Beslutsunderlag
Styrelsen 2022-01-17
Diarienummer 0027/21

Handläggare: Karin Lange, administrativ chef
Telefon: 031 – 368 54 59
E-post: karin.lange@gshab.goteborg.se

Dataskyddsenhetens årsrapport 2021

Förslag till beslut

Information avseende dataskyddsenhetens årsrapport för 2021 antecknas.

Ärendet

Ärendet avser anmälan till styrelsen av dataskyddsenhetens årsrapport för datasskyddsarbetet 2021. Dataskyddsenheten har arbetat fram en modell för sitt kontrollarbete som utgår från en gemensam kontrollplan för stadens verksamheter. Utifrån kontrollplanen gjordes två fördjupade kontroller under våren som resulterade i en delårsrapport. Delårsrapporten anmäldes till styrelsen vid sammanträdet 2021-06-14. I föreliggande ärende anmäls den årsrapport som dataskyddsenheten lämnat för 2021. Årsrapporten innehåller resultatet för de fasta kontrollpunkter där granskning skett samt uppföljning av tidigare års kontroller. Dataskyddsenheten genomförde granskningen genom att ställa ut ett 80-tal likalydande frågor till samtliga verksamheter i staden. För några av kontrollpunkterna anser Stadshus att svaren gett missvisande resultat då dessa inte varit aktuella för Stadshus under året, vilket även framgår i kommentarerna i årsrapporten. Göteborgs Stadshus AB och kommunstyrelsen har haft samma dataskyddsombud 2021 och bolaget samverkar med stadsledningskontoret i sitt dataskyddsarbete. Dataskyddsenheten har vid årsskiftet lämnat information om att enheten utses till dataskyddsombud, i stället för en enskild person vid enheten.

Enligt dataskyddsenhetens systematik för sitt kontrollarbete kan årsrapporten komma att presenteras av representant från enheten efter överenskommelse.

Styrelsen föreslås att anteckna årsrapporten.

Bedömning ur ekonomisk, ekologisk och social dimension

Ärendet avser anmälan av den årsrapport som dataskyddsenheten lämnat. Bolaget har inte funnit några särskilda aspekter på frågan utifrån dessa dimensioner.

Bilaga

1. Dataskyddsenhetens årsrapport för dataskyddsarbetet 2021

Eva Hessman

Vd, Göteborgs Stadshus AB

Dataskyddsenheten

Göteborgs Stad

Årsrapport för dataskyddsarbetet 2021

Göteborgs Stadshus AB

2021-12-23

Innehåll

1 Dataskyddsarbetet ... 3

1.1 Att förvalta ett förtroende ... 3

1.2 Dataskyddsenhetens gemensamma arbete ... 3

2 Kontrollarbetet ... 4

2.1 Ett systematiskt arbete ... 4

2.2 Rättsutveckling som påverkat kontrollarbetet under året ... 4

2.2.1 Tredjelandsöverföringar (överföringar till länder utanför EU/EES) ... 4

2.2.2 Rätt beslutsnivå ... 5

2.2.3 Kommungemensamma interna tjänster ... 6

2.3 Årets kontrollarbete ... 6

2.3.1 Fördjupad kontroll ... 6

2.3.2 Fasta kontrollpunkter ... 7

2.4 Resultat av fasta kontrollpunkter för Göteborgs Stadshus AB ... 8

2.4.1 Kontrollpunkt 1: Dataskyddsorganisation ... 8

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter ... 9

2.4.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser ... 9

2.4.4 Kontrollpunkt 4: Personuppgiftsregister ... 10

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd ... 10

2.4.6 Kontrollpunkt 6: Utbildning ... 10

2.4.7 Kontrollpunkt 7: Integritetspolicy ... 11

2.4.8 Kontrollpunkt 8: Mejl och dokumenthantering ... 11

2.4.9 Kontrollpunkt 9: Konsekvensbedömning/samråd ... 11

2.4.10 Kontrollpunkt 10: IT-projekt och upphandling ... 12

2.4.11 Kontrollpunkt 11: IT-system och digitala verktyg ... 12

2.4.12 Kontrollpunkt 12: Hantering av registrerades rättigheter ... 13

2.5 Uppföljning ... 13

2.5.1 Uppföljning av genomförda kontroller 2018 - 2020 ... 13

2.6 Sammanfattande rekommendationer ... 15

3 Bilagor ... 16

3.1 Bilaga 1: Diagram över resultat av fasta kontrollpunkter, i jämförelse med Göteborgs Stads genomsnitt. ... 16

1 Dataskyddsarbetet

1.1 Att förvalta ett förtroende

Att få ta del av och hantera andra människors personliga uppgifter innebär att förvalta ett stort förtroende. Dataskyddsförordningen 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. Lagen har höga sanktionsavgifter, men det är inte därför det är viktigt att lagen följs. Att personuppgifter hanteras lagenligt bör snarare vara en självklarhet i syfte att visa omsorg om det förtroende som givits den som har att hantera uppgifterna.

Enligt lagstiftningen har dataskyddsombudet bland annat till uppgift att ge råd och information till den personuppgiftsansvarige i dataskyddsfrågor. Dataskyddsombudet har även till uppgift att övervaka efterlevnaden av dataskyddsförordningen hos personuppgiftsansvariga.

Dataskyddsombudet ska enligt lagstiftningen rapportera till högsta förvaltningsledning dvs. styrelse eller nämnd. Detta för att den högsta ledningen ska få den information som behövs för att kunna bedöma vilka prioriteringar som ska göras och vilka risker som organisationen är beredd att ta. Dataskyddsombudet fattar inte beslut åt verksamheten. Ytterst vilar ansvaret för att verksamheterna följer lagen på nämnd/styrelse. De råd och rekommendation som ges av dataskyddsombudet syftar till att ge ledningen underlag för att kunna fatta väl underbyggda beslut.

1.2 Dataskyddsenhetens gemensamma arbete

Dataskyddsenheten har under det gångna året regelbundet skickat ut nyhetsbrev innehållandes omvärldsbevakning och information från enheten. Däremellan har enheten även informerat verksamheterna om förändringar i lagstiftning och praxis.

Enheten har också tillgängliggjort en digital grundutbildning som alla stadens bolag och förvaltningar har fått tillgång till, och som fritt kan användas av verksamheterna. Det har även arrangerats ett flertal lärarledda utbildningar, bland annat en grundutbildning och en utbildning riktad till yrkesgruppen kommunikatörer. Genom att hålla utbildningarna digitalt har flera hundra personer inom stadens verksamheter haft möjlighet att delta. Då intresset varit stort kommer dataskyddsenheten fortsätta anordna utbildningar inom olika ämnesområden.

För att skapa möjligheter för samarbete och erfarenhetsutbyte i dataskyddsfrågor har enheten under året anordnat två nätverksträffar för stadens

dataskyddskontakter. Teman för nätverksträffarna har anpassats utefter de frågor enheten identifierat att många av stadens verksamheter arbetar med.

2 Kontrollarbetet

2.1 Ett systematiskt arbete

Dataskyddsenheten har under året tagit fram gemensamma rutiner för kontrollarbetet, med syfte att skapa ett enhetligt, transparent och systematiskt arbetssätt för Göteborgs Stads verksamheter. Kontrollerna följer en årsplan, nedan kallad ”Kontrollplan”.

Kontrollplanen skickades ut i januari 2021, med en redogörelse för planerade kontroller under året samt relevanta tidpunkter. Kontrollplanen redogjorde dels för två fördjupade kontroller, som valdes ut efter verksamhetens riskområden, dels återkommande fasta kontrollpunkter som årligen kommer att stämmas av för att se var verksamheten befinner sig i sitt dataskyddsarbete. Av kontrollplanen framgick också att en uppföljning kommer att ske av tidigare lämnade rekommendationer.

Under första halvåret har dataskyddsombudet genomfört de fördjupade kontrollerna. Under andra halvåret har dataskyddsombudet genomfört en kontroll av de fasta kontrollpunkterna samt gjort en uppföljning av tidigare lämnade rekommendationer i tidigare utförda kontroller.

2.2 Rättsutveckling som påverkat kontrollarbetet under året

Rättsutvecklingen under året har föranlett dataskyddsombudet att särskilt uppmärksamma behandlingen av personuppgifter som påverkats av nya rättsfall och rekommendationer. Ett antal händelser har också gjort att enheten har haft anledning att analysera stadens struktur rörande kommungemensamma interna tjänster.

2.2.1 Tredjelandsöverföringar (överföringar till länder utanför EU/EES)

I juli 2020 kom en dom från EU-domstolen kallad Schrems II-domen. Frågan i målet var om det avtal som fanns mellan EU och USA gav tillräckligt skydd för personuppgifter för att dessa lagligen skulle få överföras till USA. Frågeställningen i sig var väckt med anledning av den omfattande datainsamling som amerikansk lagstiftning möjliggör för amerikanska säkerhetsorgan av icke-amerikanska medborgares uppgifter. Rättsfallet rörde bulkinsamling av data ”in transit” men frågan är principiellt intressant eftersom i princip alla verksamheter som faller under amerikansk jurisdiktion kan förmås överlämna annans data, även i de fall

denna finns utanför USA. Domstolen ogiltigförklarade avtalet och fastslog att det kan krävas omfattande säkerhetsåtgärder för att kunna överföra uppgifter till USA eller andra länder med liknande lagstiftning. Skyddsåtgärderna behövde i princip omöjliggöra för utländska myndigheter att kunna få del av uppgifterna, genom exempelvis kryptering eller anonymisering. Domen har fått stor påverkan, och sedan den kom har därför frågan om tredjelandsöverföringar varit ständigt aktuell. Under året har också några vägledningar publicerats av Europeiska dataskyddsstyrelsen, EDPB, ett organ där samtliga länders tillsynsmyndigheter samverkar. Domen har inneburit att en översyn av aktuella personuppgiftsbehandlingar har behövt ske för att ta reda på om någon överföring sker till USA eller i vissa fall även annat land. Begreppet överföring är dessutom brett och inkluderar även att ge någon i USA åtkomst till uppgifter, även när uppgifterna befinner sig inom EU. Domstolen har uppmanat tillsynsmyndigheterna i respektive land att börja agera i frågan.

Kommentarer och rekommendationer

Om denna översyn ännu inte genomförts rekommenderar dataskyddsombudet att detta arbete prioriteras, så verksamheten får en tydlig riskbild och kan vidta åtgärder eller fatta nödvändiga beslut.

2.2.2 Rätt beslutsnivå

Frågan om tredjelandsöverföringar har varit omfattande och har berört såväl användningen av olika system (M365, Google) som sociala medier, cookies, osv. Frågan är komplex eftersom stora investeringar gjorts under den tid som avtalet mellan EU och USA var i kraft och förutsättningarna nu ändrats. Det har också förelegat en osäkerhet om USA tänker ändra sin lagstiftning, om leverantörerna kommer att skapa nya koncernkonstellationer eller om nya förhandlingar mellan EU och USA kan leda till ett nytt avtal (vilket idag endast är möjligt om amerikansk lagstiftning först ändras). Mer än ett år har dock passerat sedan domen kom och några nya lösningar för att kunna överföra personuppgifter till USA i klartext finns fortfarande inte. Det innebär att det idag i de flesta fall saknas lagliga möjligheter för överföring av personuppgifter till USA. Om en verksamhet väljer att fortsätta att behandla personuppgifter utan att ha säkerställt en laglig överföring så innebär detta ett accepterande av risk för förtroendeskada, skadestånd och sanktionsavgift. Ett accepterande skulle även kunna förstås som att man medvetet väljer att bryta mot gällande lagstiftning och riskera de registrerades fri- och rättigheter.

Kommentarer och rekommendationer

Nämnd/styrelse är ansvarig för att verksamheten följer lagen. Nämnd/styrelse rekommenderas att säkerställa att beslut som innebär en avvikelse från gällande dataskyddslagstiftning fattas på behörig nivå.

2.2.3 Kommungemensamma interna tjänster

De kommungemensamma interna tjänsterna erbjuds och levereras idag av Intraservice. Vad som utgör en kommungemensam intern tjänst beslutas av stadsdirektören, på delegation av kommunstyrelsen, efter samråd med förvaltnings- och bolagsledningar.

Enligt stadens styrande dokument så är det för många av stadens verksamheter obligatoriskt att använda tjänsterna. I vissa fall pekar styrande dokument ut exakt vilket system som utgörs av tjänsten, tex. M365, medan det i andra fall endast anges typ av tjänst. Intraservice roll innebär att upphandla och/eller teckna avtal med en underleverantör för stadens räkning. I styrande dokument anges att Intraservice ska betraktas som leverantör och därmed ett personuppgiftsbiträde (dvs. någon som behandlar personuppgifter för annans räkning) åt stadens bolag och förvaltningar.

Den personuppgiftsansvarige är den som bestämmer ändamål och medel med en behandling. I normala fall är det respektive bolag och nämnd som är personuppgiftsansvarig för de personuppgiftsbehandlingar som sker inom verksamheten. När det kommer till stadens kommungemensamma interna tjänster blir detta dock ofta problematiskt eftersom verksamheterna ibland inte har någon möjlighet att påverka vissa av de ändamål och medel för behandlingar som sker inom dessa tjänster. Utifrån detta uppstår frågor om vilket ansvar som Intraservice och kommunstyrelsen har för dessa tjänster, samt hur stadens struktur för kommungemensamma interna tjänster påverkar fördelningen av personuppgiftsansvaret för de behandlingar där dessa tjänster används. Oaktat vad som anges i styrande dokument skulle utgångspunkten, vid en rättslig prövning, vara vem som faktiskt hade rådighet att besluta om ändamål och medel.

Kommentarer och rekommendationer

Utifrån ett ansvarsperspektiv, då sanktionsavgifter i normalfallet riktas mot den som är personuppgiftsansvarig, rekommenderar dataskyddsombudet att bolaget säkerställer att de har tillgång till komplett och aktuell information om de kommungemensamma interna tjänster som används i bolaget och att eventuell tredjelandsöverföring i tjänsterna är laglig. Då det är Intraservice som är personuppgiftbiträde för de kommungemensamma interna tjänsterna så är det Intraservice som på anmodan ska tillse att denna information ges till bolaget.

2.3 Årets kontrollarbete

2.3.1 Fördjupad kontroll

De fördjupade kontrollerna har bestått av Integritetspolicy och Personuppgiftsregister. Dessa kontroller har genomförts under våren och resultatet har kommunicerats i maj 2021.

Dataskyddsombudet har i rapporten avseende de fördjupade kontrollerna haft några rekommendationer till verksamheten vilka har följts upp under punkten 2.5.2.

2.3.2 Fasta kontrollpunkter

För att ge verksamheten en bild av hur långt man har kommit i det systematiska dataskyddsarbetet har dataskyddsenheten tagit fram en enkät utifrån de fasta kontrollpunkterna. Enkäten är avsedd att spänna över de viktigaste delarna inom dataskyddsarbetet för att på så sätt fånga in en större bredd av frågor. Enkäten består av tolv punkter där varje punkt innehåller ett antal delfrågor i form av påståenden och/eller skattningsfrågor. Verksamheten har fått besvara frågorna utifrån aktuellt läge inom verksamheten.

I arbetet används en modell som består av fyra kategorier, vilka representerar fyra olika mognadsnivåer. Verksamheten har utifrån svaren på den enkät som skickats ut från dataskyddsenheten fått ett värde som indikerar vilken mognadsnivå verksamheten befinner sig på inom respektive kontrollpunkt. Genom att arbeta med förbättringsområden möjliggörs ett riskbaserat arbetssätt för både verksamhet och dataskyddsombud, då resultaten ger en bild av vad verksamheten kan behöva prioritera i dataskyddsarbetet framåt.[1]

Resultaten från enkäten ger en generell ögonblicksbild för respektive kontrollpunkt. Enkäten kommer att upprepas kommande år. Avsikten med detta arbetssätt är att både att få en bild av nuläget och att kunna åskådliggöra de förändringar som vidtas över tid. Enkäten har ej främst för avsikt att peka ut brister utan ska ses som en vägledning för verksamheten och ett verktyg för att identifiera relevanta prioriteringar. Syftet är att få till ett långsiktigt och systematiskt arbetssätt som möjliggör uppföljning över tid.

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

Beskrivning av mognadsnivåer

Mognadsnivåer	Färgkod
Nivå 1. Bolaget har självskattat sig lågt på flertalet av de ingående komponenterna i kontrollpunkten. Kan indikera att kontrollpunkten är ett prioriterat förbättringsområde avseende dataskydd.	
Nivå 2. Bolaget har självskattat sig lågt på flera punkter av de ingående komponenterna i kontrollpunkten. Kan indikera att flera prioriterade förbättringar finns inom kontrollpunkten avseende dataskydd.	
Nivå 3. Bolaget har självskattat sig lågt på några av de ingående komponenterna i kontrollpunkten. Kan indikera att ett mindre antal prioriterade förbättringar finns inom kontrollpunkten avseende dataskydd.	
Nivå 4. Bolaget har självskattat sig högt på flera av de ingående komponenterna i kontrollpunkten. Kan indikera att det finns få eller inga prioriterade förbättringar inom kontrollpunkten avseende dataskydd.	

2.4 Resultat av fasta kontrollpunkter för Göteborgs Stadshus AB

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.

Kommentarer och rekommendationer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig utifrån frågornas formulering i kontrollpunkten. Bolagets dataskyddsombud kommer att tillsammans med verksamheten göra en djupare analys av kontrollpunktens ingående komponenter för att bedöma eventuella förbättringsområden gällande dataskydd.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Kommentarer och rekommendationer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig utifrån frågornas formulering i kontrollpunkten. Bolagets dataskyddsombud kommer att tillsammans med verksamheten göra en djupare analys av kontrollpunktens ingående komponenter för att bedöma eventuella förbättringsområden gällande dataskydd.

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.

Kommentarer och rekommendationer:

Resultatet för kontrollpunkten är missvisande lågt då bolaget har haft svårt utifrån frågornas formulering att besvara vissa frågor i kontrollpunkten med ett lämpligt värde utifrån bolagets verksamhet. Bolagets dataskyddsombud kommer att tillsammans med verksamheten göra en djupare analys av kontrollpunktens ingående komponenter för att bedöma eventuella förbättringsområden gällande dataskydd.

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.

Kommentarer och rekommendationer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig utifrån frågornas formulering i kontrollpunkten. Bolagets dataskyddsombud kommer att tillsammans med verksamheten göra en djupare analys av kontrollpunktens ingående komponenter för att bedöma eventuella förbättringsområden gällande dataskydd.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Kommentarer och rekommendationer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig utifrån frågornas formulering i kontrollpunkten. Bolagets dataskyddsombud kommer att tillsammans med verksamheten göra en djupare analys av kontrollpunktens ingående komponenter för att bedöma eventuella förbättringsområden gällande dataskydd.

2.4.6 Kontrollpunkt 6: Utbildning

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

Kommentarer och rekommendationer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig utifrån frågornas formulering i kontrollpunkten. Bolagets dataskyddsombud kommer att tillsammans med verksamheten göra en djupare analys av kontrollpunktens ingående komponenter för att bedöma eventuella förbättringsområden gällande dataskydd.

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.

Kommentarer och rekommendationer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig utifrån frågornas formulering i kontrollpunkten. Bolagets dataskyddsombud kommer att tillsammans med verksamheten göra en djupare analys av kontrollpunktens ingående komponenter för att bedöma eventuella förbättringsområden gällande dataskydd.

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.

Kommentarer och rekommendationer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig utifrån frågornas formulering i kontrollpunkten. Bolagets dataskyddsombud kommer att tillsammans med verksamheten göra en djupare analys av kontrollpunktens ingående komponenter för att bedöma eventuella förbättringsområden gällande dataskydd.

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.

Kommentarer och rekommendationer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig utifrån frågornas formulering i kontrollpunkten. Bolagets dataskyddsombud kommer att tillsammans med verksamheten göra en djupare analys av kontrollpunktens ingående komponenter för att bedöma eventuella förbättringsområden gällande dataskydd.

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.

Kommentarer och rekommendationer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig utifrån frågornas formulering i kontrollpunkten. Bolagets dataskyddsombud kommer att tillsammans med verksamheten göra en djupare analys av kontrollpunktens ingående komponenter för att bedöma eventuella förbättringsområden gällande dataskydd.

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.

Kommentarer och rekommendationer:

Dataskyddsombudet bedömer verksamhetens självskattning som rimlig utifrån frågornas formulering i kontrollpunkten. Bolagets dataskyddsombud kommer att tillsammans med verksamheten göra en djupare analys av kontrollpunktens ingående komponenter för att bedöma eventuella förbättringsområden gällande dataskydd.

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.

Kommentarer och rekommendationer:

Resultatet för kontrollpunkten är missvisande lågt då bolaget har haft svårt utifrån frågornas formulering att besvara vissa frågor i kontrollpunkten med ett lämpligt värde utifrån bolagets verksamhet. Bolagets dataskyddsombud kommer att tillsammans med verksamheten göra en djupare analys av kontrollpunktens ingående komponenter för att bedöma eventuella förbättringsområden gällande dataskydd.

2.5 Uppföljning

2.5.1 Uppföljning av genomförda kontroller 2018 - 2020

Dataskyddsombudet har under året följt upp vilka åtgärder som vidtagits avseende tidigare års lämnade rekommendationer av gjorda kontroller.

Kontroll 1 (2018): Organisatoriska förutsättningar för dataskyddsarbetet.

Verksamheten gavs följande rekommendationer:

Det är positivt att Stadshus AB har tagit fram en informationstext. Det är vidare positivt att den finns på hemsidan. Det finns dock utrymme för förbättringar och kompletteringar. Informationstexten kan klargöra att den registrerade kan klaga hos tillsynsmyndigheten samt att den registrerade har fler rättigheter än de som är uppräknade. Vidare bör texten finnas att tillgå utan att den registrerade ska behöva ladda ner en fil.

Kommentarer och rekommendationer:

Bolaget har åtgärdat enligt rekommendationerna. Se även årets (2021) kontroll av Integritetspolicy.

Uppföljning av genomförda kontroller 2021

Verksamheten har fått en kort enkät med frågor om åtgärder har vidtagits med anledning av dataskyddsombudets lämnade rekommendationer för de genomförda kontrollerna under våren 2021.

Kontroll 1 (2021): Personuppgiftsregister

Verksamheten gavs följande rekommendationer:
För att säkerställa ett korrekt och vid var tid uppdaterat personuppgiftsregister rekommenderar dataskyddsombudet att bolaget klargör roller, ansvar och arbetssätt i den rutin som bolaget arbetar med att ta fram. Dataskyddsombudet rekommenderar även bolaget se över bland annat rättslig grund för de behandlingar som utförs i bolaget. Vid stickprovskontrollerna så förekom behandlingar med upp till tre rättsliga grunder. Det råder osäkerhet om hur många rättsliga grunder som får förekomma vid en enskild behandling. Artikel 29-gruppen, nu ersatt med Europeiska dataskyddsstyrelsen, anser att en behandling av personuppgifter för ett ändamål bara kan ha en rättslig grund1. Oavsett osäkerheten utifrån hur många rättsliga grunder som en enskild behandling får ha så bör bolaget säkerställa att de rättsliga grunder som anges är relevanta. En behandling med många rättsliga grunder kan även göra det svårt för den registrerade att förstå med vilken rättslig grund hens behandling sker utifrån.”

Kommentarer och rekommendationer:
Arbetet är pågående i bolaget och är kopplat till och delvis beroende av den översyn av bolagets klassificeringsstuktur som sker. I samband med översynen kommer behandlingarnas rättsliga grund att stämmas av så att de i registret anges korrekt och följsamt till regelverket. Arbetet beräknas pågå under våren 2022. En genomgång tillsammans med leverantör för personuppgiftsregistret kommer ske i början av 2022.

Dataskyddsombudet kommer att följa upp arbetet under 2022.

Kontroll 2 (2021): Integritetspolicy

Verksamheten gavs följande rekommendationer:
Dataskyddsombudet har läst igenom den information som ges av bolaget. Dataskyddsombudets uppfattning är att informationen som ges till anställda och kunder är lättåtkomlig och lättbegriplig. En förbättring som bolaget skulle kunna göra är att lägga in en mer detaljerad beskrivning av de vanligaste personuppgiftsbehandlingarna som bolaget utför. Dataskyddsombudet har även lämnat förbättringsförslag av mestadels redaktionell karaktär till dataskyddskontakten.”

Kommentarer och rekommendationer:
Bolaget har justerat i den information som lämnas av bolaget utifrån de förbättringsförslag som dataskyddsombudet lämnat både vad gäller beskrivningen

av personuppgiftsbehandlingar och de av mer redaktionell karaktär. Justeringarna gjordes i anslutning till att delårsrapporten lämnades till Stadshus.

2.6 Sammanfattande rekommendationer

För att på ett praktiskt plan kunna identifiera vad verksamheten behöver arbeta med inom ramen för respektive kontrollpunkt behövs en mer 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.

3 Bilagor

3.1 Bilaga 1: Diagram över resultat av fasta kontrollpunkter, i jämförelse med Göteborgs Stads genomsnitt.