Göteborgs Stad

Göteborgs Stads Kollektivtrafik AB

Kontrollplan för dataskyddsarbetet 2021

2021-01-22

Innehåll

1 Bakgrund

1.1 Dataskyddsförordningen

Dataskyddsförordningen (DSF) trädde i kraft i 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, med respekt för den enskildes integritet och med beaktande av lämpliga säkerhetsåtgärder.

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

1.1.1 Personuppgiftsansvarig

En personuppgiftsansvarig kan vara en fysisk person, juridisk person, en offentlig myndighet, institution eller ett annat organ. Varje förvaltning med egen nämnd räknas som en egen offentlig myndighet. I juridisk mening så är därmed ytterst varje enskild nämnd eller styrelse ansvarig för att de personuppgiftsbehandlingar som organisationen hanterar utförs i enlighet med gällande regelverk. För att följa dataskyddsarbetet och hålla nämnden/styrelsen informerad bör enligt dataskyddsförordningen ett dataskyddsombud, med särskild sakkunskap i fråga 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 hur arbetet ska utföras. Dataskyddsombudet är inte heller ansvarig för att lagstiftningen efterlevs.

Dataskyddsombudet är även kontaktperson för de registrerade och tillsynsmyndigheten.

2 Kontrollplan för dataskyddsarbetet 2021

2.1 Syfte och mål

Dataskyddsombudets uppgift att övervaka den personuppgiftsansvariges efterlevnad av förordningen regleras i artikel 39 DSF. 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 2021.

Målsättningen 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. Maximera 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 riskbedömning avseende verksamhetens personuppgiftsbehandlingar och tas fram i dialog med verksamheten. Primära fokusområden och prioriteringar utgår från eventuella problem som bedöms utgöra en högre risk för dataskyddet i verksamheten.

Gemensamt för stadens verksamheter har dataskyddsenheten identifierat två riskområden som är särskilt relevanta, utifrån att respektive personuppgiftsansvarig har möjlighet att genom att bedriva ett systematiskt dataskyddsarbete påverka omfattningen av de risker som dessa områden inbegriper. Det första riskområdet innefattar ekonomisk skada (exempelvis skadestånd och sanktionsavgifter), vars risker beror på huruvida verksamheten i sin personuppgiftshantering säkerställer att dataskyddsförordningen följs. Det andra riskområdet innefattar förtroendeskada (så som exempelvis försämrat varumärke och minskad tillit) och är beroende av verksamhetens förmåga att hantera de registrerades rättigheter enligt dataskyddsförordningen.

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.

b) Den andra delen är en fördjupad kontroll av 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. Genom att ha en årlig uppföljning av de fasta kontrollpunkterna kommer varje personuppgiftsansvarig kunna följa utvecklingen av dataskyddsarbetet inom verksamheten över tid.

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 2021**

Månad	**Huvudaktivitet**	**Övriga aktiviteter**
Januari	Kontrollplan för året lämnas till nämnd/styrelse	Uppföljning och kontroll av övriga fasta kontrollpunkter kommer ske löpande under året.
Februari-April	Fördjupad kontroll av utvalda verksamhetsspecifika kontrollpunkter genomförs	
Maj	Fördjupad kontroll slutförs och rekommendationer lämnas till verksamheten	
Juni	Delårsrapportering avseende verksamhetens dataskyddsarbete för nämnd/styrelse	
September-Oktober	Uppföljning av tidigare lämnade rekommendationer	
November	Årsrapport lämnas till verksamheten	
December	Årsrapport presenteras för nämnd/styrelse	

3 Kontrollpunkter

3.1 Fasta kontrollpunkter

De fasta kontrollpunkternas omfattning utgår från principerna om inbyggt dataskydd och dataskydd som standard (enligt artikel 25 DSF). 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 DSF, 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 personuppgiftsansvarig, 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 principen om inbyggt dataskydd avses att man tar hänsyn till förordningen vid utformning av IT-system och rutiner, och på så sätt från början säkerställer att både kraven i dataskyddsförordningen uppfylls och att den registrerades rättigheter skyddas. Principen om dataskydd som standard innebär att personuppgifter i standardfallet inte behandlas i onödan, vilket kan göras genom att ha lämpliga tekniska och organisatoriska åtgärder som standard.

Med principerna som utgångspunkt har elva kontrollpunkter definierats, av både organisatorisk och teknisk karaktär, vilka 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 som hanterar punkterna så att kontrollerna över tid kommer att kräva mindre och mindre arbete.

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 incidenten, 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 2021**

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

Fokusområde 1: Personuppgiftsincidenter (kontrollpunkt 2)

Hantering av personuppgiftsincidenter under 2020
Personuppgiftsansvariga och personuppgiftsbiträden ska arbeta medvetet och proaktivt för att förhindra personuppgiftsincidenter. Om det ändå sker en incident ska det finnas förutsättningar för att hantera den snabbt och på rätt sätt. Den personuppgiftsansvarige är enligt artikel 33.5 DSF skyldig att dokumentera samtliga inträffade incidenter, oavsett risknivå. Dokumentationsskyldigheten är kopplad till ansvarsskyldigheten i artikel 5.2 DSF, som innebär att den personuppgiftsansvarige ska ansvara för och kunna visa att de grundläggande principerna för dataskydd efterlevs. Dokumentationen ska innefatta omständigheterna kring incidenten, dess effekter och de korrigerande åtgärder som vidtagits.

Om det inte är osannolikt att en inträffad personuppgiftsincident medför en risk för registrerades fri- och rättigheter ska, enligt artikel 33 DSF, den personuppgiftsansvarige anmäla incidenten till Integritetsskyddsmyndigheten (tidigare Datainspektionen) inom 72 timmar efter det att personuppgiftsansvarig fått vetskap om incidenten. Den personuppgiftsansvarige behöver vid varje inträffad incident bedöma i vilken utsträckning som den uppkomna incidenten påverkar de registrerades fri- och rättigheter.

Kontrollen avser undersöka verksamhetens dokumentation av vilka rutiner/handlingsplaner som finns för att hantera incidenter samt verksamhetens dokumentation avseende redan inträffade personuppgiftsincidenter. Genomlysningen syftar till att undersöka om det finns förutsättningar för verksamheten att hantera personuppgiftsincidenter på ett korrekt sätt som följer DSF och om rutiner/handlingsplaner får önskat genomslag i praktiken. Genomlysningen syftar även till att skapa en överblick av de incidenter som inträffat under året, för att utifrån den kunna upptäcka eventuella mönster eller återkommande typer av incidenter.

Fokusområde 2: Utbildning (kontrollpunkt 6)

För att en organisation ska ha möjlighet att följa dataskyddsförordningen krävs det att personalen har fått adekvat utbildning. Vilken typ av utbildning eller hur djupgående den behöver vara varierar beroende på vad medarbetaren har för arbetsuppgifter. Alla som på något sätt behandlar personuppgifter behöver dock ha tillräckliga kunskaper för att t.ex. kunna identifiera en personuppgiftsincident, samt ha förutsättningar för att i övrigt göra rätt. Detta kräver viss grundläggande kunskap.

För att undersöka om medarbetarna har tillräcklig kunskap om dataskydd eller om det krävs ytterligare utbildningsinsatser kommer det därför att ske en kontroll av kunskapsnivån.

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.

5 Avrapportering till nämnd/styrelse

5.1 Delårsrapportering

I juni månad kommer respektive nämnd/styrelse att få en delårsrapportering 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/ert dataskyddsombud. Frågor kan också alltid ställas till dso@intraservice.goteborg.se.