Styrelsehandling 16
Älvstranden Utveckling AB
Diarienummer 0036/22
2023-02-06
Handläggare:
Emma Einarsson, bolagets datsskyddskontakt
samt Nina Maldevik Havner, dataskyddsombud
dataskyddsenheten på Intraservice

# Informationsärende – Årsrapport granskning av bolagets dataskyddsarbete

## Sammanfattning

Under 2022 har Stadens dataskyddsombud granskat hur Älvstranden Utveckling efterlever dataskyddsförordningen.

En del av denna granskning innebär att dataskyddsombudet har genomfört kontroller av dataskyddsarbetet inom den personuppgiftsansvariges organisation. Dessa kontroller specificeras genom en kontrollplan som innehåller tidplan och särskilda fokusområden för kontrollarbetet 2022.

Målsättningen är att detta 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.

Nina Maldevik Havner, representant för Dataskyddsombudet Intraservice, ger en uppdatering om dataskyddsarbetet på sammanträdet.

## Bedömning av ärendets principiella beskaffenhet

Bolaget bedömer att ärendet inte är av principiell beskaffenhet.

## Bilagor

Bilaga 1. Årsrapport granskning av Älvstranden Utvecklings dataskyddsarbete 2022.

Göteborgs Stad

# Årsrapport för dataskyddsarbetet 2022

## Älvstranden Utveckling AB

2022-12-23

# Innehåll

# 1 Dataskydd i kommunal verksamhet

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 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. 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 uppgifterna.

Arbetet med att säkerställa att personuppgifter behandlas enligt reglerna i GDPR 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 på förvaltningar och bolag inom Göteborgs Stad. I det framåtsyftande arbetet är GDPR ett viktigt redskap för att kunna säkerställa en digitalisering som håller över tid.

## 1.1 Göteborgs Stads dataskyddsombud

Dataskyddsenheten på Intraservice är Göteborgs Stads dataskyddsombud. Vad som är dataskyddsombudets uppgifter framgår direkt av lagstiftningen i GDPR.[1] Dataskyddsombudets viktigaste uppgift är att övervaka att stadens förvaltningar och bolag följer dataskyddslagstiftningen. Detta sker bland annat genom att samla in information om hur personuppgifter behandlas och genom att kontrollera hur bestämmelser och interna styrdokument som styr dataskyddsarbetet efterlevs.

Dataskyddsombudet har också till uppgift att ge råd och information till förvaltningar och bolag i dataskyddsfrågor. Detta sker genom att dataskyddsombudet är behjälplig när frågor rörande behandlingen av personuppgifter uppkommer hos verksamheterna. Dataskyddsombudet erbjuder också regelbundet utbildningar för stadens medarbetare. Rådgivning ges även till förvaltningar och bolag när dessa genomför konsekvensbedömningar, vilket är en skyldighet som följer av GDPR. Efter att ha identifierat ett särskilt behov av stöd i arbetet med konsekvensbedömningar, har dataskyddsenheten under 2022 tagit fram mallar och mallstöd för det arbetet.

Det är nämnd/styrelse som har det yttersta ansvaret för att verksamheterna följer dataskyddslagstiftningen och dataskyddsombudet ska enligt lag rapportera om detta till högsta förvaltningsnivå.[2] Dataskyddsombudet har inte mandat att fatta beslut åt verksamheterna. Det är i stället genom råd och rekommendationer som dataskyddsombudet bistår verksamheterna med underlag för att dessa själva ska kunna fatta väl underbyggda beslut.

[1] Artikel 39 i GDPR
[2] Artikel 38.3 i GDPR

# 2 Granskning av dataskyddsarbetet 2022

## 2.1 Dataskyddsombudets kontrollfunktion

Dataskyddsombudets uppgift att övervaka den personuppgiftsansvariges efterlevnad av förordningen regleras i artikel 39 i GDPR. I Göteborgs Stad innebär en del av denna övervakning att dataskyddsombudet genomför kontroller av dataskyddsarbetet inom den personuppgiftsansvariges organisation.

Enligt dataskyddsregelverket ska dataskyddsombudet arbeta utifrån en riskbaserad metod som utgår från risker för de registrerades fri- och rättigheter. Genom att utgå från en sådan metod minskas risken för negativa konsekvenser även för verksamheten själv. Sådana konsekvenser kan omfatta bland annat skadestånd, sanktionsavgifter, försämrat varumärke eller minskad tillit för verksamheten.

För dataskyddsombudet är kontrollarbetet ett sätt att få en bild av vilka risker och/eller brister som eventuellt föreligger inom en verksamhet. Genom kontroller kan dataskyddsombudet kartlägga verksamhetens dataskyddsarbete, och därigenom hjälpa verksamheten att få en nulägesbild av hur de faktiskt ligger till i sitt dataskyddsarbete. Denna kartläggning kan sedan användas som ett stöd för verksamheten i sitt fortsatta arbete med dataskydd. Kontrollarbetets syfte är inte främst att peka ut brister utan ska ses som en vägledning för verksamheten och ett verktyg för att identifiera relevanta prioriteringar. Det är sedan 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. I det arbetet är dataskyddsombudet behjälplig med rådgivning utifrån verksamhetens behov och de risker som identifierats.

## 2.2 Fördjupad kontroll

### 2.2.1 Kontroll av personuppgiftsincidenter 2022

Den fördjupade kontrollen har bestått av personuppgiftsincidenter. Resultatet av kontrollen presenteras i sin helhet i bilaga 2.

Dataskyddsombudet har i rapporten avseende den fördjupade kontrollen haft vissa anmärkningar och har därför lämnat ett antal rekommendationer till verksamheten för åtgärd.

Organisationen behöver uppdatera och komplettera befintliga dokument anvisning/instruktion för hanteringen av personuppgiftsincidenter som bör minst innehålla följande:

- Beskrivning för att kunna avgöra vad som är en personuppgiftsincident.
- Rutiner för att bedöma riskerna för personer som har drabbats av personuppgiftsincidenten.
- Rutiner för anmälan av incident till tillsynsmyndigheten inom 72 timmar efter upptäckten.
- Rutiner för vilken information som ska inkluderas i en anmälan till tillsynsmyndigheten.
- Rutiner för att hantera incidenter som har inträffat hos personuppgiftsbiträdet.
- Rutiner för när och hur de registrerade ska informeras.

### 2.2.2 Uppföljning av tidigare genomförda kontroller

Dataskyddsombudet har följt upp vilka åtgärder som vidtagits avseende tidigare lämnade rekommendationer.

Kontroll: Behandling av anställdas personuppgifter samt IT-system och digitala verktyg.

Verksamheten gavs följande rekommendationer:

Bolaget gavs rekommendation att se över avtal i samband med flytt till Intraservice då det saknades en del information i de avtal som bolaget har/hade med Framtidens IT.

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten inväntar Intraservices tjänsteavtal som inte är klart då ett arbete pågår mellan Intraservice och de migrerande bolagen.

Beträffande personuppgiftsbiträdesavtal gäller fortfarande ursprunglig rättsakt för kommungemensamma interna tjänster. Fortsatt uppföljning kommer ske inom ramen för de fasta kontrollpunkterna om ingen särskilt föranleder att det behöver följas upp separat.

## 2.3 Årlig kontroll av dataskyddsarbetet

Verksamhetens interna dataskyddsarbete följs årligen upp 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.

### 2.3.1 Metod och risknivåer

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.[3]

Beskrivning av risknivåer

| Risknivåer | 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 har ett systematiskt dataskyddsarbete. | |

## 2.4 Älvstranden Utveckling AB dataskyddsarbete 2022

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.

### 2.4.1 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.

[3] I arbetet med enkäten har dataskyddsenheten utgått från Myndigheten för samhällsskydd och beredskaps (MSB) uppföljningsstruktur för den offentliga förvaltningens systematiska informationssäkerhetsarbete.

Dataskyddsombudets kommentarer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig utifrån frågornas formulering i kontrollpunkten och ser ingen anledning att göra någon annan bedömning än verksamheten.

### 2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter


Kontrollpunkten avser verksamhetens förutsättningar och rutiner för att identifiera och hantera personuppgiftincidenter.

Dataskyddsombudets kommentarer:

Kontrollpunkten har i år också varit föremål för dataskyddsombudets fördjupade kontroll. Med ledning i det som framkommit i den fördjupade kontrollen gör dataskyddsombudet delvis en annan bedömning än bolaget. Dataskyddsombudets bedömning är att verksamheten har ett fungerande arbete med god kompetens hos ansvariga dataskyddskontakter, men att de rutiner som bolaget har för sitt arbete bör ses över, uppdateras i relevanta delar och testas. För detaljerade kommentarer och rekommendationer hänvisas till bilaga 2 ”fördjupad kontroll” och avsnitt 2.2.1 i denna årsrapport.

### 2.4.3 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.

Dataskyddsombudets kommentarer:

Dataskyddsombudet ser ingen anledning att göra någon annan bedömning än verksamheten. Med ledning i verksamhetens svar så finns de rutiner på plats som enligt bolaget behöver finnas.

Undantaget är rutiner/arbetssätt för att kunna utföra efterlevnadskontroller av anlitade personuppgiftsbiträden. Detta är inget som är unikt för bolaget utan är en genomgående brist för de flesta verksamheter inom Göteborgs Stad, mycket beroende på att det är en svårarbetad fråga. Dataskyddsombudets rekommendation är att verksamheten tar fram sådana rutiner/arbetssätt som möjliggör för verksamheten att utföra regelbundna efterlevnadskontroller i syfte att leva upp till omsorgsplikten i artikel 28 i GDPR.

### 2.4.4 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.

Dataskyddsombudets kommentarer:

Bolaget har på denna punkt angett värden som sammanlagt placerar bolaget inom risknivå tre. Verksamheten har angett att de har under eller upp till 75 % av sina behandlingar i ett register, samtidigt framgår det av verksamhetens svar att det saknas fungerande rutiner för att uppdatera registret med nya eller förändrade behandlingar. Dataskyddsombudets bedömning utifrån bolagets svar är att bolaget kommit en bra bit på väg, men att verksamheten nu behöver ta sista steget i detta arbete genom att skapa ett komplett register. Rekommendationen är därför att uppdatera registret med samtliga behandlingar samt ta fram rutiner/arbetssätt för att säkerställa att registret hålls uppdaterat vid tillkomsten av nya eller förändrade behandlingar.

### 2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd


Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Bolagets svar indikerar att verksamheten har en övergripande strategi för dataskydd och att kontrollpunkten inte innehåller några stora risker. Dataskyddsombudet har i det stora hela ingen anledning att göra någon annan bedömning. Men med ledning i bolagets svar rekommenderas verksamheten att regelbundet genomföra interna kontroller för att tillse följsamhet gentemot GDPR.

### 2.4.6 Kontrollpunkt 6: Utbildning


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

Dataskyddsombudets kommentarer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig. Bolagets svar indikerar att det finns risker inom kontrollpunkten som behöver hanteras.

Positivt är att verksamheten regelbundet genomför utbildningsinsatser och ger medarbetarna möjlighet till kunskapshöjande åtgärder. Mindre positivt är att bolaget uppger att den allmänna kunskapsnivån inte är tillfredsställande. Rekommendationen är därför att bolaget fortsätter med sina regelbundna utbildningsinsatser samt utreder behovet av olika anpassade utbildningsinsatser, som också dokumenteras och säkerställer att verksamheten upprätthåller en god kunskap i dataskyddsfrågor.

### 2.4.7 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.

#### Dataskyddsombudets kommentarer:

Verksamheten har här skattat sig själva med det högsta värdet. Dataskyddsombudet har ingen anledning att göra någon annan bedömning än bolaget i denna del. Verksamheten rekommenderas att möjliggöra för de registrerade att på ett enkelt sätt nå bolagets integritetspolicy från samtliga av verksamhetens digitala kanaler.

### 2.4.8 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.

#### Dataskyddsombudets kommentarer:

Bolagets svar indikerar att verksamheten i stort har de rutiner och arbetssätt på plats som krävs för mejl och dokumenthantering. Samtidigt ställer sig dataskyddsombudet frågande till delar av bolagets självskattning. Bland annat har verksamheten svarat ”vet ej” på frågan om de registrerade informeras om hur deras personuppgifter hanteras direkt i samband med upprättande av kontakt via e-post. Dataskyddsombudet rekommenderar att bolaget följer rekommendation på IMY:s hemsida gällande e-posthantering i sin helhet, även om bolaget enligt uppgift numera har e-postsignaturer i sina svarsmejl. Rekommendationen till verksamheten är att även kontrollera aktualiteten hos de behandlingar som informationsklassificerats.

### 2.4.9 Kontrollpunkt 9: Konsekvensbedömning/samråd


Kontrollpunkten avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras, samt rutiner kopplat till detta.

Dataskyddsombudets kommentarer:

Verksamhetens svar indikerar att det förekommer höga risker inom kontrollpunkten som kräver åtgärder. Av bolagets egen skattning framgår att det saknas dokumenterade arbetssätt och rutiner för att arbeta med konsekvensbedömningar. Dataskyddsombudets rekommendation är att bolaget tar ett helhetsgrepp på frågan och tar fram rutiner/arbetssätt för att identifiera personuppgiftsbehandlingar med hög risk för de registrerade samt genomför, dokumenterar och följer upp konsekvensbedömningar.

### 2.4.10 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.

Dataskyddsombudets kommentarer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig utifrån frågornas formulering i kontrollpunkten och ser ingen anledning att göra någon annan bedömning än verksamheten. Utefter bolagets svar rekommenderas dock verksamheten att involvera dataskyddsombudet från start vid uppstart av nya IT-projekt eller tjänster där personuppgifter hanteras.

### 2.4.11 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.

Dataskyddsombudets kommentarer:

Dataskyddsombudet bedömer bolagets självskattning som rimlig och ser ingen anledning att göra någon annan bedömning än verksamheten. Med ledning i verksamhetens svar är bolagets IT-chef processägare och enligt uppgift finns

fungerande rutiner för behörighetstilldelning anpassade utifrån medarbetarens arbetsuppgifter. Som ett led i ett systematiskt arbetssätt kan dataskyddsombudet, tillsammans med verksamheten, komma att följa upp arbetet under 2023.

### 2.4.12 Kontrollpunkt 12: Hantering av registrerades rättigheter


Kontrollpunkten avser verksamhetens förutsättningar och rutiner för att hantera de registrerades rättigheter, till exempel registerutdrag eller radering.

Dataskyddsombudets kommentarer:

Bolagets svar indikerar att kontrollpunkten innehåller omfattande risker som kräver omgående åtgärder. Med ledning i verksamhetens svar så förefaller det saknas medvetenhet om de registrerades rättigheter inom organisationen. det saknas också rutiner för att hantera begäran om registerutdrag. Efter avstämningsmötet korrigerade bolaget sin ursprungliga skattning och uppgav att rutiner för att hantera registerutdrag finns och fungerar.

Dataskyddsombudet har inte blivit involverad i några frågor gällande registrerades rättigheter under året och saknar därför inblick i hur arbetet med att säkerställa dessa fungerar i bolaget. Medvetenheten gällande registrerades rättigheter är kopplat till den generella kunskapen om dataskydd och kan alltid höjas.

## 2.5 Sammanfattande rekommendationer

För att på ett praktiskt plan kunna identifiera vad verksamheten behöver arbeta med inom ramen för respektive kontrollpunkt behövs en noggrann genomgång av enkätresultaten. I detta rekommenderas verksamheten att samråda med dataskyddsombudet för att se hur arbetet framåt bör utformas och vilka delar som bör prioriteras utifrån verksamhetens risker. Även för verksamheter med låga risker krävs kontinuerliga insatser för att denna risknivå ska bibehållas.

Utifrån identifierade risker rekommenderar dataskyddsombudet att bolaget under 2023 prioriterar följande delar av dataskyddsarbetet:

- Kontrollpunkt 9: Konsekvensbedömning/samråd:
  Påbörja arbetet med att kartlägga och genomföra konsekvensbedömningar för samtliga behandlingar med höga risker.
  Ta fram nödvändiga rutiner för samtliga delar av konsekvensbedömningsområdet.

- Kontrollpunkt 12: Hantering av registrerades rättigheter:
  Öka medarbetarnas kunskap om de registrerades rättigheter och i vilka fall rättigheterna begränsas.

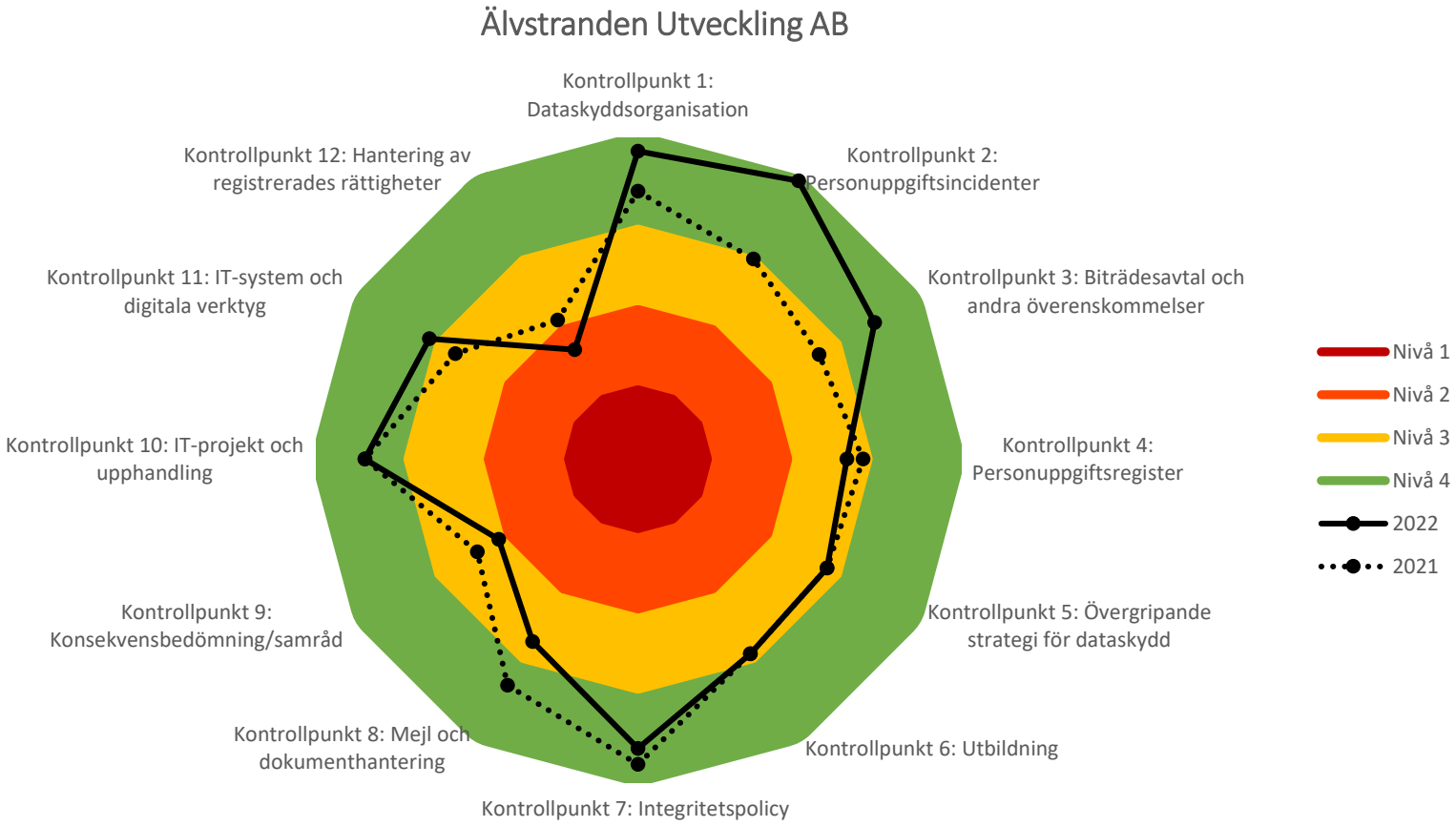
Säkerställ att fungerande rutiner finns för hantering av registrerades rättigheter.

# 3 Bilagor

Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2021.

Bilaga 2: Fördjupad kontroll 2022

# Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2021.



**Bilaga 2**

# Fördjupad kontroll 2022: Älvstranden

Kontrollpunkt 2: Hantering av personuppgiftsincidenter under 2021

## Bakgrund

Den fördjupade kontrollen gällande personuppgiftsincidenter har haft till syfte att undersöka om det finns förutsättningar för verksamheten att hantera personuppgiftsincidenter på ett korrekt sätt som följer dataskyddsförordningen och om förvaltningens rutiner/handlingsplaner får önskat genomslag i praktiken. Kontrollen har genomförts i två delar där del ett har bestått av att verksamheten har ombetts att skicka in dokumentation av rutiner/handlingsplaner för hanteringen av incidenter och dokumentation över inträffade incidenter under 2021. Del två har bestått av frågor kopplade till organisationens incidenthantering.

## lakttagelser från kontrollen

Personuppgiftsincidenter kan leda till allvarliga konsekvenser för registrerade personer och det är av stor vikt att de hanteras på ett korrekt sätt. Enligt dataskyddsförordningen ska vissa typer av personuppgiftsincidenter anmälas till tillsynsmyndigheten och i vissa fall ska även de registrerade informeras. Även de personuppgiftsincidenter som inte behöver anmälas till tillsynsmyndigheten ska dokumenteras.

### IMY:s checklista vid personuppgiftsincidenter

Integritetsskyddsmyndigheten (IMY) har på sin hemsida publicerat en checklista för personuppgiftsansvariga att använda i sitt arbete med personuppgiftsincidenter. Den består dels av vilka åtgärder personuppgiftsansvariga kan vidta i sitt proaktiva arbete med personuppgiftsincidenter, dels vad som behöver göras vid redan inträffade incidenter. IMY lyfter bl.a. att de som behandlar personuppgifter behöver veta hur man identifierar en personuppgiftsincident och vikten av att rutiner och handlingsplaner finns på plats för att kunna begränsa och hantera en redan inträffad incident. Av rutinerna bör det framgå hur en bedömning av riskerna för de registrerade går till och i förlängningen om det behöver upprättas en anmälan till tillsynsmyndigheten och om de registrerade ska informeras.

### Rutiner och handlingsplaner

Älvstranden Utveckling AB har som svar på del 1 av denna kontroll uppgett att bolaget endast haft en personuppgiftsincident under 2021 som även anmäldes till IMY. Bolaget har bifogat en gedigen dokumentation kring sin hantering av personuppgiftsincidenten. Eventuella personuppgiftsincidenter dokumenteras och registreras i bolagets diarium. Bolaget förefaller dock inte ha någon etablerad skriftlig rutin för sin hantering av personuppgiftsincidenter vid tidpunkt för utförd skrivbordskontroll. Som svar på dataskyddsombudets uppföljande frågor i del 2 av denna kontroll uppger bolaget att man betraktar röjande eller risk för röjande av personuppgifter som personuppgiftsincidenter. Ett förtydligande kring att även andra händelser kan utgöra personuppgiftsincidenter, till exempel radering eller förstöring av uppgifter, framkom i dialog med verksamheten.

Bolaget uppger att kontakt alltid tas med dataskyddsombudet för diskussion kring huruvida personuppgiftsincidenten behöver anmälas till IMY. Genom utbildningar anser bolaget att verksamheten säkerställer att personalen får tillräckliga kunskaper om vad en personuppgiftsincident är och hur de ska agera när en sådan inträffar. Bolaget arbetar med olika typer av handböcker för sina olika processer. Handböckerna är tillgängliga via intranätet. En sådan handbok finns också för hantering av personuppgifter och här beskrivs en kortfattad rutin för hur personuppgiftsincidenter ska hanteras.

I dialog med verksamheten framkommer att fokus är på utbildning, att sprida kunskap i organisationen och att involvera alla led i dataskyddsarbetet. Så även när det handlar om att identifiera och hantera personuppgiftsincidenter. Bolaget saknar dock mer detaljerad och fastställd skriftlig rutin för att bedöma personuppgiftsincidenter, till exempel information om vem som ska fatta beslut om att anmäla till tillsynsmyndigheten, när och vem som ska informera de registrerade, vilken information som ska tillhandahållas de registrerade med mera. En anvisning innehållande de delar som saknas håller på att tas fram enligt uppgift till dataskyddsombudet.

### Dataskyddsombudets rekommendationer

Bolaget behöver komplettera sin handbok på intranätet alternativt ta fram ett separat dokument i enlighet med Göteborgs Stads riktlinje för styrande dokument i de delar som saknas enligt ovan.

Kravet och vikten av att ha skriftlig dokumentation bör ses i ljuset av att uppfylla principen om ansvarsskyldighet i artikel 5 i GDPR. Genom tydlighet kring utpekat internt ansvar och vem eller vilka som fattar beslut och kan involveras vid inträffade personuppgiftsincidenter säkerställer bolaget en skyndsam och effektiv hantering. I dialog med verksamheten är dataskyddsombudets intryck också att verksamheten till stor del redan arbetar så idag, vilket är positivt. Tanken med fungerande rutiner och bra dokumentation är också att de ska fungera över tid, vid exempelvis dataskyddskontakternas frånvaro eller andra organisatoriska förändringar.

Dataskyddsombudet vill särskilt poängtera att avsaknaden av skriftliga eller dokumenterade kompletteringar inte i sig behöver betyda att en verksamhet saknar arbetssätt eller god beredskap. Tvärtom, i bolagets fall så vittnar dokumentationen som dataskyddsombudet fått ta del av kring en inträffad personuppgiftsincident under 2021och även de svar som verksamheten lämnat i övrigt, om att kunskap finns inom organisationen om hur personuppgiftsincidenter ska bedömas och hanteras.

Utifrån bolagets verksamhet utförs en relativt begränsad mängd personuppgiftsbehandlingar och de behandlingar som innehåller höga risker är i princip begränsade till HR-området. Verksamheten arbetar också med att aktivt sprida kunskap om personuppgiftsincidenter till medarbetarna och har av allt att döma ett fungerande arbete.

Bolaget har angett att verksamheten haft en enda personuppgiftsincident under 2021. Oavsett verksamhet är det normalt att det sker ett flertal personuppgiftsincidenter varje år och enligt IMY:s årsrapport 2021 är handhavandefel eller mänskliga faktorn vanligaste orsaken. Det är naturligtvis inte omöjligt att det faktiskt inte förekommit fler personuppgiftsincidenter mot bakgrund av att bolaget trots allt inte hanterar några stora mängder personuppgifter. Men det kan också handla om en underrapportering, där bristande kunskaper hos medarbetare om vad som kan vara en incident kan vara en orsak. Andra orsaker till avsaknaden av incidenter kan vara att medarbetare vid mindre

incidenter inte förstått/ansett det som värt att lägga tid på rapportering på grund av att det inneburit ringa konsekvenser för den registrerade.

Ytterligare anledningar kan vara hög arbetsbelastning eller den allmänmänskliga känslan av att inte vilja skylta med sina tillkortakommanden. Det behöver som sagt var inte vara så, men avsaknaden av uppdaterade och funktionella skriftliga rutiner/handlingsplaner gör att det är svårt för en utomstående att bilda sig en uppfattning om exakt hur personuppgiftsincidenthanteringen fungerar inom bolaget. Bolaget behöver därför se över sina rutiner i skriftlig form för att kunna visa att verksamheten uppfyller ansvarsskyldigheten i artikel 5 i GDPR. För att undvika personuppgiftsincidenter är det viktigt att arbeta medvetet och förebyggande. Dataskyddsombudet rekommenderar att mallar och processer testas regelbundet och i möjligaste mån i så verklighetstrogna miljöer som möjligt.

## Sammanfattning

Organisationen behöver uppdatera och komplettera befintliga dokument anvisning/ instruktion för hanteringen av personuppgiftsincidenter som bör minst innehålla följande:

- Beskrivning för att kunna avgöra vad som är en personuppgiftsincident.
- Rutiner för att bedöma riskerna för personer som har drabbats av personuppgiftsincidenten.
- Rutiner för anmälan av incident till tillsynsmyndigheten inom 72 timmar efter upptäckten.
- Rutiner för vilken information som ska inkluderas i en anmälan till tillsynsmyndigheten.
- Rutiner för att hantera incidenter som har inträffat hos personuppgiftsbiträdet.
- Rutiner för när och hur de registrerade ska informeras.

## Bilagor

1. Information om fördjupad kontroll 2022
2. Fördjupad kontroll 2022, hantering av personuppgiftsincidenter 2021 (del 1)
3. Fördjupad kontroll 2022, hantering av personuppgiftsincidenter 2021 (del 2)

# Fördjupad kontroll 2022

## Kontrollpunkt 2: Hantering av personuppgiftsincidenter under 2021

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 GDPR skyldig att dokumentera samtliga inträffade incidenter, oavsett risknivå. Dokumentationsskyldigheten är kopplad till ansvarsskyldigheten i artikel 5.2 GDPR, 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 GDPR, den personuppgiftsansvarige anmäla incidenten till Integritetsskyddsmyndigheten 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.

## Tillvägagångssätt

Den fördjupade kontrollen kommer att genomföras i två delar. I del ett ombeds ni att skicka in dokumentation av rutiner/handlingsplaner för att hantera incidenter samt er dokumentation avseende redan inträffade personuppgiftsincidenter. I del två ombeds ni att svara på ett antal frågor kopplade till er incidenthantering.

Dataskyddsombudet kommer sedan att sammanställa underlaget i en delårsrapport som lämnas in i juni.

# Fördjupad kontroll 2022

## Hantering av personuppgiftsincidenter under 2021

Del 1: Dokumentation för er att skicka in till ert dataskyddsombud:

1. Rutiner/handlingsplaner/instruktioner för att hantera personuppgiftsincidenter
2. Dokumentation av inträffade personuppgiftsincidenter
    a. Dokumentation av incidenter som har anmälts till tillsynsmyndigheten
    b. Dokumentation av incidenter som endast har dokumenterats internt
3. Dokumentation av utredningar kring potentiella personuppgiftsincidenter

Underlaget ska ha inkommit till ert dataskyddsombud **senast den 7 mars 2022.**

Har du frågor, kontakta ditt dataskyddsombud.

# Fördjupad kontroll 2022

## Hantering av personuppgiftsincidenter under 2021

**Del 2**

Frågor att besvara:

1. Vilken metod/vilket tillvägagångssätt som används för att bedöma huruvida händelsen är en personuppgiftsincident eller ej.
    a. *Om det framgår av rutin/handlingsplan/instruktion, hänvisa till vilket dokument samt på vilken sida detta framgår.*
2. Vilken metod/vilket tillvägagångssätt som används för att bedöma huruvida incidenten ska anmälas till tillsynsmyndigheten.
    a. *Om det framgår av rutin/handlingsplan/instruktion, hänvisa till vilket dokument samt på vilken sida detta framgår.*
3. Hur ni säkerställer att era anställda vet vad en personuppgiftsincident är och hur de ska gå tillväga vid inträffade personuppgiftsincidenter.

Svar inkommit till ert dataskyddsombud **senast den 10 juni 2022.**

Har du frågor, kontakta ditt dataskyddsombud.