

Styrelsehandling nr 8
Datum 2022-03-29
Diarienummer BB2022-0218

Handläggare
Viktor Hjärtström
Telefon: 031-731 50 77
E-post: viktor.hjartstrom@bostadsbolaget.se

Årsrapport för dataskyddsarbetet 2021

Informationsärende

Styrelsen Göteborgs stads bostadsaktiebolag:

Anteckna rapport beträffande Bostadsbolagets dataskyddsarbete.

Sammanfattning

Varje år genomför dataskyddsenheten på Intraservice en kontroll över bolagets dataskyddarbete. Kontrollen består av ett antal fasta kontrollpunkter samt utvalda fördjupade kontroller. I årsrapporten presenteras resultat av kontrollen för 2021 och rekommendationer om hur bolaget ska förbättra arbetet med dataskydd enligt Dataskyddsförordningen (GDPR).

Bedömning ur ekonomisk dimension

Bolaget inte har funnit några aspekter på frågan utifrån denna dimension.

Bedömning ur ekologisk dimension

Bolaget inte har funnit några aspekter på frågan utifrån denna dimension.

Bedömning ur social dimension

Bolaget inte har funnit några aspekter på frågan utifrån denna dimension.

Samverkan

Ärendet har inte bedömts vara föremål för samverkan.

Bilagor

1. Årsrapport för dataskyddsarbetet 2021



Årsrapport för dataskyddsarbetet 2021

Göteborgs Stads Bostads 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	Tredjelandsoverföringar (överföringar till länder utanför EU/EES)	5
2.2.2	Rätt beslutsnivå.....	5
2.2.3	Kommungemensamma interna tjänster	6
2.3	Årets kontrollarbete	7
2.3.1	Fördjupad kontroll.....	7
2.3.2	Fasta kontrollpunkter	7
2.4	Resultat av fasta kontrollpunkter för Göteborgs Stads Bostads AB	
	9	
2.4.1	Kontrollpunkt 1: Dataskyddsorganisation	9
2.4.2	Kontrollpunkt 2: Personuppgiftsincidenter.....	9
2.4.3	Kontrollpunkt 3: Biträdesavtal och andra överenskommelser	
	10	
2.4.4	Kontrollpunkt 4: Personuppgiftsregister	10
2.4.5	Kontrollpunkt 5: Övergripande strategi för dataskydd	10
2.4.6	Kontrollpunkt 6: Utbildning	11
2.4.7	Kontrollpunkt 7: Integritetspolicy	11
2.4.8	Kontrollpunkt 8: Mejl och dokumenthantering	12
2.4.9	Kontrollpunkt 9: Konsekvensbedömning/samråd	12
2.4.10	Kontrollpunkt 10: IT-projekt och upphandling.....	13
2.4.11	Kontrollpunkt 11: IT-system och digitala verktyg	13
2.4.12	Kontrollpunkt 12: Hantering av registrerades rättigheter	14
2.5	Särskilda iakttagelser.....	14
2.5.1	Tredjelandsoverföring och användningen av sociala medier	
	14	
2.6	Uppföljning	15
2.6.1	Uppföljning av genomförda kontroller 2018 - 2020.....	15
2.6.2	Uppföljning av genomförda kontroller 2021.....	15

2.7	Sammanfattande rekommendationer	16
2.7.1	Rekommendation för hantering av resultaten	17
3	Bilagor	18
3.1	Bilaga 1: Diagram över resultat av fasta kontrollpunkter, i jämförelse med Göteborgs Stads genomsnitt.	18

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 förmåns 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 personuppgiftsbehandlingsprocesser 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 accepterade 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 bolagsledningarna.

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 majoriteten av verksamheterna inte alltid har någon möjlighet att påverka ändamål och oftast inte har någon reell möjlighet att påverka 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 riktas mot den som är personuppgiftsansvarig, samt eftersom frågan berör dataskyddsarbetet inom alla de förvaltningar och bolag som använder dessa tjänster, rekommenderas dataskyddsombudet att frågan om roller och ansvar utreds och tydliggörs i kommande styrmodell.

Flera av de kommungemensamma interna tjänsterna medför dessutom risker ur ett dataskyddsrättsligt perspektiv, särskilt kopplat till tredjelandsöverföringar.

Dataskyddsenheten har uppmärksammat att det ofta är oklart i vilken utsträckning som stadens förvaltningar och bolag är medvetna om dessa risker och det egna ansvar man har för att hantera dem i rollen som personuppgiftsansvarig.

Förvaltningar och bolag rekommenderas säkerställa att de har tillgång till komplett och aktuell information/fakta om de tjänster som används, samt att de har kompetens att bedöma riskerna för sina behandlingar utifrån ett verksamhetsperspektiv.

2.3 Årets kontrollarbete

2.3.1 Fördjupad kontroll

De fördjupade kontrollerna har bestått av

Fokusområde 1: Dataskyddsorganisationen.

Fokusområde 2: Biträdesavtal och andra överenskommelser.

Dessa har genomförts under året och har berörts i delårsrapporten i enlighet med det som angivits i kontrollplanen.

Dataskyddsombudet har i rapporten avseende de fördjupade kontrollerna lämnat ett antal rekommendationer till verksamheten. Hur verksamheten hanterat de rekommendationer som lämnades i vårens fördjupade kontroll har följts upp under hösten.

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 risknivåer. Verksamheten har utifrån svaren på den enkät som skickats ut från dataskyddsenheten fått 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.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.

Beskrivning av risknivåer

Risiknivåer	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.	

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

2.4 Resultat av fasta kontrollpunkter för Göteborgs Stads Bostads 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:

Verksamheten har angett att de har någorlunda goda organisatoriska förutsättningar för att kunna bedriva ett effektivt och fungerande dataskyddsarbete. Fortsätt stödja det goda arbetet och ge den interna dataskyddsorganisationen möjlighet att förbättra arbetet ytterligare. Det är av stor vikt att man avsätter stöd och resurser för att kunna få rätt förutsättningar för att utföra arbetet. Där ingår att se över roller och ansvarsfördelning samt hur dataskyddsarbetet rapporteras till högsta ledningsnivå.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter



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

Kommentarer och rekommendationer:

Dataskyddsorganisationen bör ges möjlighet att kontinuerligt se över och förbättra verksamhetens rutiner för hanteringen av personuppgiftsincidenter samt även informera verksamhetens medarbetare om detta. Det är av grundläggande vikt att kunna identifiera och hantera inträffade personuppgiftsincidenter. Det är även av stor vikt för verksamheten att följa upp inträffade incidenter då dessa ger dataskyddsorganisationen möjlighet att se över och förbättra sina rutiner avseende hanteringen av personuppgiftsincidenter. Utöver detta interna intresse till förbättringsmöjligheter så är det även viktigt att säkerställa riktig och rätt anmälan till Integritetsskyddsmyndigheten. Det är även viktigt att stärka medarbetarnas kunskapsnivå om personuppgiftsincidenter och hur de ska hanteras.

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:

Verksamheten behöver säkerställa att det finns rutiner för att identifiera och reglera förhållandet med personuppgiftsbiträden och eventuella underbiträden. Det finns behov av att kontrollera så att personuppgiftsbiträdesavtal har tecknats i de fall det krävs och att avtal därefter regelbundet följs upp. Det finns även behov av att säkerställa att andra nödvändiga överenskommelser eller avtal har tecknats när det finns en gemensam eller delad hantering av personuppgifter.

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:

Ett aktuellt och uppdaterat personuppgiftsregister kan vara ett användbart hjälpmedel i verksamhetens dataskyddsarbete. Verksamheten behöver säkerställa att samtliga personuppgiftsbehandlingar dokumenteras i personuppgiftsregistret och att all nödvändig information då läggs in i registret. Det finns därför behov av rutiner för att tillförsäkra att registret regelbundet uppdateras. Den interna dataskyddsorganisationen bör även fundera över på vilket sätt personuppgiftsregistret kan användas som del i det löpande dataskyddsarbetet.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd



Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Kommentarer och rekommendationer:

Ett systematiskt dataskyddsarbete bör bedrivas utifrån övergripande strategier för verksamheten avseende både dataskydd och informationssäkerhet. Det är därför av stor vikt att verksamheten säkerställer att det finns en övergripande strategi för arbetet med dataskydd men även en informationssäkerhetspolicy som anger hur personuppgifter kan behandlas i exempelvis IT-system, datorer och mobila enheter. Det måste dessutom säkerställas att verksamhetens informationstillgångar identifieras och värderas utifrån behovet av konfidentialitet, riktighet och tillgänglighet i enlighet med stadens styrande dokument inom informationssäkerhet. Verksamheten behöver också regelbundet genomföra kontroller för att se hur dataskyddsförordningen efterlevs.

2.4.6 Kontrollpunkt 6: Utbildning



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

Kommentarer och rekommendationer:

För att kunna säkerställa ett fullgott dataskyddsarbete behöver verksamhetens medarbetare ha kunskap om hur de ska hantera personuppgifter på rätt sätt. Förvaltningen behöver därför även fortsättningsvis ge medarbetarna möjlighet att delta i både interna och externa utbildningsinsatser för att höja den allmänna kunskapsnivån om dataskydd. Den lokala dataskyddsorganisationen bör också ges rätt förutsättningar för att kunna genomföra informationsinsatser. För att kunna säkerställa att medarbetarna erbjuds rätt utbildningsinsatser måste verksamheten kartlägga vilka utbildningar och andra kompetenshöjande insatser som behövs samt följa upp kunskapsnivån efter genomförda utbildningar.

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:

Integritetspolicyns syfte är att informera registrerade om verksamhetens behandling av personuppgifter i enlighet med de krav som ställs i dataskyddsförordningen. Informationen ska vara uppdaterad samt finnas lättillgänglig. Verksamheten uppmuntras att fortsätta det goda arbetet.

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:

Det är av stor vikt att verksamheten säkerställer att det finns en dokumenthanteringsplan som omfattar alla verksamhetsdelar och att det finns rutiner för när handlingar med personuppgifter gallras. Det finns även behov av att se över verksamhetens informationsklassificering av personuppgiftsbehandlingar och kontrollera så att detta görs i enlighet med Göteborgs Stads riktlinjer för informationssäkerhet. För att detta ska kunna efterlevas förutsätts att det skapas en medvetenhet hos medarbetarna om dokumenthantering samt gallringsbestämmelser. Registrerade behöver få information om verksamhetens personuppgiftsbehandling via exempelvis information i e-postsignatur eller autosvar.

Fortsätt det goda arbetet med att säkerställa så att dokumenthanteringsplanen överensstämmer med verkligheten samt skapa tydliga ägare.

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:

Syftet med konsekvensbedömningar är att förebygga risker och på så sätt även minimera riskerna vid sådana behandlingar av personuppgifter som innebär en hög risk för de registrerades fri- och rättigheter. Det finns behov av att säkerställa att en

bedömning av risk har genomförts avseende samtliga av verksamhetens personuppgiftsbehandlingsrutiner, att det finns rutiner för att genomföra och dokumentera konsekvensbedömningar. Verksamheten behöver även se till så att det finns rutiner för att uppdatera en befintlig konsekvensbedömning vid förändringar. Verksamheten måste också ta fram ett arbetssätt för att inhämta de registrerades synpunkter på en behandling i vissa fall. Det är även av vikt att verksamheten ser över hur beslut om att acceptera risker i en konsekvensbedömning fattas och dokumenteras samt att det finns rutiner för att följa upp beslutade åtgärder. Verksamheten behöver också ta fram ett arbetssätt för att inhämta de registrerades synpunkter i vissa fall.

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:

Det finns ett behov av att säkerställa att dataskyddsperspektivet finns med i arbetet med nya IT- och digitaliseringslösningar samt vid utvecklingen av redan befintliga system och tjänster. Vid upphandlingen av nya system/tjänster så behöver det tas med i kravställningen att det finns en anpassning till inbyggt dataskydd och dataskydd som standard. Verksamheten bör även ha som rutin att dataskyddsombudet involveras från start i dessa processer.

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:

Ett välfungerande arbete behövs för att säkerställa att IT-system och digitala verktyg är förenliga med dataskyddsförordningen. För ett välfungerande arbete behöver man kartlägga och sammanställa information om samtliga IT-system och digitala verktyg som verksamheten använder. Behörigheter till IT-systemen

behöver kontinuerligt ses över och anpassas efter behov. Verksamheten behöver utföra kontroller så att IT-system och digitala verktyg används på rätt sätt. Därför är det även nödvändigt att verksamheten ser till att informera om korrekt användning samt minimera möjligheterna för felanvändning.

Fortsätt stödja det goda arbetet och ge den interna dataskyddsorganisationen möjlighet att förbättra arbetet ytterligare.

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:

Verksamheten behöver öka medarbetarnas kunskap om de registrerades rättigheter och i vilka fall rättigheterna begränsas. Verksamheten behöver säkerställa att det finns rutiner för att sammanställa nödvändig information vid en begäran om registerutdrag. Det finns även behov av att se till så att det finns rutiner för att hantera olika situationer som kan uppstå, till exempel att ett samtycke från en registrerad dras tillbaka.

2.5 Särskilda iakttagelser

2.5.1 Tredjelandsoverföring och användningen av sociala medier

De flesta sociala medier som används inom staden är ägda av amerikanska organisationer som i sina avtalsvillkor anger att överföring till tredjeland sker. Eftersom en behandling av personuppgifter i sociala medier därmed innebär en otillåten tredjelandsoverföring har frågan om användandet av dessa plattformar varit, och fortsätter att vara, högaktuell. Dataskyddsenheten har tillsammans med stadsledningskontoret tagit fram rekommendationer till stadens förvaltningar och bolag för hanteringen av sociala medier. Denna rekommendation utgår ifrån att alla helst ska avstå från att behandla personuppgifter i sociala medier, såvida inte risk för otillåten tredjelandsoverföring kan uteslutas. Om en verksamhet väljer att fortsätta att behandla personuppgifter i sociala medier innebär detta ett accepterande av risk som det bör fattas ett beslut om på lämplig nivå.

Verksamheten använder sig idag av sociala medier. Kontroller görs inom kommentarsfälten. Kommunikationsledningen arbetar pågående med en riskanalys. Verksamheten ska även ta del av ovan nämnda rekommendationer för att vidare kunna bedöma handling.

2.6 Uppföljning

2.6.1 Uppföljning av genomförda kontroller 2018 - 2020

Dataskyddsombudet har under året följt upp vilka åtgärder som vidtagits avseende tidigare års lämnade rekommendationer av gjorda kontroller. För uppföljning av ytterligare kontroller än årets vänligen tag kontakt med dataskyddsombudet.

2.6.2 Uppföljning av genomförda kontroller 2021

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

Kontroll 1 (2021): Dataskyddsorganisationen

I delårsrapporten konstaterades att dataskyddsombudet ställer sig positiv till planerad rekrytering och förstärkning av bolagets informationssäkerhet samt dataskyddsorganisation.

Sedan dess har verksamheten genomgått förändringar med roller inom dataskyddsarbetet. Dessa två nya resurser arbetar aktivt med att skapa en systematisk och fungerande dataskyddsorganisation. Området som påbörjats är registerförteckningen och kartläggningen av personuppgiftsbehandlingar. Att få systematik, ägare av område och ansvar för uppdatering av registerförteckning.

Kontroll 2 (2021): Biträdesavtal och andra överenskommelser

Ett arbete finns även för att se över biträdesavtal. Att det finns på plats och vart de finns. För att samla och få en överblick samt få en samlad bild över behovet. Börjat med att inventera den information som finns samt upprättande av en handlingsplan.

Ytterligare i delårsrapporten nämndes att utarbetande och tecknande av biträdesavtal är ett förbättringsområde där bl.a. inventering och prioritering av biträdesavtalen mot bakgrund av Schrems II är klar. Förhandling pågår med två leverantörer gällande kompletterande åtgärder för att säkerställa adekvat skydd.

Detta arbete är pågående och inventering har gjorts. En leverantör har valts bort helt på grund av tredjelandsproblematik.

Det nämns även i delårsrapporten att dataskyddsombudets bedömning är att verksamhetens förbättringsområden kvarstår när det gäller medarbetarnas medvetenhet och kunskaper. Rådet är att verksamheten identifierar behov samt gör en handlingsplan gällande olika utbildningsinsatser till särskilda grupper i verksamheten.

Sedan dess har verksamheten sett över detta. Det finns interna utbildningar för medarbetare men även för ledning. Ledningen är engagerade i dataskydd och verksamheten ska se över att ha en egen utbildningsportal så att man ser uppföljning på utbildningarna. Det finns förhoppningar om att göra egna utbildningar. Verksamheten har uppmärksammat att det finns en generell rädsla över att göra fel och därmed konstaterar man att det behövs skapas en trygghet i vad man får göra genom att skapa tydlighet. Här har verksamheten bland annat utbildat kring personuppgiftsincidenter, vilket har gett resultat i det att incidenter faktiskt uppmärksammas och hanteras.

Utöver detta arbetar verksamheten aktivt med CCTV och har tagit fram arbetssätt för detta ur ett bredare perspektiv.

Kommentarer och rekommendationer:

Mot bakgrund av detta och av dataskyddsombudets tidigare lämnade anmärkningar så har verksamheten arbetat aktivt med fokusområden men även ytterligare områden. Detta visar på ett kontinuerligt arbete för att bättra på de registrerades fri- och rättigheter. Det faktum att verksamheten börjar med kartläggning av personuppgiftsbehandling visar på att verksamheten förstår att man måste veta vad man har och gör med personuppgifterna innan man kan ta ytterligare steg i dataskyddsarbetet.

Fortsatt uppföljning kommer ske inom ramen för de fasta kontrollpunkterna om ingen särskilt föranleder att punkten behöver följas upp separat.

2.7 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.

2.7.1 Rekommendation för hantering av resultaten

Sammanfattningsvis rekommenderas verksamheten att:

- Ta hjälp av dataskyddsombudet så mycket som möjligt, särskilt när dataskyddsorganisationen är så pass ung och rätt hantering av personuppgifter kan säkerställas mer sömlöst tidigt i processer.
- Skapa tydliga ansvarsroller inom dataskyddsarbetet för att hålla arbetet uppdaterat.
- Fortsätt att utbilda och skapa tydlighet för medarbetarna i deras dagliga hantering av personuppgifter.
- Säkerställ att konsekvensbedömningar görs och dataskyddsombudet involveras.
- Säkerställ rutiner för att följa upp om det skett processförändringar, organisationsförändringar m.m. som kan påverka personuppgiftshantering, roller och ansvar.
- Fortsätta säkerställ biträdesavtal – rutiner för att följa upp förändringar i tjänst, avtal etc.
- Fortsätta säkerställ att överföring av personuppgifter till tredjeland har laglig grund.
- Säkerställ rutiner för förvaltning av personuppgiftsregistret.
- Säkerställ information till de registrerade om sina rättigheter.

3 Bilagor

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

