Göteborgs Stad

Årsrapport för dataskyddsarbetet 2023

Miljö- och klimatnämnden

2023-12-18

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.	

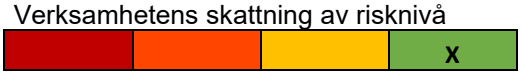
3.2 Resultat från kontrollen 2023

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. Resultatet innebär en marginell höjning jämfört med förra årets skattning.

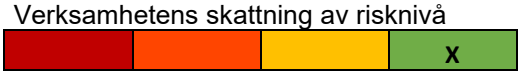
Dataskyddsombudet delar verksamhetens bedömning och anser att verksamheten har ett systematiskt arbete inom kontrollpunkten och inga risker av betydelse föreligger. Även inom verksamheter med låga risker krävs det dock kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare.

Dataskyddskontakterna har uppgett följande i november. Under året har man börjat använda en gemensam brevlåda för dataskyddsfunktionen för att förtydliga interna kontaktvägar. Ansvar och roller har förtydligats i interna styrande dokument. Utbildning har hållits med chefer och under dessa utbildningar har bland annat ansvarsfrågan tydliggjorts. Förvaltningen har en ytterligare dataskyddskontakt som har permanentats.

Dataskyddsombudet ser positivt på de åtgärder som vidtagits och uppmuntrar verksamheten att fortsätta det goda arbetet.

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. Resultatet innebär en marginell höjning jämfört med förra årets skattning.

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 dock kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare.

Dataskyddskontakterna har uppgett följande. Under året har det genomförts en utbildning i informationshantering i vilken incidentrapportering har belysts särskilt. Verksamheten har dragit stora lärdomar från incidenten gällande alkohol- och tobakssystem som inträffade i oktober 2022 och man har vuxit i kunskap och i sin

förmåga att hantera incidenter. Dataskyddskontakterna sammanställer inträffade personuppgiftsincidenter på årsbasis och har en plan för att analysera materialet.

Dataskyddsombudet har fått ta del av en sammanställning gällande 2022 och noterar att verksamheten verkar ha en god överblick på incidenter som inträffat och har en strukturerad dokumentation. Materialet vittnar om att verksamheten har förmåga att upptäcka och hantera incidenter. Mot bakgrund av detta gör dataskyddsombudet bedömningen att det verkar finns goda förutsättningar att arbeta proaktivt i frågan. Dataskyddsombudet rekommenderar att verksamheten gör en analys av de incidenter som inträffat under 2023 och att verksamheten drar slutsatser kring sårbarheter och tendenser, samt vidtar eventuella förbättringsåtgärder för att minska risken för liknande incidenter i framtiden.

Förvaltningen har utvärderat och uppdaterat rutindokument och andra dokument kopplat till frågan om hantering av personuppgiftsincidenter och har under hösten skickat över detta till dataskyddsombudet. Dataskyddsombudet har lämnat rekommendationer och ser positivt på att förvaltningen har uppdaterat verksamhetens dokumenterade arbetssätt i frågan. Dataskyddsombudet rekommenderar att förvaltningen, efter korrigering utifrån föreslagna tillägg och justeringar, implementerar dokumenten. Förvaltningen rekommenderas även att på sikt utvärdera dokumentens ändamålsenlighet.

3.2.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Verksamhetens skattning av risknivå

	X		

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder. Resultatet innebär inga förändringar jämfört med förra året. I årsrapporten för 2022 rekommenderade dataskyddsombudet att förvaltningen skulle prioritera den här kontrollpunkten.

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

Verksamheten uppskattar att biträdesavtal finns tecknat i 75 % av fallen. Vid genomgång av resultatet i årsrapporten i november har dataskyddskontakterna lyft svårigheter att som personuppgiftsansvarig leva upp till ansvarsskyldigheten vad gäller de kommungemensamma tjänsterna. Svårigheterna hänger bland annat samman med att det finns organisatoriska brister vad gäller de kommungemensamma tjänsterna och att man som personuppgiftsansvarig har begränsad insyn i och möjlighet att påverka de aktuella personuppgiftsbehandlingarna.

Förvaltningen har under hösten delgett dataskyssombudet ett nyligen framtaget rutindokument för ingående av personuppgiftsbiträdesavtal. Dataskyddsombudet

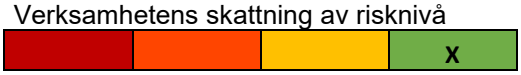
har lämnat rekommendationer gällande dokumentet och ser positivt på att förvaltningen har dokumenterat arbetssättet i frågan. Vid genomgång av resultatet i årsrapporten i november har dataskyddskontakterna berättat att dokumentet redan har implementerats och att chefer har informerats om det. Förvaltningen rekommenderas att på sikt utvärdera dokumentets ändamålsenlighet.

Utifrån förvaltningens skattning i enkäten rekommenderar dataskyddsombudet att förvaltningen utreder vad som behöver göras för att bättre leva upp till ansvarsskyldigheten som personuppgiftsansvarig. Det gäller både frågan om efterlevnadskontroller av personuppgiftsbiträden och att bedöma hela kedjan av underbiträden. Förvaltningen rekommenderas vidta åtgärder för att åstadkomma en sådan förbättring och att dokumentera arbetssättet.

Vid genomgång av resultatet i årsrapporten i november har dataskyddskontakterna berättat att man håller på att ta fram ett dokument för uppföljning av biträden. Dataskyddsombudet ser positivt på detta och uppmuntrar det fortsatta arbetet.

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. Resultatet innebär inga förändringar jämfört med förra året.

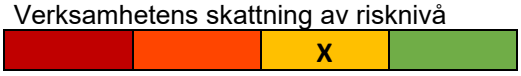
Dataskyddsombudet har inte fått några direkta indikationer som medför en annan bedömning än den som förvaltningen har gjort, men har inte heller kontrollerat behandlingsregistret särskilt. Dataskyddsombudet har dock haft en översiktlig diskussion med dataskyddskontakterna kring dataskyddenhetens nya formulär för behandlingsregistret.

Dataskyddskontakterna har uppgett följande. Verksamheten har kartlagt och dokumenterat de behandlingar som hör till verksamhetens kärnverksamhet och har påbörjat kartläggning av de verksamhetsområden som är gemensamma för staden (VO1-2). Verksamheten har för avsikt att påbörja kontinuerlig uppföljning och att ta fram ett arbetssätt för detta. Verksamheten uppskattar att behandlingar finns upptagna till 75 %.

Dataskyddsombudet ser positivt på de åtgärder som vidtagits och uppmuntrar förvaltningen i det fortsatta arbetet med att föra in samtliga behandlingar i registret. Verksamheten rekommenderas fullfölja intentionen om att ta fram ett dokumenterat arbetssätt för att säkerställa att nya eller förändrade behandlingar upptas i registret.

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. Resultatet innebär inga förändringar jämfört med förra året.

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.

Dataskyddskontakterna har uppgett följande. Verksamheten använder stadens riktlinje för informationssäkerhet. Nämnden har beslutat om en policy för informationshantering. Verksamheten har påbörjat ett arbete med att ta fram en lokal anvisning för informationshantering som innefattar både informationssäkerhet och dataskydd. Verksamhetshandbokens funktionalitet för årlig prövning används för att hålla dokument uppdaterade. Verksamheten följer stadens riktlinje för styrande dokument och har påbörjat arbetet med att ta fram en lokal anvisning. Dataskyddsombudet ser positivt på de redan vidtagna åtgärderna och på planeringen och rekommenderar verksamheten att fullfölja arbetet.

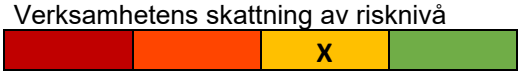
Utifrån verksamhetens skattning i enkäten rekommenderar dataskyddsombudet att verksamheten antar ett dokumenterat arbetssätt för att säkerställa efterlevnad av kraven enligt GDPR vid anordnade av fysiska och digitala sammankomster (till exempel möten/utbildningar/föreläsningar eller större evenemang).

Vidare rekommenderar dataskyddsombudet att verksamheten fortsätter att vidta åtgärder för att implementera dataskyddsarbetet på bredden så att frågorna och perspektivet blir integrerat i det dagliga arbetet. Dataskyddskontakterna kan vara en motor, men för ett fullt genomslag krävs ett brett engagemang.

Utifrån verksamhetens skattning i enkäten rekommenderar dataskyddsombudet även att förvaltningen antar ett internt styrande dokument för behandling av personuppgifter som på en övergripande nivå anger principer för hur man inom organisationen ska hantera personuppgifter vad gäller skydd av bland annat IT-system, datorer och mobila enheter. Verksamheten bör ha dokumenterat hur medarbetare ska hantera IT-system, datorer och mobila enheter och hur dessa får användas i det dagliga arbetet. Det kan exempelvis handla om lösenordrutiner och appanvändning.

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. Resultatet innebär inga förändringar jämfört med förra året.

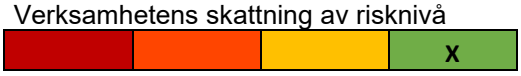
Dataskyddsombudet delar verksamhetens bedömning om att det finns risker som behöver åtgärdas, men gör precis som verksamheten bedömningen att de inte är omfattande, brådskande eller allvarliga. Trots detta finns det ändå områden där verksamheten behöver genomföra åtgärder.

Dataskyddskontakterna har uppgett för dataskyddsombudet att det har getts ett antal utbildningar under året för olika målgrupper i verksamheten. Verksamheten har för avsikt att genomföra en årlig kunskapsmätning hos alla medarbetare samt repetitionsutbildningar. I december 2023 ska det hållas ett chefsmöte med tema informationshantering och digitalisering.

Dataskyddsombudet ser positivt på de insatser som gjorts och de som planeras för framtiden och vill uppmuntra det goda arbetet. Dataskyddsombudets allmänna rekommendation är att verksamheten regelbundet gör en analys av kunskapsnivån och kunskapsbehovet inom verksamheten utifrån olika roller, ansvar och arbetsuppgifter, samt genomför och/eller deltar i utbildnings- och informationsinsatser för att möta dessa behov.

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. Resultatet innebär inga förändringar jämfört med förra årets skattning.

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

Bakgrunden till dataskyddsombudets något mer försiktiga bedömning är att informationsplikten behöver ses i ett större perspektiv. Verksamheten har i dialog med dataskyddsombudet arbetat med integritetspolicyn under året och vidtagit förbättringsåtgärder utifrån dataskyddsombudets rekommendationer. Dataskyddskontakterna har uppgett att hemsidan saknar funktionalitet för att

åstadkomma information i olika lager. Trots det goda arbetet med den externa integritetspolicyn vill dataskyddsombudet i sammanhanget lyfta att kontrollpunkten i år har ändrats från att fokusera på integritetspolicyn till att avse informationsplikten i stort. Informationsplikten är långtgående och omfattar mer än den externa integritetspolicyn.

Dataskyddsenheten höll under året en informationsinsats på temat och tog fram ett informationsmaterial i samband med detta. Verksamheten rekommenderas läsa igenom materialet och att utvärdera i vilken mån verksamheten lever upp till kraven och att vidta eventuella förbättringsåtgärder. Informationsplikten handlar alltså inte bara om att ha en integritetspolicy på hemsidan. Det finns även vissa kvalitativa krav kopplat till hur informationen förmedlas, när den ska förmedlas och att den verkligen ska nå fram till den registrerade. Information kan behöva förmedlas på olika sätt i olika sammanhang. Slutmålet är med andra ord inte att ta fram en informationstext, utan snarare att den registrerade verkligen får kunskap om behandlingen så att den registrerade i förlängningen kan utöva sina rättigheter.

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. Resultatet innebär en höjning jämfört med förra årets skattning.

Dataskyddsombudet delar till viss del verksamhetens bedömning, men gör till skillnad ifrån verksamheten bedömningen att det inom kontrollpunkten förekommer risker som kräver omgående åtgärder. Denna bedömning görs mot bakgrund av bristerna vad gäller gallring (se beskrivning nedan).

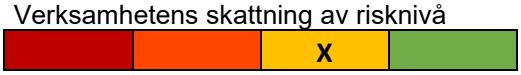
Dataskyddskontakterna har uppgett följande. Dokumenthanteringsplanen är klar vad gäller de verksamhetsområden som rör kärnverksamheten och arbete pågår vad gäller de verksamhetsområden som är gemensamma för staden. Under 2024 planerar verksamheten att arbeta med uppföljning av dokumenthanteringsplanen. I dagsläget saknas möjlighet att verkställa digital gallring i flertal system, däribland diariet. En informationsinsats gällande gallring planeras under 2024. Dataskyddsombudet rekommenderar att verksamheten omgående vidtar åtgärder för att säkerställa att det finns teknisk möjlighet att gallra och att gallring görs enligt gallringsbeslut.

Som tidigare nämnts rekommenderar dataskyddsombudet att verksamheten fullföljer arbetet med dokumenthanteringsplanen. Som nämnts vid kontrollpunkt fem om övergripande styrning, så arbetar verksamheten aktivt med informationssäkerhetsfrågor. Dataskyddsombudet rekommenderar att

verksamheten drar nytta av informationsklassningsarbetet för att få en enhetlig och säker hantering vad gäller personuppgifter som är av liknande art och känslighet.

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. Resultatet innebär en höjning jämfört med förra årets skattning. I årsrapporten för 2022 rekommenderade dataskyddsombudets att förvaltningen skulle prioritera den här kontrollpunkten.

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.

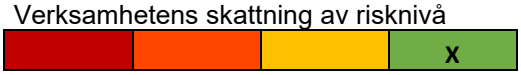
Dataskyddsombudet rekommenderar att verksamheten utreder vad som behöver göras för att förvaltningen bättre ska kunna säkerställa att konsekvensbedömningar genomförs innan riskfyllda behandlingar påbörjas och att verksamheten vidtar åtgärder för att åstadkomma en förbättring på den här punkten.

Vidare, utifrån förvaltningens skattning i enkäten, rekommenderar dataskyddsombudet att verksamheten antar ett dokumenterat arbetssätt för att säkerställa att konsekvensbedömningar uppdateras vid förändringar. Verksamheten rekommenderas också anta ett dokumenterat arbetssätt vad gäller hantering av risk. Detta inbegriper att få på pränt hur verksamheten ska hantera beslutsfattande om att vidta åtgärder för att möta kvarstående risker och hur detta ska dokumenteras. Verksamheten bör även dokumentera hur verksamheten ska arbeta med uppföljning av beslutade riskhanteringsåtgärder.

Dataskyddskontakterna har uppgett att man sedan tidigare har tagit fram ett utkast på rutin för arbetet med konsekvensbedömningar. Verksamheten har för avsikt att få till ett systematiskt arbetssätt i frågan. Dataskyddsombudet rekommenderar verksamheten att fullfölja arbetet med rutinen för konsekvensbedömningar så att den kan implementeras och göras känd bland medarbetarna.

3.2.10 Kontrollpunkt 10: IT-projekt och upphandling

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Resultatet innebär inga förändringar jämfört med förra årets skattning.

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 dock kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare.

Vid avstämning med dataskyddskontakterna i november har dataskyddskontakterna berättat följande. Verksamheten är medveten om kraven och har intern kompetens att genomföra konsekvensanalyser och att bedöma risker. Verksamheten arbetar systematiskt och strukturerat i informationshanteringen och tar del av aktuell utveckling inom området och har en löpande dialog kring informationssäkerhet med leverantörer.

I samband med genomgång av årsrapporten i november har dataskyddskontakterna även berättat följande. Verksamheten har ett arbetssätt för att involvera dataskyddsombudet från start vid uppstart av nya IT-projekt och/eller vid införandet av nya tjänster där personuppgifter kommer att hanteras. Arbetssättet är dock inte dokumenterat. Eftersom det finns en delfråga som är formulerad utifrån att arbetssättet ska vara dokumenterat, så har verksamheten angett ett lite lägre värde på den här delfrågan.

Dataskyddsombudet ser positivt på att det verkar finnas ett väl fungerande arbetssätt och att verksamheten involverar dataskyddsombudet. För att göra hanteringen mindre personberoende anser dataskyddsombudet att det kan vara lämpligt att verksamheten dokumenterar arbetssättet, men det viktiga är att arbetet fungerar i praktiken.

3.2.11 Kontrollpunkt 11: IT-system och digitala verktyg

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Resultatet innebär inga förändringar jämfört med förra årets skattning.

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 dock kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare.

Vid avstämning i november har dataskyddskontakterna berättat följande. Verksamheten är medveten om kraven, upprätthåller intern IT-dokumentation, har en samlad sammanställning över verksamhetens informationsbärare (IT-stöd), lämpliga styrande dokument och arbetsrutiner inom området. Verksamheten introducerar alla nya medarbetare till verksamhetens IT-stöd på ett systematiskt sätt. Verksamheten arbetar hårt med att hålla manualer och arbetsinstruktioner aktuella.

Utifrån verksamhetens skattning i enkäten rekommenderar dataskyddsombudet att verksamheten antar ett dokumenterat arbetssätt för att systematiskt kunna följa upp och kontrollera att verksamhetens användning av system och/eller andra digitala verktyg ligger i linje med antagna styrande dokument. Vid genomgång av årsrapporten i november har dataskyddskontakterna berättat att denna delfråga finns upptagen i planeringen framåt och att förvaltningscontrollern är vidtalad. Dataskyddsombudet rekommenderar att verksamheten fullföljer dessa intentioner.

Vidare utifrån skattningen i enkäten rekommenderar dataskyddsombudet att verksamheten antar ett dokumenterat arbetssätt för att säkerställa dataskyddsperspektivet vid införandet och användandet av kostnadsfria tjänster såsom gratisappar och sociala medier.

3.2.12 Kontrollpunkt 12: Hantering av registrerades rättigheter

Verksamhetens skattning av risknivå

		X	

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Resultatet innebär inga förändringar jämfört med förra årets skattning.

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.

Dataskyddskontakterna har uppgett följande. Verksamheten har påbörjat framtagandet av rutiner gällande hantering av de registrerades rättigheter.

Vid genomgång av årsrapporten i november har dataskyddskontakterna kommenterat skattningen på delfrågan om dokumenterat arbetssätt för att hantera

ett tillbakadragande av samtycke från en registrerad. Verksamheten är medveten om att samtycke som huvudregel inte är en lämplig rättslig grund för myndigheter att använda sig av och därför använder sig verksamheten som regel inte av den rättsliga grunden. Dataskyddsombudet rekommenderar att verksamheten ser över behovet av att dokumentera hanteringen av samtycke, inbegripet hur ett tillbakadragande av samtycke ska hanteras.

Dataskyddsombudet rekommenderar att verksamheten fortsätter att tillvarata de registrerades rättigheter både genom hantering i konkreta förfrågningar från de registrerade och genom faktiska personuppgiftsbehandlingar. Vad gäller de dokument som finns framtagna för hantering av förfrågningar från de registrerade, så rekommenderar dataskyddsombudet att verksamheten utvärderar dokumentens ändamålsenlighet samt den praktiska hanteringen och vidtar eventuella behövliga förbättringsåtgärder.

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 i EDP Vision

Verksamheten gavs följande rekommendationer:

- Se över och dokumentera ert arbetssätt för tilldelning av behörigheter.
- Se över och dokumentera ert arbetssätt för uppföljning av tilldelade behörigheter.
- Inför åtkomstkontroll/logguppföljning i form av regelbundna slumpmässiga stickprovskontroller.
- Utred och följ upp sekretessfrågor, kopplat till behörighetsstyrning, tillsammans med förvaltningsjurist.
- Utred behovet av att genomföra konsekvensbedömningar av behandlingarna i systemet, alternativt dokumentera varför sådana inte anses vara nödvändiga.

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten har vidtagit och/eller planerar vidta åtgärder i enlighet med rekommendationerna. Vad gäller rekommendationen om åtkomstkontroll/logguppföljning så har verksamheten uppgett följande. Det sker inte någon sådan kontroll i dagsläget, men man undersöker vilken typ av loggning som sker i systemet och vad förvaltningen respektive leverantören kan se. Verksamheten har uppgett att man önskar ha dialog med dataskyddsombudet i ett

antal frågor kopplat till detta. Dataskyddsombudet välkomnar denna dialog och föreslår att dessa frågor följs upp inom ramen för de löpande avstämningarna under året.

Kontroll (2022): Fast kontrollpunkter. Kontrollpunkt 9: Integritetspolicy

Verksamheten gavs följande rekommendationer:

> Verksamheten har genomgående besvarat enkätfrågorna inom kontrollpunkten med höga värden. Dataskyddsombudet instämmer dock inte i verksamhetens bedömning och anser att det saknas väsentliga delar i policyn, bland annat avseende hantering av cookies. Men att informationen även brister i andra avseenden rörande de krav på information till de registrerade som följer av artikel 13 och 14 i GDPR. Förvaltningen har tagit fram ett uppdaterat förslag till policy och Dataskyddsombudets rekommendation är därför att verksamheten tillsammans med dataskyddsombudet tittar på vilka delar av policyn som behöver kompletteras och genomför dessa uppdateringar för att kraven i dataskyddsförordningen ska kunna efterlevas. Kontrollpunkten kommer att följas upp under 2023

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten har vidtagit och planerar vidta 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.

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 5: Övergripande styrning av dataskyddsarbetet**

Anta ett dokumenterat arbetssätt för att säkerställa efterlevnad av kraven enligt GDPR vid anordnade av fysiska och digitala sammankomster (till exempel möten/utbildningar/föreläsningar eller större evenemang).

Vidta åtgärder för att implementera dataskyddsarbetet på bredden så att frågorna och perspektivet blir integrerat i det dagliga arbetet.

Anta ett internt styrande dokument för behandling av personuppgifter som på en övergripande nivå anger principer för hur man inom organisationen ska hantera personuppgifter vad gäller skydd av bland annat IT-system, datorer och mobila enheter.

- **Kontrollpunkt 8: E-post och dokumenthantering**

Vidta åtgärder för att säkerställa att det finns teknisk möjlighet att gallra och att gallring görs enligt gallringsbeslut.

- **Kontrollpunkt 9: Konsekvensbedömning/samråd**

Utred vad som behöver göras för att förvaltningen bättre ska säkerställa att konsekvensbedömningar genomförs innan riskfyllda behandlingar påbörjas och vidtar åtgärder för att åstadkomma ens ådan förbättring.

Anta ett dokumenterat arbetssätt för att säkerställa att konsekvensbedömningar uppdateras vid förändringar.

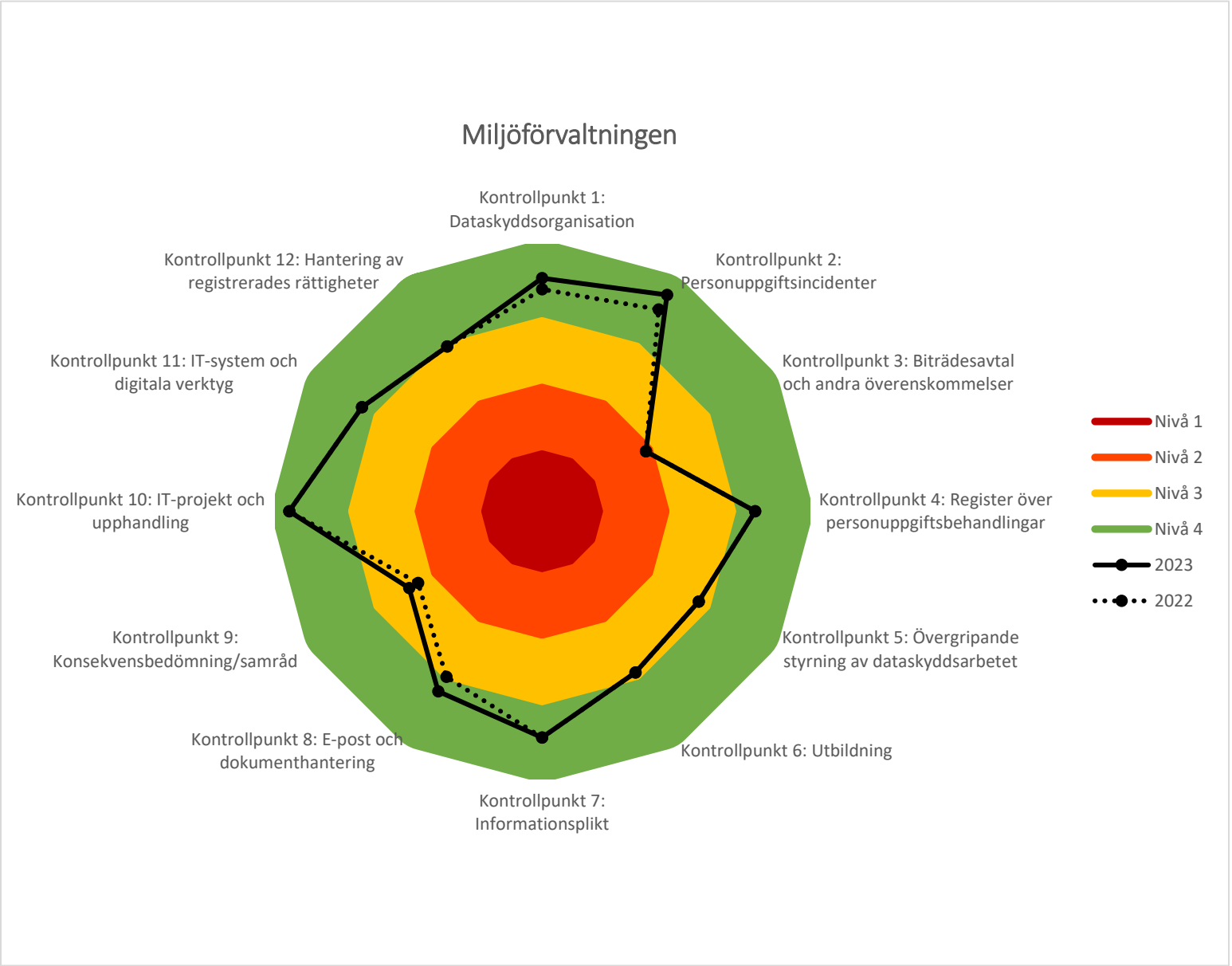
Anta ett dokumenterat arbetssätt vad gäller hantering av risk. Få på pränt hur verksamheten ska hantera beslutsfattande om att vidta åtgärder för att möta kvarstående risker och hur detta ska dokumenteras. Dokumentera hur verksamheten ska arbeta med uppföljning av beslutade riskhanteringsåtgärder.

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

Miljöförvaltningen

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 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.