



Årsrapport för dataskyddsarbetet 2023

Nämnden för inköp och upphandling

2023-12-19

Innehåll

1	Inledning	3
1.1	Dataskyddsombud i Göteborgs Stad	3
2	Särskilda iakttagelser 2023	4
2.1	Stadenövergripande	4
2.1.1	Förutsättningar för en hållbar digitalisering	4
2.2	Verksamhetsspecifika	5
2.2.1	Fortsatt utredning av personuppgiftsansvar	5
3	Granskning av dataskyddsarbetet 2023.....	6
3.1	Kontroll av fasta kontrollpunkter.....	6
3.2	Resultat från kontrollen 2023	6
3.2.1	Kontrollpunkt 1: Dataskyddsorganisation	7
3.2.2	Kontrollpunkt 2: Personuppgiftsincidenter	7
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	9
3.2.6	Kontrollpunkt 6: Utbildning	9
3.2.7	Kontrollpunkt 7: Informationsplikt	10
3.2.8	Kontrollpunkt 8: E-post och dokumenthantering.....	11
3.2.9	Kontrollpunkt 9: Konsekvensbedömning/samråd	11
3.2.10	Kontrollpunkt 10: IT-projekt och upphandling	12
3.2.11	Kontrollpunkt 11: IT-system och digitala verktyg	12
3.2.12	Kontrollpunkt 12: Hantering av registrerades rättigheter	13
3.3	Uppföljning	14
3.3.1	Uppföljning av rekommendationer lämnade inom ramen för tidigare genomförda kontroller	14
4	Rekommenderade fokusområden 2024	15
5	Bilagor	16

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.

2.2 Verksamhetsspecifika

2.2.1 Fortsatt utredning av personuppgiftsansvar

I tidigare årsrapporter för dataskyddsarbetet har dataskyddsombudet rekommenderat att förvaltningen utreder ansvar och roller för personuppgiftsbehandlingar i tjänster som levereras i staden efter införande av ny styrmodell (Göteborgs Stads riktlinje för styrning, samordning och finansiering av digital utveckling och förvaltning). Förvaltningen har påbörjat arbetet med att kartlägga behandlingar i de tjänster man ansvarar för och har kommit en bra bit på vägen. Dataskyddsombudet ser mycket positivt på förvaltningens arbete som utgår från de faktiska omständigheter som föreligger i varje enskilt fall. Förvaltningen uppmanas att fortsätta arbeta på samma sätt framöver – kartlägga behandlingar och reglera ansvar.

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 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. Eftersom den interna dataskyddsorganisationen fortfarande är relativt ny handlar det om att fortsätta kompetensutveckla, informera och förtydliga kommunikationsvägar. Det är speciellt viktigt att relevant information om dataskyddsfrågor når rätt nivå/befattning/roll inom verksamheten genom definierade rapporteringsvägar. Det är positivt att förvaltningen sedan förra året har tillfört fler resurser till den interna dataskyddsorganisationen.

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 och inga risker av betydelse föreligger.

Trots detta finns det ändå förbättringsåtgärder att vidta bland annat avseende förvaltningens systematiska arbete kopplat till kontrollpunkten. Specifikt gäller det förvaltningens systematiska uppföljning av inträffade incidenter och regelbunden information till medarbetarna om vad personuppgiftsincidenter är och hur de ska hanteras. Detta är delar som förvaltningen med fördel kan lägga till i den övergripande styrningen av dataskyddsfrågor.

3.2.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

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.

Förvaltningen har en framtagna rutin för hantering av personuppgiftsbiträdesavtal och andra överenskommelser. Flera av de punkter som förvaltningen uppgett låga svar på omfattas av den framtagna rutinen. Bristerna under kontrollpunkten ligger troligtvis i att förvaltningen i stort saknar kunskap om rutinen samt hur den faktiskt används i praktiken. Förvaltningen bör jobba på att ta fram arbetssätt för att kontinuerligt kunna genomföra efterlevnadskontroller av anlitade personuppgiftsbiträden. Detta för att kunna kontrollera så att biträdet uppfyller villkoren enligt biträdesavtalet. Eftersom förvaltningen redan jobbar mycket med avtalsuppföljning inom ramen för ramavtal, kan förvaltningen dra nytta av det arbetssättet i förhållande till dataskydd/personuppgiftsbiträden också. Vidare bör förvaltningen säkerställa att det finns intern kompetens för att kunna bedöma hela kedjan av underbiträden vid anlitande av nytt personuppgiftsbiträde. För förtydligande kan den framtagna rutinen också kompletteras med att även underleverantörer bör bedömas.

Dataskyddsombudet bedömning är att förvaltningen kommit långt i sitt arbete med att bedöma ansvar för personuppgiftsbehandlingar, men när det gäller bedömningar av personuppgiftsansvaret i förhållande till andra aktörer i staden är förvaltningen också beroende av andra förvaltningar/bolags insatser. Vissa saker kan förvaltningen inte själva styra över utan tvingas förhålla sig till hur Staden styrs.

3.2.4 Kontrollpunkt 4: Register över personuppgiftsbehandlingar

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.

Förvaltningens dataskyddskontakter har nyligen tagit fram en rutin för hantering av registerförteckningen, som i många delar täcker in kontrollpunkten.

Dataskyddskontakten har också nyligen tagit ett omtag med det befintliga registret för att uppdatera det och se över utformning/upplägg. Dataskyddsombudet

bedömer att förvaltningen är på god väg i sitt arbete med behandlingsregistret och har vidtagit många av de rekommendationer som lämnades i förra årets årsrapport för dataskyddsarbetet. Nästa steg är att dataskyddskontakterna använder registret som en del i det löpande dataskyddsarbetet samt att rutinen för hantering sprids ut i övriga organisationen.

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. Förvaltningen har, tack vare fler resurser till den interna dataskyddsorganisationen, fått upp förvaltningens ögon för dataskyddsarbetet. Det är därför dataskyddsombudets bedömning att förvaltningen i dagsläget jobbar på ett mer strategiskt sätt kopplat till dataskydd och att man prioriterar utifrån risker. De åtgärder som kvarstår under kontrollpunkten är följande:

- Identifiera och värdera informationstillgångar enligt Stadens styrande dokument.
- Ta fram rutiner/andra dokumenterade arbetssätt för att efterleva kraven enligt GDPR vid anordnande av fysiska och digitala sammankomster, såsom möten/utbildningar/föreläsningar/eventemang.
- Ta fram rutiner/dokumenterade arbetssätt för att genomföra regelbundna interna kontroller för att säkerställa följsamhet mot GDPR.

Förvaltningen rekommenderas prioritera rutin för hantering av personuppgifter vid event och dylikt eftersom detta är något förvaltningen uppgår ofta och utan någon särskild kontroll kopplat till GDPR.

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.

Dataskyddsbudeten 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. För att ge medarbetare inom förvaltningen goda förutsättningar för att följa lagstiftningen inom dataskyddsområdet krävs regelbundna informations- och/eller utbildningsinsatser. Om nivån på kunskap, trots regelbundna möjligheter till utbildning, är låg, bör förvaltningen se över vilka andra åtgärder som kan vidtas. Riktade insatser till olika avdelningar, såsom förvaltningen gjorde under 2023 till upphandlingsavdelningen, kan vara ett alternativ.

3.2.7 Kontrollpunkt 7: Informationsplikt



Dataskyddsbudeten bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger.

Dataskyddsbudeten delar till stor del verksamhetens bedömning. Dataskyddsbudeten gör dock till skillnad ifrån verksamheten bedömningen att det ändå föreligger risker inom kontrollpunkten, även om dessa inte bedöms som omfattande, brådskande eller allvarliga.

Dataskyddsbudeten har identifierat följande riskområden där verksamheten behöver vidta åtgärder:

- Säkerställ att informationsplikten uppfylls även i andra hänseenden än i integritetspolicyn. Det gäller bland annat förvaltningens två externa hemsidor där information om personuppgiftsbehandling saknas. Men även i förhållande till information för anställda, information vid event och information vid upphandling. För det sistnämnda håller förvaltningen på att ta fram en standardtext som kommer biläggas alla upphandlingar och som informerar om personuppgiftsbehandlingen.

Dataskyddsenheten höll under våren 2023 en särskild informationsinsats rörande informationsplikten enligt GDPR. Dataskyddsbudeten bedömning är rent generellt att det finns stora brister i den information som lämnas till de registrerade, detta gäller inte enbart inköp och upphandlingsförvaltningen utan är en genomgående brist hos i princip samtliga verksamheter i Göteborgs Stad. Bristerna består både i vilken information som lämnas och sättet på vilket informationen lämnas. Förvaltningen rekommenderas därför att:

- 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.

Dataskyddsombudet vill särskilt lyfta en positiv åtgärd som förvaltningen vidtagit. I arbetet med rutiner för dataskydd har dataskyddskontakterna också tagit fram en rutin som heter ”informera de registrerade”. I den beskrivs övergripande vilken information som ska lämnas, när informationen ska lämnas, hur informationen ska lämnas och undantag från informationsplikten.

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 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 uppger att det finns brister kopplat till dokumenthanteringsplanen. En korrekt, uppdaterad dokumenthanteringsplan är en förutsättning för att förvaltningen ska kunna följa principen om lagringsminimering. Dataskyddsombudet ser därför att förvaltningen bör prioritera arbetet med dokumenthantering. Det gäller både planen i sig – säkerställa att den är uppdaterad – samt arbetssätt och information till medarbetarna. Verksamheten rekommenderas att framåt ta fram en handlingsplan för arbetet med informationsklassning, som ett led i att tillförsäkra rätt nivå av skydd för personuppgifter.

Under arbetet med årsrapporten har förvaltningen informerat dataskyddsombudet om att en ny dokumenthanteringsplan är antagen.

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

Men även inom verksamheter med låga risker krävs det kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare. Förvaltningen har fortfarande en viss skuld när det kommer till konsekvensbedömningar och en del behandlingar som uppfyller kraven för när en konsekvensbedömning ska göras, men som inte är gjort. För att få det jobbet gjort krävs dels information till andra medarbetare inom förvaltningen om när en konsekvensbedömning ska göras, dels att den interna dataskyddsorganisationen har tid och möjlighet att bistå vid dessa bedömningar. Förvaltningen har tagit fram en rutin som beskriver hur förvaltningen ska arbeta med konsekvensbedömningar vilket dataskyddsombudet ser som positivt.

3.2.10 Kontrollpunkt 10: IT-projekt och upphandling

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder.

Dataskyddsombudet delar verksamhetens bedömning om att det förekommer risker som är omfattande och kräver omgående åtgärder.

Dataskyddsombudets bedömning är att bristerna till stor del handlar om bristande kunskap kring dataskydd. Förvaltningen har under året gjort en riktad insats mot upphandlingsavdelningen där dataskyddsenheten informerade om grundläggande dataskydd, vilket var en positiv åtgärd. Dataskyddsombudet rekommenderar att förvaltningen fortsätter att kartlägga vart liknande behov finns och säkerställa att korrekt utbildning ges. Det är framför allt viktigt utifrån förvaltningens roll som vägledande/stöttande inom upphandling, att medarbetarna har kompetens att ställa krav även inom dataskyddsområdet. Dataskyddsombudet har flertalet gånger blivit involverad i upphandlingar där kompetens kring dataskydd saknats. Förvaltningen rekommenderas att se över medarbetarnas kompetens och arbetssätt för att de ska kunna göra nödvändiga bedömningar av leverantörer och behandlingar, särskilt kopplat till IT-system och molntjänster.

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.

Dataskyddsbudeten delar verksamhetens bedömning om att det förekommer risker som är omfattande och kräver omgående åtgärder.

Förvaltningen rekommenderas särskilt:

- Säkerställa att alla medarbetare inom förvaltningen får korrekt kunskap kring dataskyddslagstiftningen.
- Ta fram förvaltningsövergripande arbetssätt/rutiner för tilldelning och uppföljning av behörigheter och åtkomster i IT-system som tar utgångspunkt i det som medarbetarna behöver ha tillgång till för att utföra sina arbetsuppgifter.
- Ta fram dokumenterade arbetssätt för att systematiskt kunna följa upp och kontrollera att användning av system och/eller andra digitala verktyg följer antagna styrande dokument.
- Ta fram dokumenterade arbetssätt för att säkerställa dataskyddsperspektivet vid införande och användande av kostnadsfria tjänster.
- Uppdatera dokumentation över samtliga IT-system och digitala verktyg som används, samt alla kommunikationskanaler.
- Säkerställ att användningen av cookies uppfyller kraven enligt GDPR.

3.2.12 Kontrollpunkt 12: Hantering av registrerades rättigheter

Verksamhetens skattning av risknivå



Dataskyddsbudeten bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger.

Dataskyddsbudeten 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. Förvaltningen rekommenderas därför att fortsatt arbeta för att bibehålla de goda förutsättningar som finns enligt skattningen.

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

Förbättringsåtgärder som dataskyddsbudeten identifierat skulle kunna vidtas inom ramen för kontrollpunkten gäller framför allt att öka kunskapen hos medarbetarna kring dataskydd och särskilt rättigheterna för de registrerade. Förvaltningen har tagit fram en rutin och när den får genomslag i stort hos förvaltningens medarbetare kommer åtgärden visa sin fulla verkningskraft.

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:

- Ta fram skriftliga rutiner för hur hantering av åtkomstkontroll/kontroll av loggar får gå till för att inte utsätta de anställda för övervakning/integritetsrisker.
- Uppdatera rutinen för behörighetshantering med att behörigheter även ska ses över även vid byte av tjänst.
- Eftersom förvaltningen har en pågående upphandling för ett system som ska ersätta Tendsign är det viktigt att man kravställer utifrån korrekt behörighetsstyrning. Förvaltningen rekommenderas också att säkerställa så personuppgiftsbiträdesavtal och instruktioner reglerar biträdets åtkomst till personuppgifter i systemet.

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten har vidtagit åtgärder i enlighet med samtliga rekommendationer. Fortsatt uppföljning kommer ske inom ramen för de fasta kontrollpunkterna om ingen särskilt föranleder att det behöver följas upp separat. Förvaltningen uppger att de har omhändertagit rekommendationerna i arbetet med att upphandla ett system som ska ersätta systemet i vilken kontrollen gjordes.

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:

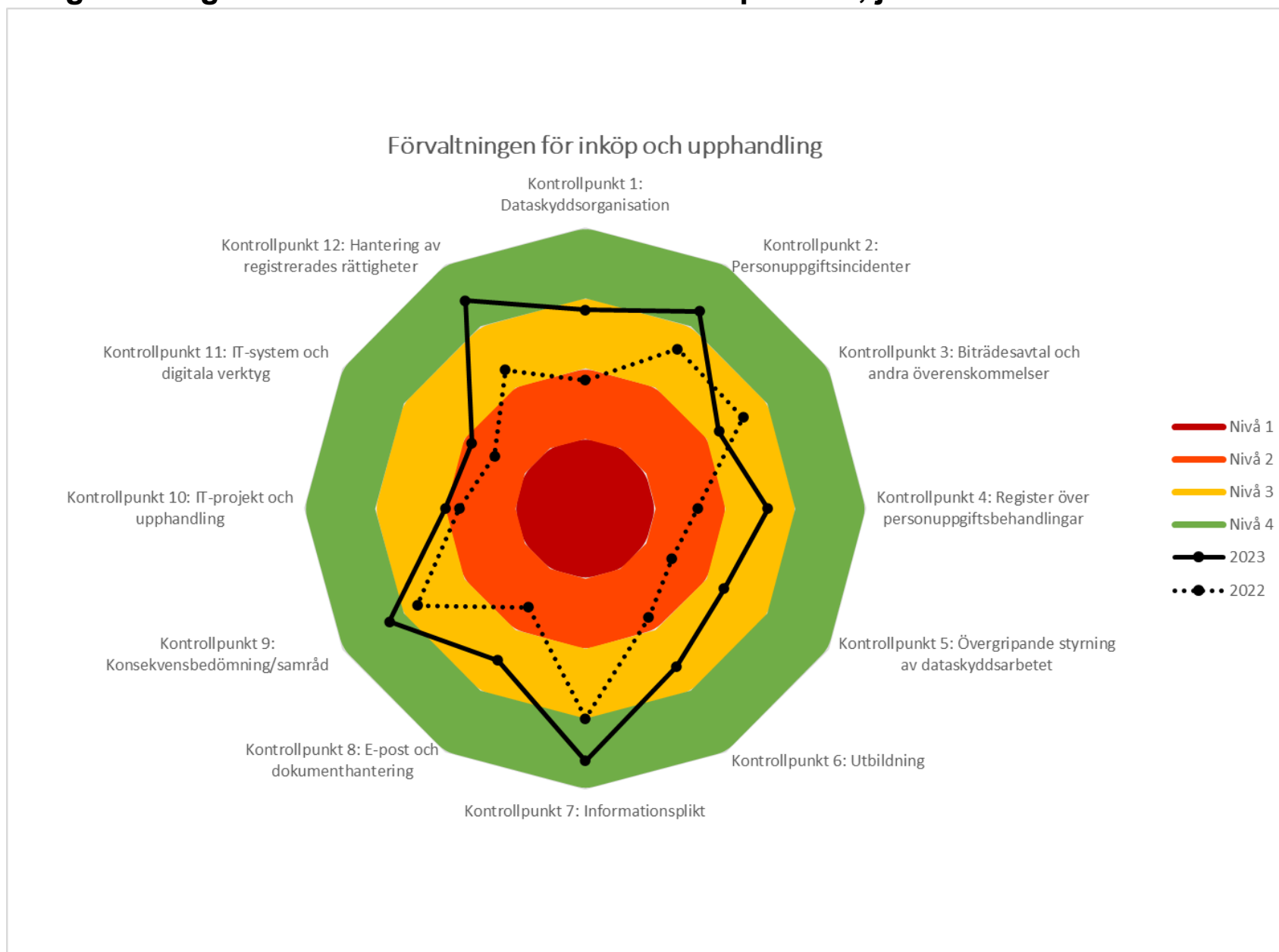
- **Kontrollpunkt 7: informationsplikt**
Se över samtliga delar i den information som lämnas till de registrerade och de arbetssätt som tillämpas för att säkerställa att informationsplikten gentemot de registrerade uppfylls.
- **Kontrollpunkt 10: IT-projekt och upphandling**
Kartlägga kompetensbrister och tillhandahålla utbildning.
- **Kontrollpunkt 11: IT-system och digitala verktyg**
Ta fram förvaltningsövergripande arbetssätt/rutiner för tilldelning och uppföljning av behörigheter och åtkomster i IT-system som tar utgångspunkt i det som medarbetarna behöver ha tillgång till för att utföra sina arbetsuppgifter.

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.





Inköp och upphandling

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.