Tjänsteutlåtande
Utfärdat 2026-04-14
Ärendenummer GST-2026-00046

Handläggare
Magnus Havås
Telefon: 031-708 7019
E-post: magnus.havas@stadsteatern.goteborg.se

Dataskyddsombudets kontrollplan 2026-2027

Förslag till beslut

I styrelsen för Göteborgs Stadsteater AB:

Styrelsen antecknar informationen.

Sammanfattning

Bolaget är ytterst ansvarig för att dataskyddslagstiftningen efterlevs i verksamheten. Till stöd utses sakkunnigt dataskyddsombud från Intraservice vars uppgift bland annat är att kontrollera bolagets dataskyddsarbete. Kontrollen består dels av övergripande kontrollpunkter, dels av fördjupade kontrollpunkter. From 2023 alternerar dessa kontroller vartannat år (2023 övergripande, 2024 fördjupade osv) för att ge bolaget mer tid att omhänderta resultaten från kontrollerna.

Bolaget har fått bifogad kontrollplan för dataskyddsarbete 2026-2027 där en fördjupande kontroll 2026 kommer att genomföras under perioden april-oktober.

Under 2026 är fokus för den fördjupade kontrollen verksamheternas hantering av personuppgiftsincidenter, med syftet att kontrollera verksamheternas efterlevnad av artikel 33 och 34 i GDPR.

Bolaget har också fått dataskyddsombudet rekommendation gällande Copilot Chatt, vilken bifogas som bilaga.

Bedömning ur ekonomisk dimension

Bolaget har inte funnit några särskilda aspekter på frågan utifrån denna dimension.

Bedömning ur ekologisk dimension

Bolaget har inte funnit några särskilda aspekter på frågan utifrån denna dimension.

Bedömning ur social dimension

Bolaget har inte funnit några särskilda aspekter på frågan utifrån denna dimension.

Bilagor som ingår i beslutsunderlaget

1. DSO Kontrollplan för dataskyddsarbetet 2026-2027
2. DSO Rekommendation Copilot Chatt 2026-03-02

Magnus Havås	Frida Edman
Ekonomichef	VD

Göteborgs Stad

Kontrollplan för dataskyddsarbetet 2026–2027

Nämnder och bolag i Göteborgs Stad

2026-02-27

Innehåll

1 Inledning

Dataskyddsförordningen (GDPR) tillkom för att särskilt skydda människors rätt till integritet, samt var och ens rätt till insyn i och kontroll över vad som sker med ens personuppgifter. 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.

Det är varje nämnd och bolag som är ytterst ansvarig för att dess verksamhet följer dataskyddslagstiftningen. Att nämnder 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.

1.1 Göteborgs Stads dataskyddsombud

I Göteborgs Stad fullgör dataskyddsenheten på Intraservice uppdraget som dataskyddsombud åt stadens bolag och nämnder. Vad som är dataskyddsombudets uppgifter framgår direkt av lagstiftningen i GDPR.[1] Dataskyddsombudet har särskild sakkunskap i dataskyddslagstiftning och arbetar oberoende med att övervaka och granska att stadens förvaltningar och bolag följer dataskyddslagstiftningen. Dataskyddsombudet har också till uppgift att ge råd och stöd till förvaltningar och bolag i dataskyddsfrågor.

Varje verksamhet ansvarar för att stödja dataskyddsombudet i utförandet av uppdraget genom att tillhandahålla de resurser som krävs för arbetet samt tillgång till personuppgifter och behandlingsförfaranden.[2] Det är också verksamhetens ansvar att säkerställa att dataskyddsombudet inte tar emot instruktioner eller utsätts för repressalier för att ha utfört sina uppgifter.[3]

[1] Artikel 39 i GDPR.
[2] Artikel 38.2 i GDPR.
[3] Artikel 38.3 i GDPR.

2 Kontrollarbetet 2026–2027

Den övergripande och viktigaste uppgiften för dataskyddsombudet är att övervaka att verksamheten följer dataskyddsförordningen. I Göteborgs Stad innebär detta bland annat att dataskyddsombudet genomför kontroller av dataskyddsarbetet inom förvaltningar och bolag. För dataskyddsombudet är kontrollarbetet ett sätt att få en bild av vilka risker och/eller brister som eventuellt föreligger inom en verksamhet. 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. Genom kontroller kan dataskyddsombudet kartlägga verksamhetens dataskyddsarbete, och denna kartläggning kan sedan användas som ett stöd av verksamheten i dess fortsatta arbete med dataskydd.

Dataskyddsombudets kontrollarbete specificeras genom denna kontrollplan, som syftar till att informera personuppgiftsansvariga om upplägg och tidplan för kontrollarbetet åren 2026 och 2027. Dataskyddsombudets kontrollarbete löper över tvåårsperioder, och en ny kontrollplan kommer att skickas ut vartannat år.

Syftet med att arbeta utefter en på förhand fastställd kontrollplan är att det ska bidra till att sätta fokus på verksamhetens dataskyddsarbete och därmed säkerställa ett kontinuerligt dataskyddsarbete som skapar förutsättningar för efterlevnad av förordningen samt göra dataskyddsarbetet till en integrerad del i verksamhetens informationssäkerhetsarbete.

2.1 Kontrollarbetets delar

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

2.1.1 Övergripande kontroll

Den övergripande kontrollen utgår från tio kontrollpunkter[4] och genomförs genom en enkät som fylls i av verksamheten. Varje kontrollpunkt innehåller ett antal delfrågor utformade som påståenden och verksamheten ska uppskatta hur väl påståendet stämmer in på verksamheten. I vissa fall efterfrågar dataskyddsombudet även att verksamheten motiverar sina svar.

Resultaten från enkäten är tänkt att ge en bild av verksamhetens dataskyddsarbete och ska kunna användas som underlag i verksamhetens löpande dataskyddsarbete. Syftet är att få till ett långsiktigt och systematiskt arbetssätt, samt åskådliggöra de förändringar som vidtas över tid.

[4] Kontrollpunkterna har utformats utifrån 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 verksamhetens processer. Se bilaga 1 för beskrivning av kontrollpunkterna.

2.1.2 Fördjupad kontroll

I utformningen av den fördjupade kontrollen utgår dataskyddsombudet från de risker som identifierats, både inom enskilda verksamheter och på en övergripande nivå. Hänsyn tas även till vad som bedöms kunna få störst effekt för flest verksamheter inom Staden. Den fördjupade kontrollen är utformad som en stickprovskontroll, vilket innebär att alla verksamheter inte kontrolleras. I stället genomförs kontrollen inom ett antal förvaltningar och bolag som dataskyddsombudet anser utgör ett representativt urval för stadens verksamheter.

Resultaten från kontrollen redovisas dels på verksamhetsnivå genom separata rapporter till berörda nämnder och bolag, dels på övergripande nivå genom en stadengemensam rapport. Den stadengemensamma rapporten är tänkt att kunna användas av flera verksamheter och genom denna kan även de verksamheter som ej varit med i kontrollen ta del av och dra lärdom från resultaten av kontrollen.

2.1.3 Uppföljning

Uppföljning av de rekommendationer som tidigare lämnats till verksamheten i samband med årsrapportering eller fördjupade kontroller genomförs årligen. Resultatet redovisas till styrelse eller nämnd i verksamhetens årsrapport.

2.2 Tidplan för kontrollarbetet 2026–2027

2026	Aktivitet
Februari	Kontrollplan för 2026–2027 lämnas till nämnder och styrelser.
April-Oktober	Fördjupad kontroll genomförs. Under 2026 är fokus för den fördjupade kontrollen verksamheternas hantering av personuppgiftsincidenter, med syftet att kontrollera verksamheternas efterlevnad av artikel 33 och 34 i GDPR.
Oktober	Uppföljning av lämnade rekommendationer.
November – december	Genomgång av innehåll i årsrapport med respektive verksamhet.
December	Årsrapport översänds till nämnd eller styrelse.

2027	Aktivitet
September	Övergripande kontroll genomförs.
Oktober	Uppföljning av lämnade rekommendationer.
November – december	Genomgång av innehåll i årsrapport med respektive verksamhet.
December	Årsrapport översänds till nämnd eller styrelse.

3 Rapportering

3.1 Årsrapport

Det är varje nämnd och bolag som är ytterst ansvarig för att dess verksamhet följer dataskyddslagstiftningen. Utifrån detta, och då dataskyddsombudet enligt lag ska rapportera om arbetet till högsta förvaltningsnivå, lämnar dataskyddsombudet årligen en rapport om respektive verksamhets dataskyddsarbete till nämnder och bolag i Göteborgs Stad. I rapporten redogör dataskyddsombudet för de iakttagelser som gjorts under året och årets kontrollarbete, samt för resultatet av den uppföljning som genomförts av hur verksamheten hanterat och arbetat med de rekommendationer som lämnats tidigare. Årsrapporten är avsedd att kunna användas som ett stöd för verksamheten i sitt fortsatta arbete med dataskydd.

3.2 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 eller bolag. Det kan också vara om dataskyddsombudet uppmärksammar att det inom verksamheten fattats beslut som är oförenliga med dataskyddslagstiftningen och dataskyddsombudets råd.

Kontakt

Frågor avseende kontrollplanen hänvisas till dataskyddsenhetens funktionsbrevlåda; dso@intraservice.goteborg.se.

Bilaga 1 – Beskrivning av kontrollpunkter

Kontrollpunkter	Beskrivning
Kontrollpunkt 1: Dataskyddsorganisation och övergripande styrning i dataskyddsarbetet	Kontrollpunkten avser verksamhetens övergripande styrning samt organisatoriska förutsättningar för att kunna bedriva ett kontinuerligt dataskyddsarbete. Dataskyddsarbetet behöver vara systematiskt med tydliga roller, ansvar och intern uppföljning. Tydlig styrning sätter ramarna för arbetet med dataskydd och främjar ett riskbaserat arbetssätt. Punkten följer upp verksamhetens dataskyddsorganisation, definierade ansvarsområden och tillhandahållna resurser för arbetet. Även verksamhetens systematiska arbete utifrån en plan för dataskyddsarbetet och hur verksamheten säkerställer involvering av dataskyddsombudet ingår i punkten.
Kontrollpunkt 2: Register över personuppgiftsbehandlingar	Kontrollpunkten avser verksamhetens efterlevnad av skyldigheten att systematiskt dokumentera alla personuppgiftsbehandlingar i form av ett register. Även verksamhetens arbete med att säkerställa ett uppdaterat och heltäckande behandlingsregister och dokumenterade arbetssätt för detta omfattas av kontrollpunkten.
Kontrollpunkt 3: Hantering av personuppgiftsincidenter	Kontrollpunkten avser verksamhetens förutsättningar för att identifiera och hantera personuppgiftincidenter, samt hur verksamheten arbetar med uppföljning av såväl arbetssätt som inträffade incidenter.
Kontrollpunkt 4: Utbildning	Kontrollpunkten avser verksamhetens arbete med att utbilda och upprätthålla kunskaper och medvetenhet i dataskyddsfrågor hos anställda.
Kontrollpunkt 5: Information till registrerade	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. Informationen som lämnas till registrerade ska överensstämma med behandlingsregistret.
Kontrollpunkt 6: Konsekvensbedömning/samråd	Kontrollpunkten avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras och genomföra denna. I detta ingår att verksamheten har dokumenterade arbetssätt för arbetet med konsekvensbedömningar och hur dataskyddsombudet involveras i arbetet. Därtill tillkommer att verksamheten har dokumenterade arbetssätt för att hantera de risker som identifieras i konsekvensbedömningen samt hur genomförda konsekvensbedömningar följs upp och hålls aktuella.

Kontrollpunkt 7: Informationshantering	Kontrollpunkten avser verksamhetens informationshantering. En aktuell och fastställd dokumenthanteringsplan med gallringsbeslut är en förutsättning för att verksamheten ska kunna säkra följsamhet gentemot dataskyddsförordningen. Vidare behöver verksamheten ha tydliga instruktioner för hur olika kategorier av personuppgifter ska hanteras i olika medel. Kontrollpunkten omfattar dessa delar samt verksamhetens arbete med att säkerställa att gallring samt användning av medel följs.
Kontrollpunkt 8: Säkerhet	Dataskydd och informationssäkerhet hänger ihop. Kontrollpunkten avser verksamhetens dokumenterade arbetssätt för arbetet med säkerhet i samband med behandlingarna, enligt kraven i artikel 32 i GDPR.
Kontrollpunkt 9: Biträdesavtal och andra överenskommelser	Kontrollpunkten avser verksamhetens bedömning kopplat till, samt hantering av, biträdesavtal och andra överenskommelser gällande dataskydd. Verksamhetens dokumenterade arbetssätt för uppdatering och uppföljning av tecknade biträdesavtal omfattas av kontrollpunkten.
Kontrollpunkt 10: 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 dokumenterade arbetssätt för arbetet, och att den registrerades personuppgifter enkelt kan lokaliseras vid efterfrågan. I kontrollpunkten ingår även verksamheternas dokumenterade arbetssätt för att hantera skadeståndsanspråk enligt artikel 82 i GDPR.

2026-03-02 Förvaltningar och bolag i Göteborgs Stad

Generell rekommendation från dataskyddsombudet gällande Copilot Chat

Ärendet

Förvaltningen för Intraservice erbjuder verksamheter i Göteborgs Stad möjligheten att använda funktionen ”Copilot Chat” via M365-plattformen. Med anledning av de risker som föreligger vid användning av Copilot Chat lämnar dataskyddsombudet en generell rekommendation till de verksamheter som vill börja använda Copilot Chat. Utöver nedanstående rekommendationer behöver verksamheterna även säkerställa att övriga krav enligt GDPR efterlevs.

Tidigare lämnade rekommendationer gällande Copilot Chat

Dataskyddsombudet lämnade i maj 2025 en rekommendation avseende förvaltningen för Intraservices riskanalys för Microsoft Copilot Chat. I rekommendationen lyfts, bland annat, att riskbilden bedöms vara ofullständig då förvaltningen utelämnat vissa risker, exempelvis risken kopplat till ”Osäkerhet och bristande kontroll över underbiträden och tredjelandsöverföringar”. Sammantaget bedömde dataskyddsombudet att de frågeställningar som behövde adresseras vad gäller Copilot Chat var betydligt mer komplexa än vad som redogjordes för i underlaget. Då risken gällande osäkerhet och bristande kontroll över underbiträden och tredjelandsöverföringar inte är unik för Copilot Chat, utan gäller hela M365-plattformen, rekommenderades förvaltningen för Intraservice även att omgående vidta tekniska och organisatoriska skyddsåtgärder för att säkerställa att användningen av plattformen är förenlig med de krav som gäller enligt GDPR.

Verksamheternas ansvar

De risker som dataskyddsombudet lyft i rekommendationen till Intraservice är tillämpliga även för de verksamheter som vill börja använda Copilot Chat. Respektive verksamhet behöver därför säkerställa att dessa är omhändertagna innan Copilot Chat aktiveras.

Identifierad risk: Överföring av data till Microsoft utan rättslig grund

Copilot Chat innebär att sökningar kan göras via Bing. För de uppgifter som skickas till Bing anger sig Microsoft vara personuppgiftsansvarig. Det finns inga säkerhetsåtgärder som förhindrar att personuppgifter skickas till Bing. Om personuppgifter skickas till Bing innebär det en delning av personuppgifter som avviker från övriga M365-hanteringen, eftersom Microsoft i detta fall tar över personuppgiftsansvaret. Om Microsoft blir personuppgiftsansvarig för uppgifterna krävs en rättslig grund för överföringen. I det fall det inte går att fastställa en giltig rättslig grund för överföringen innebär det att behandlingen är olaglig.

Rekommenderad hantering

I det fall en rättslig grund för överföringen inte kan identifieras rekommenderas verksamheten att stänga av möjligheten att använda sökningar via Bing vid användning av Copilot Chat.

Identifierad risk: Osäkerhet och bristande kontroll över underbiträden och tredjelandsöverföringar

Microsoft har, trots att det specifikt efterfrågats, inte kunnat lämna en lista över de underbiträden som används för att tillhandahålla Stadens M365-miljö, inkluderat Copilot Chat. I stället hänvisar man till listan över samtliga möjliga underbiträden som är tillgänglig via Microsofts hemsida. Utifrån att Microsoft själva inte kan redogöra för vilka underbiträden som används finns det risk för att samtliga angivna kan aktualiseras, vilket innebär möjliga tredjelandsöverföringar till flera länder utan adekvat skyddsnivå.

Rekommenderad hantering

Verksamheten rekommenderas kartlägga alla överföringar till tredjeland och detta i alla led, dvs. även vidareöverföringar. Om underbiträdena i sin tur har underbiträden behöver verksamheten även bedöma följande led så att verksamheten har koll på, och kan redogöra för, hela kedjan. Att kartlägga sina överföringar innebär att veta vilka uppgifter som överförs till vilket land och för vilket ändamål. Detta innebär att när en internationell molninfrastruktur, likt M365, används måste den personuppgiftsansvarige bedöma om och när personuppgifter kommer att överföras till tredjeländer.[1]

När verksamheten fått en bild av vilka överföringar, inklusive vidareöverföringar, som förekommer och till vilka länder dessa görs, ska en bedömning av vilka överföringsmekanismer som är tillämpliga genomföras.

Överföringar och vidareöverföringar med stöd av adekvansbeslut enligt artikel 45 i GDPR

För överföringar som sker med stöd av ett adekvansbeslut ska verksamheten bedöma:

- Huruvida beslutet om adekvat skyddsnivå är i kraft
- Huruvida de överföringar som görs på den personuppgiftsansvariges vägnar omfattas av ett sådant beslut (till exempel kategorier av personuppgifter eller sektorer som faller inom ramen för tillämpningsområdet).[2]

Om en vidareöverföring stödjer sig på ett adekvansbeslut enligt artikel 45 i GDPR behöver den personuppgiftsansvarige säkerställa att överföringen faktiskt omfattas av åberopat adekvansbeslut.[3] Denna bedömning bör dokumenteras i samband med kartläggningen ovan.

Överföringar och vidareöverföringar med stöd av annat överföringsverktyg enligt artikel 46 i GDPR

För de länder som saknar adekvat skyddsnivå behöver verksamheten göra en egen bedömning om det valda överföringsverktyget ger väsentligen samma skydd för personuppgifterna som inom EU/EES.[4] Verksamheten kan utgå från en bedömning som

[1] EDPB:s rekommendationer 01/2020, punkterna 10–13.
[2] EDPB Yttrande 22/2024 pt 93
[3] Ibid. pt. 94-95
[4] Se steg 3 i EDPB:s rekommendationer 01/2020 samt EDPB:s rekommendationer 02/2020.

leverantören genomfört men verksamheten behöver alltid själv kontrollera och värdera denna bedömning samt om nödvändigt komplettera den.[5]

Om en vidareöverföring grundas på artikel 46 i GDPR behöver den personuppgiftsansvarige, i enlighet med ansvarsskyldighetsprincipen, kunna visa att vidareöverföringen sker i enlighet med det åberopade skyddsinstrumentet och att personuppgiftsbiträdet/underbiträdet uppfyller de krav som följer av detta.[6]

Identifierad risk: Nya funktioner kan medföra nya risker

Under hösten 2025 fick dataskyddsombudet information från förvaltningen för Intraservice om att Copilot Chat skulle göras tillgängliga via alla M365-applikationer i januari 2026. Detta skulle innebära att Copilot Chat skulle kunna användas direkt i Word, Excel, Powerpoint, Outlook, Onenote etc. Denna funktionalitet har, till dataskyddsombudets kännedom, ännu inte införts i Göteborgs Stad.

Rekommenderad hantering

1) De verksamheter som vill använda Copilot Chat rekommenderas ta höjd för att denna funktionalitet kan komma att införas i närtid och uppdatera sina konsekvensbedömningar, inkl. riskbedömningar, därefter.

2) De verksamheter som angett att inga personuppgifter ska behandlas via Copilot Chat behöver se över ifall de tekniska och organisatoriska säkerhetsåtgärder som är tänkta att styra detta är tillräckliga när Copilot Chat tillgängliggörs direkt i applikationerna.

Sammantagen bedömning och rekommendation

Det saknas i dagsläget grundläggande dataskyddsrättsliga bedömningar för användningen av M365-plattformen inom Göteborgs Stad. Detta innebär att det saknas en sammanhållen bedömning av de verktyg och applikationer som redan används i M365-plattformen. Att M365-plattformen redan används inom Göteborgs Stad är i sig inte ett argument för att fortsätta utöka användningen utan att grunderna först utreds och bedöms. En utökad användning av M365-plattformen där nya funktioner införs kan komma att medföra en ökad personuppgiftshantering, vilket i sin tur innebär att riskerna för de registrerade kan öka. Det åligger varje verksamhet som vill vidareutveckla den egna användningen av M365-plattformen, med nya applikationer och/eller AI-verktyg såsom Copilot Chat, att säkerställa att användningen är förenlig med dataskyddslagstiftningen.

Innan dess att ovan risker omhändertagits och nödvändiga grundläggande dataskyddsrättsliga bedömningar av förutsättningarna för användningen av M365-plattformen genomförts bedömer dataskyddsombudet att det saknas förutsättningar för att utöka användningen av och/eller införa nya funktioner i M365.

Rekommendation

Dataskyddsombudet avråder förvaltningar och bolag från att utöka användningen av och/eller införa nya funktioner i M365 innan dess att dataskyddsrättsliga bedömningar av förutsättningarna för användningen av M365-plattformen genomförts.

---

[5] Se EDPB:s yttrande 22/2024 punkt 96. Av samma yttrande framgår av punkterna 82-84 även att den personuppgiftsansvarige (PUA) har en skyldighet att vidta lämpliga åtgärder för att GDPR inte överträds, det faller på PUA att kontrollera om biträdet kan lämna tillräckliga garantier att genomföra de åtgärder som PUA fastställt enligt artikel 28.1 i GDPR.
[6] Ibid. pt. 97.