Införandet av EU Dataskyddsförordning i Göteborgs Stad

Analysrapport
2017-10-24

Riskanalys avseende informationssäkerhet för

Störningsjouren i Göteborg AB

1 Sammanfattning

I det förberedande arbetet i införandet av EU:s Dataskyddsförordnings har Störningsjouren i Göteborg AB genomfört en kartläggning av informationssäkerheten och personuppgiftshanteringen i verksamhetens processer och system. En riskanalys har identifierat risker samt undersökt sannolikhet och konsekvens av verksamhetens personuppgiftsbehandlingar. Åtgärdsförslag för respektive identifierat riskområde har tagits fram.

Merparten av personuppgiftsbehandlingen bedöms ligga informationssäkerhetsklass 1 med undantag för den utredande, rapporterande och handläggande behandlingen av störningar och oriktiga hyresförhållanden samt personaladministrativ behandling och IT-säkerhet som bedöms skyddsvärda i informationssäkerhetsklass 2. Behandlingen sker under sekretess med kontrollerad behörighetsstyrning och personuppgiftskontroll, därmed bedöms behandlingen uppfylla informationssäkerhetsnivå 2.

Personuppgiftsbehandlingar sker under rättslig förpliktelse och i allmänt intresse. Lagring- och uppgiftsminimering är rutin.

Utgångspunkten är att verksamheten ska uppfylla Dataskyddsförordningens säkerhetsnivå avseende behandling av personuppgifter samt kravet på ansvarsskyldighet och bevis på att principerna följs. Riskanalysen visar att vissa åtgärder behövs vidtas för att Störningsjouren skall kunna efterleva den nya förordningens krav. Störningsjouren har som målsättning en god efterlevnad av den nya förordningen och förutsatt att identifierade risker åtgärdas och kan verifieras i den kommande säkerhetsgranskningen kan verksamheten uppfylla målet innan Dataskyddsförordningen träder i kraft.

2 Bakgrund

EU:s Dataskyddsförordning ska börja tillämpas under våren 2018 och blir då direkt tillämplig i samtliga medlemsstater. Dataskyddsförordningen ersätter den nuvarande Personuppgiftslagen. Många av dataskyddsförordningens begrepp och principer går att återfinna i Personuppgiftslagens bestämmelser. Störningsjouren har idag bra efterlevnad av Personuppgiftslagen och därmed goda förutsättningar till bra efterlevnad av Dataskyddsförordningen. Den nya förordningen innebär dock en del stora förändringar och nya bestämmelser, personuppgiftsansvarig och personuppgiftsbiträdes ansvar utökas och registrerades rättigheter förstärks. En riskanalys och eventuella åtgärdsförslag är en förutsättning för verksamhetens anpassning och följsamhet av den nya Dataskyddsförordningen

3 Analysområdet

Störningsjouren har kartlagt personuppgiftsbehandlingar i verksamhetens samtliga processer och system samt kund- och leverantörsavtal. Analysen riktar in sig på områden som bedöms behöva en högre informationssäkerhet såsom personaladministrativ hantering av personuppgifter samt rapport, utredning och handläggning av störningar och oriktiga hyresförhållanden.

4 Informationssäkerhetsklassning

Personuppgifter som hanteras i bolagets utredande och rapporterande verksamhet, personaladministrativ behandling samt hantering rörande IT-säkerhet bedöms ligga i

informationsklass 2 avseende konfidentialitet och riktighet och i informationsklass 1 avseende tillgänglighet. Personaladministration samt rapport och utredning om oriktiga hyresförhållanden och störningsärenden är skyddade av sekretess enlig Offentlighet- och sekretesslagen. Kontinuerlig informationskontroll, rättning av felaktigheter, uppgifts- och lagringsminimering genomförs. Rådande informationssäkerhet bedöms därmed som minimum grundsäkerhetsnivå gällande tillgänglighet och förhöjd gällande konfidentialitet och riktighet.

5 Informationsbärare

Störningsjouren använder sig av verksamhetsspecifika system för hantering av ekonomi, personal, rapportering av störningsärenden och utredning av dessa samt övrig dokumentation, administration och kommunikation. Riskanalysen har visat att Störningsjouren personuppgiftsbiträden måste tydliggöra i personuppgiftsbiträdesavtal att säkerhetskraven uppfylls med beskrivningar, inbyggt dataskydd (Privacy by design) och regelbundna verifieringar.

Följande informationsbärare används i verksamheten:

MS Office (offline)
Office 365 (sharepoint, onedrive)
E-post (Exchange/Outlook)
Lotus Notes
Fast 2
Hogia personal
Hogia Lön
Raindance
Nattrapportsystem
Tele2 telefoni
Telefoni mobiltelefoner
Nätverksskrivare
Skype

6 Behandling av personuppgifter

6.1 Ändamål med behandling av personuppgifter

Störningsjouren behandlar kunders och dess hyresgästers personuppgifter för att fullgöra avtal med kommunens bostadsbolag samt i allmänt intresse på kommunens uppdrag att främja trygghet och säkerhet i stadens bostadsområden. Medarbetares personuppgifter behandlas för att administrativt kunna överblicka anställning och löneutbetalning med rättslig förpliktelse som arbetsgivare.

6.2 Typ av personuppgifter

I den personaladministrativa hanteringen förekommer personuppgifter om namn, roll, enhet, anställningsnummer, användaridentitet och kontaktuppgifter. Personuppgifter kan förekomma i löpande text. Bilder på medarbetare används för id-korthantering.

I handläggning av störningsärenden och utredning av oriktiga hyresförhållanden finns personuppgifter om namn, kontaktuppgifter, födelsedatum, objekt- och lägenhetsnummer. I handläggarnas löpande text förekommer namn. I inkommande

material som är nödvändigt för utredning kan förekomma känsliga personuppgifter. Störningsjourens handläggare har mycket god efterlevnad av Personuppgiftslagen. Dataskydd som standard (Privacy by default) är rutin redan idag med minimering av uppgifter, lagring och fritext samt åtkomstbegränsning och anonymisering. Då verksamheten hanterar enskilda personers boendesituation är hantering av känsliga uppgifter som inkommer i brev och e-post eller under utredande undersökning oundviklig. Uppgifter av det här slaget hanteras med sekretess. Information som är irrelevant eller av ringa eller tillfällig betydelse rensas ur akten vid inaktualitet.

Gallring sker enligt dokumenthanteringsplanen och i enlighet med gällande branschstandard.

1. Styrande dokument och styrelsehandlingar bevaras
2. Störningsrapporter gallras automatiskt var 3:e månad
3. Ärendeakter gällande utredning av störning och oriktiga hyresförhållanden gallras 2 år efter avslutat ärende.
4. Ärenden som ingår i rättsliga processer bevaras efter aktrensning enligt Arkivlagen 3§.
5. Handlingar och korrespondens av tillfällig eller ringa betydelse gallras vid inaktualitet
6. Minnesanteckningar och arbetsmaterial gallras vid inaktualitet

6.3 Tillåten behandling

Personuppgifter behandlas av verksamheten för fullgörande av personaladministrativt arbete samt kommunikation och lagring av personaladministrativt material vilket även är en del av verksamhetens fullgörande gentemot anställningsavtalet. Enligt 10§ personuppgiftslagen och dataskyddsförordningens artikel 6 får behandling ske utan individens samtycke. Endast personer som uppbär en roll gällande personaladministrativt arbete kommer att ha åtkomst till de personuppgifter som behandlas.

Kunder och deras hyresgästers personuppgifter behandlas i verksamheten för att fullgöra avtal och i allmänt intresse på kommunens uppdrag att arbeta för säkerhet och trygghet i Stadens bostadsområden. Behandlingen utgör en grundläggande nödvändig behandling i verksamheten och får ske utan individens samtycke enligt 10§ Personuppgiftslagen och artikel 6 Dataskyddsförordningen. I handläggningsärenden kan förekomma känsliga personuppgifter. Dessa skyddas enlig Offentlighet- och sekretesslagen 26:11, *sekretess till skydd för enskild vid kommunal bostadsförmedling*. Laglig grund för behandling utan samtycke finns i Dataskyddsförordningen artikel 9 och 6. All behandling är behörighetsstyrd och nivåstyrd för respektive användarroll.

6.4 Information till registrerade

Information till de registrerade är ett åtgärdsområde. Texter ska uppdateras för att vara i linje med Dataskyddsförordningens krav. Enligt Dataskyddsförordningens artikel 13 skall information till registrerad innehålla uppgifter om:

- vem är personuppgiftsansvarig
- kontaktuppgifter till personuppgiftsansvarig och dataskyddsombud
- behandlingens ändamål och rättslig grund för behandlingen
- vilka personuppgifter behandlas

- uppgiftslagring, tillgång och radering, riktighet och rättelse samt rätten att dra tillbaka sitt samtycke
- överföring av uppgifter till annan mottagare och tredjelandsöverföring,

6.5 Personuppgiftsbiträde

Riskanalysen visar att större delen av verksamhetens avtal med leverantörer som behandlar personuppgifter för vår räkning saknar fullgott personuppgiftebiträdesavtal. Nya eller kompletterande personuppgiftsbiträdesavtal skall upprättas i enlighet med dataskyddsförordningens krav och som standard för branschen.

6.6 Överföring av personuppgifter till tredje land

Riskanalysen har inte identifierat någon personuppgiftsöverföring till tredje land.

7 Avtal och överenskommelser

Följande punkter har beaktats i riskanalysen. I åtgärdsplanen ingår översyn och komplettering av uppgifter som saknas i ingångna avtal

- Leverantören kommer att tillämpa svensk lagstiftning
- Leverantören kommer att vidta lämpliga säkerhetsåtgärder i linje med Stadens grundsäkerhetsnivå (nivå 1) generellt samt i linje med förhöjd säkerhetsnivå (nivå 2) avseende konfidentialitet gällande hantering av känsliga/särskilda personuppgifter
- Leverantören har ett ISO27001-certifikat som inkluderar tjänsten
- Det finns möjligheter till kontroll genom att leverantören årligen kommer att tillhandahålla en revisionsrapport av oberoende granskare av tjänsten och av säkerhetsåtgärder
- Störningsjouren kommer alltid att kunna ställa frågor om personuppgiftsbehandlingen.
- Leverantören kommer att bistå med information och utredningsunderlag vid utredning av incidenter
- Leverantören kommer att rapportera allvarliga incidenter som rör personuppgiftshanteringen för vidarerapportering till Datainspektionen och registrerade inom 72 timmar
- Leverantören kommer att anlita underleverantörer. Störningsjouren kan vid varje givet tillfälle underrätta sig om vilka underleverantörer är
- Varken leverantören eller underleverantörer får behandla personuppgifterna för några andra ändamål än vad som preciserats
- Vid en uppsägning av tjänsten kommer data och metadata att flyttas till annan lösning. Leverantören kommer att bistå med detta. I samband med detta raderas all data hos leverantör/underleverantörer

För kommungemensamma tjänster finns styrande dokument som reglerar ansvarsförhållandet till Intraservice Göteborg Stad.

För de tjänster där Framtidens IT står som driftsansvarig finns ett serviceavtal, SLA (service level agreement) som garanterar en överenskommen nivå av service och support.

8 Riskanalys

8.1 Generellt

Identifierade risker har säkerhetsklassificerat utifrån konfidentialitet, riktighet och tillgänglighet.

Kravnivå	Konfidentialitet	Riktighet	Tillgänglighet
Nivå 2	Känslig information som kan medföra allvarlig skada för egen eller annan organisations verksamhet eller för enskild person om den röjs för obehörig	Information som kan medföra allvarlig skada för egen eller annan organisations verksamhet eller för enskild person om den är felaktig.	Information som ingår eller stöder kontinuerlig och kritisk verksamhet där avbrott innebär att man inte kan upprätthålla nödvändig tillgänglighet och servicenivå. Avbrott kan medföra allvarlig skada för egen eller annan organisations verksamhet eller för enskild person.
Nivå 1 **Grundsäkerhetsnivå**	Information som kan medföra skada för egen eller annan organisations verksamhet eller för enskild person om den röjs för obehörig	Information som kan medföra skada för egen eller annan organisations verksamhet eller för enskild person om den är felaktig	Information som ingår i eller stöder kontinuerlig verksamhet där avbrott kan medföra skada för egen eller annan organisations verksamhet eller för enskild person
Nivå 0	Information som är öppen och avsedd för eller kan spridas till en obestämd krets mottagare utan risk för negativa konsekvenser. Spridning medför ingen skada.	Information som kan förändras utan risk för negativa konsekvenser. Oriktig information medför försumbar eller ingen skada.	Information med lågt verksamhetsberoende. Kan vara otillgänglig en längre tid utan risk för negativa konsekvenser. Brist på åtkomst medför försumbar eller ingen skada.

Följande hantering bedöms behöva förhöjd säkerhetsnivå:

Säkerhetsnivå 2
Konfidentialitet
Personaladministrativt (anställning, löner, friskvård, rehabilitering, behörigheter, tillbud och incidenthantering)
Säkerhet (ex: id, loggar, lösenord)
Diarium Sekretesshandlingar

Rapportering, handläggning och utredning av störning- och oriktiga hyresförhållanden

Säkerhetsnivå 2
Riktighet
Personaladministrativt (behörigheter, anställning, rehabilitering)
Säkerhet ex: loggar, lösenord, id)
Diarium Sekretesshandlingar
Rapportering, handläggning och utredning av störning- och oriktiga hyresförhållanden

Den förhöjda säkerhetsnivån bedöms säkerställd genom rutiner för sekretesshantering, behörighetsstyrd tillgång, personuppgiftskontroll samt dataskydd som standard (privacy by default).

8.2 Deltagare

Analysen leddes av Louise Ternlind, administratör och projektledare för GDPR-införandet på Störningsjouren. Följande personer deltog i analysen:

Sofia Gärdsfors, VD, Störningsjouren
Annika Öby, Verksamhetschef, Störningsjouren
Christian Haberler, Ekonomichef, Störningsjouren.
Sandra Halilovic, Avd. Oriktiga hyresförhållanden. (behandling utredning oriktiga hyresförhållanden)
Ann-Sofi Andersen, Processledare Trygghetskonsulent Dag. (behandling störningsärenden)

8.3 Utvärdering och åtgärdsförslag

8.3.1 Sannolikhet och konsekvensnivåer

Sannolikhetsnivå	**Sannolikhet att scenariot uppkommer**
Hög	> 75 %
Medel	25 – 75 %
Låg	< 25 %

Konsekvensnivå	**Beskrivningar (exempel)**
Mycket allvarlig	Olagligt Förödande för verksamheten Processproblem kan inte hanteras inom överskådlig tid, katastrofala förseningar Avgörande för verksamhetens trovärdighet Mycket stor ekonomisk påverkan Missnöjd brukare/kund lämnar och övergår till konkurrent Brukare/kunder riskerar att drabbas av dödsfall Mycket stor påverkan på medarbetare Medarbetare lämnar verksamheten/blir sjuk/risk för dödsfall
Allvarlig	Gråzonen för vad som är lagligt Långa och allvarliga avbrott i verksamheten Processproblem måste hanteras med stöd av extern hjälp. Stora förseningar. Kan hota verksamhetens trovärdighet Har stor ekonomisk påverkan Missnöjd brukare/kund överväger att lämna /gå till konkurrent Brukare/kunder kan drabbas av allvarlig fysisk/psykisk skada Stor påverkan på medarbetare Medarbetare befaras att på lång sikt lämna verksamheten/bli sjuk/drabbas av allvarlig fysisk/psykisk skada
Måttlig	Mindre avbrott i verksamheten, stör delar av verksamheten Processproblem kan hanteras av ordinarie personal eller med visst extern stöd. Vissa förseningar Kan påverka verksamhetens trovärdighet Missnöjd brukare/kund får reducerat förtroende, men lämnar ej Viss ekonomisk påverkan Viss påverkan på medarbetare. Påverkas negativt på kort sikt

Ta hänsyn till vid konsekvensbedömning
– Informationstillgångarnas värde *(kostnader för att återställa, återskapa, ersätta etc)* – Operativa verksamhetskonsekvenser *(processer (myndighetsutövning), medarbetare etc)* – Strategiska/framtida verksamhetskonsekvenser *(påverkan på Bolagets trovärdighet, badwill etc samt potentiellt missbruk av information som erhållits/spridits)* – Lagbrott, avtalsbrott eller bristande följsamhet mot stadens regelverk *(PuL, OSL, FL etc)* – Annan skada inom egna verksamheten *(fysisk, person, miljö/natur etc)* – Ekonomisk skada/men eller annan skada utanför den egna verksamheten såsom annan verksamhet i eller utanför staden, partners, samverkansparter, brukare, kommuninnevånare, tredje man, miljö-/naturskador etc

8.3.2 Risk och konsekvensanalyser

Tabellen ska läsas med färgkoderna där grön färg innebär ”grönt ljus” och rött är stoppsignal och innebär att risken är hög att skada/problem uppkommer varför specifika tillkommande säkerhetsåtgärder måste införas för att kunna använda tjänsten. Om krysset hamnar på gult måste risken hanteras på något sätt innan man kan gå vidare. Det kan göras genom att undersöka frågan närmare med leverantören eller att vidta riskreducerande åtgärder.

<table>
<tr><td>Beskrivning risk 1</td><td colspan="4">Obehörig får del av personuppgifter genom felaktig hantering av leverantören.</td></tr>
<tr><td rowspan="2">Beskrivning av konsekvens om risk realiseras</td><td colspan="4">Oönskad spridning av personuppgifter kan leda till kränkning av de registrerades integritet och kan orsaka skada och men för enskild eller dess anhöriga, förlust av förtroende för Störningsjouren och sanktionsavgift för bristande dataskydd.</td></tr>
<tr><td colspan="4">Konsekvensen medför att informationsförluster kan uppkomma avseende:
Konfidentialitet: X | Riktighet: | Tillgänglighet:</td></tr>
<tr><td rowspan="4">Konsekvens</td><td>Mycket allvarlig</td><td>X</td><td></td><td></td></tr>
<tr><td>Allvarlig</td><td></td><td></td><td></td></tr>
<tr><td>Måttlig</td><td></td><td></td><td></td></tr>
<tr><td>Försumbar</td><td></td><td></td><td></td></tr>
<tr><td colspan="2" rowspan="2"></td><td>Låg</td><td>Medel</td><td>Hög</td></tr>
<tr><td colspan="3">Sannolikhet</td></tr>
<tr><td colspan="5">Kommentar: Baserat på att det är ett lagbrott anses konsekvensen mycket hög men samtidigt anses driftansvarig Framtidens IT ha adekvata skyddsåtgärder för att minimera risken.

Samtliga leverantörsavtal ska uppdateras med fullgott PUB-avtal. Leverantören ska visa att de har tydliga rutiner, kontroller och loggning av åtkomst. Årliga efterlevnadskontroller av skyddsåtgärder görs av oberoende part. Ovanstående ska verifieras i en säkerhetsgranskning.</td></tr>
</table>

<table>
<tr><td>Beskrivning risk 2</td><td colspan="4">Obehörig får del av personuppgifter genom felaktig användarhantering</td></tr>
<tr><td rowspan="2">Beskrivning av konsekvens om risk realiseras</td><td colspan="4">Oönskad spridning av personuppgifter kan leda till kränkning av de registrerades integritet och kan orsaka skada och men för enskild eller dess anhöriga, förlust av förtroende för Störningsjouren och sanktionsavgift för bristande dataskydd.</td></tr>
<tr><td colspan="4">Konsekvensen medför att informationsförluster kan uppkomma avseende:
Konfidentialitet [X] Riktighet [ ] Tillgänglighet [ ]</td></tr>
<tr><td rowspan="5">Konsekvens</td><td>Mycket allvarlig</td><td>X</td><td></td><td></td></tr>
<tr><td>Allvarlig</td><td></td><td></td><td></td></tr>
<tr><td>Måttlig</td><td></td><td></td><td></td></tr>
<tr><td>Försumbar</td><td></td><td></td><td></td></tr>
<tr><td></td><td>Låg</td><td>Medel</td><td>Hög</td></tr>
<tr><td colspan="2"></td><td colspan="3">Sannolikhet</td></tr>
<tr><td colspan="5">Kommentar: Baserat på att det är ett lagbrott anses konsekvensen mycket hög. Sannolikheten av felaktig hantering bedöms vara låg då Störningsjouren har god följsamhet av Personuppgiftslagen, informationssäker sekretesshantering, behörighetskontroll, personuppgiftkontroll, fritextkontroll, uppgifts- och lagringsminimering.

Ytterligare skyddsåtgärder avseende information, användarrutiner och tekniska lösningar behöver sättas upp för att möta och minimera risken. Informationen ska kontinuerligt kommuniceras i utbildningsinsatser, vara del av introduktion för nyanställda och periodiskt återkommande. Internkontroller görs med periodiska stickprov. Tekniska säkerhetskontroller utförs av oberoende part.</td></tr>
</table>

<table>
<tr><td>Beskrivning risk 3</td><td colspan="4">Obehörig får del av sekretessbelagd information/ känsliga personuppgifter genom felaktig användarhantering</td></tr>
<tr><td rowspan="2">Beskrivning av konsekvens om risk realiseras</td><td colspan="4">Oönskad spridning av personuppgifter kan leda till kränkning av de registrerades integritet och kan innebära allvarlig skada och men för enskild eller dess anhöriga om uppgifter sprids om enskilds personliga förhållanden som t ex hälsotillstånd, eller skyddade adresser och personuppgifter sprids.
Förlust av förtroende för Störningsjouren och sanktionsavgift för bristande dataskydd.</td></tr>
<tr><td colspan="4">Konsekvensen medför att informationsförluster kan uppkomma avseende:

Konfidentialitet [X] | Riktighet [ ] | Tillgänglighet [ ]</td></tr>
<tr><td rowspan="4">Konsekvens</td><td>Mycket allvarlig</td><td>X</td><td></td><td></td></tr>
<tr><td>Allvarlig</td><td></td><td></td><td></td></tr>
<tr><td>Måttlig</td><td></td><td></td><td></td></tr>
<tr><td>Försumbar</td><td></td><td></td><td></td></tr>
<tr><td colspan="2" rowspan="2"></td><td>Låg</td><td>Medel</td><td>Hög</td></tr>
<tr><td colspan="3">Sannolikhet</td></tr>
<tr><td colspan="5">Kommentar: Baserat på att det är ett lagbrott anses konsekvensen mycket hög. Sannolikheten av felaktig hantering bedöms vara låg då Störningsjouren har god följsamhet av Personuppgiftslagen, informationssäker sekretesshantering, behörighetskontroll, personuppgiftkontroll, fritextkontroll, uppgifts- och lagringsminimering.

Ytterligare skyddsåtgärder avseende information, användarrutiner och tekniska lösningar behöver sättas upp för att möta och minimera risken. Informationen ska kontinuerligt kommuniceras i utbildningsinsatser, vara del av introduktion för nyanställda och periodiskt återkommande. Internkontroller görs med periodiska stickprov. Tekniska säkerhetskontroller utförs av oberoende part.</td></tr>
</table>

<table>
<tr><td>Beskrivning risk 4</td><td colspan="4">Avbrott vid systemincidenter. Systemleverantören går i konkurs, köps upp av intressent som inte respekterar ingånget avtal eller att tjänsten avvecklas</td></tr>
<tr><td rowspan="2">Beskrivning av konsekvens om risk realiseras</td><td colspan="4">Avbrott kan innebära informationsförlust, ekonomisk förlust, verksamhetsnyttoförlust och avtalsbrott om verksamhetens arbete inte kan utföras. Kan framtvinga hävande av avtal. Nedlagt arbete går till spillo. Medarbetare och kunder tappar förtroende för verksamheten.</td></tr>
<tr><td colspan="4">Konsekvensen medför att informationsförluster kan uppkomma avseende:
Konfidentialitet: X | Riktighet: X | Tillgänglighet: X</td></tr>
<tr><td rowspan="5">Konsekvens</td><td>Mycket allvarlig</td><td></td><td></td><td></td></tr>
<tr><td>Allvarlig</td><td></td><td>X</td><td></td></tr>
<tr><td>Måttlig</td><td></td><td></td><td></td></tr>
<tr><td>Försumbar</td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td>Låg</td><td>Medel</td><td>Hög</td></tr>
<tr><td colspan="3"></td><td>Sannolikhet</td></tr>
<tr><td colspan="5">Kommentar: Om risken inträffar är konsekvensen allvarlig men hanterbar om åtgärder har tagits för att trygga eventuella avbrott och incidenter.

Åtgärder ska innefatta periodiskt utförd säkerhetskopiering av system med fullständig återläsning av information. Avbrottsplan skall granskas, uppdateras och kommuniceras till medarbetare. Granskning av avtal görs för att säkra den juridiska aspekten.</td></tr>
</table>

<table>
<tr><td>Beskrivning risk 5</td><td colspan="5">Personuppgiftsincidenter rapporteras inte</td></tr>
<tr><td rowspan="2">Beskrivning av konsekvens om risk realiseras</td><td colspan="5">Intrång, potentiella angrepp och obehörig tillgång till personuppgifter hanteras inte. Risk för vidare spridning av personuppgifter och till följd kränkning, skada och men för registrerade. Förlorat förtroende för Störningsjourens informationshantering.
Brist i följsamhet av DSF medför sanktioner.

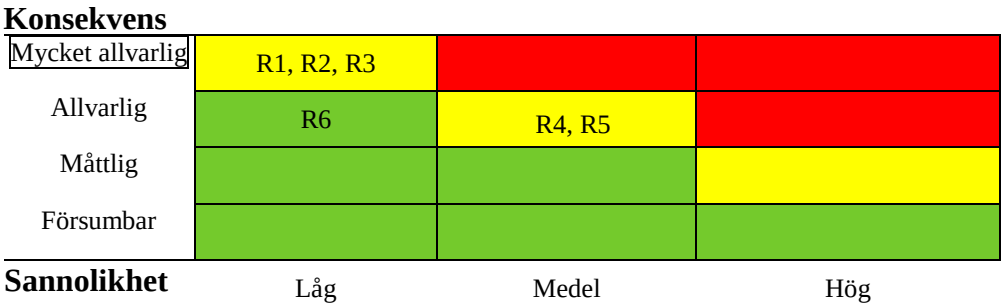
Artikel 33, 34 Personuppgiftsincident
Säkerhetsincident innebär oavsiktlig eller olaglig förstöring, förlust eller ändring av personuppgifter samt obehörigt röjande av eller obehörig åtkomst till personuppgifter</td></tr>
<tr><td colspan="5">Konsekvensen medför att informationsförluster kan uppkomma avseende:
Konfidentialitet: X
Riktighet: X
Tillgänglighet: X</td></tr>
<tr><td rowspan="4">Konsekvens</td><td>Mycket allvarlig</td><td></td><td></td><td></td></tr>
<tr><td>Allvarlig</td><td></td><td>X</td><td></td></tr>
<tr><td>Måttlig</td><td></td><td></td><td></td></tr>
<tr><td>Försumbar</td><td></td><td></td><td></td></tr>
<tr><td colspan="2" rowspan="2"></td><td>Låg</td><td>Medel</td><td>Hög</td></tr>
<tr><td colspan="3">Sannolikhet</td></tr>
<tr><td colspan="5">Kommentar: Konsekvensen bedöms vara allvarlig och säkerhetsåtgärder måste upprättas.

Åtgärder: Upprättande av anvisningar och rutiner för incidentrapportering, teknisk informationssäkerhet ska testas och utvärderas. Periodiska kontroller av behörigheter och återkommande internrevisioner/kontroller (säkerhet, tillförlitlighet och funktion) ska genomföras. Rutiner och skyldigheter i dataskyddsförordningen kommuniceras till medarbetare.</td></tr>
</table>

<table>
<tr><td>Beskrivning risk 6</td><td colspan="4">Bristande kommunikation. Medarbetare förstår inte DSF och säker personuppgiftsbehandling. Registrerade och användare av Störningsjourens tjänster har inte information om vår personuppgiftshantering.</td></tr>
<tr><td rowspan="2">Beskrivning av konsekvens om risk realiseras</td><td colspan="4">Felaktig behandling av personuppgifter.
Användare och registrerade tappar förtroendet för Störningsjourens informationssäkerhet.
Sanktioner för bristande följsamhet av DSF</td></tr>
<tr><td colspan="4">Konsekvensen medför att informationsförluster kan uppkomma avseende:
Konfidentialitet X | Riktighet X | Tillgänglighet X</td></tr>
<tr><td rowspan="5">Konsekvens</td><td>Mycket allvarlig</td><td></td><td></td><td></td></tr>
<tr><td>Allvarlig</td><td>X</td><td></td><td></td></tr>
<tr><td>Måttlig</td><td></td><td></td><td></td></tr>
<tr><td>Försumbar</td><td></td><td></td><td></td></tr>
<tr><td></td><td>Låg</td><td>Medel</td><td>Hög</td></tr>
<tr><td colspan="2"></td><td colspan="3">Sannolikhet</td></tr>
<tr><td colspan="5">Kommentar: Risken kan medföra allvarliga konsekvenser. Sannolikheten är låg då Störningsjourens medarbetare har god kännedom om sekretess och personuppgiftshantering.

En kommunikationsplan är upprättad i bolagets införandeplan av DSF, utbildningsinsatser från Staden, koncernen och bolaget är planerade. Kommunikationsinsatserna utvärderas löpande och kunskapsnivån testas och kompletteras vid behov. Störningsjourens målsättning är att visa öppenhet och tydlighet avseende personuppgiftshantering, åtgärder planeras för att öka transparensen ytterligare.</td></tr>
</table>

8.4 Summering



ID	Beskrivning av risk	Bedömning	Åtgärd	Prioritet
R1, R2, R3	Obehörig får del av personuppgifter och sekretessuppgifter/känsliga personuppgifter genom felaktig hantering av leverantören eller användare	Ytterligare åtgärder behövs för att uppnå säker grundnivå	**Åtgärder är planerade. Åtgärdsplan upprättas.** Granskning av leverantörers PUB-avtal. Komplettering/ nytecknande enligt DSF kravställning på personuppgiftsbiträden Säkerhetsgranskning Efterlevnadskontroller av systemleverantörer Tekniska kontroller av oberoende part Höja medarbetares kunskapsnivå med internkommunikation och utbildning. Dataskydd ingår i nyanställdas introduktion och därefter återkommande information som del i verksamhetens utbildningsplan Rutinbeskrivningar och anvisningar för säker informationshantering. Internkontroll av medarbetares efterlevnad av DSF	1

R4, R5	Bristande rutiner vid personuppgiftsincidenter och avbrott	Ytterligare åtgärder behövs för att uppnå säker grundnivå	**Åtgärder är planerade**. **Åtgärdsplan upprättas.** Rutinbeskrivningar om avbrott och incidentrapportering upprättas. Mallar för incidentrapport tas fram Tekniska säkerhetskontroller (säkerhetskopiering och fullständig återläsning) genomförs periodiskt. Handlingsplan för informationsförlust, intrång, obehörig tillkomst Behörighet -och åtkomstkontroller genomförs periodiskt. Medarbetare informerade om rättigheter och skyldigheter i dataskyddsförordningen.	2
R6	Brister i intern och extern kommunikation		**Kommunikationsplan är upprättad.** Medarbetarutbildning enligt kommunikationsplan Extern information enligt kommunikationsplan Löpande utvärdering av utbildning-och informationsinsatser. Kontroll av medarbetares kunskapsnivå.	3

8.5 Sammanfattande bedömning

Förutsatt att föreslagna åtgärder genomförs samt att den kommande säkerhetsgranskningen kan verifiera att Störningsjouren i Göteborg AB uppfyller tillämpliga säkerhetskrav utvisar analysen att verksamheten möter Dataskyddsförordningens krav på informationssäkerhet.

9 Nästa steg

9.1 Beslut om behandling av säkerhetsrisker

Med denna rapport som underlag beslutar informationsägaren om åtgärder och hantering av riskerna.

9.2 Övervakning av status på säkerhetsrisker

Informationsägaren behöver årligen, och därutöver vid större förändringar i verksamheten eller informationshanteringen, utvärdera denna riskanalys för att på så sätt försäkra sig om att riskerna är hanterade enligt beslut samt om det finns behov av kompletterande riskanalys.

9.3 Granskning av informationssäkerhetsnivå

Informationsägaren behöver försäkra sig om att verksamheten uppfyller tillämpliga säkerhetskrav. En granskning ska genomföras för att ge staden svar på om man verkligen vidtagit de säkerhetsåtgärder som krävs. Om granskningen visar på brister ska dessa analyseras, utvärderas och hanteras i en kompletterande riskanalys.

Råd om informationssäkerhetskontroller finns på Stadens intranät under Styr- och stöddokument för informationssäker