Stockholms stad

# GDPR Årsrapport

År 2023

Norra innerstadens stadsdelsnämnd

**GDPR årsrapport**
Januari 2024

**Dnr:**2024/1
**Kontaktperson:** Jennifer Gavin

# 1 Bakgrund

Dataskyddsförordningen trädde i kraft som lag i Sverige den 25 maj 2018. Syftet med förordningen var att skapa enhetliga dataskyddsregler inom EU avseende respekt för privatlivet och rätten till skydd av personuppgifter enligt artikel 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Dataskyddsförordningen syftar även till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna i EU.

Enligt dataskyddsförordningen är varje nämnd och bolagsstyrelse inom Stockholms stad ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Det innebär att nämnd och bolagsstyrelse behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter.

Varje nämnd och bolagsstyrelse i Stockholms stad har i enlighet med dataskyddsförordningen utnämnt ett Dataskyddsombud (”DSO”). DSO:n har till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå.

Denna årsrapport är således ett medel för nämnd och styrelse att ta emot de råd och rekommendationer som DSO:n är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i vad DSO:ns granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Årsrapporten syftar till att nämnd/bolagsstyrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd/bolagsstyrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

Dataskyddsförordningen bygger på grundläggande principer och en av dessa principer är ansvarsskyldigheten. Den innebär att nämnd eller bolagsstyrelse ska kunna *visa* att verksamheten efterlever dataskyddsförordningen. Årsrapporten är en mycket viktig del av denna *dokumenteringsskyldighe*t. Årsrapporten är även ett medel för nämnds/bolagsstyrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

# Innehåll

# 2 Sammanfattning

I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport.

Den 1 juli 2023 lades Norrmalms stadsdelsförvaltning och Östermalms stadsdelsförvaltning samman och bildade den nya stadsdelen Norra innerstadens stadsdelsnämnd. Denna årsrapport avser Norra innerstadens stadsdelsnämnd och rapporteringsperioden avser således 1 juli – 31 december 2023.

Årsrapporten består dels av granskning kring sex obligatoriska rapporteringsområden som Personuppgiftsansvarig (”PUA”) som ett minimum ska informera sig om årligen, dels granskningar som DSO på egen hand genomfört utifrån separata riskbedömningar.

Det kan sammanfattningsvis konstateras att förvaltningen redovisat acceptabla eller goda resultat vid granskning kring följande områden:

- Registerförteckning
- Individens rättigheter
- Personuppgiftsincidenter
- Uppdaterade styrdokument

Vad gäller nedanstående områden har dock allvarliga brister identifieras:

- Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar
- Konsekvensbedömningar

För de områden som brister identifierats har åtgärder föreslagits. Vissa av dessa åtgärder är redan påbörjade och kommer slutföras under 2024.

# 3 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som Personuppgiftsansvarig (”PUA”) som ett minimum ska informera sig om årligen för att kunna anses leda och styra dataskyddsarbetet så som dataskyddsförordningen avser.

De obligatoriska rapporteringsområdena är registerförteckning, styrdokument, tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar, konsekvensbedömningar, individens rättigheter och personuppgiftsincidenter.

Nedan redogörs för nämndens eller bolagets status och DSO:ns slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:ns genomförda uppföljning och granskning.

## 3.1 Registerförteckning

### 3.1.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Antal behandlingar som är registrerade? | 351 |
| Har nödvändiga uppdateringar gjorts? | Ja |
| Bedöms registerförteckningen vara fullständig? | Registerförteckningen bedöms i allt väsentligt vara fullständig |
| Har verksamheten lämpliga rutiner för registerföring? | Ja |

### 3.1.2 Syfte

Dataskyddsförordningens artikel 30 ställer krav på att PUA måste inventera alla personuppgifter som behandlas i verksamheten och dokumentera dem i en så kallad registerförteckning.

En registerförteckning skapar en intern synlighet och förståelse för vilka personuppgifter som behandlas samt hur de hanteras. Registerförteckningen är dataskyddsarbetets centrala utgångspunkt.

Syftet med detta rapporteringsområde är således att rapportera till PUA hur väl verksamheten har lyckats inventera sina personuppgifter och upprätta en registerförteckning.

### 3.1.3 Resultat

Under våren 2023 genomfördes, inför sammanläggningen av de två stadsdelarna, ett stort arbete för att sammanföra de tidigare två förvaltningarnas båda registerförteckningar vilket resulterade i dokument med totalt 351 behandlingar registrerade. Dokumentet har under hösten 2023 uppdaterats i viss mån men det kan vid granskningen konstateras att det finns ett behov av att respektive verksamhet säkerställer att registerförteckningen är komplett och ändamålsenlig.

### 3.1.4 DSO anger hur allvarliga bristerna är på en skala

| | |
|---|---|
| | Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten |
| | Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder |
| X | Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga |
| | Inga brister av nämnvärd betydelse identifierade |

### 3.1.5 DSO ger råd och rekommendationer till PUA

DSO bedömer att det finns risk för brister i förvaltningens registerförteckning mot bakgrund av att verksamheten inte säkerställt att den är komplett och ändamålsenlig under hösten 2023. För att säkerställa att riskerna inte realiseras föreslås samtliga ansvariga avdelningschefer få i uppdrag att säkerställa att respektive avdelning under våren 2024 granskar sin avdelnings del av registerförteckningen och reviderar eller kompletterar vid behov.

## 3.2 Styrdokument

### 3.2.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Finns lämplig styrande dokumentation på plats? | Ja |
| Håller innehållet i de existerande dokumenten lämplig kvalitet? | Ja |
| Är dokumenten pedagogiska och ger de ett tillräckligt stöd? | Ja |
| Är dokumenten uppdaterade? | Ja |
| Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov? | Ja |

### 3.2.2 Syfte

En röd tråd i Dataskyddsförordningen är att viktiga arbetssätt och rutiner ska vara dokumenterade. Detta följer bland annat av kravet på att den personuppgiftsansvarige måste kunna visa att dataskyddsförordningens principer för behandling av personuppgifter efterlevs (artikel 5). Genom styrdokument kommunicerar personuppgiftsansvarig till sin verksamhet om vad som gäller och vad som förväntas vid hantering av personuppgifter. Att styrdokument finns nedtecknade, beslutade och kommunicerade medför att verksamheten får dataskyddsinformation och kan behålla kunskapen över tid och tillämpa den på ett konsekvent sätt.

Syftet med rapporteringen av området är tvådelad: dels att bedöma om verksamheten har styrdokument antagna och på plats, dels ska rapporteringen visa om dokumentationen innehållsmässigt håller en lämplig kvalitet, i vilket ingår bl.a. att dokumentationen ska vara uppdaterad och aktuell.

### 3.2.3 Resultat

Den 23 maj 2023 lanserade Stockholms stad ett nytt intranät. På intranätet finns en sida med rubriken ”GDPR” där stadsgemensam information om och dokument angående stadens arbete för att fullgöra sina skyldigheter enligt Dataskyddsförordningen framgår.

Norra innerstadens stadsdelsförvaltning hänvisar i mångt och mycket till denna stadsgemensamma sida samt dess tillhörande styrdokument för att säkerställa en likvärdig hantering av personuppgifter inom staden.

Utöver den stadsgemensamma informationen finns ett antal lokala dokument kopplat till hanteringen av personuppgifter inom stadsdelen. Dessa dokument har efter sammanläggningen granskats av dataskyddsombudet och de dokument som ansetts ha högst relevans har reviderats. Exempel på dokument som reviderats under hösten 2023 är:

- ”Informationssäkerhet till chefer inom Norra innerstaden” – ett informationsblad med grundläggande information om förvaltningens arbete och skyldigheter enligt dataskyddsförordningen.
- ”Norra innerstadens rapporteringsmall för personuppgiftsincidenter”
- ”Vägledning vid de registrerades begäran om tillgång, rättelse och radering av personuppgifter”

Sammanfattningsvis bedöms det finnas styrdokument och informationsmaterial lättillgängligt på intranätet. De dokument och texter som bedöms mest relevanta och som nyttjas mest frekvens av verksamheterna har genomgått en översyn och vid behov har dokumenten och informationen reviderats.

### 3.2.4 DSO anger hur allvarliga bristerna är på en skala

| | |
|---|---|
| | Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten |
| | Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder |
| | Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga |
| X | Inga brister av nämnvärd betydelse identifierade |

### 3.2.5 DSO ger råd och rekommendationer till PUA

DSO bedömer att det finns relevanta och uppdaterade styrdokument. DSO har gått igenom samtliga dokument och har gjort uppdateringar där det varit nödvändigt.

Då inga brister identifierats lämnas inga förslag på åtgärder. Däremot är det viktigt att säkerställa att befintliga dokument ständigt hålls uppdaterade och att nya dokument, vid behov, upprättas.

## 3.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

### 3.3.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats? | 2 |
| Är klassade personuppgiftsbehandlingar aktuella? | Nej |

### 3.3.2 Syfte

För att kunna skydda information (inklusive personuppgifter) med rätt slags skydd ska verksamheten informationsklassa sin information. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av Sveriges kommuner och regioners verktyg KLASSA. Utan informationsklassningen har verksamheten inte förutsättningar att välja rätt åtgärder för att skydda sin information. Det är därför av stor betydelse för dataskyddsarbetet att personuppgiftsansvarig ges en uppdaterad bild varje år av huruvida informationsklassning är genomförd för personuppgifter som verksamheten hanterar.

### 3.3.3 Resultat

Förvaltningen har totalt informationsklassat 2 behandlingar under hösten 2023. Samtliga av dessa avser nya behandlingar eller nyttjande av nya system. Inga befintliga eller pågående behandlingar har inom ramen för Norra innerstadens stadsdelsnämnd informationsklassats.

### 3.3.4 DSO anger hur allvarliga bristerna är på en skala

| | |
|---|---|
| X | Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten |
| | Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder |
| | Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga |

| | |
|---|---|
| | Inga brister av nämnvärd betydelse identifierade |

### 3.3.5 DSO ger råd och rekommendationer till PUA

DSO bedömer att det finns allvarliga brister kopplat till förvaltningens arbete med informationsklassning. I och med sammanläggningen av de två stadsdelsförvaltningarna behöver även tidigare genomförda informationsklassningar att uppdateras. För att åtgärda de brister som påvisats kopplat till informationsklassningar behöver arbetet med att genomföra klassningar intensifieras under kommande år.

Förvaltningens informationssäkerhetssamordnare föreslås få i uppdrag att ta fram en konkret plan för vilka och när informationsklassningar ska genomföras för att säkerställa att arbetet med informationsklassning håller en hög takt under 2024.

## 3.4 Konsekvensbedömningar

### 3.4.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av? | Nej |
| Har alla potentiella högriskbehandlingar konsekvensbedömts? | Nej |
| Är de genomförda bedömningarna aktuella? | Ja |

### 3.4.2 Syfte

Konsekvensbedömningen anses liksom registerförteckning och informationsklassning som ett viktigt verktyg för verksamhetens dataskyddsarbete. En konsekvensbedömning ska enligt dataskyddsförordningens artikel 35 utföras om en behandling av personuppgifter sannolikt leder till en hög risk för den registrerades integritet, rättigheter och friheter. En konsekvensbedömning har till syfte att identifiera och dokumentera risker kopplade till en viss behandling, samt att bedöma sannolikheten och konsekvensen om riskscenariot skulle inträffa. Baserat på bedömningen kan/ska riskförebyggande åtgärder vidtas.

En konsekvensbedömning är en arbetsrutin som ska utföras av verksamheten innan en behandling påbörjas. Däremot medför dock kravet på konsekvensbedömning att även personuppgiftsbehandlingar som redan existerade när dataskyddsförordningen trädde i kraft behöver kartläggas och utredas i fråga om behovet av att utföra en konsekvensbedömning.

Det är viktigt att PUA genom årsrapporten får en uppdaterad bild av hur fullständig verksamhetens situation är i fråga om konsekvensbedömningar avseende dataskydd.

### 3.4.3 Resultat

Under året har förvaltningen genomfört 1 konsekvensbedömning. Denna konsekvensbedömning avser en ny behandling i nyttjandet av ett nytt system. Inga befintliga eller pågående behandlingar har

inom ramen för Norra innerstadens stadsdelsnämnd varit föremål för konsekvensbedömningar.

### 3.4.4 DSO anger hur allvarliga bristerna är på en skala

| | |
|---|---|
| X | Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten |
| | Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder |
| | Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga |
| | Inga brister av nämnvärd betydelse identifierade |

### 3.4.5 DSO ger råd och rekommendationer till PUA

DSO bedömer att det finns allvarliga brister kopplat till förvaltningens arbete med konsekvensbedömningar. För att åtgärda dessa brister behöver arbetet med att genomföra konsekvensbedömningar intensifieras under kommande år. Arbetet med konsekvensbedömningar bör integreras med arbetet att säkerställa informationsklassningar.

## 3.5 Individens rättigheter

### 3.5.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer? | 4 |
| Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar? | 4 |

### 3.5.2 Syfte

Registrerade personer har enligt dataskyddsförordningen (artikel 12–22) ett antal rättigheter som på olika sätt ska garantera att den registrerade personen har insyn i hur dennes personuppgifter hanteras samt har en viss kontroll över personuppgiftsbehandlingen. Det är ett krav enligt förordningen att den verksamhet som är personuppgiftsansvarig – dvs. i stadens fall nämnder och bolag – tillgodoser rättigheterna i fråga. Rättigheterna medför en rätt att ställa krav på att verksamheten vidtar vissa åtgärder, som exempelvis att lämna ut ett så kallat registerutdrag eller att rätta vissa uppgifter. Radering, den så kallade ”rätten att bli glömd”, är dock sällan aktuell i någon större mån eftersom stadens verksamheter lyder under krav på bevarande till följd av offentlighetsprincipen. Verksamheten har enligt dataskyddsförordningen artikel 12.3 en skyldighet att vidta åtgärder inom trettio dagar efter att ha mottagit begäran.

### 3.5.3 Resultat

Under året har 4 begäran om registerutdrag, begränsning eller radering inkommit. Samtliga har hanterats av verksamheten inom 30 dagar. Förvaltningen har rutiner för hur begäran ska hanteras.

### 3.5.4 DSO anger hur allvarliga bristerna är på en skala

| | |
|---|---|
| | Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten |
| | Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder |

| | |
|---|---|
| | Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga |
| X | Inga brister av nämnvärd betydelse identifierade |

### 3.5.5 DSO ger råd och rekommendationer till PUA

DSO bedömer att det inte finns några brister identifierade kopplat till förvaltningens arbete med att säkerställa den enskildes rättigheter. Då inga brister identifierats lämnas inga förslag på åtgärder.

## 3.6 Personuppgiftsincidenter

### 3.6.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Hur upptäcks personuppgiftsincidenter? | Vanligtvis genom anställd eller utomstående/registrerad informerar förvaltningen |
| Hur många personuppgiftsincidenter har dokumenterats? | 9 |
| Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte? | 3 |
| Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten? | 3 |

### 3.6.2 Syfte

Med begreppet personuppgiftsincident avses enligt dataskyddsförordningen (artikel 4.12) ”en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.”

Rapporteringsskyldighet gäller som huvudregel för alla personuppgiftsincidenter. Undantag från rapporteringsskyldigheten gäller enbart om det är ”osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter” (se artikel 33). Detta innebär att de flesta personuppgiftsincidenter ska rapporteras till Integritetsskyddsmyndigheten (IMY), inte senare än 72 timmar efter att verksamheten fått vetskap om incidenten. Om personuppgiftsincidenten sannolikt leder till hög risk för fysiska personers rättigheter och friheter, ska rapportering även ske till de berörda registrerade personerna, utan dröjsmål.

### 3.6.3 Resultat

Under året har 9 incidenter rapporterats i förvaltningen varav 3 incidenter har anmälts till Integritetsskyddsmyndigheten (IMY). Av

de 3 incidenterna som anmälts har samtliga anmälts inom 72 timmar från upptäckt av incidenten.

Kunskapsnivån gällande personuppgiftsincidenter bedöms vara god inom förvaltningen. Vid inträffade incidenter vidtas åtgärder snabbt och verksamheterna genomför aktiviteter för att minska risken att incidenterna inträffar igen.

Det finns information på intranätet om hur verksamheterna ska gå tillväga för att utreda och anmäla personuppgiftsincidenter. En checklista vägleder verksamheten om vilken information som behöver tas fram för att hantera incidenten. Av delegationsordningen framgår vilken funktion som anmäler personuppgiftsincidenter.

### 3.6.4 DSO anger hur allvarliga bristerna är på en skala

| | |
|---|---|
| | Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten |
| | Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder |
| | Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga |
| X | Inga brister av nämnvärd betydelse identifierade |

### 3.6.5 DSO ger råd och rekommendationer till PUA

DSO bedömer att det inte finns några brister identifierade kopplat till förvaltningens arbete med att säkerställa den enskildes rättigheter. Då inga brister identifierats lämnas inga förslag på åtgärder däremot vill DSO påpeka att det är av största vikt att förvaltningen vidtar åtgärder för att underhålla den höga kunskapsnivån under kommande år.

# 4 Genomförda granskningar under året

## 4.1 Sammanfattning

Under 2023 har nedanstående områden granskats av förvaltningens dataskyddsombud. Nedan följer en beskrivning och resultat av dessa granskningar.

- *Registerförteckning* – personuppgifter hanteras felaktigt.
- *Personuppgiftsbiträdesavtal* – risk att personuppgifterna hanteras utan att ansvarsfrågan för hanteringen är reglerad.

## 4.2 Syfte

En av dataskyddsombudets viktigaste uppgifter är att övervaka verksamhetens efterlevnad av dataskyddsförordningen. En central del av det arbetet är att göra återkommande granskningar av hur väl dataskyddsförordningen efterlevs. Resultaten av granskningarna påverkar i stor utsträckning vilka beslut verksamheten kan fatta i fråga om dataskyddsåtgärder. För PUA är det därför av stor betydelse att få rapportering om vilka granskningar som gjorts under det gångna året och vad resultaten av granskningarna är.

## 4.3 Genomförda granskningar och deras resultat

*Granskning 1 – Översyn av registerförteckningen*

Under året har DSO granskat förvaltningens registerförteckning. Granskningen visar att det finns behov av revidering för att säkerställa att den är komplett och ändamålsenlig.

För närmare beskrivning och mer information se avsnitt 3.1.

| | |
|---|---|
| | Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten |
| | Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder |
| X | Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga |

| | |
|---|---|
| | Inga brister av nämnvärd betydelse identifierade |

*Granskning 3 – Personuppgiftsbiträdesavtal*

Dataskyddsförordningen anger två situationer då ett biträdesavtal behöver ingås.

Första situationen framgår av artikel 28.3 och rör avtal mellan en personuppgiftsansvarig och ett personuppgiftsbiträde:

- När ett personuppgiftsbiträde behandlar personuppgifter åt den personuppgiftsansvariga, ska behandlingen regleras genom avtal (eller annan rättsakt). Avtalet ska vara bindande för den personuppgiftsansvariga och personuppgiftsbiträdet.

Andra situationen framgår av artikel 28.4 och rör avtal mellan ett personuppgiftsbiträde och underbiträden:

- När ett personuppgiftsbiträde anlitar ett underbiträde som ska utföra en specifik behandling, på den personuppgiftsansvarigas vägnar, måste det finnas ett avtal (eller annan rättsakt) mellan personuppgiftsbiträdet och underbiträdet.

Under året har DSO granskat förvaltningens personuppgiftsbiträdesavtal. Granskningen visar att det inte upprättats något med leverantörer under 2023. För de nya system förvaltningen implementerat under 2023 finns dock stadsövergripande personuppgiftsbiträdesavtal.

Av granskningen kan det dock konstateras att det är oklart huruvida förvaltningen fullgjort sina skyldigheter enligt dataskyddsförordningen och upprättat personuppgiftsavtal med personuppgiftsbiträden. DSO rekommenderar därför att en inventering av samtliga avtal med personuppgiftsbiträden genomförs samt att det skyndsamt, i de fall det behövs, upprättas personuppgiftsbiträdesavtal.

| | |
|---|---|
| | Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten |
| X | Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder |

| | |
|---|---|
| | Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga |
| | Inga brister av nämnvärd betydelse identifierade |

## 4.4 DSO ger råd och rekommendationer till PUA

Utifrån 2023 års granskningar lämnar DSO följande råd:

- PUA, dvs. stadsdelsnämnden, bör följa upp förvaltningens arbete med att säkerställa en komplett, ändamålsenlig och tydlig registerförteckning.
- PUA, dvs. stadsdelsnämnden, bör följa upp förvaltningens arbete med att genomföra en inventering av samtliga avtal med personuppgiftsbiträden för att säkerställa att personuppgiftsbiträdesavtal upprättas i de fall det behövs.

# 5 Risker inom dataskydd

## 5.1 Sammanfattning

De primära riskerna som identifierats i verksamheten utifrån ett dataskyddsperspektiv under 2023 bedöms utgöras av:

- *Bristfälliga informationsklassningar* – Risk att förvaltningen inte säkerställer att behandlingar genomgått informationsklassning och därmed att samtliga tekniska och organisatoriska åtgärder för att skydda registrerade inte är vidtagna.

- *Bristfälliga konsekvensbedömningar* – Risk att förvaltningen inte identifierar behandlingar av personuppgifter som innebär en hög risk för den registrerades integritet, rättigheter och friheter inte identifieras och att åtgärder för att förhindra att riskerna införlivas därmed inte vidtas.

- *Bristande organisation för ett ändamålsenligt och rättssäkert informationssäkerhetsarbete*

## 5.2 Syfte

Verksamheten har ansvar för att göra vissa typer av riskanalyser som exempelvis konsekvensbedömningar och informationsklassningar. Dessa riskanalyser ger dock inte en heltäckande bild av samtliga personuppgiftsrisker i verksamheten. Dataskyddsombudet behöver som underlag för sin egen planering och sitt löpande arbete ha kontinuerlig överblick över dessa risker i verksamhetens samtliga personuppgiftsbehandlingar. Exempelvis krävs en sådan överblick för att kunna välja ut vilka områden som bör granskas under det kommande året eller för att avgöra vilka råd som dataskyddsombudet behöver lämna till verksamheten om dataskyddsåtgärder som behöver vidtas.

## 5.3 Resultatet av riskkartläggningen

*Risk 1 – Bristande informationsklassningar*

Att förvaltningen inte säkerställer att behandlingar genomgått informationsklassningar och därmed heller inte säkerställer att samtliga tekniska och organisatoriska åtgärder för att skydda registrerades rättigheter vidtagits bedöms utgöra en allvarlig risk.

Under 2023 har Norra innerstadens stadsdelsförvaltning genomfört två informationsklassningar inom Norra innerstadens stadsdelsförvaltning, se ovan under rubrik 3.3. Sammanläggningen av Östermalm och Norrmalms stadsdelsförvaltning innebär dels att tidigare genomförda informationsklassningar behöver genomföras på nytt, dels att nya system och nyttjanden behöver informationsklassas.

Dataskyddsombudet rekommenderar att förvaltningens informationssäkerhetssamordnare får i uppdrag att ta fram en konkret plan för när och vilka informationsklassningar som ska genomföras under 2024 för att säkerställa att arbetet med informationsklassning intensifieras.

| | |
|---|---|
| X | Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten |
| | Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder |
| | Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga |
| | Inga brister av nämnvärd betydelse identifierade |

### *Risk 2 – Bristfälliga konsekvensbedömningar*

Det är av stor vikt att förvaltningen identifierar behandlingar av personuppgifter som innebär en hög risk för den registrerades integritet, rättigheter och friheter samt vidtar åtgärder för att förhindra att riskerna införlivas.

Granskningen av genomförda konsekvensbedömningar under 2023 visar att det enbart genomförts 1 konsekvensbedömning inom Norra innerstadens stadsdelsförvaltning, se ovan under rubrik 3.4. Bristen bedöms därmed utgöra en allvarlig risk.

Dataskyddsombudet rekommenderar att förvaltningens informationssäkerhetssamordnare får i uppdrag att inom ramen för ovanstående åtgärd även integrera behovet av att genomföra konsekvensbedömningar.

| | |
|---|---|
| X | Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten |

| | |
|---|---|
| | Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder |
| | Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga |
| | Inga brister av nämnvärd betydelse identifierade |

### *Risk 3 – Bristande organisation för ett ändamålsenligt och rättssäkert informationssäkerhetsarbete*

Det har identifierats ett behov av att resurssätta funktioner som inom förvaltningens verksamheter för att säkerställa ett ändamålsenligt och rättssäkert informationssäkerhetsarbete. Dataskyddsombud och förvaltningens informationssäkerhetssamordnare har i en skrivelse redogjort för behovet och givit förslag på åtgärder enligt ovan. Det är en brist att förvaltningen inte resurssatt och prioriterat arbetet för ett ändamålsenligt och rättssäkert informationssäkerhetsarbete och dataskyddsombudet rekommenderar därför att följande åtgärder vidtas inom ramen för verksamhetsåret 2024:

1. Varje avdelning bör utse en person som utses som dataskyddshandläggare med uppdrag att driva avdelningens frågor kopplat till dataskydd och informationssäkerhet.
2. Förvaltningens dataskyddsombud och informationssäkerhetssamordnare bör ges i uppdrag att regelbundet sammankalla de utsedda dataskyddshandläggarna för att leda och prioritera det förvaltningsövergripande arbetet kopplat till dataskydd och informationssäkerhet.
3. Förvaltningen bör implementera PM3 som metod för att säkerställa ett strategiskt och effektivt arbete med dataskydd och informationssäkerhet.
4. Följande områden bör prioriteras under 2024:
   - Säkerställa att förvaltningen har en komplett och ändamålsenlig registerförteckning
   - Säkerställa att dataskyddshandläggarna erhåller en gedigen utbildning för att säkerställa att de kan fullgöra sitt uppdrag.
   - Säkerställa att förvaltningens har ett effektivt arbete med informationssäkerhetsklassningar inklusive konsekvensbedömningar.

- Säkerställa att förvaltningens samtliga chefer och medarbetare erhåller utbildningsmaterial för att öka kunskapen om dataskydd och rättssäkerhet.

| | |
|---|---|
| | Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten |
| | Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder |
| X | Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga |
| | Inga brister av nämnvärd betydelse identifierade |

## 5.4 DSO ger råd och rekommendationer till PUA

PUA, dvs. stadsdelsnämnden, bör följa förvaltningens arbete för att säkerställa att ovanstående risker minimeras och elimineras. För detta har det föreslagits åtgärder i denna rapport, se avsnitt 4.4 samt 5.3.

# 6 Planerade granskningar under det nya verksamhetsåret

## 6.1 Sammanfattning

De största och återkommande riskerna och där DSO identifierat behov av störst åtgärder under 2023 bör följas upp under 2024 för att säkerställa att arbetet genomförts i enlighet med plan.

Relevanta granskningsområden inom verksamheten under 2024 bedöms därmed utgöras av:

- *Informationsklassningar*
- *Konsekvensbedömningar*
- *Organisation för ett ändamålsenligt och rättssäkert informationssäkerhetsarbete*

## 6.2 Syfte

En av uppgifterna i rollen som dataskyddsombud är att granska personuppgiftsansvarigs efterlevnad av dataskyddsförordningen. Granskningsområdena bör lämpligen väljas utifrån ett riskbaserat synsätt, det vill säga att fokus bör ligga på områden där verksamhetens mest relevanta risker har identifierats i riskanalysen och i de övriga rapporteringspunkter i årsrapporten som visar på brister. Därigenom åstadkoms en röd tråd i dataskyddsarbetet från ett verksamhetsår till nästa samtidigt som de största riskerna elimineras eller åtminstone sänks till en mer acceptabel nivå.

Följande granskningar planeras att genomföras under 2024. Utifrån kontinuerlig riskbedömning kan planering och prioritering av granskningar förändras under året.

## 6.3 Planerade granskningar

*Granskning 1 – Informationsklassningar*
Kontroll av att förvaltningen per februari 2024 har en konkret plan för när förvaltningens behandlingar ska informationsklassas samt att genomförda informationsklassningar dokumenteras i förvaltningens registerförteckning.

*Granskning 2 - Konsekvensbedömningar*
Kontroll av att förvaltningen under 2024 i samband med informationsklassningar även gör bedömningen av om konsekvensbedömningar bör genomföras och i de fall det är

nödvändigt att sådana konsekvensbedömningar genomförs och dokumenteras i förvaltningens registerförteckning.

### *Granskning 3 – Organisation för ett ändamålsenligt och rättssäkert informationssäkerhetsarbete*

Kontroll av att förvaltningen under 2024 genomför de åtgärder som syftar till att säkerställa en organisation för ett ändamålsenligt och rättssäkert informationssäkerhetsarbete som anges under rubriken 5.3 ”Risk 3 – bristande organisation för ett ändamålsenligt och rättssäkert informationssäkerhetsarbete” ovan.