

Styrelsehandling nr 9

Styrelsedatum: 2022-02-11

Diarienummer: FBU2022-0001

Handläggare:

Jenny-Maria Ericsson-Deogan

Telefon: 031-719 31 56

E-post: jenny-maria.ericsson@framtiden.se

Årsrapport för dataskyddsarbete 2021

Informationsärende

Styrelsen för Framtiden Byggutveckling AB:

Årsrapport för dataskyddsarbetet 2021 antecknas

Ärendet

På sammanträdet 2021-05-10 antecknade styrelsen en kontrollplan för dataskyddsarbetet 2021.

Ärendet innehåller en årsrapport över verksamhetens dataskyddsarbete för 2021. Rapporten innehåller information om verksamhetens samarbete med dataskyddsombudet, genomförda kontroller, lämnade rekommendationer samt en övergripande bedömning av status på verksamhetens personuppgiftshantering utifrån fasta kontrollpunkter.

För att möjliggöra en direkt kommunikation mellan dataskyddsombud och personuppgiftsansvarig nämnd/styrelse ska återrapporten presenteras i möte med nämnd/ styrelse. Dataskyddsombudet besökte styrelsemötet 2021-11-16, vid detta möte var inte årsrapporten färdigställd. Den presenteras i stället här som en information.

Bedömning ur ekonomisk dimension

Ärendet är av administrativ karaktär och bolaget har inte funnit några särskilda aspekter på frågan utifrån denna dimension.

Bedömning ur ekologisk dimension

Ärendet är av administrativ karaktär och bolaget har inte funnit några särskilda aspekter på frågan utifrån denna dimension.

Bedömning ur social dimension

Ärendet är av administrativ karaktär och bolaget har inte funnit några särskilda aspekter på frågan utifrån denna dimension.

Samverkan

Ärendet har inte varit föremål för samverkan

Bilaga

1. Årsrapport dataskyddarbete 2021
2. Kontrollplan dataskyddsarbete 2021



Årsrapport för dataskyddsarbetet 2021

Framtiden Byggutveckling AB

2021-12-23

Innehåll

1	Dataskyddsarbetet	4
1.1	Att förvalta ett förtroende	4
1.2	Dataskyddsenhetens gemensamma arbete	4
2	Kontrollarbetet	5
2.1	Ett systematiskt arbete	5
2.2	Rättsutveckling som påverkat kontrollarbetet under året	5
2.2.1	Tredjelsöverföringar (överföringar till länder utanför EU/EES)	5
2.2.2	Rätt beslutsnivå	6
2.2.3	Kommungemensamma interna tjänster	6
2.3	Årets kontrollarbete	8
2.3.1	Fördjupad kontroll	8
2.3.2	Fasta kontrollpunkter	8
2.4	Resultat av fasta kontrollpunkter för Framtiden Byggutveckling AB	10
2.4.1	Kontrollpunkt 1: Dataskyddsorganisation	10
2.4.2	Kontrollpunkt 2: Personuppgiftsincidenter	10
2.4.3	Kontrollpunkt 3: Biträdesavtal och andra överenskommelser	11
2.4.4	Kontrollpunkt 4: Personuppgiftsregister	11
2.4.5	Kontrollpunkt 5: Övergripande strategi för dataskydd	12
2.4.6	Kontrollpunkt 6: Utbildning	12
2.4.7	Kontrollpunkt 7: Integritetspolicy	13
2.4.8	Kontrollpunkt 8: Mejl och dokumenthantering	13
2.4.9	Kontrollpunkt 9: Konsekvensbedömning/samråd	14
2.4.10	Kontrollpunkt 10: IT-projekt och upphandling	14
2.4.11	Kontrollpunkt 11: IT-system och digitala verktyg	15
2.4.12	Kontrollpunkt 12: Hantering av registrerades rättigheter	15
2.5	Särskilda iakttagelser	16
2.5.1	Tredjelsöverföring och användningen av sociala medier	16
2.6	Uppföljning	16
2.6.1	Uppföljning av genomförda kontroller 2018 - 2020	16
2.6.2	Uppföljning av genomförda kontroller 2021	17

2.7	Sammanfattande rekommendationer	17
2.7.1	Rekommendation för hantering av resultaten	18
3	Bilagor	19
3.1	Bilaga 1: Diagram över resultat av fasta kontrollpunkter, i jämförelse med Göteborgs Stads genomsnitt	19

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 Tredjelandsoverföringar (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 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, rekommenderar 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 Dataskyddsorganisation.

Fokusområde 2 Hantering av registrerades rättigheter.

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.

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

Beskrivning av risknivåer

Riskenivåer	Färgkod
Nivå 1. Höga risker identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten.	
Nivå 2. Risker identifierade som bedöms vara omfattande och/eller kräver omgående åtgärder.	
Nivå 3. Risker identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga.	
Nivå 4. Inga direkta risker av betydelse identifierade. Indikerar att verksamheten har ett systematiskt dataskyddsarbete.	

2.4 Resultat av fasta kontrollpunkter för Framtiden Byggutveckling 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 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 uppmanas 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.

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 personuppgiftsbehandlingar, 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 Tredjelandsöverföring 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 tredjelandsöverföring 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 tredjelandsöverföring 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.

Det pågår en riskbedömning med DSF konsult och hur sociala medier ska hanteras. För närvarande använder verksamheten Instagram, Youtube, Facebook och LinkedIn.

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.

Kontroll 1 (2018): Organisatoriska förutsättningar för dataskyddsarbetet.

Verksamheten gavs följande rekommendationer:

Ett bra dataskyddsarbete kännetecknas av ständig förbättring vilket är en viktig delkomponent för att uppnå följsamhet mot dataskyddsförordningen. Dataskyddsombudets uppfattning utifrån de möten som ägt rum med dataskyddskontakten samt granskat avstämningsunderlag är att Framtiden Byggutveckling AB arbetar aktivt med dataskyddsfrågor. I nuläget är bolagets dataskyddskontakt att betrakta som dataskyddsorganisationen i bolaget. Bolaget har identifierat den sårbarhet som finns och planerar att skapa en ny dataskyddsorganisation. Dataskyddsombudet ställer sig positivt till den framtida dataskyddsorganisationen. Bedömningen är dock att organisationen bör skynda på arbetet samt ta fram lämplig arbetsinstruktion/arbetsflöde för organisationen. Det är viktigt att arbetet fungerar rent praktiskt och att strategierna får det tydliga genomslag som avsetts. Detta inte minst i syfte att visa att lämpliga organisatoriska åtgärder har vidtagits utifrån dataskyddsförordningens krav. Avslutningsvis är dataskyddsombudets uppfattning att dataskyddskontakten ger dataskyddsombudet goda förutsättningar för att utföra sitt arbete.

Kommentarer och rekommendationer:

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

2.6.2 Uppföljning av genomförda kontroller 2021

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

Kontroll 1 (2021): Dataskyddsorganisation

Gällande dataskyddsorganisationen så har verksamheten tillsatt en resurs som dataskyddskontakt. I övrigt arbetar verksamheten mycket gemensamt med moderbolaget i dataskyddsfrågor. De största fokusområdena inom verksamheten kring just personuppgiftsbehandling ligger inom ramen för hantering av de anställdas personuppgifter och tillhörande löneprocesser.

Kontroll 2 (2021): De registrerades rättigheter

Gällande hantering av registrerades rättigheter så är det inget nytt som tillkommit inom området utöver att man delges information när man anställs.

Ingen registerförteckning har skapats i Draftit men däremot har verksamheten kartlagt en löneregisterhantering samt behörighetshantering.

Verksamheten har ingen egen handlingsplan för sin verksamhet vad gäller sitt dataskyddsarbete. Istället arbetar verksamheten med koncernens gruppering och det arbete som läggs upp där följer verksamheten.

Utöver detta arbetar verksamheten med att säkerställa så att biträdesavtal finns på plats samt att tredjelandsoverföring kartläggs och säkerställs utifrån de krav som finns.

Överlag så är IT-beredskapen förstärkt på koncernnivå och det mesta i dataskyddsarbetet drivs av koncernens råd.

Kommentarer och rekommendationer:

Verksamhetens satta strategi gällande dataskyddsfrågor är att arbeta nära moderbolaget. 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 dataskyddsbudet 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.

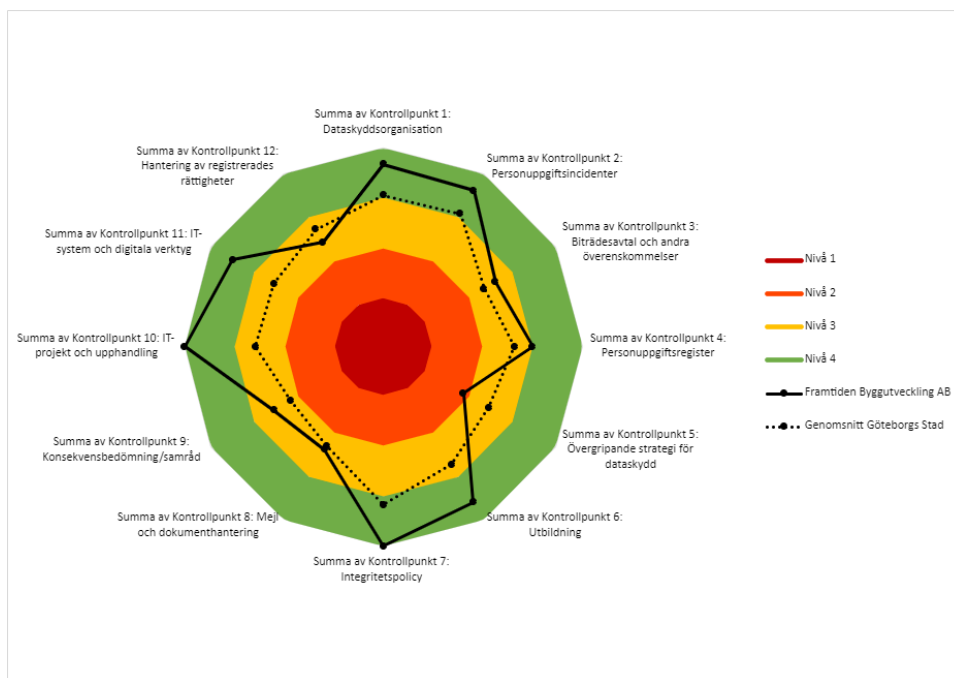
2.7.1 Rekommendation för hantering av resultaten

Sammanfattningsvis rekommenderas verksamheten att:

- Säkerställa och förbättra/anpassa rutiner för personuppgiftsincidenter.
- 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.
- Fortsätt säkerställ biträdesavtal –rutiner för att följa upp förändringar i tjänst, avtal etc.
- Fortsätt säkerställ att överföring av personuppgifter till tredjeland har laglig grund.
- Säkerställ rutiner för förvaltning av personuppgiftsregistret. Med ett personuppgiftsregister som uppdateras löpande så ökar chanserna för verksamheten att kunna upptäcka vilka områden inom dataskydd som behöver prioriteras. Genom detta får verksamheten även ökad kännedom om särskilda områden avviker från den koncerngemensamma hanteringen och därför särskilt behöver uppmärksammas och anpassas.
- 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.





Framtiden Byggutveckling AB

Kontrollplan för dataskyddsarbetet 2021

2021-01-27

Innehåll

1	Bakgrund	3
1.1	Dataskyddsförordningen.....	3
1.1.1	Personuppgiftsansvarig	3
1.1.2	Dataskyddsombud.....	3
2	Kontrollplan för dataskyddsarbetet 2021	4
2.1	Syfte och mål.....	4
2.2	Ett riskbaserat arbetssätt	4
2.3	Upplägg	5
2.3.1	Verksamhetsspecifika förutsättningar	5
2.4	Tidplan för kontroller 2021	5
3	Kontrollpunkter	6
3.1	Fasta kontrollpunkter	6
3.1.1	Beskrivning av fasta kontrollpunkter	7
3.2	Fördjupad kontroll 2021	9
4	Uppföljning	9
4.1	Uppföljning av lämnade rekommendationer	9
4.1.1	Uppföljning av hittills genomförda kontroller.....	9
5	Avrapportering till nämnd/styrelse	10
5.1	Delårsrapportering.....	10
5.2	Årsrapport.....	10
5.3	Särskilt yttrande till högsta ledning.....	10
5.4	Beslutanderätten i dataskyddsfrågor.....	10
6	Kontakt	11

1 Bakgrund

1.1 Dataskyddsförordningen

Dataskyddsförordningen (DSF) trädde i kraft i maj 2018 och är en EU-förordning med syfte att skydda fysiska personers grundläggande fri- och rättigheter, att garantera ett likvärdigt skydd samt att säkerställa det fria flödet av personuppgifter inom unionen. Förordningen kompletteras av dataskyddslagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning. Dessa samspelar även med annan speciallagstiftning.

Dataskyddsförordningen ställer höga krav på organisationers behandling av enskildas personuppgifter. Utöver att insamlingen av personuppgifterna ska vara tillåten, måste den personuppgiftsansvarige dessutom hantera dessa uppgifter på ett korrekt sätt, med respekt för den enskildes integritet och med beaktande av lämpliga säkerhetsåtgärder.

Efterlevnaden av lagstiftningen övervakas av Integritetsskyddsmyndigheten och överträdelser kan leda till bland annat sanktionsavgifter eller skadestånd.

1.1.1 Personuppgiftsansvarig

En personuppgiftsansvarig kan vara en fysisk person, juridisk person, en offentlig myndighet, institution eller ett annat organ. Varje förvaltning med egen nämnd räknas som en egen offentlig myndighet. I juridisk mening så är därmed ytterst varje enskild nämnd eller styrelse ansvarig för att de personuppgiftsbehandlingar som organisationen hanterar utförs i enlighet med gällande regelverk. För att följa dataskyddsarbetet och hålla nämnden/styrelsen informerad bör enligt dataskyddsförordningen ett dataskyddsombud, med särskild sakkunskap i fråga om dataskyddslagstiftning och praxis, utses för att bistå den ansvarige med att övervaka den interna efterlevnaden av förordningen.

1.1.2 Dataskyddsombud

Dataskyddsombudet ska ge råd och information till den personuppgiftsansvarige samt övervaka efterlevnaden av dataskyddsförordningen och annan relevant dataskyddslagstiftning. Det innebär bland annat att kontrollera hur den personuppgiftsansvarige behandlar personuppgifter, att bestämmelser och interna styrdokument följs samt att ge råd och stöd vid konsekvensbedömningar. Dataskyddsombudet ska enligt dataskyddsförordningen utföra sitt arbete på ett oberoende sätt gentemot den som är personuppgiftsansvarig och får inte instrueras av denne hur arbetet ska utföras. Dataskyddsombudet är inte heller ansvarig för att lagstiftningen efterlevs.

Dataskyddsombudet är även kontaktperson för de registrerade och tillsynsmyndigheten.

2 Kontrollplan för dataskyddsarbetet 2021

2.1 Syfte och mål

Dataskyddsombudets uppgift att övervaka den personuppgiftsansvariges efterlevnad av förordningen regleras i artikel 39 DSF. En del av denna övervakning innebär att dataskyddsombudet genomför kontroller av dataskyddsarbetet inom den personuppgiftsansvariges organisation. Dessa kontroller specificeras genom denna kontrollplan som syftar till att informera personuppgiftsansvariga om tidplan och särskilda fokusområden för kontrollarbetet år 2021.

Målsättningen med att arbeta utefter en på förhand fastställd kontrollplan är att det ska bidra till att sätta fokus på verksamhetens dataskyddsarbete och därmed:

1. Säkerställa ett kontinuerligt dataskyddsarbete som skapar förutsättningar för efterlevnad av förordningen.
2. Maximera ett riskbaserat arbetssätt och därigenom minimera risken för lagbrott.
3. Göra dataskyddsarbetet till en integrerad del i verksamhetens informationssäkerhetsarbete.

2.2 Ett riskbaserat arbetssätt

Enligt dataskyddsregelverket ska dataskyddsombudet arbeta utifrån en riskbaserad metod. Kontrollplanen utgår därför ifrån dataskyddsombudets riskbedömning avseende verksamhetens personuppgiftsbehandlingar och tas fram i dialog med verksamheten. Primära fokusområden och prioriteringar utgår från eventuella problem som bedöms utgöra en högre risk för dataskyddet i verksamheten.

Gemensamt för stadens verksamheter har dataskyddsenheten identifierat två riskområden som är särskilt relevanta, utifrån att respektive personuppgiftsansvarig har möjlighet att genom att bedriva ett systematiskt dataskyddsarbete påverka omfattningen av de risker som dessa områden inbegriper. Det första riskområdet innefattar ekonomisk skada (exempelvis skadestånd och sanktionsavgifter), vars risker beror på huruvida verksamheten i sin personuppgiftshantering säkerställer att dataskyddsförordningen följs. Det andra riskområdet innefattar förtroendeskada (så som exempelvis försämrat varumärke och minskad tillit) och är beroende av verksamhetens förmåga att hantera de registrerades rättigheter enligt dataskyddsförordningen.

2.3 Upplägg

Kontrollarbetet består av tre delar som tillsammans syftar till att ge såväl dataskyddsbud som personuppgiftsansvariga en överblick över verksamhetens dataskyddsarbete och dess följsamhet gentemot förordningen.

- a) Den första delen består av fasta kontrollpunkter där varje punkt bedöms årligen. Bedömningen görs genom löpande kontroller, genom deltagande i verksamhetens arbete och i förekommande fall utifrån given information.
- b) Den andra delen är en fördjupad kontroll av utvalda verksamhetsspecifika kontrollpunkter.
- c) Den tredje delen är en uppföljning och bedömning av hur verksamheten hanterat tidigare lämnade rekommendationer.

Kontrollarbetets olika delar kommer sammanställas och presenteras i årsrapporten för nämnd/styrelse. Genom att ha en årlig uppföljning av de fasta kontrollpunkterna kommer varje personuppgiftsansvarig kunna följa utvecklingen av dataskyddsarbetet inom verksamheten över tid.

2.3.1 Verksamhetsspecifika förutsättningar

Dataskyddsbudets arbete kommer att bedrivas utifrån verksamhetens specifika förutsättningar. Identifierade aktiviteter kan därför komma att justeras utifrån händelser som inträffar i verksamheterna eller i omvärlden.

2.4 Tidplan för kontroller 2021

Månad	Huvudaktivitet	Övriga aktiviteter
Januari	Kontrollplan för året lämnas till nämnd/styrelse	Uppföljning och kontroll av övriga fasta kontrollpunkter kommer ske löpande under året.
Februari- April	Fördjupad kontroll av utvalda verksamhetsspecifika kontrollpunkter genomförs	
Maj	Fördjupad kontroll slutförs och rekommendationer lämnas till verksamheten	
Juni	Delårsrapportering avseende verksamhetens dataskyddsarbete för nämnd/styrelse	
September- Oktober	Uppföljning av tidigare lämnade rekommendationer	
November	Årsrapport lämnas till verksamheten	
December	Årsrapport presenteras för nämnd/styrelse	

3 Kontrollpunkter

3.1 Fasta kontrollpunkter

De fasta kontrollpunkternas omfattning utgår från principerna om inbyggt dataskydd och dataskydd som standard (enligt artikel 25 DSF). Verksamhetens följsamhet mot förordningen beror till stor del på hur väl dessa principer har integrerats i verksamhetens ordinarie processer. Att principerna har en central roll i arbetet med dataskydd blir särskilt tydligt i beaktandesats (skäl) 78 DSF, som anger att ”skyddet av fysiska personers rättigheter och friheter i samband med behandling av personuppgifter förutsätter att lämpliga tekniska och organisatoriska åtgärder vidtas”, och därtill att personuppgiftsansvarig, för att kunna visa att förordningen efterlevs, bör anta interna strategier och vidta åtgärder särskilt för att uppfylla principerna om inbyggt dataskydd och dataskydd som standard.

Med principen om inbyggt dataskydd avses att man tar hänsyn till förordningen vid utformning av IT-system och rutiner, och på så sätt från början säkerställer att både kraven i dataskyddsförordningen uppfylls och att den registrerades rättigheter skyddas. Principen om dataskydd som standard innebär att personuppgifter i standardfallet inte behandlas i onödan, vilket kan göras genom att ha lämpliga tekniska och organisatoriska åtgärder som standard.

Med principerna som utgångspunkt har elva kontrollpunkter definierats, av både organisatorisk och teknisk karaktär, vilka är gemensamma för alla verksamheter inom Göteborgs Stad. De punkter som fastställts utgör en del av fundamentet i lagstiftningen. Syftet med arbetssättet är att tillsammans hitta strategier, rutiner och arbetssätt som hanterar punkterna så att kontrollerna över tid kommer att kräva mindre och mindre arbete.

Kontrollpunkter
1. Dataskyddsorganisation
2. Personuppgiftsincidenter
3. Biträdesavtal och andra överenskommelser
4. Personuppgiftsregister
5. Övergripande strategi för dataskydd
6. Utbildning
7. Integritetspolicy
8. Mejl- och dokumenthantering
9. Konsekvensbedömning/samråd
10. IT-projekt och upphandling
11. IT-system och digitala verktyg
12. Hantering av registrerades rättigheter

3.1.1 Beskrivning av fasta kontrollpunkter

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.

Kontrollpunkt 2: Personuppgiftsincidenter

Kontrollpunkten avser verksamhetens förutsättningar för att identifiera och hantera personuppgiftsincidenter. För att uppfylla ansvarsskyldigheten bör verksamhetens rutin för hanteringen vara dokumenterad. I de fall verksamheten är både personuppgiftsansvarig och personuppgiftsbiträde bör rutinen omfatta båda scenarier. I kontrollpunkten ingår även översyn av verksamhetens rutin för att bedöma incidenten, hantering av eventuell anmälan till tillsynsmyndigheten samt hur rutinerna tillgängliggörs och kommuniceras inom verksamheten. Även efterlevnad av verksamhetens dokumentationsskyldighet, att alla inträffade personuppgiftsincidenter registreras, innefattas.

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.

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.

Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd. En verksamhetsspecifik strategi som anger ramarna för arbetet med dataskydd kan både främja ett riskbaserat arbetssätt och bidra till en kontinuitet i dataskyddsarbetet.

Kontrollpunkten innefattar även verksamhetens strategi för att integrera dataskyddsfrågorna i det övriga informationssäkerhetsarbetet, samt hur verksamheten arbetar med egna interna kontroller för att säkerställa att dataskyddsförordningen efterlevs.

Kontrollpunkt 6: Utbildning

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

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.

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.

Kontrollpunkt 9: Konsekvensbedömning/samråd

Kontrollpunkten avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras samt genomföra denna. Även verksamhetens rutiner för arbetet med konsekvensbedömningar samt hur dataskyddsombudet involveras i arbetet ingår. Därtill tillkommer verksamhetens rutin för att hantera de risker som identifieras i konsekvensbedömningen, samt hur genomförda konsekvensbedömningar följs upp och hålls aktuella.

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.

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.

Kontrollpunkt 12: Hantering av registrerades rättigheter

Kontrollpunkten avser verksamhetens förutsättningar för att hantera de registrerades rättigheter, till exempel registerutdrag eller radering. En förutsättning för att verksamheten ska kunna hantera de registrerades rättigheter är att man har en process och rutiner för arbetet, så att den registrerades personuppgifter enkelt kan lokaliseras vid efterfrågan. Även verksamhetens rutin för att hantera ett tillbakadragande av samtycke ingår i kontrollpunkten.

3.2 Fördjupad kontroll 2021

Den fördjupade kontrollen utgår från verksamhetens specifika risker. För verksamhetsåret har följande punkt/punkter fastställts:

Fokusområde 1: Dataskyddsorganisationen

Fokusområde 2: Hantering av registrerades rättigheter främst anställdas personuppgifter.

4 Uppföljning

4.1 Uppföljning av lämnade rekommendationer

I dataskyddsförordningen anges att dataskyddsombudet ska rapportera direkt till den personuppgiftsansvariges eller personuppgiftsbitrådets högsta förvaltningsnivå, för att säkerställa att högsta ledningen är medveten om dataskyddsombudets råd och rekommendationer. Detta är grunden för ett proaktivt arbetssätt och utgör en trygghet för nämnd/styrelse som uppmärksammas på status och observerade brister i dataskyddsarbetet. Det är då också av vikt för nämnd/styrelse att veta hur eventuella rekommendationer/brister omhändertagits. Dataskyddsombudet kommer därför årligen att följa upp hanteringen av de rekommendationer som lämnats till verksamheten och rapportera detta i årsrapporten.

4.1.1 Uppföljning av hittills genomförda kontroller

Sedan dataskyddsförordningen trädde i kraft i maj 2018 har dataskyddsombudet genomfört årliga kontroller för er verksamhet. Dessa kontroller kommer att följas upp inom ramen för de fasta kontrollpunkterna under 2021. Under året kommer dataskyddsombudet att se över vilka åtgärder som vidtagits med anledning av de rekommendationer som lämnats vid tidigare kontroller.

Exempelvis genomförd kontroll 1 (2018): Organisatoriska förutsättningar för dataskyddsarbetet följs upp inom kontrollpunkt: Dataskyddsorganisation.

5 Avrapportering till nämnd/styrelse

5.1 Delårsrapportering

I juni månad kommer respektive nämnd/styrelse att få en delårsrapportering för dataskyddsarbetet av dataskyddsombudet. Fokus för delårsrapporteringen är den verksamhetspecifika fördjupade kontrollen som genomförs under våren.

Genom en delårsrapportering säkerställs att personuppgiftsansvarig nämnd/styrelse hålls informerad om dataskyddsombudets observationer av verksamhetens personuppgiftshantering. Formen för rapporteringen anpassas efter dataskyddsombudets bedömning av verksamhetens behov.

5.2 Årsrapport

Verksamhetens dataskyddsarbete kommer att sammanställas i en skriftlig årsrapport till nämnd/styrelse. Årsrapporten kommer innehålla information om verksamhetens samarbete med dataskyddsombudet, genomförda kontroller, lämnade rekommendationer samt en övergripande bedömning av status på verksamhetens personuppgiftshantering utifrån fasta kontrollpunkter.

För att möjliggöra en direkt kommunikation mellan dataskyddsombud och personuppgiftsansvarig nämnd/styrelse ska årsrapporten presenteras i möte med nämnd/styrelse.

5.3 Särskilt yttrande till högsta ledning

Om det skulle uppstå situationer där den ansvarige fattar beslut som är oförenliga med den allmänna dataskyddsförordningen och dataskyddsombudets råd, till exempel om en allvarlig brist kvarstår och inte åtgärdas, har dataskyddsombudet möjlighet att klargöra sin avvikande ståndpunkt genom ett yttrande riktat till högsta förvaltningsnivå och till dem som fattar besluten.

5.4 Beslutanderätten i dataskyddsfrågor

Beslutanderätten i dataskyddsfrågor ligger alltid på den personuppgiftsansvarige och aldrig på dataskyddsombudet. Dataskyddsombudet är en specialist med en rådgivande roll och är en resurs som, på ett oberoende sätt, fokuserar på dataskyddsfrågorna i verksamheten och på det sättet bistår den personuppgiftsansvarige med bedömningar och råd. Om nämnden/styrelsen väljer att inte följa dataskyddsombudets rekommendationer ska skälen till detta motiveras och dokumenteras i enlighet med god praxis samt för att uppfylla ansvarsskyldigheten. Detta är även viktigt för det fall frågan senare skulle bli föremål för tillsyn.

6 Kontakt

Eventuella frågor och synpunkter hänvisas i första hand till er kontaktperson/ert dataskyddsombud. Frågor kan också alltid ställas till dso@intraservice.goteborg.se.