Planering för dataskyddsarbetet för 2023

# ****Inledning****

GS dataskyddsombud har under 2022 granskat bolagets dataskyddsarbete utifrån 12 fasta kontrollpunkter, 1 fördjupad kontrollpunkt samt uppföljning av tidigare kontrollpunkt. Som har resulterats i en årsrapport med rekommendationer, som kommer att följas upp av dataskyddsombudet löpande.

Genom att ha en årlig uppföljning av de fasta kontrollpunkterna kommer personuppgiftsansvarige (styrelsen) kunna följa utvecklingen av dataskyddsarbetet inom bolaget över tid. Eftersom de 12 kontrollpunkterna är samma för alla förvaltningar och bolag kommer också en jämförelse mellan dessa att kunna göras. Dataskyddsombudets granskning är också till god hjälp för bolagets planering, genomförande och uppföljning av dataskyddsarbetet.

## Beskrivning av aktiveter

Utifrån kontrollpunkterna planerar GS följande aktiviteter, se bilaga 1.

## Behov av resurser för genomförandet

Dataskyddsarbetet som planeras för året kräver insatser för verksamheten och de resurser som är utsedda att ingå i GS dataskyddsorganisation.

## Uppföljning av aktiviteterna

Dataskyddskontakten kommer i samråd med dataskyddsombudet följa upp aktiviteterna och kontinuerliga avstämningsmöten. Dataskyddsombudet kommer också att sammanställa granskningen i en rapport som ska redovisas för styrelsen vid årets slut.

## Prioriterade delar

## GS kommer under 2023 prioritera följande delar i enlighet med dataskyddsombudets rekommendationer,

**Kontrollpunkt 3:** Biträdesavtal och andra överenskommelser

**Kontrollpunkt 4:** Personuppgiftsregister

**Kontrollpunkt 10**: IT-projekt och upphandling

En bild som visar text

Automatiskt genererad beskrivning

**Bilaga 1**

|  |  |  |  |
| --- | --- | --- | --- |
| Fasta kontrollpunkter enligt data-skyddsombudet | Beskrivning | Granskningens kommentar | Planerade och prioriterade aktiviteter för 2023 |
| 1. Dataskydds-organisation | Organisatoriska förutsättningar för att kunna bedriva ett kontinuerligt dataskyddsarbete, och omfattar bland annat bolagets dataskyddsorganisation, definierade ansvarsområden och rapporteringsvägar för involverade funktioner samt tillhandahållna resurser för arbetet. | Indikation på att dataskydd inte är integrerad och naturlig del i verksamhetens alla delar. Det saknas rutiner för att regelbundet involvera DSO.  **Rekommendation** att utvärdera arbetssätt och undersöka om det är ändamålsenligt och effektivt.  Utreda hur olika verksamhetsdelar involveras i dataskyddsarbetet för att säkerställa att dataskyddsorganisationen når ut till samtliga delar. För att göra dataskydd till en naturlig och självklar del av det dagliga arbetet krävs också att det inom alla delar finns förståelse för att GDPR är en lag jämte de många andra som måste följas och att lagstiftningen varken är valbar eller något som kan prioriteras bort. | Ta fram instruktioner som säkerställer att DSO på ett mer systematiskt sätt informeras om och involveras i alla frågor rörande dataskydd.  Säkerställa att DSK och DSO har kontinuerliga och dokumenterade avstämningsmöten. |
| 2. Personuppgifts-incidenter (även fördjupad kontrollpunkt) | GS förutsättningar för att identifiera och hantera personuppgiftsincidenter. | Arbetet med personuppgiftsincidenter sker enligt skattningen på ett övergripande och systematiskt och effektivt sätt. DSO delar överlag med denna uppfattning men finns åtgärder som behöver vidtas.  Förutsättning att regelbundet informera medarbetare om vad personuppgiftsincidenter är och hur de ska hanteras. Det är en grundläggande förutsättning för ett fullgott dataskyddsarbete att alla som behöver det fått utbildning och information om dataskydd i detta ingår att utbilda om personuppgiftsincidenthantering. | Tar fram en rutin för att regelbundet och vid behov säkerställa att medarbetare informeras om vad personuppgifter är och hur dessa ska hanteras inom bolaget.  Säkerställa att samtliga får en målgruppsanpassad microutbildning i introduktionspaketet. |
| 3. Biträdesavtal och andra överenskommelser    *Prioriterad* | Granskningen innefattar GS dokumentation av biträdesavtal och andra överenskommelser gällande dataskydd och förutsätter att bolaget har identifierat samt registrerat personuppgiftsbiträden i personuppgiftsregistret. Även bolagets rutiner för uppdatering och uppföljning av tecknade biträdesavtal innefattas. | Omfattande risker som omgående kräver åtgärder. Bolaget har angett att det finns tecknat personuppgiftsbiträdesavtal i ca 50 % av fallen då detta krävs, att det till stor del saknas efterlevnadskontroller och att det inte finns tillräckliga rutiner/kompetens för att bedöma hela kedjan av biträden/underbiträden.  Avsaknaden av biträdesavtal utgör en hög risk för bolaget, rekommenderas att GS omgående genomför en kartläggning av behandlingar där biträden anlitas för att kunna identifiera i vilka fall det behöver upprättas PUB-avtal.  **Rekommenderas** att under året prioritera arbetet med PUB-avtal.  **Rekommenderas** att ta fram rutiner för att kontrollera anlitade biträden samt vid anlitande av nya biträden kontrollera dess underbiträden. | Ta fram instruktioner för att kontrollera anlitade biträden samt vid anlitande av nya biträden kontrollera deras underbiträden. Utifrån det ansvar bolaget har vid anlitande av biträden enl 28 GDPR (omsorgsplikten) föreligger här en risk att GS inte kan uppfylla kraven enligt GDPR.  Se över processer och instruktioner som säkerställer att det finns PUB-avtal. |
| 4. Personuppgiftsregister    *Prioriterad* | Skyldighet att systematiskt dokumentera alla personuppgiftsbehandlingar i form av ett register. Även bolagets arbete med, och rutin för att säkerställa ett uppdaterat och heltäckande personuppgiftsregister innefattas. | Det finns en ansvarsfördelning att hålla behandlingarna i registret uppdaterade men i princip saknas allt övrigt. Behandlingarna som finns i registret innehåller inte all information som krävs vilket innebär en stor risk för GS.  Enligt skattningen uppfyller GS inte sina skyldigheter enl GDPR.  **Rekommenderas** att under året prioritera arbetet med personuppgiftsregistret. | Uppdatera personuppgiftsregistret, systemstöd DraftIt. |
| 5. Övergripande strategi för dataskydd | GS övergripande strategi för att arbeta med dataskydd. | GS svar indikerar på att det finns risker som kräver åtgärder, särskilt vad gäller en övergripande strategi och systematiskt arbeta med dataskyddsfrågor.  **Rekommenderas** att i dokumenterade handlings- och/eller verksamhetsplan, rutiner och policys tydliggöra sin strategi för det övergripande dataskyddsarbetet.  **Rekommenderas** att säkerställa att informationstillgångarna identifieras och värderas utifrån behovet av konfidentialitet, riktighet och tillgänglighet i enlighet med stadens styrande dokument inom informationssäkerhet.  **Rekommenderas** att ta fram och fastställa en informationssäkerhetspolicy som tydligt och enkelt sätt tillgängliggörs för berörda medarbetare. | Tydliggöra strategi för det övergripande dataskyddsarbetet.  Identifiera informationstillgångarna.  Ta fram en informationssäkerhetspolicy. |
| 6. Utbildning | Avser arbetet med att utbilda och upprätthålla kunskapsnivån i dataskyddsfrågor hos anställda. | Medarbetare ges regelbundet möjlighet att delta i utbildningar och att det i hög utsträckning genomförs regelbundna utbildningsinsatser. Dock kan utläsas att den allmänna kunskapsnivån inte är tillräckligt god., att kunskapsnivån inte följs upp tillräckligt och att det behöver ske en kartläggning av kunskapsnivå och utbildningsbehov för roller och befattningar. En grundläggande förutsättning att kunna säkerställa ett fullgott dataskyddsarbete är att verksamhetens medarbetare har tillräcklig kunskap om hur personuppgifter ska hanteras på rätt sätt.  **Rekommenderas** att kartlägga vilka utbildningar och andra kompetenshöjande insatser som behövs samt följa upp kunskapsnivån efter genomförda utbildningar.  **Rekommenderas** att GS ser över de regelbundna utbildningarna som erbjuds och säkerställer att dessa leder till en högre allmän kunskapsnivå inom dataskydd. | Kartlägga utbildningar och kompetenshöjande insatser samt följa upp kunskapsnivån.  Se över de regelbundna utbildningarna och säkerställa en högre kunskapsnivå inom dataskydd. |
| 7. Integritetspolicy | Utformning samt tillhandahållande av dess integritetspolicy till registrerade (både internt och externt). Även GS rutin för att upprätthålla en aktuell integritetspolicy omfattas. | Indikation för att det finns höga risker, En försämring mot granskning 2021, men detta ger en rättvisare bild och hur GS uppfyller sina skyldigheter enligt GDPR. DSO anser det är positivt att GS har insikt i vilka brister som finns och belyser aktuella risker. Det ställs höga krav på PUA att informera de registrerade om hur deras personuppgifter behandlas. En förutsättning för detta är att ha en överblick, kontroll och kunskap om de behandlingar som utförs. GS har i vissa delar arbetat med att se och över och revidera informationen som ges till de registrerade, vilket är positivt. Det är fortfarande många behandlingar som det fortfarande inte ges information om kvarstår ett stort arbete.  **Rekommenderas** kartlägga vilka behandlingar man i dagsläget inte informerar om, ta fram en plan för hur denna information ska ges och arbeta med att säkerställa att den är komplett.  **Rekommenderas** att ta fram rutiner som anger både instruktioner kring när/hur policyn ska uppdateras och också utpeka vem/vilken roll som ansvarar för att detta görs. Ytterligare rekommendationer kopplat till informationsskyldigheten framgår även av den fördjupade kontrollen. | Uppdatera befintlig extern integritetspolicy som finns publicerad på hemsidan samt läggs upp i Dokumentcenter för revidering efter 330 dagar.  Färdigställa den interna integritetspolicyn samt lägga upp i Dokumentcenter för revidering efter 330 dagar. |
| 8. Mejl och dokumenthantering | GS rutiner för mejl och dokumenthantering. I detta är en aktuell och fastställd dokumenthanteringsplan med gallringsbeslut en förutsättning för att GS ska kunna säkra följsamhet gentemot dataskyddsförordningen. Även bolagets rutin för att säkerställa att gallringsrutiner för personuppgifter följs innefattas. | Rekommenderas att följa upp och kontrollera att hanteringen av personuppgifter i e-post genomförs i enlighet med gällande rutiner och anvisningar. Principerna i uppgifts- och lagringsminimering är grundläggande i dataskyddsförordningen. Det ställs höga krav på att hantera uppgifter tillräckligt säkert. Granskningen visar att det finns behov av att se över verksamhetens informationsklassificering av personuppgiftsbehandlingar, och att kontrollera att detta görs i enlighet med Göteborgs Stads riktlinjer för informationssäkerhet. Det behöver tas fram anvisningar för hur information i olika informationsklasser ska hanteras och vilka lagringsytor som får användas. Dessa bedömningar behöver regelbundet ses över.  **Rekommenderas** att ta fram en handlingsplan för arbetet med att informationsklassificera personuppgiftsbehandlingar, anvisning för hur lagring/hantering får ske samt rutiner som säkerställer en regelbunden uppföljning av klassningen. | Uppdatera befintlig informationshanteringsplan med informationsklassificera personuppgiftsbehandlingar enligt GBG Stads riktlinjer för informationssäkerhet. |
| 9. Konsekvens-bedömning/samråd | Kontrollen innefattar GS förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras samt rutiner kopplat till detta. | Att genomföra konsekvensbedömningar är i många fall ett absolut krav, om detta inte genomförs finns risk för att GS missar vidta åtgärder som behövs för att säkerställa de registrerades rättigheter. Vilket kan innebära sanktionsavgifter vid en tillsyn. Arbetet med konsekvensbedömningar bör vara en del av den övergripande strategin för dataskyddsarbetet och dataskyddsorganisationen bör fungera på ett sätt som säkerställer att inga nya eller förändrade behandlingar påbörjas utan att en bedömning görs om behovet av en konsekvensbedömning.  **Rekommenderas** att GS gör en kartläggning för att identifiera vilka högriskbehandlingar som konsekvensbedömningar saknas samt ta fram en handlingsplan för att genomföra dem.  **Rekommenderas** också att ta fram rutiner för att säkerställa att konsekvensbedömningar genomförs i rätt tid och i enlighet med GDPR, samt uppföljning av genomförda konsekvensbedömningar samt rutin för att följa upp beslutade åtgärder.  **Rekommenderas** att ta fram rutiner för inhämtande av registrerades synpunkter. | Kartlägga högriskbehandlingar som saknar konsekvensbedömning och genomföra dem.  Säkerställa att nytt arbetssätt från oktober 2022 efterlevs vid förändring eller införande av nytt system kontaktas Dataskyddskontakten som håller samman arbetet med involverade från verksamheten, så att ev konsekvensbedömningar utförs i rätt tid. |
| 10. IT-projekt och upphandling    *Prioriterad* | Kontrollpunkten avser GS 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. | DSO vill särskilt lyfta införandet av det nya systemet för händelserapportering där dataskyddsfrågor inte beaktats i tillräcklig utsträckning eller i rätt tid. DSO har själv fått be om uppdateringar och lägesrapporter och dataskyddsbedömningar har enligt DSO inte avhandlats med tillräcklig hänsyn till gällande lagstiftning. Trots att bolaget arbetat med införandet under lång tid har dataskyddsfrågorna först beaktats mot slutet och i mycket när anslutning till införandet trots medvetenhet om att underlag tar tid att ta fram och att ändringar och justeringar kan behöva göras beroende på vilka risker som framkommer vid en konsekvensbedömning. Hanteringen visar enligt DSO på bristande kompetens och indikerar att det saknas förståelse för vikten att säkerställa skydd för personuppgifter.  **Rekommenderas** att ta fram rutiner för att säkerställa dataskyddsperspektivet från start vid införandet av nya lösningar.  **Rekommenderas** att ta fram rutiner för att via kravställning säkerställa skyddet av personuppgifter och säkerställa följsamhet. | Säkerställa att det nya arbetssättet som är beslutad på GS efterlevs vid förändring eller införande av nytt system kontaktas Dataskyddskontakten som håller samman arbetet med involverade från verksamheten, så att ev konsekvensbedömningar utförs i rätt tid och involverar dataskyddsombudet från start. |
| 11. IT-system och digitala verktyg | GS rutiner för att säkerställa att bolagets 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. | Indikation på att GS inte har överblick över sina IT-system och digitala verktyg, kontroll över hur det ges tillgång/behörighet till dessa och hur användandet följs upp och kontrolleras.  **Rekommenderas** att GS kartlägger alla IT-system och digitala verktyg och säkerställer att de kontrolleras för följsamhet mot GDPR.  **Rekommenderas** att ta fram rutiner att säkerställa att dataskyddsperspektivet vid införande av kostnadsfria tjänster som t ex gratisappar. Det behöver även finnas överblick över kommunikationskanaler och rutin för att kontrollera att dessa uppfyller kraven enligt GDPR. | Kartlägga IT-system och digitala verktyg.  Ta fram rutiner för att säkerställa införandet av kostnadsfria tjänster. |
| 12. Hantering av registrerades rättigheter | Kontrollpunkten avser verksamhetens förutsättningar och rutiner för att hantera de registrerades rättigheter, till exempel registerutdrag eller radering. | Bolaget anser sig i viss mån ha koll på hantering av begäran om registerutdrag men att det finns brister vad gäller beredskap för att hantera vissa andra rättigheter.  **Rekommenderas** att genom utbildning eller informationsinsatser för att stärka medvetenheten om registrerades rättigheter, ta fram process för att få fram efterfrågad information vid begäran om registerutdrag samt säkerställa att bolaget har förutsättningar att bedöma inkomna invändningar. | Uppdatera IT-stöd DraftIt för att därifrån kunna ta ut registerutdrag vid en begäran.  Fortsatt utbildning för att öka medvetenheten om den registrerades rättigheter. |
| Fördjupad kontrollpunkt | Beskrivning | Granskningens kommentar |  |
| Kamerabevakning | DSO har i rapporten gjort flera iakttagelser som innebär att bolaget avseende sin kamerabevakning inte uppfyller kraven enligt aktuell rättslig reglering. | * Utreda och slutligen ta ställning till samt dokumentera bedömning av personuppgiftsansvaret avseende kamerabevakning på spårvagnar * Utreda behandlingen och personuppgiftsansvaret vid den behandling av personuppgifter som sker via tillgång till bildströmmar från trafikkontorets kameror. Om rättsliga förutsättningar saknas behöver behandlingen omedelbart avbrytas. * Genomför översyn av beslut om tillstånd för kamerabevakning vid depå Slottsskogen och depå Majorna * Utreda och ta ställning till om kameror i porttelefoner utgör kamerabevakning enligt definitionen och om tillstånd behöver sökas * Utreda och dokumentera ändamål och rättslig grund för kameror i porttelefoner. Om ändamål och rättslig grund saknas behöver behandlingen avbrytas. * Se över lagringstid för inspelat material och tydligt motivera och dokumentera bedömningarna * Dokumentera ändamål och rättslig grund för kamerabevakning vid depåer * Genomföra/färdigställa konsekvensbedömningar för samtliga behandlingar gällande kamerabevakning där detta krävs. * Komplettera styrande dokument med information om vad som gäller för kamerabevakning/personuppgiftsbehandlingar via kamera vid depåer samt porttelefoner * Skyndsamt åtgärda bristande information till registrerade avseende kamerabevakning/personuppgiftsbehandlingar vid depåer samt porttelefoner. Om bolaget har personuppgiftsansvar för behandling via trafikkontorets kameror behöver informationsplikten uppfyllas även här. | Säkerställa att följande punkter som DSO påpekat blir åtgärdade. |
| Uppföljning av tidigare kontroller | Fördjupad kontroll (2021): Hantering av anställdas personuppgifter: Positioneringsteknik (GPS) | Granskningens kommentar | **Aktiviteter 2023** |
|  |  | Uppföljningen visar att verksamheten har påbörjat åtgärder i enlighet med lämnade rekommendationer. Bolaget har pågående konsekvensbedömningar avseende personlarm och GPS-enheter i bilar och arbetar med att ta fram heltäckande information till de registrerade. | Säkerställa att konsekvensbedömningen efter kommentar från DSO.  Säkerställa att dekaler blir uppsatt i bilarna. |