



Årsrapport för dataskyddsarbetet 2023

Göteborg Energi AB

2023-12-19

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 ...	7
3.2.5	Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet	8
3.2.6	Kontrollpunkt 6: Utbildning	8
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 registrerade rättigheter	12
3.3	Uppföljning	13
3.3.1	Uppföljning av rekommendationer lämnade inom ramen för tidigare genomförda kontroller	13
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 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.

I likhet med årsrapporten 2022 är dataskyddsombudets fortsatta bedömning att bolaget har goda organisatoriska förutsättningar för att kunna bedriva ett effektivt och fungerande dataskyddsarbete. Dataskyddsombudet ser det som positivt att det finns representanter inom bolagets olika avdelningar representerade i den interna dataskyddsgruppen.

Även om bolaget hamnar inom samma risknivå som vid årsrapporten 2022 noterar dataskyddsombudet att resultatet är lägre jämfört med tidigare år. I samband med avstämningar har bolaget informerat om att det pågår ett omstrukturerings-/förändringsarbete inom den interna dataskyddsorganisationen, bland annat på grund av personalförändringar. Bolaget rekommenderas att försäkra sig om att den interna dataskyddsorganisationen inte ges mindre resurser än tidigare och att de goda organisatoriska förutsättningar som för närvarande finns bibehålls.

Under året har dataskyddsombudet regelbundet blivit inbjuden till möten med bolagets dataskyddsgrupp, vilket dataskyddsombudet ser som mycket positivt och är något som bolaget uppmuntras att fortsätta med. Bolaget uppmuntras även till att se över hur dataskyddsombudet kan involveras i mer verksamhetsspecifika frågor eller projekt, som exempelvis vid upphandlingar.

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

3.2.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Verksamhetens skattning av risknivå



Dataskyddsbudets bedömning

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

Bolaget uppskattar att avtal har tecknats med ca 90 % av de biträden som anlitas av bolaget. Det har även pågått ett intensivt arbete och vidtagits åtgärder under året med att kartlägga och teckna avtal med biträden där sådana saknas. Verksamheten upplever dock att det finns utmaningar att teckna biträdesavtal, särskilt när avrop sker via stadens ramavtal och med äldre leverantörer där leverantörsavtal snart löper ut. Bolaget rekommenderas att fortsätta kartlägga vilka avtal som saknas samt att framåt säkerställa att personuppgiftsbiträdesavtal ingås i direkt anslutning till att ett personuppgiftsbiträde anlitas.

Dataskyddsbudet noterar även att det kvarstår risker kopplade till efterlevnadskontroller av anlitade personuppgiftsbiträden. Vid avstämningar har verksamheten lyft att det finns ambitioner på att se över hur efterlevnadskontroller av anlitade personuppgiftsbiträden kan utföras, vilket dataskyddsbudet ser som positivt. Bolaget rekommenderas att se över om en rutin/anvisning och metoder bör tas fram för ändamålet.

3.2.4 Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Verksamhetens skattning av risknivå



Dataskyddsbudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsbudet har inte fått några direkta indikationer som medför en annan bedömning än den som bolaget gör, men har inte heller kontrollerat behandlingsregistret särskilt.

Till skillnad från föregående år uppskattar bolaget att ca 75 % av bolagets personuppgiftsbehandlingar finns upptagna i nuvarande behandlingsregister. I samband med genomgången av årsrapporten 2022 uppgav bolaget att samtliga behandlingar fanns upptagna. Utifrån verksamhetens skattning kan

dataskyddsbudet utläsa att det finns ett behov av att upprätta rutiner för att tillförsäkra att behandlingsregistret regelbundet uppdateras och att det finns särskilt utpekade ansvariga för uppgiften. Bolaget rekommenderas även att komplettera registret med de behandlingar som saknas.

Förutom att behandlingsregistret är ett lagkrav, kan behandlingsregistret också vara ett värdefullt verktyg i samband med det löpande dataskyddsarbetet, exempelvis vid hantering av registrerades begäran om registerutdrag och arbetet med informationsplikten.

3.2.5 Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet



Dataskyddsbudets bedömning

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

Utifrån skattningen kan dataskyddsbudet utläsa att det kvarstår risker kopplat till att anta ett riskbaserat arbetssätt i dataskyddsfrågor. För att säkerställa att resurser sätts in där det främst behövs bör bolaget identifiera vilka som är de största riskerna inom verksamheten och se över hur arbetet med att hantera dessa ska prioriteras. Då dataskyddsbudet fått information om att det sker omstruktureringar inom den interna dataskyddsorganisationen är dataskyddsbudets bedömning att bolaget bör prioritera omstruktureringen/förändringsarbetet inom den interna dataskyddsorganisationen under 2024 för att säkerställa att de goda organisatoriska förutsättningar som för närvarande finns bibehålls.

Vidare skattar bolaget sig lågt avseende att genomföra regelbundna interna kontroller för att säkerställa följsamhet gentemot GDPR. Utifrån skattningarna på övriga kontrollpunkter kan dataskyddsbudet utläsa att bolaget har flera rutiner/anvisningar på plats. För att tillförsäkra sig om att de utformade arbetssätten är ändamålsenliga och att de får genomslag i praktiken rekommenderas bolaget att framledes genomföra interna kontroller.

3.2.6 Kontrollpunkt 6: Utbildning



Dataskyddsbudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsbudet har inte fått några direkta indikationer som medför en annan bedömning än den som bolaget gör, men har inte heller kontrollerat kunskapsnivån särskilt.

Utifrån verksamhetens skattning kan dataskyddsbudet utläsa att det finns ett behov av att kartlägga vilken nivå av dataskyddskunskaper som olika befattningars arbete kräver och planera utbildnings- och informationsinsatser utifrån identifierade behov. Bolaget rekommenderas därför att framåt se över medarbetares utbildnings- och informationsbehov utifrån arbetsuppgifter och befattning samt säkerställa att utbildningarna och informationsinsatserna anpassas efter behov. På så sätt ges medarbetarna rätt förutsättningar att integrera dataskyddsperspektivet i sitt dagliga arbete och att hantera personuppgifter korrekt utifrån sin roll inom bolaget.

3.2.7 Kontrollpunkt 7: Informationsplikt

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 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 risknivån.

Vid genomgång av bolagets externa integritetspolicy på hemsidan kan dataskyddsbudet se att den är omfattande och lättillgänglig, vilket är positivt. Bolaget rekommenderas dock att se över hur information om lagringstid lämnas till registrerade. Dataskyddsbudet bedömer det som tveksamt om hänvisning till dokumenthanteringsplan som den registrerade inte har tillgång till kan anses tillräckligt. Det kan vara tillräckligt att hänvisa till kriterierna för hur lagringstiden bedöms om exakt lagringstid inte anges. Den registrerade ska dock, utifrån sin egen situation, i så fall kunna bedöma lagringstiden utifrån kriterierna.

Dataskyddsbudet vill i sammanhanget lyfta att kontrollpunkten i år har ändrats till att avse informationsplikten. Informationsplikten är långtgående och omfattar mer än den externa integritetspolicyen. För att informationsplikten ska anses vara uppfylld finns det krav på såväl när informationen ska lämnas, vilken information som lämnas och hur den lämnas. Personuppgiftsansvariga ska även informera om alla personuppgiftsbehandlingar som genomförs. Bolaget rekommenderas därför att säkerställa att även ytterligare information tillhandahålls registrerade i samband med behandlingar utöver det som lämnas i den externa integritetspolicyen.

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.

Dataskyddsombudet noterar att bolaget har skattat sig högre jämfört med föregående år, även om bolaget hamnar på samma risknivå. Utifrån skattningen kan det utläsas att dokumenthanteringsplanen har kompletterats, att rutiner har tagits fram för att kontrollera att handlingar gallras enligt gällande gallringsbeslut samt att det finns rutiner/anvisningar om hur information i olika informationsklasser ska hanteras och vilka lagringsytor som får användas.

Utifrån skattningen kan dataskyddsombudet utläsa att bolaget har ett behov av att fortsätta arbeta med informationsklassificering utifrån Göteborgs Stads riktlinjer för informationssäkerhet. Bolaget rekommenderas att framåt ta fram en handlingsplan för arbetet med informationsklassning, som ett led i att tillförsäkra rätt nivå av skydd för personuppgifter.

Vidare kvarstår risker kopplat till att informera registrerade om hur deras personuppgifter hanteras direkt i samband med upprättad kontakt. Detta är nära kopplat till informationsplikten i kontrollpunkt 7. I samband med genomgången av årsrapporten uppgav verksamheten att flertalet anställda numera har en länk till den externa integritetspolicyn i sin e-postsignatur, men att det saknas för ett fåtal anställda. Enligt verksamheten pågår ett arbete internt för att se över hur det kan åtgärdas.

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 verksamhetens bedömning om att det finns risker som behöver åtgärdas.

Precis som föregående år anger bolaget att samtliga av verksamhetens personuppgiftsbehandlings har kontrollerats utifrån höga risker. Vidare anges att det för ca 75 % av de behandlingar som innebär en hög risk och/eller kräver en

konsekvensbedömning finns framtagna och fastställda konsekvensbedömningar. För de återstående behandlingarna finns en planering att genomföra konsekvensbedömningar för ungefär hälften. Utifrån bolagets egen skattning och gjorda iakttagelser under året, gör dataskyddsbudet bedömningen att det inom kontrollpunkten föreligger behov av att fortsätta utveckla arbetet ytterligare. Det är viktigt att verksamheten säkerställer att det finns rutiner för att identifiera riskfyllda personuppgiftsbehandlingar, att det finns en långsiktig handlingsplan för genomförandet av konsekvensbedömningar samt att planerade konsekvensbedömningar genomförs. Bolaget rekommenderas även att rådfråga dataskyddsbudet i de fall tröskelanalyser genomförs, särskilt då bolaget bedömer att en konsekvensbedömning inte krävs.

Även i år identifierar verksamheten att det finns behov av åtgärder kopplat till beslutsmandat om åtgärdande av risker samt tydlighet kring ansvar för genomförandet av åtgärderna. Det saknas även fortsatt rutiner för att följa upp de åtgärder som ska hantera identifierade risker i gjorda konsekvensbedömningar. Rekommendationerna från årsrapporten 2022 kvarstår därmed i dessa delar.

3.2.10 Kontrollpunkt 10: IT-projekt och upphandling



Dataskyddsbudets bedömning

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

Även om dataskyddsbudet har fått övergripande information om planerade upphandlingar/införandet av nya system har dataskyddsbudet inte involverats särskilt i någon fråga. Dataskyddsbudet kan därför inte göra någon särskild bedömning gällande risknivån.

I likhet med föregående år rekommenderas bolaget framåt att säkerställa att dataskyddsbudet involveras i ett tidigt skede och på ett systematiskt sätt vid uppstart av nya IT-projekt, vid införande av nya system/tjänster eller i samband med upphandlingar.

3.2.11 Kontrollpunkt 11: IT-system och digitala verktyg



Dataskyddsbudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsbudet delar till viss del verksamhetens bedömning, men gör till

skillnad ifrån verksamheten bedömningen att det inom kontrollpunkten förekommer risker som är omfattande och som kräver åtgärder.

Utifrån bolagets egen skattning kvarstår risker kopplade till att bolaget inte har en tydlig överblick över sina kommunikationskanaler och att det saknas rutiner för att kontrollera att användningen av dessa kanaler följer dataskyddslagstiftningen. Bolaget rekommenderas fortsatt att kartlägga vilka kanaler som används inom bolaget för att få en tydlig överblick av helheten.

I årsrapporten 2022 rekommenderades bolaget att kartlägga sina behandlingar med koppling till användningen av sociala medier och att genomföra en konsekvensbedömning för att kontrollera att behandlingarna är förenliga med GDPR. Dataskyddsombudet och verksamheten har även haft en dialog kring användningen av Facebook-pixeln under året. Trots att förutsättningarna för överföringar till amerikanska leverantörer har ändrats finns flera aspekter att ta hänsyn till än enbart tredjelandsproblematiken. Bolaget rekommenderas att kartlägga vilka behandlingar och vilka personuppgifter som behandlas kopplat till användningen av sociala medier och analysverktyget, 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 och analysverktyget som kräver en konsekvensbedömning.

Vid genomgång av bolagets användning av cookies har dataskyddsombudet noterat att bolaget har vidtagit åtgärder för att inhämta aktiva samtycken för cookies från besökarna. Dataskyddsombudet ser det som mycket positivt att bolaget har arbetat med cookiehanteringen under året. I både årsrapporten för 2022 och i avstämning med verksamheten under året har dataskyddsombudet uppmärksammat bolaget på att det föreligger en direkt, eller en risk för, tredjelandsöverföring kopplat till bolagets användning av cookies. Bolaget rekommenderas att säkerställa att överföringen sker i enlighet med kap. V i GDPR.

I övrigt har dataskyddsombudet ingen tydlig inblick i bolagets arbete med IT-system och behörighetsstyrning, men har ingen anledning att göra en annan bedömning än den som verksamheten har gjort i dessa delar.

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 endast involverats i några fåtal frågor kopplat till kontrollpunkten och har ingen anledning att göra en annan bedömning än den som verksamheten har gjort avseende risknivån. Bolaget rekommenderas därför att fortsatt arbeta för att bibehålla de goda förutsättningar som finns enligt skattningen.

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): Kamerabevakning

Verksamheten gavs följande rekommendationer:

- Gör separata bedömningar gällande ändamål och rättslig grund för skyddsobjekten respektive för övriga anläggningar där kamerabevakning sker.
- Gör en tröskelanalys för att utreda om en konsekvensbedömning bör göras.
- Dokumentera varför lagringstiden på 30 dagar är nödvändig.
- Ta fram nya och tydliga informationsskyltar gällande kamerabevakningen och sätt upp på samtliga områden som kamerabevakas.
- Säkerställ att anställda och allmänheten blir informerade om kamerabevakningen.

Kommentarer och rekommendationer:

I uppföljningen anger verksamheten att åtgärder är vidtagna för nästintill samtliga rekommendationer.

Verksamheten uppger att separata bedömningar gällande ändamål och rättslig grund har gjorts och dokumenterats i det styrande dokumentet ”Göteborg Energis grundsäkerhetskrav för fysiskt och tekniskt skydd, Bilaga 2 – Tabell för kamerabevakningssystem”. Vidare uppger verksamheten att en tröskelanalys har genomförts för att utreda om en konsekvensbedömning bör göras. Under året har också nya informationsskyltar för kamerabevakningen tagits fram. Verksamheten har även i avstämningar med dataskyddsombudet uppgett att informationen i analog form avseende kamerabevakningen kan hämtas ut vid bolagets reception, vilket dataskyddsombudet ser som mycket positivt.

Uppföljningen visar att verksamheten har arbetat utifrån rekommendationerna under året. Fortsatt uppföljning kommer ske inom ramen för den löpande dialogen under 2024 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 dataskyddsbudet 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 dataskyddsbudet särskilt kommer att följa upp framåt. Uppföljningen kommer ske löpande under det kommande året, i dialog med verksamheten.

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

- Kontrollpunkt 1: Dataskyddsorganisation

Säkerställ att de goda organisatoriska förutsättningar som för närvarande finns bibehålls vid förändringen/omstruktureringen av den interna dataskyddsorganisationen.

- Kontrollpunkt 9: Konsekvensbedömning/samråd

Säkerställ att det finns rutiner för att identifiera riskfyllda personuppgiftsbehandlingsplaner, att det finns en långsiktig handlingsplan för genomförandet av konsekvensbedömningar samt att planerade konsekvensbedömningar genomförs.

- Kontrollpunkt 11: IT-system och digitala verktyg

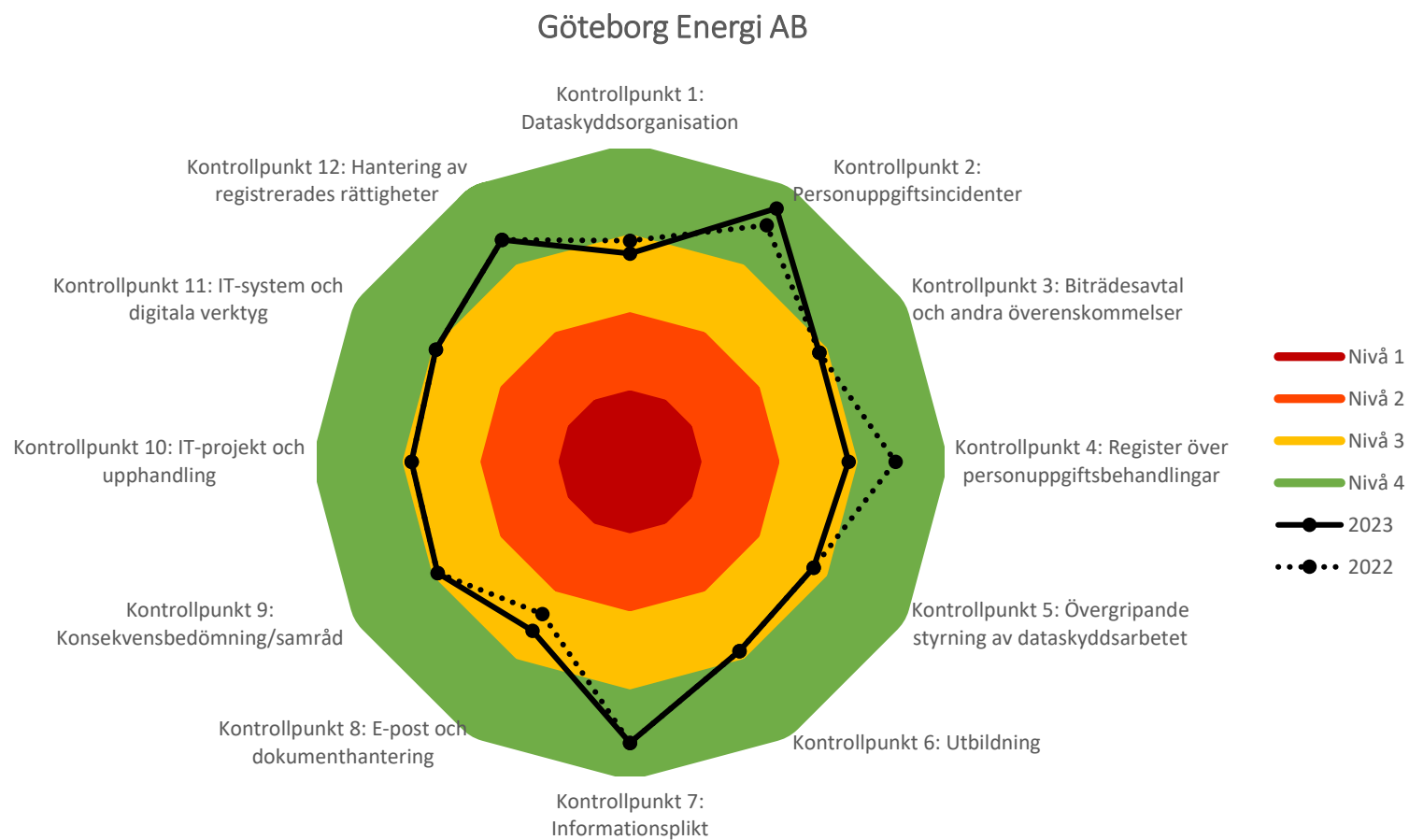
Kartlägga vilka behandlingar och vilka personuppgifter som behandlas av bolaget kopplat till användningen av sociala medier, utreda om profilering sker och identifiera vilka ansvarsförhållanden som råder för de olika behandlingarna.

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.





Göteborg Energi 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 lämnade 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.