataskydds-ombudets 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

Dataskyddsombudets 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 dataskyddsombudet arbeta utifrån en riskbaserad metod. Riskbedömningen utgår från riskerna för de registrerades fri- och rättigheter. Kontrollplanen utgår från dataskyddsombudets 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 dataskyddsombud 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 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: 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 person-uppgifter 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.