Göteborgs Stad

Gryaab

Kontrollplan för dataskyddsarbetet 2022

2022-01-21

Innehåll

1 Bakgrund

1.1 Dataskyddsförordningen

Dataskyddsförordningen (GDPR) trädde i kraft den 25 maj 2018 och är en EU-förordning med syfte att skydda fysiska personers grundläggande fri- och rättigheter, att garantera ett likvärdigt skydd samt att säkerställa det fria flödet av personuppgifter inom unionen. Förordningen kompletteras av dataskyddslagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning. Dessa samspelar även med annan speciallagstiftning.

Dataskyddsförordningen ställer höga krav på organisationers behandling av enskildas personuppgifter. Utöver att insamlingen av personuppgifterna ska vara tillåten, måste den personuppgiftsansvarige dessutom hantera dessa uppgifter på ett korrekt sätt. Detta ska ske med respekt för den enskildes integritet och genom att vidta lämpliga säkerhetsåtgärder.

Efterlevnaden av lagstiftningen övervakas av Integritetsskyddsmyndigheten och överträdelser kan bland annat leda till sanktionsavgifter eller skadestånd.

1.1.1 Personuppgiftsansvarig

En personuppgiftsansvarig kan vara en fysisk person eller juridisk person, en offentlig myndighet, institution eller ett annat organ. Varje förvaltning med egen nämnd räknas som en egen offentlig myndighet. Varje enskild nämnd eller styrelse är ytterst ansvarig för att organisationen behandlar personuppgifter i enlighet med gällande regelverk. För att följa dataskyddsarbetet och hålla nämnden/styrelsen informerad bör, enligt dataskyddsförordningen, ett dataskyddsombud, med särskild sakkunskap om dataskyddslagstiftning och praxis, utses för att bistå den ansvarige med att övervaka den interna efterlevnaden av förordningen.

1.1.2 Dataskyddsombud

Dataskyddsombudet ska ge råd och information till den personuppgiftsansvarige samt övervaka efterlevnaden av dataskyddsförordningen och annan relevant dataskyddslagstiftning. Det innebär bland annat att kontrollera hur den personuppgiftsansvarige behandlar personuppgifter, att bestämmelser och interna styrdokument följs samt att ge råd och stöd vid konsekvensbedömningar. Dataskyddsombudet ska enligt dataskyddsförordningen utföra sitt arbete på ett oberoende sätt gentemot den som är personuppgiftsansvarig och får inte instrueras av denne i hur arbetet ska utföras. Dataskyddsombudet är inte heller ansvarig för att lagstiftningen efterlevs.

Dataskyddsombudet är även kontaktperson för de registrerade och tillsynsmyndigheten. Dataskyddsenheten kommer under 2022 att bli dataskyddsombud för förvaltningar och bolag i Göteborgs Stad.

2 Kontrollplan för dataskyddsarbetet 2022

2.1 Syfte och mål

Dataskyddsombudets uppgift att övervaka den personuppgiftsansvariges efterlevnad av förordningen regleras i artikel 39 GDPR. En del av denna övervakning innebär att dataskyddsombudet genomför kontroller av dataskyddsarbetet inom den personuppgiftsansvariges organisation. Dessa kontroller specificeras genom denna kontrollplan som syftar till att informera personuppgiftsansvariga om tidplan och särskilda fokusområden för kontrollarbetet år 2022.

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.

2.2 Ett riskbaserat arbetssätt

Enligt dataskyddsregelverket ska dataskyddsombudet arbeta utifrån en riskbaserad metod. Kontrollplanen utgår därför ifrån dataskyddsombudets bedömning avseende risker kopplat till verksamhetens personuppgiftsbehandlingar.

Riskbedömningen utgår ifrån riskerna för de registrerades fri- och rättigheter. Det tas även hänsyn till potentiella konsekvenser för verksamheten. Både till risken för ekonomisk skada (exempelvis skadestånd och sanktionsavgifter), samt till risken för förtroendeskada (så som exempelvis försämrat varumärke och minskad tillit). Genom ett systematiskt och proaktivt dataskyddsarbete kan risken för att drabbas av någon av dessa följder minimeras.

2.3 Upplägg

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

a) Den första delen består av fasta kontrollpunkter där varje punkt bedöms årligen. Bedömningen görs genom löpande kontroller, genom deltagande i verksamhetens arbete och i förekommande fall utifrån given information.

Genom att ha en årlig uppföljning av de fasta kontrollpunkterna kommer varje personuppgiftsansvarig kunna följa utvecklingen av dataskyddsarbetet inom verksamheten över tid.

b) Den andra delen är en fördjupad kontroll av en eller flera utvalda verksamhetsspecifika kontrollpunkter.

c) Den tredje delen är en uppföljning och bedömning av hur verksamheten hanterat tidigare lämnande rekommendationer.

Kontrollarbetets olika delar kommer sammanställas och presenteras i årsrapporten för nämnd/styrelse.

2.3.1 Verksamhetsspecifika förutsättningar

Dataskyddsombudets arbete kommer att bedrivas utifrån verksamhetens specifika förutsättningar. Identifierade aktiviteter kan därför komma att justeras utifrån händelser som inträffar i verksamheterna eller i omvärlden.

2.4 Tidplan för kontroller 2022

Månad	Aktivitet
Januari	Kontrollplan för året lämnas till nämnd/styrelse Årsrapport presenteras för nämnd/styrelse (januari/februari)
Februari - april	Fördjupad kontroll av utvalda verksamhetsspecifika kontrollpunkter genomförs
Maj - juni	Fördjupad kontroll slutförs och delårsrapport lämnas till verksamheten *(rapportering inför nämnd/styrelse sker vid behov)*
September - november	Uppföljning av tidigare lämnade rekommendationer Kontroll av fasta kontrollpunkter
December	Årsrapport lämnas till verksamheten

3 Kontrollpunkter

3.1 Fasta kontrollpunkter

De fasta kontrollpunkternas omfattning utgår från principerna om inbyggt dataskydd och dataskydd som standard (enligt artikel 25 GDPR). Verksamhetens följsamhet mot förordningen beror till stor del på hur väl dessa principer har integrerats i verksamhetens ordinarie processer. Att principerna har en central roll i arbetet med dataskydd blir särskilt tydligt i beaktandesats

(skäl) 78 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 punkter som fastställts utgör en del av fundamentet i lagstiftningen. Syftet med arbetssättet är att tillsammans hitta strategier, rutiner och arbetssätt så att kontrollerna över tid kommer att kräva mindre och mindre arbete.

De fasta kontrollpunkterna kontrolleras genom en enkät som kommer att vara återkommande varje år. Enkäten utgår ifrån 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 att fylla i enkäten.

Resultaten från enkäten ger en generell ögonblicksbild för respektive kontrollpunkt. Avsikten med detta arbetssätt är att både att få en bild av nuläget och att kunna åskådliggöra de förändringar som vidtas över tid. Enkäten har ej främst för avsikt att peka ut brister utan ska ses som en vägledning för verksamheten och ett verktyg för att identifiera relevanta prioriteringar. Syftet är att få till ett långsiktigt och systematiskt arbetssätt som möjliggör uppföljning över tid.

Kontrollpunkter
1. Dataskyddsorganisation
2. Personuppgiftsincidenter
3. Biträdesavtal och andra överenskommelser
4. Personuppgiftsregister
5. Övergripande strategi för dataskydd
6. Utbildning
7. Integritetspolicy
8. Mejl- och dokumenthantering
9. Konsekvensbedömning/samråd
10. IT-projekt och upphandling
11. IT-system och digitala verktyg
12. Hantering av registrerades rättigheter

3.1.1 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: Personuppgiftsregister

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 personuppgiftsregister innefattas.

Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd. En verksamhetsspecifik strategi som anger ramarna för arbetet med dataskydd kan både främja ett riskbaserat arbetssätt och bidra till en kontinuitet i dataskyddsarbetet.

Kontrollpunkten innefattar även verksamhetens strategi för att integrera dataskyddsfrågorna i det övriga informationssäkerhetsarbetet, samt hur verksamheten arbetar med egna interna kontroller för att säkerställa att dataskyddsförordningen efterlevs.

Kontrollpunkt 6: Utbildning

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

Kontrollpunkt 7: Integritetspolicy

Kontrollpunkten avser verksamhetens utformning samt tillhandahållande av dess integritetspolicy till registrerade (både internt och externt). Även verksamhetens rutin för att upprätthålla en aktuell integritetspolicy omfattas.

Kontrollpunkt 8: Mejl och dokumenthantering

Kontrollpunkten avser verksamhetens rutiner för mejl och dokumenthantering. I detta är en aktuell och fastställd dokumenthanteringsplan med gallringsbeslut en förutsättning för att verksamheten ska kunna säkra följsamhet gentemot dataskyddsförordningen. 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 dataskyddsförordningen. 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, till exempel registerutdrag eller radering. 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.

3.2 **Fördjupad kontroll 2022**

Den fördjupade kontrollen utgår från verksamhetens specifika risker. För verksamhetsåret har följande punkt/punkter fastställts:

Fokusområde: Behörighetsstyrning (kontrollpunkt 11)

För att säkerställa säkerheten och en korrekt personuppgiftshantering inom en verksamhet behöver både tekniska och organisatoriska åtgärder vidtas. Exempel på tekniska säkerhetsåtgärder är att system utformas så att endast behöriga personer kan göra sökningar och att det finns behörighetskontrollsystem. En viktig och effektiv organisatorisk åtgärd i en verksamhet är behörighetsstyrning.

I artikel 32.2 i dataskyddsförordningen ställs krav på att den personuppgiftsansvarige i samband med bedömning av lämplig säkerhetsnivå ska ta särskild hänsyn till risker i synnerhet från bland annat obehörig åtkomst till personuppgifter. Obehörig är den som inte har legitim anledning att ta del av en handling eller uppgift i sin tjänsteutövning. Bestämmelser om sekretess utgör oftast en utgångspunkt för vilka uppgifter som någon får ta del av. Genom en ändamålsenlig behörighetsstyrning kan det säkerställas att ingen obehörig åtkomst sker inom verksamheten. Behörighetsstyrning sker genom att bland annat bedriva ett arbete med att avgöra hur stor tillgång till uppgifter i ett verksamhetssystem som en medarbetare med en viss funktion eller roll ska ha. Det är viktigt att behörigheterna är anpassade och begränsade till det som är nödvändigt och i enlighet med gällande rättslig reglering. Dessutom behöver behörigheterna löpande kontrolleras och följas upp samt att åtkomstkontroller genomförs. En felaktig eller bristfällig behörighetsstyrning kan leda till exempelvis inskränkningar av den enskildes integritet eller personuppgiftsincidenter.

Den fördjupade kontrollen avser undersöka hur behörighetsstyrning används för att begränsa vilka uppgifter som medarbetarna får ta del av. Verksamhetens rutiner för tilldelning av behörigheter och åtkomster i IT-system kommer att granskas. Kontrollen kommer även omfatta verksamhetens uppföljning av medarbetares behörigheter och åtkomst till personuppgifter i IT-system samt om logg-/åtkomstkontroller används för att upptäcka och motverka obehörig åtkomst.

Syftet med den fördjupade kontrollen är att undersöka om medarbetares tillgång till personuppgifter är anpassade och begränsade till det som är nödvändigt för att medarbetaren ska kunna utföra sina arbetsuppgifter, att åtkomstkontroller genomförs och att därmed risken för obehörig åtkomst inom verksamheten minimeras.

4 Uppföljning

4.1 Uppföljning av lämnade rekommendationer

I dataskyddsförordningen anges att dataskyddsombudet ska rapportera direkt till den personuppgiftsansvariges eller personuppgiftsbiträdets högsta förvaltningsnivå, för att säkerställa att högsta ledningen är medveten om dataskyddsombudets råd och rekommendationer. Detta är grunden för ett proaktivt arbetssätt och utgör en trygghet för nämnd/styrelse som uppmärksammas på status och observerade brister i dataskyddsarbetet. Det är då också av vikt för nämnd/styrelse att veta hur eventuella rekommendationer/brister omhändertagits. Dataskyddsombudet kommer därför årligen att följa upp hanteringen av de rekommendationer som lämnats till verksamheten och rapportera detta i årsrapporten.

4.1.1 Uppföljning av hittills genomförda kontroller

Sedan dataskyddsförordningen trädde i kraft i maj 2018 har dataskyddsombudet genomfört ett antal kontroller för er verksamhet. För det fall att rekommendationer för tidigare kontroller kvarstår genomförs en särskild uppföljning. I annat fall kommer kontrollerna att följas upp inom ramen för de fasta kontrollpunkterna.

5 Rapportering till nämnd/styrelse

5.1 Delårsrapportering

I juni månad kommer respektive nämnd/styrelse att få en delårsrapport för dataskyddsarbetet av dataskyddsombudet. Fokus för delsårsrapporteringen är den verksamhetsspecifika fördjupade kontrollen som genomförs under våren.

Genom en delårsrapportering säkerställs att personuppgiftsansvarig nämnd/styrelse hålls informerad om dataskyddsombudets observationer av verksamhetens personuppgiftshantering. Formen för rapporteringen anpassas efter dataskyddsombudets bedömning av verksamhetens behov.

5.2 Årsrapport

Verksamhetens dataskyddsarbete kommer att sammanställas i en skriftlig årsrapport till nämnd/styrelse. Årsrapporten kommer innehålla information om verksamhetens samarbete med dataskyddsombudet, genomförda kontroller,

lämnade rekommendationer samt en övergripande bedömning av status på verksamhetens personuppgiftshantering utifrån fasta kontrollpunkter.

För att möjliggöra en direkt kommunikation mellan dataskyddsombud och personuppgiftsansvarig nämnd/styrelse ska årsrapporten presenteras i möte med nämnd/styrelse.

5.3 Särskilt yttrande till högsta ledning

Om det skulle uppstå situationer där den ansvarige fattar beslut som är oförenliga med den allmänna dataskyddsförordningen och dataskyddsombudets råd, till exempel om en allvarlig brist kvarstår och inte åtgärdas, har dataskyddsombudet möjlighet att klargöra sin avvikande ståndpunkt genom ett yttrande riktat till högsta förvaltningsnivå och till dem som fattar besluten.

5.4 Beslutanderätten i dataskyddsfrågor

Beslutanderätten i dataskyddsfrågor ligger alltid på den personuppgiftsansvarige och aldrig på dataskyddsombudet. Dataskyddsombudet är en specialist med en rådgivande roll och är en resurs som, på ett oberoende sätt, fokuserar på dataskyddsfrågorna i verksamheten och på det sättet bistår den personuppgiftsansvarige med bedömningar och råd. Om nämnden/styrelsen väljer att inte följa dataskyddsombudets rekommendationer ska skälen till detta motiveras och dokumenteras i enlighet med god praxis samt för att uppfylla ansvarsskyldigheten. Detta är även viktigt för det fall frågan senare skulle bli föremål för tillsyn.

6 Kontakt

Eventuella frågor och synpunkter hänvisas i första hand till er kontaktperson. Frågor kan också alltid ställas till dso@intraservice.goteborg.se.