Malmö stad

Granskning av efterlevnad dataskyddsförordningen (GDPR)

Januari 2022

Building a better working world

1. Sammanfattning

EY har på uppdrag av de förtroendevalda revisorerna i Malmö stad granskat efterlevnaden av dataskyddsförordningen GDPR. Syftet med granskningen var att bedöma om kommunstyrelsen, servicenämnden, funktionsstödsnämnden och gymnasie- och vuxenutbildningsnämnden säkerställer ett ändamålsenligt dataskyddsarbete.

Granskningen har baserats på EY:s metodik för mognadsbedömning av implementeringen av dataskyddsförordningen. Genom metodiken värderas kommunstyrelsen och respektive nämnds arbete gentemot EY:s standardiserade skala för dataskyddsarbete inom kommunal sektor. Metoden är kvalitetssäkrad och utgår från god praxis för dataskyddsarbete.

Den samlade bedömningen är att kommunstyrelsen och de granskade nämnderna inte i tillräcklig utsträckning har säkerställt att dataskyddsarbetet bedrivs ändamålsenligt. Det är vår bedömning att det finns en övergripande organisation och arbetsgång med tillhörande roller. Det finns bland annat rutiner för risk- och sårbarhetsanalyser och riktlinjer för personuppgiftsincidenter. Trots detta råder oklarheter mellan kommunstyrelsen och nämnderna vad avser ansvaret för dataskyddsarbetet. Likaså är det inte säkerställt att dataskyddsombudet står utan intressekonflikt i granskning av eget arbete. Bedömningen grundar sig vidare på att kommunstyrelsen och nämnderna inte säkerställt att riskanalyser och konsekvensbedömningar genomförs på ett strukturerat sätt, samt att registerförteckningarna är kompletta. Därtill anser vi att kommunstyrelsen och nämnderna saknar tillräckliga kontroller, uppföljning och rapportering av dataskyddsarbetet. Avslutningsvis menar vi att utbildningsinsatserna för samtliga anställda är otillräckliga. Det saknas enligt vår mening ett systematiskt arbete som säkerställer en god kunskapsnivå avseende dataskydd och informationssäkerhet.

Enligt EY:s granskningsmetodik framkommer att kommunstyrelsen och nämnderna generellt har en låg mognadsgrad sett till kommunens storlek, riskbild samt den mängd personuppgifter som de hanterar. På en femgradig skala lämnas följande mognadsbedömningar:

- Kommunstyrelsen – 2,61
- Servicenämnden – 2,47
- Gymnasie- och vuxenutbildningsnämnden – 2,42
- Funktionsstödsnämnden – 2,47

Av granskningsresultatet lämnas ett stort antal rekommendationer till såväl kommunstyrelsen som de granskade nämnderna. Rekommendationerna är uppdelade enligt angelägenhet (rekommendationer som *inledningsvis* bör åtgärdas och rekommendationer som *därefter* bör åtgärdas*)*. Rekommendationerna återfinns på sida 20.

Innehållsförteckning

1. Sammanfattning 1
2. Inledning 3
2.1. Bakgrund 3
2.2. Syfte och revisionsfrågor 4
2.3. Avgränsning 4
2.4. Metod 5
2.5. Revisionskriterier 7
2.6. Definitioner 8
3. Granskningsresultat 9
3.1. Styrning och organisation 9
3.1.1. Iakttagelser 9
3.1.2. Bedömning 10
3.2. Personuppgiftsbehandling 11
3.2.1. Iakttagelser 11
3.2.2. Bedömning 13
3.3. Kontroll och uppföljning 13
3.3.1. Iakttagelser 13
3.3.2. Bedömning 14
4. Samlad bedömning 15
4.1. Samlad bedömning per nämnd och kommunstyrelsen 15
4.2. Svar på revisionsfrågor 17
4.3. Våra rekommendationer 20
5. Bilaga 1: Detaljerade granskningsresultat 23
5.1. Kommunstyrelsen 23
5.2. Servicenämnden 40
5.2.1. Nuläge och iakttagelser 42
5.3. Gymnasie- och vuxenutbildningsnämnden 50
5.3.1. Nuläge och iakttagelser 52
5.4. Funktionsstödsnämnden 60
5.4.1. Nuläge och iakttagelser 62
Bilaga 2: Förteckning över intervjuade funktioner 71
5.6. Stadskontoret 71
5.7. Serviceförvaltningen 71
5.8. Gymnasie- och vuxenutbildningsförvaltningen 71
5.9. Funktionsstödsförvaltningen 71
6. Bilaga 3: Dokumentförteckning..... 72
6.1. Kommunstyrelsen 72
6.2. Servicenämnden 73
6.3. Gymnasie- och vuxenutbildningsnämnden 73
6.4. Funktionsstödsnämnden 73
7. Bilaga 4: Definitioner..... 74

2. Inledning

2.1. Bakgrund

Den 25 maj 2018 trädde dataskyddsförordningen (GDPR, The General Data Protection Regulation) i kraft.

Dataskyddsreglerna grundar sig i de mänskliga rättigheterna. Alla människor har rätt till respekt för privat- och familjeliv och till skydd av sina personuppgifter. Alla verksamheter måste följa dataskyddsreglerna vid behandling av personuppgifter.

Dataskyddsförordningen gäller för behandling av personuppgifter. Med personuppgifter menas varje upplysning som rör en identifierad eller identifierbar fysisk person. Det som avgör är om uppgiften, enskilt eller i kombination med andra uppgifter, kan knytas till en levande person.

I dataskyddsförordningen finns ett antal grundläggande principer som kan sägas vara kärnan i förordningen. Principerna gäller för all personuppgiftsbehandling och sätter de yttersta ramarna för vad som är en tillåten behandling.

Principerna innebär bland annat att personuppgiftsansvariga:

- måste ha stöd i dataskyddsförordningen för att få behandla personuppgifter
- bara får samla in personuppgifter för specifika, särskilt angivna och berättigade ändamål
- inte ska behandla fler personuppgifter än vad som behövs för ändamålen
- ska se till att personuppgifterna är riktiga
- ska radera personuppgifterna när de inte längre behövs
- ska skydda personuppgifterna, till exempel så att inte obehöriga får till-gång till dem och så att de inte förloras eller förstörs
- ska kunna visa att ni lever upp till dataskyddsförordningen och hur ni gör det.

Inför att personuppgifter ska behandlas behövs det göras en konsekvensbedömning.

Malmö stads nämnder är personuppgiftsansvariga och anlitar personuppgiftsbiträde. Personuppgiftsansvarig är den som bestämmer för vilka ändamål uppgifterna ska behandlas och hur behandlingen ska gå till. Personuppgiftsbiträde är den som behandlar personuppgifter för den personuppgiftsansvariges räkning.

I dataskyddsförordningen finns en skyldighet för organisationer att anmäla vissa typer av personuppgiftsincidenter till Integritetsmyndigheten (IMY). En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks.

Det spelar ingen roll om det har skett oavsiktligt eller med avsikt. I båda fall är det personuppgiftsincidenter.

En personuppgiftsincident kan få allvarliga konsekvenser för registrerade personer i form av till exempel ekonomisk skada eller kränkning av deras friheter och rättigheter. En personuppgiftsincident som inte hanteras på ett lämpligt sätt kan påverka tilltron till den organisation som behandlar personuppgifter. Den kan också leda till sanktionsavgifter.

Malmö stad anmälde en personuppgiftsincident till IMY den 29 april 2021.

Under 2020 har Stadsrevisionen genomfört fördjupade granskningar av IT-säkerhet samt digitalisering.

Utifrån genomförd riskanalys har de förtroendevalda revisorerna beslutat att genomföra en granskning av Malmö stads hantering av personuppgifter.

2.2. Syfte och revisionsfrågor

Syftet med granskningen är att bedöma om kommunstyrelsen, servicenämnden, funktionsstödsnämnden och gymnasie- och vuxenutbildningsnämnden säkerställer ett ändamålsenligt dataskyddsarbete.

- Har dataskyddsarbetet inom Malmö stad organiserats på ett tydligt och ändamålsenligt sätt? Bedrivs ett effektivt arbete?
- Är de olika rollerna i Malmö stads dataskyddsarbete tydliga?
- Avsätts tillräckliga resurser (exempelvis personella och ekonomiska) för ett tillräckligt dataskyddsarbete?
- Bedrivs ett aktivt och strukturerat dataskyddsarbete där dataskyddsfrågor beaktas vid befintliga och tillkommande behandlingar av personuppgifter?
- Säkerställs att dataskyddsombudet och/eller förvaltningarnas dataskyddssamordnare blir involverade vid styrelsens/nämndernas behandlingar av personuppgifter (exempelvis vid nya personuppgiftsbehandlingar vid inköp av nya IT-system)?
- Hanteras personuppgiftsincidenter i enlighet med lagkrav och Malmö stads riktlinjer? Är Malmö stads riktlinjer för att hantera personuppgiftsincidenter tillräckliga?
- Genomförs kontroll, uppföljning och återrapportering av Malmö stads dataskyddsarbete?

2.3. Avgränsning

Granskningen avgränsas till kommunstyrelsen, servicenämnden, funktionsstödsnämnden och gymnasie- och vuxenutbildningsnämnden.

Granskningen omfattar kommunstyrelsens eget dataskyddsarbete, dess tillhandahållande av dataskyddsombud och dess uppsikt över nämnder. Granskningen omfattar servicenämndens eget dataskyddsarbete och dess ansvar för kommungemensam IT.

Granskningen har utförts genom dokumentstudier av bland annat styrdokument, nämndernas protokoll och beslutsunderlag, riktlinjer, rutiner med mera.

Intervjuer har genomförts med tjänstepersoner på berörda förvaltningar som har sakkunskap kring respektive nämnders dataskyddsarbete.

2.4. Metod

Granskningen är utförd med utgångspunkt i EY:s metod för granskning av mognadsgrad gentemot dataskyddsförordningen. Metoden är kvalitetssäkrad och utgår från god praxis för dataskyddsarbete.

EY:s metodik består av ett ramverk med 116 frågor. Frågorna är kategoriserade i 12 delområde kopplade till dataskyddsförordningen. Ramverket utgår från ett internkontrollperspektiv. Syftet är att bedöma eventuella avvikelser samt risker kopplat till brister i personuppgiftshanteringen. Bedömningen av mognadsgraden har skett i samverkan mellan GDPR-specialister från EY. EY:s specialister sammanställer svaren och redogör för avvikelser inom ovan nämnda 12 områden. En bedömning av mognadsgrad sker på en femgradig skala utifrån observationerna.

Frågorna är såväl direkt som indirekt kopplade till krav från förordningen. Indirekt koppling utgörs exempelvis av styrning och underhåll av arbetet med att upprätthålla regeluppfyllnaden. För enkelhetens skull används ordet ”krav” synonymt i rapporten oavsett om det avser en direkt eller indirekt koppling. Metoden understryker premissen att det är av vikt att inte enbart granska huruvida enskilda kontroller är på plats eller att enskilda krav är täckta; det är även av särskild vikt att säkerställa att styrning och uppföljning av regeluppfyllnad sker systematiskt.

De 12 områdena som granskats inom uppdraget är:

1. Styrande dokument/styrning
2. Riskhantering
3. Kontroll
4. Organisation och ansvar
5. Behandling av personuppgifter
6. Val av skyddsåtgärder
7. Inbyggt dataskydd
8. Hantering av leverantörsrelationer
9. Hantering av incidenter
10. Information till registrerade

11. Begäran från registrerade
12. Profilering

Mognadsgrad beskrivs på en standardiserad skala enligt nedan:

1. Begynnande – Det finns ingen dokumentation eller uppföljning, händelser hanteras ad hoc.
2. Upprepbar – Viss grundläggande dokumentation finns, men denna kan variera mellan olika enheter och vara bristfällig i sin omfattning och tillämpning.
3. Definierad – Det finns dokumenterade processer och dessa tillämpas i stor mån genom hela organisationen.
4. Förvaltad – Förutom väl dokumenterade processer som tillämpas i hela organisationen, finns det dessutom ett system för uppföljning.
5. Optimerad – Baserat på uppföljningen finns också rutiner för kontinuerlig förbättring och uppdatering av processer och ramverk.

Ett delområdes färgkod visar den genomsnittliga mognadsgraden baserat på dess underfrågor. Respektive krav har inte viktats. Mognadsgraden indikerar vilka delområden som har störst förbättringsbehov. På grund av genomsnittsberäkningen kan dock ett delområde med grön färgkod fortfarande sakna viktiga kontroller. Brister i efterlevnad framkommer dock i observationerna och rekommendationerna inom respektive fråga.

Granskningen inleddes genom insamling och analys av underlag såsom policyer, strategi- och styrdokument och dylikt. Därefter totalt fyra arbetsmöten (intervjuer) med nyckelpersoner inom respektive förvaltning (se *Bilaga 1: Förteckning över intervjuade funktioner*). Vid arbetsmötena avhandlades samtliga 12 delområden. Efter att resultaten från arbetsmötena analyserat sammanställdes ett rapportutkast som de intervjuade givits möjlighet att sakkontrollera. Efter sakkontrollen har rapporten justerats baserat på inkomna iakttagelser. Rapporten har innan sakkontrollen kvalitetssäkrats av EY:s verksamhetsrevisorer samt den för uppdraget utsedda kvalitetskontrollanten.

Granskningen har utförts enligt nedan tidplan:

Förberedelser och planering	September 2021
Insamling och analys av dokumentation	Oktober 2021
Arbetsmöten	Oktober 2021
Rapportskrivning samt intern kvalitetssäkring	November 2021
Faktagranskning av Malmö stad	December 2021
Justering samt färdigställande av rapport	December 2021
Avrapportering och slutpresentation	Januari 2022

2.5. Revisionskriterier

Kommunallagen

Kommunstyrelsen ska i enlighet med kommunallagen 6 kap. 1 § leda och samordna förvaltningen av kommunens eller regionens angelägenheter och ha uppsikt över övriga nämnders och eventuella gemensamma nämnders verksamhet.

Enligt 6 kap. 6 § ska nämnderna var och en inom sitt område se till att verksamheten bedrivs i enlighet med de mål och riktlinjer som fullmäktige har bestämt samt de bestämmelser i lag eller annan författning som gäller för verksamheten. Nämnderna ska därtill se till att den interna kontrollen är tillräcklig och att verksamheten bedrivs på ett i övrigt tillfredsställande sätt.

Kommunstyrelsens reglemente

Styrelsen ska enligt reglemente utifrån ett helhetsperspektiv leda kommunens verksamhet genom att utöva en samordnad styrning och leda arbetet med att ta fram nämndövergripande styrdokument för kommunen. Styrelsen ansvarar därtill, utöver angivna uppgifter i reglementet, för uppgifter vilka inte lagts på annan nämnd.

Styrelsen är i enlighet med reglemente anställningsmyndighet för Malmö stads dataskyddsombud och genom denna tillhandahålla specialistkompetens och lokal tillsyn i dataskyddslagstiftningen.

Styrelsen ansvarar för det övergripande arbetet med informationssäkerhet. Därtill har styrelsen ett övergripande ansvar för säkerhet och riskhantering i kommunen. Styrelsen har också det övergripande ansvar för styrdokument inom kommungemensam IT.

Servicenämndens reglemente

Servicenämnden ansvarar enligt reglemente för kommungemensam IT. Syftet är att hålla samman kommunens IT- verksamhet. Detta gäller såvida inte annan nämnd ansvarar för viss specifik IT-verksamhet.

Servicenämnden får inom ramen för detta ansvar leda, utveckla och samordna stadens gemensamma IT-och digitaliseringsfrågor, informationssystem samt digital infrastruktur.

Kommunstyrelsens och samtliga granskade nämnders reglemente

Enligt kommunstyrelsens och de granskade nämnders reglementen framgår att samtliga har personuppgiftsansvar för de personuppgifter som de behandlar i sin respektive verksamhet. Samtliga nämnder ansvarar tillsammans med kommunstyrelsen för framtagandet av

styrdokument i form av riktlinjer, principer, policydokument, tillämpningsanvisningar och dylikt.

Övriga revisionskriterier

Granskningen omfattar utöver ovan nämnda revisionskriterier *dataskyddsförordningen (GDPR)* samt *riktlinjer för behandling av personuppgifter i Malmö stad (KS 2018-05-02).* Förutsättningarna enligt kriterierna lyfts kontinuerligt i rapporten utifrån dess relevans för granskningen.

2.6. Definitioner

Se bilaga 4.

3. Granskningsresultat

I detta kapitel presenteras de övergripande resultaten från genomförd granskning med utgångspunkt från revisionsfrågorna. Mognadsbedömningarna för kommunstyrelsen och respektive nämnd återfinns i bilaga 1. Iakttagelserna och bedömningarna i detta kapitel utgår från informationen som inhämtats för kommunstyrelsen och de granskade nämnderna.

3.1. Styrning och organisation

I detta delkapitel besvaras följande revisionsfrågor:

- Har dataskyddsarbetet inom Malmö stad organiserats på ett tydligt och ändamålsenligt sätt? Bedrivs ett effektivt arbete?
- Är de olika rollerna i Malmö stads dataskyddsarbete tydliga?
- Avsätts tillräckliga resurser (exempelvis personella och ekonomiska) för ett tillräckligt dataskyddsarbete?

3.1.1. Iakttagelser

Det övergripande arbetet med dataskyddsförordningen baseras på kommungemensamma riktlinjer för behandling av personuppgifter. I dagsläget saknas det dock en övergripande informationssäkerhetspolicy som riktlinjerna grundar sig i. *Riktlinjer för behandling av personuppgifter* fastställdes av kommunstyrelsen i maj 2018 och gäller samtliga nämnder. Enligt uppgift revideras riktlinjerna vid behov. Riktlinjerna planeras att revideras under våren 2022. Detta innebär att riktlinjerna för personuppgiftsbehandling inte kommer att ha reviderats över en period på fyra år.

Majoriteten av styrdokumenten har utarbetats av kommunstyrelsen. De övergripande riktlinjerna ska enligt arbetsmodellen brytas ner till mer detaljerade instruktioner och rutiner i respektive nämnd. Det är dock upp till respektive nämnd att välja vilka styrdokument som ska ärvas och vilka som ska utvecklas lokalt. Ansvaret för att säkerställa att kompletterande/nämndsspecifika styrdokument finns på plats och förblir aktuella ligger på respektive nämnd. I granskningen noterades att det saknas ett definierat tillvägagångssätt som säkerställer att styrdokumenten anpassas för respektive nämnd.

Organiseringen av arbetet med dataskyddsförordningen är dokumenterad i de övergripande riktlinjerna för behandling av personuppgifter. Kommunstyrelsen ansvarar för att ta fram kommungemensamma riktlinjer och rutiner. Respektive nämnd är dock personuppgiftsansvariga. Ansvaret för att tillse att dataskyddsarbetet sker i enlighet med gällande lagkrav är således fördelat på respektive nämnd. Därmed har också respektive

nämnd i uppgift att säkerställa att det finns ändamålsenliga rutiner. Likaså att tillse att de efterlevs.

Organisationen består av ett flertal funktioner. Dataskyddsombud (DSO), dataskyddssamordnare (DSS), dataskyddskoordinator (koordinator) och systemägare har särskilt ansvar för dataskyddsarbetet inom tjänstemannaorganisationen. DSO är en central roll för hela Malmö stad. Det är en av DSO:s uppgifter att stötta respektive samordnare och koordinator i frågor rörande dataskyddsförordningen. Likaså att granska efterlevnaden av dataskyddsförordningen. I granskningen framkom att DSO medverkat i framtagandet och implementationen av gällande rutiner.

Det framkommer att kommunen under sommaren 2021 saknade ett DSO. När ordinarie DSO var föräldraledig anlitade kommunen en extern konsult. Denne avslutade enligt uppgift sitt uppdrag i förtid varpå det uppstod en vakans till dess att ordinarie DSO återgick till arbetet.

Det framförs vid intervjuerna att det upplevs råda en resursbrist kopplat till arbetet med dataskyddsförordningen. Flertalet intervjuade representanter uttrycker också att de inte har möjlighet att utföra sina arbetsuppgifter ändamålsenligt på grund av tidsbrist. Därtill framkommer att systemägarskapet medför en mängd krav varav vissa inte kan uppfyllas på grund av bristande kunskaper och tid.

Det saknas ett centralt verktyg eller en process för att genomföra utbildningar kopplat till dataskyddsarbetet. Det är upp till respektive nämnd att planlägga, utforma, samt genomföra relevanta utbildningsinsatser. Det framkommer av intervjuer att de granskade nämnderna inte har genomfört strukturerade och regelbundna utbildningsinsatser kopplat till dataskyddsarbetet. Det saknas därtill en övergripande utbildningsplan.

Utbildningar har enligt uppgift genomförts sporadiskt. Det framförs vid intervju att det över en begränsad period anordnades utbildningar genom ett centralt utbildningsverktyg. Det har dock inte specificerats vilken period detta avsåg. Det har inte genomförts obligatoriska utbildningsinsatser för kommunens samtliga anställda, exempelvis vid nyanställning eller vid byte av anställning.

3.1.2. Bedömning

Det är vår bedömning att kommunstyrelsen och de granskade nämnderna har definierat och dokumenterat den övergripande organisationen för arbetsgången med tillhörande roller. Dock bedömer vi att det råder vissa oklarheter i ansvarsfördelningen mellan nämnder och kommunstyrelsen vilka inte är adresserade i gällande styrdokument. Därtill anser vi att styrdokument inte uppdateras med en tillräckligt hög frekvens för att förbli aktuella och riktiga över tid.

Det är inte säkerställt att dataskyddsombudet (DSO) kan agera självständigt utan eventuella intressekonflikter som kan uppstå av att granska sitt eget arbete. I granskningen har det även framkommit att dataskyddsrollerna inte är tillräckligt tydligt definierade. Det noteras att det råder delade meningar kring när DSO ska involveras i olika centrala processer så som begäran från registrerade, incidenthantering samt vid eventuell granskning. Det är därtill vår bedömning att det är problematiskt att kommunen saknade DSO en period under sommaren 2021.

Det är vår bedömning att kommunstyrelsen och de granskade nämnderna inte tillsett att utbildning av samtliga anställda sker systematiskt och i nödvändig utsträckning. Ansvaret för utbildning inom dataskydd och informationssäkerhet är inte reglerat i reglemente. Mot bakgrund av att respektive nämnd har ansvar sina egna behandlingar av personuppgifter kan ansvaret för utbildning indirekt också anses ligga på respektive nämnd. Det är dock vår erfarenhet att det är fördelaktigt om sådan utbildning hanteras centralt av kommunstyrelsen. Detta i syfte att säkerställa att samtliga anställda får en tillräcklig utbildning och medvetenhet kring vikten av dataskydd och informationssäkerhet.

Slutligen anser vi att kommunstyrelsen och de granskade nämnderna inte har säkerställt att det finns tillräckligt med resurser för att bedriva ett ändamålsenligt arbete. Vi lutar bedömningen på att det i flertalet intervjuer framförs att det saknas resurser för att bedriva dataskyddsarbetet i önskvärd och tillräcklig utsträckning. Mot bakgrund av omfattningen av de brister som framkommer i dataskyddsarbetet instämmer vi i denna beskrivning.

3.2. Personuppgiftsbehandling

I detta delkapitel besvaras följande revisionsfrågor:

- Säkerställs att dataskyddsombudet och/eller förvaltningarnas dataskyddssamordnare blir involverade vid styrelsens/nämndernas behandlingar av personuppgifter (exempelvis vid nya personuppgiftsbehandlingar vid inköp av nya IT-system)?
- Bedrivs ett aktivt och strukturerat dataskyddsarbete där dataskyddsfrågor beaktas vid befintliga och tillkommande behandlingar av personuppgifter?

3.2.1. Iakttagelser

Kommunstyrelsens och nämndernas arbete med att säkerställa ett ändamålsenligt dataskyddsarbete grundas i genomförandet av risk- och sårbarhetsanalyser. Dessa analyser baseras i sin tur på en dokumenterad rutin för inventering och klassificering av informationstillgångar. Rutinen beskriver vilka arbetsuppgifter som krävs för analysen, samt när en ny eller uppdaterad analys ska genomföras. Resultaten från analysen ligger till grund för vilka krav som ställs på de olika behandlingarna av personuppgifter och vilka kontroller som bör implementeras. Konsekvensbedömning ska exempelvis genomföras ifall

riskanalysen påvisar att behandlingen kan leda till en hög risk. Den som ansvarar för ett visst system (systemägare) är densamme som ansvarar för att tillse att riskanalyser och konsekvensbedömningar utförs. Vid behov kan DSO och samordnare involveras i den riskanalys som utförs vid klassificering, men det finns inget dokumenterat krav på att de måste deltaga. Det framförs att det finns en skriftlig mall men att denna kommer att vidareutvecklas så att den passar Malmö stads dataskydds- och informationssäkerhetsarbete.

Det framkommer att ett arbete med att föra över registerförteckningar till ett stadsgemensamt systemstöd har påbörjats. Syftet är att underlätta löpande uppföljning av arbetet. I dagsläget hanterar dock de flesta nämnderna registerförteckningar i Excel. Det finns en skriftlig instruktion för handläggning av registerförteckningar, men det har under intervjuer framgått att alla registerförteckningar dock inte är uppdaterade. Det sker ingen uppföljning som säkerställer efterlevnad i praktiken.

Det finns arkivbestämmelser som specificerar när gallring ska ske. Det finns dock ingen formell kontroll som säkerställer att gallring av personuppgifter verkställs i enlighet med arkivbestämmelserna. Samordnarna ansvarar för att kontrollera registerförteckningarnas riktighet. DSO använder sig utav registerförteckningar som ett verktyg för uppföljning av dataskyddsarbetet. En behandlings ändamål ska fastställas och dokumenteras innan personuppgiftsbehandling påbörjas samt uppdateras vid förändrade omständigheter. Det finns dock ingen systematik för att kontrollera efterlevnad i praktiken. DSO har följt upp behandlingars ändamål på olika sätt inom ramen för sitt uppdrag, exempelvis genom kontroll av ändamålsbeskrivningar i registerförteckningen. Det finns dock ingen dokumenterad plan eller process som beskriver hur och när DSO granskar att behandlingar sker på rätt grund.

Begreppen *laglig grund* och *ändamålsbeskrivning* för insamlade personuppgifter behandlas under så kallade nätverksträffar. Träffar anordnas för dataskyddssamordnare och informationssäkerhetssamordnare. Vid träffarna lyfts frågor kring lagstiftning och uppdateringar diskuteras. Träffar för informationssäkerhetssamordnare anordnas åtta gånger per år, samt en timma varje fredag för praktiska frågor.

Det framkommer att en omfattande del av ansvaret för att genomföra kontroller kopplat till dataskyddsarbetet faller på systemägare. Dessa upplever dock att de i stor utsträckning saknar nödvändig kunskap för att genomföra sådana kontroller. Det saknas exempelvis dokumenterade instruktioner för hur behörighetskontroller ska genomföras i praktiken. Rutiner för hantering av begäran från registrerade finns men det saknas tydliga instruktioner som beskriver hur de appliceras i praktiken. Exempelvis framgår det ej vem som ansvarar för respektive steg, hur man kommer fram till att en registrerad har rätt till begränsning eller vilka tekniska åtgärder som kan vidtas för att säkerställa att uppgifter begränsas.

3.2.2. Bedömning

Det är vår bedömning att det finns tillräckliga kommungemensamma rutiner för hur risk- och sårbarhetsanalyser ska genomföras. Vi anser dock inte att de granskade nämnderna har säkerställt att riskanalyser och konsekvensbedömningar genomförs strukturerat och i enlighet med dokumenterade rutiner.

Kommunstyrelsen och nämnderna har ej heller säkerställt att registerförteckningarna är kompletta samt förblir riktiga över tid. Det saknas en komplett bild över samtliga behandlingar inom kommunen med tillhörande risker. Därmed är det en risk att implementerade skyddsåtgärder och kontroller inte motsvarar eller möjliggör en ändamålsenlig personuppgiftshantering.

3.3. Kontroll och uppföljning

I detta delkapitel besvaras följande revisionsfrågor:

- Genomförs kontroll, uppföljning och återrapportering av Malmö stads dataskyddsarbete?
- Hanteras personuppgiftsincidenter i enlighet med lagkrav och Malmö stads riktlinjer? Är Malmö stads riktlinjer för att hantera personuppgiftsincidenter tillräckliga?

3.3.1. Iakttagelser

Det finns centralt framtagna rutiner för hantering av incidenter vilka riktar sig till kommunens medarbetare och chefer. Respektive nämnd har därtill möjlighet att ta fram egna rutiner om så behövs. Varje verksamhet ansvarar för att dokumentera de incidenter som uppkommit inom den egna verksamheten.

När en incident identifierats ska den utan onödigt dröjsmål anmälas till närmsta chef eller till stadens systemstöd för incidenthantering. Chefen som mottagit anmälan ska rådgöra med förvaltningens dataskyddssamordnare. Samordnare avgör om ärendet ska meddelas vidare till DSO för bedömning om anmälan till IMY. Incidenter ska enligt rutinerna alltid dokumenteras. I granskningen framkommer dock att samtlig information inte alltid loggas. Det har ej heller säkerställts att rutinen för incidenthantering efterlevs i praktiken.

Det har inte genomförts någon strukturerad granskning eller uppföljning av arbetet kopplat till dataskyddsförordningen. Det är upp till respektive nämnd att internt följa upp sitt arbete samt att bestämma hur uppföljning av dataskyddsarbetet ska gå till.

DSO arbetar inte utefter en fastställd och dokumenterad granskningsplan för att säkerställa efterlevnad av dataskyddsförordningen. DSO inhämtar information på flera olika sätt, exempelvis genom uppföljningsmöten och nätverksträffar, granskning av

registerförteckningar, insamling av material avseende dataskyddsarbetet, juridisk rådgivning samt genom att lämna synpunkter på genomförda konsekvensbedömningar. Det har inte säkerställts att samtliga dokumenterade rutiner efterlevs i praktiken, eller att definierade kravställningar uppfylls.

Personuppgiftsbiträdesavtal (PUB-avtal) tecknas med nya leverantörer (tredje part). Systemägarna följer upp eventuella problem med leverantörer. Det saknas dock en dokumenterad rutin för att säkerställa att tredjeparter lever upp till dataskyddsförordningen. Därtill framkommer att det inte genomförts systematiska uppföljningar av tredjeparters efterlevnad av dataskyddsförordningen eller kommunens definierade krav.

Rapportering av dataskyddsarbetet sker i dagsläget sporadiskt och huvudsakligen informellt via nätverksträffar. Det finns inga dokumenterade krav att samordnare regelbundet ska rapportera till DSO. I granskningen har det också framkommit att det råder oklarheter om vad som ska rapporteras i samband med dataskyddsarbetet och till vem detta ska rapporteras.

3.3.2. Bedömning

Det är vår bedömning att kommunstyrelsen och nämnderna inte har säkerställt att kontroller och uppföljning av arbetet med dataskyddsförordningen sker i nödvändig utsträckning. Kontroll och uppföljning sker i dagsläget sporadiskt och utan grund i dokumenterad plan. Då det ej heller genomförs strukturerade granskningar av efterlevnaden finns det en risk att rutiner och processer inte efterlevs i praktiken.

Det är därtill vår bedömning att kommunstyrelsen och nämnderna inte har säkerställt en tillräcklig rapportering kopplat till dataskyddsarbetet. Detta medför att en risk att dataskyddsarbetet inte får den synlighet och de resurser som krävs för att bedrivas ändamålsenligt.

Det är vår bedömning att riktlinjen för hantering av personuppgiftsincidenter är tillräcklig och följer lagkraven. Det är däremot vår bedömning att riktlinjerna inte efterföljs för samtliga incidenter.

4. Samlad bedömning

Granskningens syfte har varit att bedöma om kommunstyrelsen, servicenämnden, funktionsstödsnämnden och gymnasie- och vuxenutbildningsnämnden säkerställer ett ändamålsenligt dataskyddsarbete. Den sammanfattande bedömningen är att kommunstyrelsen och de granskade nämnderna inte i tillräcklig utsträckning har säkerställt att dataskyddsarbetet bedrivs ändamålsenligt. Det är vår bedömning att det finns en övergripande organisation och arbetsgång med tillhörande roller. Det finns bland annat rutiner för risk- och sårbarhetsanalyser och riktlinjer för personuppgiftsincidenter. Trots detta råder oklarheter mellan kommunstyrelsen och nämnderna vad avser ansvaret för dataskyddsarbetet. Likaså är det inte säkerställt att dataskyddsombudet står utan intressekonflikt i granskning av eget arbete. Bedömningen grundar sig vidare på att kommunstyrelsen och nämnderna inte säkerställt att riskanalyser och konsekvensbedömningar genomförs på ett strukturerat sätt, samt att registerförteckningarna är kompletta. Därtill anser vi att kommunstyrelsen och nämnderna saknar tillräckliga kontroller, uppföljning och rapportering av dataskyddsarbetet. Avslutningsvis menar vi att utbildningsinsatserna för samtliga anställda är otillräckliga. Det saknas enligt vår mening ett systematiskt arbete som säkerställer en god kunskapsnivå avseende dataskydd och informationssäkerhet.

4.1. Samlad bedömning per nämnd och kommunstyrelsen

I bilaga 1 återfinns detaljerade granskningsresultat per nämnd och kommunstyrelsen. Kommunstyrelsen och nämnderna har däri bedömts baserat på deras respektive arbete med dataskydd och informationssäkerhet. De samlade bedömningarna är:

Kommunstyrelsen

Det är vår bedömning att kommunstyrelsen behöver stärka dataskyddsarbetet. Kommunstyrelsen uppvisar dock enligt vår mening goda ambitioner till fortsatt utveckling av dataskyddsarbete. Kommunstyrelsen har genomfört omstruktureringar inom organisationen för att utöka bemanningen av personal med kunskap inom dataskyddsfrågor vid kommunens nämnder/förvaltningar. Kommunstyrelsen har därtill utarbetat ett flertal relevanta kommungemensamma styrdokument och rutiner i enlighet med sitt samordnande ansvar. Det har däremot inte säkerställts att nämnderna och dess förvaltningar får det stöd de behöver för att anpassa kommungemensamma styrdokument och rutiner till den egna verksamheten. Detta är nödvändigt för att på lång sikt bedriva ett ändamålsenligt dataskyddsarbete. Det finns en god förståelse för vikten av informationsklassificering och riskarbete men det saknas enligt vår bedömning en rutin för att säkerställa efterlevnad över tid.

Kommunstyrelsen har inte säkerställt att det finns tillräckligt med resurser för att bedriva ett ändamålsenligt dataskyddsarbete. Vidare saknas det en dokumenterad rutin som säkerställer att kommungemensamma riktlinjer och styrdokument förblir riktiga och uppdaterade över tid. Slutligen har det under granskningen framkommit att det saknas definierade planer för hur arbetet med granskning och utbildning ska bedrivas. Det är enligt vår bedömning och erfarenhet av vikt att kommunstyrelsen centralt säkerställer att utbildningsplan upprättas och utbildningsinsatser genomförs för samtliga anställda. Likaså att kommunstyrelsen tar fram fler kommungemensamma instruktioner för behörighetskontroller.

Enligt EY:s granskningsmetodik bedöms kommunstyrelsen uppnå en mognadsgrad för dataskyddsarbetet på 2,61 av 5 (se mer i bilaga 1). Det är vår bedömning att mognadsgraden är låg sett till kommunens storlek, riskbild samt den mängd personuppgifter som kommunstyrelsen är ansvarig för.

Servicenämnden

Det är vår bedömning att servicenämnden behöver stärka sitt dataskyddsarbete. Vi noterar att det finns en god förståelse för vikten av att genomföra riskanalyser och konsekvensbedömningar. Likaså vikten av att utbilda sin personal inom dataskyddsfrågor. Samtidigt som nämnden uppvisar goda ambitioner finns det i dagsläget ett flertal förbättringsområden relaterat till dataskyddsarbetet. Serviceförvaltningen har enligt vår mening inte tillräckligt med resurser för att bedriva ett önskvärt och ändamålsenligt dataskyddsarbete. Detta framförallt avseende det kontinuerliga riskhanteringsarbetet och granskningen av regelverkens efterlevnad. Nämnden bör säkerställa att det genomförs riskanalyser kopplat till samtliga IT-system, samt konsekvensbedömningar för de behandlingar där det anses vara relevant.

Enligt EY:s granskningsmetodik bedöms servicenämnden uppnå en mognadsgrad för dataskyddsarbetet på 2,47 av 5 (se mer i bilaga 1). Det är vår bedömning att mognadsgraden är låg sett till kommunens storlek, riskbild samt den mängd personuppgifter som nämnden är ansvarig för.

Gymnasie- och vuxenutbildningsnämnden

Det är vår bedömning att gymnasie- och vuxenutbildningsnämnden behöver stärka sitt dataskyddsarbete. Nämnden behöver däri förbättra arbetet med att anpassa kommungemensamma styrdokument och rutiner till den egna verksamheten samt säkerställa dess efterlevnad. Det finns även ett behov av att se över rutinerna för incidenthantering då det inte är säkerställt att de efterlevs i praktiken. Nämnden har enligt vår mening inte säkerställt att samtliga behandlingar finns dokumenterade i registerförteckningen samt att de förblir riktiga över tid. Det har även identifierats att riskanalyser och konsekvensbedömningar inte har kunnat utföras enligt dokumenterad rutin. Nämnden bör också tillse att registerförteckningen är komplett, samt att risk- och konsekvensbedömningar sker

systematiskt och enligt dokumenterade rutiner. Det är avslutningsvis vår bedömning att nämnden inte säkerställt att förvaltningen har de nödvändiga resurserna för att bedriva ett önskvärt och ändamålsenligt dataskyddsarbete.

Enligt EY:s granskningsmetodik bedöms servicenämnden uppnå en mognadsgrad för dataskyddsarbetet på 2,42 av 5 (se mer i bilaga 1). Det är vår bedömning att mognadsgraden är låg sett till kommunens storlek, riskbild samt den mängd personuppgifter som nämnden är ansvarig för.

Funktionsstödsnämnden

Det är vår bedömning att funktionsstödsnämnden behöver stärka sitt dataskyddsarbete. Nämnden har enligt vår mening inte i tillräcklig utsträckning anpassat kommungemensamma styrdokument och rutiner för den egna verksamheten, eller säkerställt dess efterlevnad. Det är därtill av vikt att nämnden tillser att riskanalyser och konsekvensbedömningar genomförs enligt dokumenterade rutiner. Likaså att registerförteckningen är komplett samt förblir riktig över tid. Det finns enligt vår bedömning ett behov av att se över rutinen för incidenthantering då det inte är styrkt att den efterlevs i praktiken. Slutligen är det vår bedömning att nämnden inte säkerställt att förvaltningen har de nödvändiga resurserna för att bedriva ett ändamålsenligt dataskyddsarbete.

Enligt EY:s granskningsmetodik bedöms servicenämnden uppnå en mognadsgrad för dataskyddsarbetet på 2,47 av 5 (se mer i bilaga 1). Det är vår bedömning att mognadsgraden är låg sett till kommunens storlek, riskbild samt den mängd personuppgifter som nämnden är ansvarig för.

4.2. Svar på revisionsfrågor

I nedan tabell besvaras revisionsfrågorna. Utförligare svar på kommunstyrelsens och nämndernas dataskydds- och informationssäkerhetsarbete ges tillsammans med mognadsbedömning enligt EY:s modell i bilaga 1.

Revisionsfråga	Svar
Har dataskyddsarbetet inom Malmö stad organiserats på ett tydligt och ändamålsenligt sätt? Bedrivs ett effektivt arbete?	Delvis. *Kommunstyrelsen:* Dataskyddsarbetet är organiserat med en central DSO, samt dataskyddssamordnare på respektive förvaltning. DSO agerar som stöd till de olika samordnarna och samarbetet beskrivs övergripande fungera bra. Det finns dock ett antal

	områden som kommunstyrelsen och de granskade nämnderna bör adressera. I vissa fall är ansvarsfördelningen mellan DSO och samordnare inte helt tydligt, exempelvis kopplat till granskning, framtagning av styrdokument samt rapportering. Det är vår uppfattning av en mer centraliserad hantering av dataskyddsarbetet är mer effektiv och ändamålsenlig. *Samtliga nämnder:* Nämnderna förlitar sig i hög utsträckning på processer, rutiner och arbetssätt från kommunstyrelsen. I varierande grad har man tagit fram anpassade varianter av dessa, men resursbrist gör ofta att arbetet inte når en tillräckligt hög nivå. När varje förvaltning själva ska ta fram sina processer och rutiner blir det mindre effektivt än om en större del av arbetet gjorts centralt.
Är de olika rollerna i Malmö stads dataskyddsarbete tydliga?	Delvis. *Kommunstyrelsen och samtliga nämnder:* Rollerna kopplade till dataskyddsarbetet har definierats och dokumenterats. Det är dock inte säkerställt att befintliga rollbeskrivningar efterlevs i praktiken. I granskningen framkommer att det råder viss osäkerhet i relation till ansvarsfördelningen samt när olika roller ska involveras och inte. Det är därför vår bedömning att den nuvarande beskrivningen av roller inte är tillräckligt tydlig för att säkerställa ett systematiskt och standardiserat arbetssätt.
Avsätts tillräckliga resurser (exempelvis personella och ekonomiska) för ett tillräckligt dataskyddsarbete?	Nej. *Kommunstyrelsen och samtliga nämnder:* I granskningen framkommer att de intervjuade upplever att det saknas resurser för att bedriva ett önskvärt dataskyddsarbete. Exempelvis saknas resurser för att kunna säkerställa att systemägare har den kunskap och tid som

	behövs för att leva upp till definierad kravställning.
Bedrivs ett aktivt och strukturerat dataskyddsarbete där dataskyddsfrågor beaktas vid befintliga och tillkommande behandlingar av personuppgifter?	Delvis. *Kommunstyrelsen och samtliga nämnder:* I granskningen noteras att kommunstyrelsen och nämnderna bedriver ett strukturerat dataskyddsarbete vid nya behandlingar av personuppgifter och vid upphandling av nya system. Det saknas dock systematik och dokumenterade processer för att över tid granska efterlevnad av riktlinjer och rutiner för befintliga behandlingar och IT-system.
Säkerställs att dataskyddsombudet och/eller förvaltningarnas dataskyddssamordnare blir involverade vid styrelsens/nämndernas behandlingar av personuppgifter (exempelvis vid nya personuppgiftsbehandlingar vid inköp av nya IT-system)?	Delvis. *Kommunstyrelsen och samtliga nämnder:* I de kommungemensamma riktlinjerna beskrivs att dataskyddssamordnare bör involveras inom samtliga steg i ett systems livscykel gällande klassificering. I granskningen framkommer dock att det inte säkerställts att registerförteckningar är kompletta. Således går det inte att bekräfta att DSO eller samordnare har översikt över, samt varit involverade i, samtliga behandlingar.
Hanteras personuppgiftsincidenter i enlighet med lagkrav och Malmö stads riktlinjer? Är Malmö stads riktlinjer för att hantera personuppgiftsincidenter tillräckliga?	Delvis. *Kommunstyrelsen och samtliga nämnder:* Det finns en central rutin för hantering av personuppgiftsincidenter i enlighet med lagkrav. Rutinen har dock inte anpassats utifrån respektive nämnds förutsättningar. Det har ej heller säkerställts att de dokumenterade rutinerna efterlevs i praktiken.

Genomförs kontroll, uppföljning och återrapportering av Malmö stads dataskyddsarbete?	Nej. Det finns ett flertal dokumenterade rutiner och styrdokument. Det är dock inte säkerställt att dessa efterlevs i praktiken. *Kommunstyrelsen:* Viss granskning och uppföljning har genomförts. Det saknas dock en definierad granskningsplan som arbetet med granskning och uppföljning är baserat på. *Samtliga nämnder:* Mycket begränsad granskning och uppföljning sker. Vid de tillfällen någon form av uppföljning gjort så är det initierat från kommunstyrelsen. Granskningsplan eller liknande saknas helt.

4.3. Våra rekommendationer

I detta avsnitt presenteras rekommendationerna baserat på genomförd granskning. Rekommendationerna presenteras dels övergripande för kommunstyrelsen och nämnderna, dels per granskad nämnd. De övergripande rekommendationerna avser de främsta riskerna för hela stadens arbete med dataskydds- och informationssäkerhetsarbetet. Våra rekommendationer kategoriseras efter vilka som bör prioriteras i ett *inledande* skede och vilka som *därefter* bör genomföras. För mer information om respektive rekommendation, se bilaga 1.

Kommunstyrelsen och samtliga granskade nämnder rekommenderas att:

Inledningsvis:

- Utarbeta en tydlig plan för granskning och uppföljning av arbetet med dataskyddsförordningen.
- Tillse att ansvarsfördelningen i arbetet kopplat till dataskyddsförordningen är tydligt definierad samt efterlevs i praktiken.

Därefter:

- Utveckla rutinen för klassificering av informationstillgångar med avseende på ostrukturerad data. Utarbeta en dokumenterad rutin för uppföljning av registerförteckningens riktighet och fullständighet över tid.

- Utarbeta rutiner som över tid säkerställer att personuppgifter endast behandlas för det eller de ändamål som de samlades in för.
- Utarbeta dokumenterade rutiner för att säkerställa att personuppgiftsbiträden och leverantörer uppfyller och agerar i enlighet med dataskyddsförordningen över tid.
- Säkerställa tillräcklig kontroll över att incidenthanteringsrutinen efterlevs i praktiken.

Kommunstyrelsen rekommenderas att:

Inledningsvis:

- Säkerställa att styrdokument förblir riktiga och aktuella över tid.
- Utarbeta instruktioner till systemägare för hur behörighetskontroller ska genomföras.
- Säkerställa att utbildningar inom dataskyddsarbetet genomförs regelbundet för kommunens samtliga anställda utefter en dokumenterad utbildningsplan.

Därefter:

- Vidareutveckla rutinen för genomförande av konsekvensbedömningar och säkerställ att rutinen efterlevs i praktiken. Säkerställa att riskanalyser sker kontinuerligt och i enlighet med dokumenterade rutiner.
- Utarbeta en dokumenterad rutin som säkerställer regelbunden och ändamålsenlig rapportering av dataskyddsarbetet.
- Tillse att DSO-rollen är tydligt definierad och att dess arbetsuppgifter saknar intressekonflikter.
- Säkerställa att DSO ges resurser och möjlighet att stötta funktionsstödsnämnden i den utsträckning som behövs.

Servicenämnden rekommenderas att:

Inledningsvis:

- Strukturerat genomföra riskanalyser och konsekvensbedömningar enligt dokumenterad rutin.
- Tillse att registerförteckningen är komplett samt förblir uppdaterad över tid.
- Tillse att systemägare har den kunskap och tid som krävs för att utföra ålagda arbetsuppgifter.
- Säkerställa att det finns tillräckligt med resurser för att utföra ett ändamålsenligt arbete kopplat till dataskyddsförordningen.

Därefter:

- Utarbeta dokumenterade rutiner som säkerställer att gallring av personuppgiftsbehandlingar verkställs inom satt tidsram.
- Utarbeta dokumenterad rutin för hur behörighetskontroller ska genomföras i servicenämndens IT-system.

Gymnasie-och vuxenutbildningsnämnden rekommenderas att:

Inledningsvis:

- Tillse att registerförteckningen är komplett samt förblir uppdaterad över tid.
- Utarbeta en rutin som säkerställer att centralt framtagna styrdokument anpassas utefter den egna verksamheten.
- Strukturerat genomföra riskanalyser och konsekvensbedömningar enligt dokumenterad rutin.
- Säkerställa att det finns tillräckligt med resurser för att utföra ett ändamålsenligt arbete kopplat till dataskyddsförordningen.

Därefter:

- Ta fram en rutin för att säkerställa att gallring av personuppgiftsbehandlingar utförs enligt definierad process.
- Utarbeta en dokumenterad rutin för hur systemägare ska utföra behörighetskontroller i gymnasie- och vuxenutbildningsnämndens IT-system.
- Ta fram och dokumentera en rutin för att säkerställa att tillräcklig information loggas i samband med incidentrapportering.

Funktionsstödsnämnden rekommenderas att:

Inledningsvis:

- Strukturerat genomföra riskanalyser och konsekvensbedömningar enligt dokumenterad rutin.
- Tillse att registerförteckningen är komplett samt förblir uppdaterad över tid
- Säkerställa att det finns tillräckligt med resurser för att utföra ett ändamålsenligt arbete kopplat till dataskyddsförordningen
- Definiera en rutin som säkerställer att centralt framtagna styrdokument anpassas utefter den egna verksamheten.

Därefter:

- Ta fram en rutin för att säkerställa att gallring av personuppgifter utförs enligt definierad process.
- Utarbeta en dokumenterad rutin för hur systemägare ska utföra behörighetskontroller i nämndens IT-system.
- Ta fram en rutin för att genomföra periodiska granskningar av höga behörigheter i nämndens IT-system.

5. Bilaga 1: Detaljerade granskningsresultat

Nedan följer en beskrivning av den övergripande nulägesbild och iakttagelser per område som har identifierats under granskningens utförande.

5.1. Kommunstyrelsen

Baserat på utförd granskning konstateras att kommunstyrelsens mognadsgrad är genomsnittlig för personuppgiftshantering jämfört med vad EY generellt observerar i en offentlig verksamhet av motsvarande storlek och karaktär. Kommunstyrelsens mognadsgrad uppnår en summa av 2,61 av 5,00. Det är trots detta vår bedömning att mognadsgraden är låg sett till kommunens storlek, riskbild samt den mängd personuppgifter som kommunstyrelsen är ansvarig för.

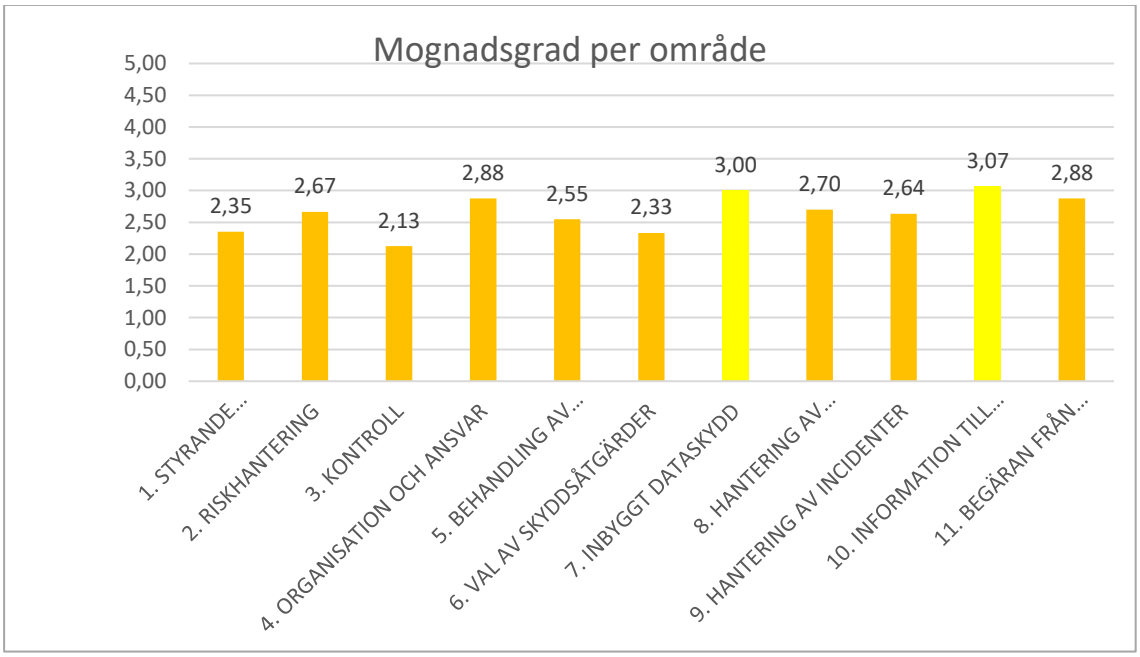
Det är vår bedömning att kommunstyrelsen behöver stärka dataskyddsarbetet. Kommunstyrelsen uppvisar dock enligt vår mening goda ambitioner till fortsatt utveckling av dataskyddsarbete. Kommunstyrelsen har genomfört omstruktureringar inom organisationen för att utöka bemanningen av personal med kunskap inom dataskyddsfrågor vid kommunens nämnder/förvaltningar. Kommunstyrelsen har därtill utarbetat ett flertal relevanta kommungemensamma styrdokument och rutiner i enlighet med sitt samordnande ansvar. Det har däremot inte säkerställts att nämnderna och dess förvaltningar får det stöd de behöver för att anpassa kommungemensamma styrdokument och rutiner till den egna verksamheten. Detta är nödvändigt för att på lång sikt bedriva ett ändamålsenligt dataskyddsarbete. Det finns en god förståelse för vikten av informationsklassificering och riskarbete men det saknas enligt vår bedömning en rutin för att säkerställa efterlevnad över tid.

Kommunstyrelsen har inte säkerställt att det finns tillräckligt med resurser för att bedriva ett ändamålsenligt dataskyddsarbete. Vidare saknas det en dokumenterad rutin som säkerställer att kommungemensamma riktlinjer och styrdokument förblir riktiga och uppdaterade över tid. Slutligen har det under granskningen framkommit att det saknas definierade planer för hur arbetet med granskning och utbildning ska bedrivas. Det är enligt vår bedömning och erfarenhet av vikt att kommunstyrelsen centralt säkerställer att utbildningsplan upprättas och utbildningsinsatser genomförs för samtliga anställda. Likaså att kommunstyrelsen tar fram fler kommungemensamma instruktioner för behörighetskontroller.

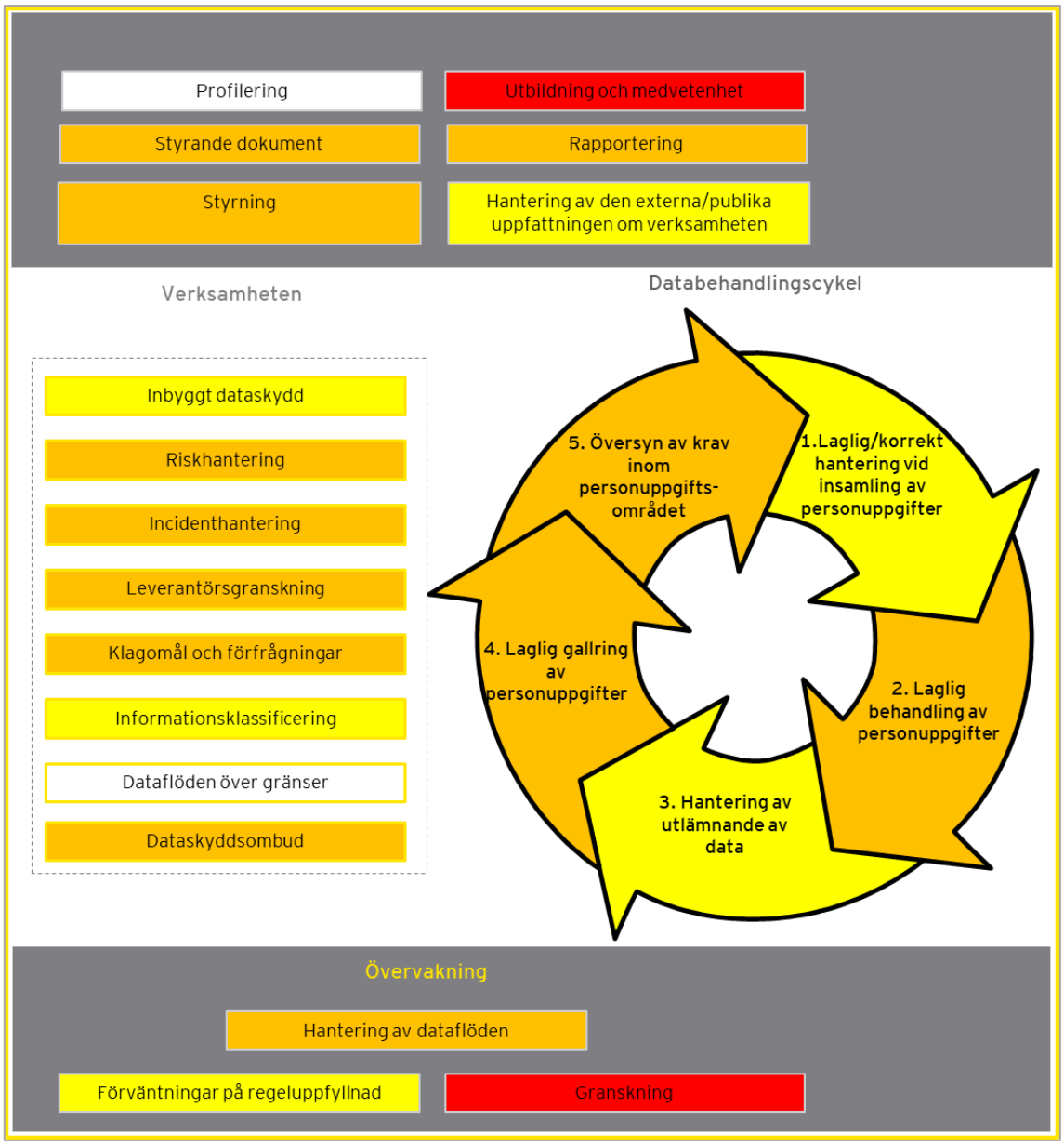
Översiktsbilderna nedan redovisar kommunstyrelsens mognadsgrad för de 12 huvudområden som granskats, samt nedbrutet på 22 underområden.

Nivå 5 representerar hög mognadsgrad medan nivå 1 representerar låg mognadsgrad. Mognadsgrad beskrivs på en standardiserad skala enligt nedan:

1. Begynnande – Det finns ingen dokumentation eller uppföljning, händelser hanteras ad hoc.
2. Upprepbar – Viss grundläggande dokumentation finns, men denna kan variera mellan olika enheter och vara bristfällig i sin omfattning och tillämpning.
3. Definierad – Det finns dokumenterade processer och dessa tillämpas i stor mån genom hela organisationen.
4. Förvaltad – Förutom väl dokumenterade processer som tillämpas i hela organisationen, finns det dessutom ett system för uppföljning.
5. Optimerad – Baserat på uppföljningen finns också rutiner för kontinuerlig förbättring och uppdatering av processer och ramverk.



Figur 1: Mognadsgrad per område



Figur 2: Grafisk överblick av mognadsgrad per område (notera att de 12 huvudområdena är uppdelade i ytterligare detalj)

Mognadsgraden beskrivs enligt den standardiserade skalan med respektive färgkod. De områden som inte var tillämpliga för granskningen är vita.

5.1.1. Nuläge och iakttagelser

Nedan följer en beskrivning av den övergripande nulägesbild och iakttagelser per område som har identifierats under granskningens utförande.

Tabell 1: Observationer inom de 12 områdena

Område	Nuläge	Iakttagelser	Mognad
Styrande dokument/ styrning	Informationssäkerhet faller inom ramen för kommunens övergripande säkerhetspolicy. Malmö stad har således ingen övergripande informationssäkerhetspolicy men har kommungemensamma riktlinjer för informationssäkerhet. *"Riktlinjer och anvisningar för informationssäkerhet i Malmö stad"* fastställdes av kommunstyrelsen 2013 och har därefter uppdaterats nästan varje år, senast 2019. Enligt riktlinjerna är det Malmö stads trygghets- och säkerhetsdirektör som ansvarar för att se till att riktlinjerna granskas och revideras varje år samt respektive ansvarig verksamhet som ansvarar för att informationssäkerheten upprätthålls och efterlevs. Befattningen som trygghets- och säkerhetsdirektör försvann dock ur organisationen för flera år sedan. Enligt intervjuade nyckelpersoner är en revidering av riktlinjerna för informationssäkerhet på gång och är planerade att antas i kommunstyrelsen under Q1 2022. Kommunen saknar i dagsläget en informationssäkerhetspolicy. Malmö stads *"Riktlinjer för behandling av personuppgifter i Malmö stad"* fastställdes av kommunstyrelsen i maj 2018, i samband med att GDPR-kraven började gälla. Riktlinjerna gäller för samtliga nämnder och helägda bolag. Respektive nämnd är personuppgiftsansvariga för sina respektive verksamhetsområden. Revidering av riktlinjerna ska ske vid behov och enligt intervjuade nyckelpersoner ska nästa revidering ske under våren 2022.	Det saknas en informationssäkerhetspolicy som är uppdaterad i enlighet med kraven i dataskyddsförordningen. Riktlinjer för personuppgiftsbehandling uppdateras med för låg frekvens för att förbli uppdaterade och riktiga över tid.	2,35

	Det finns ett centralt dataskyddsombud (DSO) för hela kommunen samt utsedda dataskyddssamordnare inom respektive förvaltning. Under juli månad 2021 fanns inget formellt DSO i tjänst. Centralt framtagna rutiner ska enligt de intervjuade ses över minst en gång per år samt vid behov. Nämnderna ska följa de centralt framtagna rutinerna men kan frångå dem om de motiverar varför.		
Risk-hantering	Enligt Malmö stads riktlinjer för informationssäkerhet ska verksamheter alltid beakta ett riskbaserat arbetssätt och bedöma den risk som uppkommer vid informationshantering. Det ska finnas en centralt framtagen metod för genomförande av risk- och sårbarhetsanalyser, vilken refereras till konsekvensbedömning gällande personuppgiftshantering. I *”Riktlinjer för behandling av personuppgifter i Malmö stad”* ingår en checklista över åtgärder som ska vidtas innan personuppgiftbehandling påbörjas. Där nämns att samråd ska ske med tillsynsmyndigheten om konsekvensbedömningen visar att behandlingen leder till hög risk för enskilda personers fri- och rättigheter. I de fall behandlingen leder till hög risk ska det enligt intervjuade nyckelpersoner finnas en riskanalys att stödja sig mot och därefter ska minimerande aktiviteter tas fram för att minska eventuella risker. Utöver registerförteckningar ska även diarieförda konsekvensbedömningar finnas. Enligt intervjuade nyckelpersoner på stadskontoret ses den informationsklassificering som utförs vid nya och förändrande behandlingar som en grundläggande riskanalys. I de fall klassificeringen inkluderar särskilda kategorier av personuppgifter ska en kompletterande konsekvensbedömning genomföras. Det finns en skriftlig mall. Det uppges att denna kommer att vidareutvecklas så att den passar Malmö stads informationssäkerhetsarbete. Den som	Det finns en dokumenterad rutin för genomförande av riskanalyser och en mall för genomförande av konsekvensbedömningar, men det behöver utvecklas tydligare instruktioner för att säkerställa att riskanalyser och konsekvensbedömningar utförs enligt definierade rutiner. Kommunstyrelsen har inte säkerställt att riskanalyser sker kontinuerligt och i enlighet med dokumenterade rutiner.	2,67

	ansvarar för ett visst system ansvarar för att riskanalyser utförs. Vid anskaffning av nytt system är enhetschefen ansvarig att tillse att riskanalys utförs. Vid anskaffning av kommungemensamt system samarbetar flera roller och funktioner från Malmö stad med klassificeringen. Informationsklassificeringen beskrivs i Malmö stads rutin för inventering och klassificering av informationstillgångar där informationens känslighet bedöms utifrån fyra kriterier och fyra kravnivåer. Klassificeringar ska genomföras under hela livscykeln. Enligt de intervjuade på stadskontoret fångas eventuella risker upp i samband med de nätverksträffar som anordnas bland förvaltningarna. Det finns ett riskbaserat tänk och rutiner för informationsklassificering. Det finns dock ett behov av att ta fram tydligare instruktioner på hur riskanalyser ska genomföras. Det finns ingen dokumenterad plan på när och hur generella riskanalyser ska genomföras utöver de analyser som utförs vid klassificering av specifik information och/eller system. Malmö stads strategiska samordnare-informationssäkerhet sammanställer frågor och aktiviteter från nämnderna och förvaltningarna i en aktivitetsplan som revideras två gånger per år.		
Kontroll	Det saknas dokumenterade rutiner för rapportering av nämndernas status för dataskyddsarbetet. Nämnderna ska följa upp sitt eget arbete internt och det är upp till respektive nämnd att bestämma hur uppföljning ska gå till. Det finns inga krav på rapportering till kommunstyrelsen eller DSO, men DSO följer upp verksamheternas arbete inom ramen för sin roll. Kommunstyrelsen har ingen fastslagen granskningsplan för att utvärdera och säkerställa att styrdokument efterlevs och att kommunen uppfyller relevanta krav på hantering av personlig information. Dock ska relevanta krav fångas upp vid	Det finns ingen dokumenterad rutin som säkerställer regelbunden och ändamålsenlig rapportering av dataskyddsarbetet. Det saknas en dokumenterad granskningsplan för att säkerställa efterlevnad av dataskyddsförordningen.	2,13

	informationsklassificeringen. Inom ramen för intern kontroll finns det stadsövergripande frågor där rapportering sker från granskad nämnd till kommunstyrelsen. Enligt riktlinjer för informationssäkerhet kan metodiken för uppföljning variera beroende på verksamhet men det finns inga dokumenterade rutiner för hur sådan uppföljning ska gå till. Enligt intervjuade nyckelpersoner anordnar Malmö stads DSO uppföljningsmöten med nämnderna/förvaltningarna för att följa upp deras arbete inom dataskydd. Det generella arbetet sker således i dagsläget genom samtal med samordnare och övriga anställda utifrån vad DSO anser vara viktigt. Det anordnas även nätverksträffar för dataskyddssamordnare och informationssäkerhetssamordnare där exempelvis aktuella frågor kring lagstiftning lyfts och uppdateringar diskuteras. Nätverksträffarna för dataskyddssamordnarna anordnas fyra gånger om året, där två sker på hösten och två på våren. Inom informationssäkerhetsarbetet görs en uppföljning av hur samordnare har arbetat utifrån sin roll, i samband med nätverksträffarna. Enligt intervjuade nyckelpersoner genomfördes en analys av vilka områden och nämnder/förvaltningar som var i behov av stöd i sitt dataskyddsarbete i samband med dataskyddsförordningens införande i maj 2018. Ingen ytterligare analys eller granskning av dataskyddsarbetet har skett efter det. Däremot har två externa granskningar (utförda av PWC respektive KPMG) av IT-området skett under det senaste året. Malmö stads centrala informationssäkerhetssamordnare följer upp resultatet från granskningarna i en aktivitetsplan som revideras två gånger per år, dock är fokus mer på verktyg för klassificering och huruvida det stämmer överens med gällande lagstiftning		
Organisation och ansvar	Kommunstyrelsen har tagit fram ett dokument kallat *”Dataskyddsförordningen – Roller och ansvar”* där beskrivningar av ett flertal olika roller kopplat till dataskyddsarbetet framgår. Vi		2,88

	intervju framfördes att omvärldsbevakning ingår i DSO:s roll och att denne följer aktuell rättspraxis inom Europa samt förmedlar vidare viktig information till dataskyddssamordnarna i förvaltningarna. Respektive nämnd är personuppgiftsansvariga för respektive verksamhetsområde och ansvarar för att tillse att personuppgiftsbehandling sker i enlighet med dataskyddsförordningens bestämmelser. DSO kan lämna synpunkter och agera rådgivare till förvaltningens dataskyddssamordnare samt ta fram vissa styrdokument. Kommunstyrelsen har anmodat nämnderna att även utse samma person till sina DSO. Varje nämnd har en utsedd dataskyddssamordnare som agerar kontaktperson gentemot det gemensamma DSO. Enligt Malmö stads riktlinjer för behandling av personuppgifter är DSO även kontaktperson för tillsynsmyndigheten där DSO enligt intervjuade expedierar ärendet vidare till dataskyddssamordnarna som i första hand blir handläggare för ärendet. Under granskningsmötet framgick det att det har anställts en ny dataskyddssamordnare för kommunstyrelsen som börjar i november 2021. Kommunen för en pågående dialog om att ytterligare förstärka resurserna för dataskyddsarbetet. Detta har inte resulterat i några konkreta planer än. Efter den senaste omorganisationen inom kommunen ökade bemanningen i förvaltningarna. Enligt intervjuade har dock bemanningen inom dataskyddsorganisationen ökat under de senaste åren. Tidigare rapporterade DSO direkt till en chefsjurist men numera sker rapportering via juridiska enheten till avdelningschefen på stadskontoret vid behov samt via informell veckovis avstämning. Enligt riktlinjer för personuppgiftsbehandling ska DSO rapportera direkt till den personuppgiftsansvariges eller personuppgiftsbiträdes högsta förvaltningsnivå.	Det är inte säkerställt att DSO-rollen är tydligt definierad och att dess arbetsuppgifter saknar intressekonflikter. Det är inte säkerställt att kommunens centrala DSO och respektive förvaltnings dataskyddssamordnare har tillräckligt med resurser för att genomföra sitt arbete.	

	I *”Riktlinjer för behandling av personuppgifter i Malmö stad”* beskrivs att tillsynsmyndigheten har möjlighet att påföra administrativa sanktionsavgifter vid överträdelser av dataskyddsförordningen. Dock uppfattar man i förvaltningarna att det inte är säkerställt om det är kommunstyrelsen eller en specifik verksamhet som hålls ansvarig i det fall sanktionsavgifter påförs. Sanktionsavgifter ska enligt intervjuade nyckelpersoner på stadskontoret ha diskuterats på nätverksträffar och utbildningar, men konsekvenser på personnivå har inte diskuterats.		
Behandling av person-uppgifter	Det hanteras en rad känsliga personuppgifter i Malmö stad. Inom kommunstyrelsen förekommer dock inte lika omfattande känsliga uppgifter som på andra nämnder. Kommunstyrelsen har upprättat en förteckning över registrerade personuppgiftsbehandlingar. Det finns dokumenterade rutiner för handläggning av registrerades rättigheter. Det finns en e-tjänst för begäran om registerutdrag, radering, rättelse, begränsning, dataportabilitet och invändning där den registrerades identitet kontrolleras via bank-id. Det finns även en fysisk blankett. Enligt rutinen skall legitimation kontrolleras vid inlämning av blanketten. Enligt intervjuade nyckelpersoner finns det blanketter för inhämtning av samtycke. Kommunen försöker dock i möjligaste mån undvika användning av samtycke. Personuppgiftsansvariga är skyldiga att föra register över personuppgiftsbehandling. I de fall personuppgiftsbiträden anlitas är det dock alltid personuppgiftsansvarig som är ytterst ansvarig för att behandling uppfyller gällande lagar och förordningar. Det har påbörjats ett arbete med att föra över registerförteckningar till ett systemstöd för att underlätta löpande uppföljning. I dagsläget hanterar dock de flesta nämnderna sina registerförteckningar i Excel och det är upp till dataskyddssamordnarna i respektive förvaltning att kontrollera	Det har inte säkerställts att registerförteckningar är kompletta och förblir riktiga över tid.	2,55

	efterlevnad. DSO använder registerförteckningarna som ett verktyg för uppföljning av förvaltningarnas arbete. Handlingar med hög risk, stort antal registrerade eller gällande nya tekniker är av särskilt intresse och följs upp utifrån vad DSO anser är viktigt. Enligt intervjuade nyckelpersoner utförs stickprov för de högst klassade systemen inom ramen för informationssäkerhetsarbetet. Checklistan för åtgärder som ska vidtas innan personuppgiftsbehandling inleds med att behandlingens ändamål och laglig grund ska fastställas och dokumenteras. Enligt intervjuade nyckelpersoner på stadskontoret nämns vikten av ändamålsbeskrivning i samband med dataskyddssamordnarnas nätverksträffar. Däremot finns ingen formell granskningsplan som fastställer hur uppföljning av dess efterlevnad ska genomföras. Enligt intervjuade nyckelpersoner används inga personuppgifter för direkt marknadsföring. Detta går enligt uppgift dock inte att definitivt att svara på utan att fråga ställs till samtliga dataskyddssamordnare för registerkontroll. Kommunstyrelsen har centralt framtagna riktlinjer för arkivbestämmelser. Det är respektive förvaltningschef som ansvarar för att förvaltningens anställda tar del av och följer dessa bestämmelser. Enskilda nämnder ska dessutom ha egna arkivredovisningar som gäller som styrdokument för respektive nämnd. Nämndernas arkivredovisning ska ange vad som ska bevaras och gallras, samt gallringsfrist. Vid förändrade förutsättningar för behandling av personuppgifter ska omklassificering genomföras. Enligt kommunstyrelsens arkivredovisning har varje avdelning på stadskontoret i uppgift att säkerställa bevarande och gallring av sin verksamhets handlingar. Vid klassificering av system och information inkluderas krav på gallring. Vissa system har inbyggt systemstöd för automatisk gallring och i de fall som sådant	Det saknas rutiner som över tid säkerställer att personuppgifter endast behandlas för det eller de ändamål som de samlades in för.	

	stöd saknas skall gallringskrav finnas med i systemförvaltarcykeln. Kravställningen som genereras vid klassificering av information inkluderar krav på behörighetshantering och spårbarhet. Det saknas dock centralt definierade rutiner för hur kommunen ska arbeta med behörighetskontroller i deras IT-system. Enligt intervjuade nyckelpersoner loggas behörigheter. När alla nämnder har kommit igång med arbetet med det nya systemstödet för bland annat registerförteckningar kommer dataflöden mellan olika system att kunna följas. Det är respektive verksamhets ansvar att upprätta skriftliga personuppgiftsbiträdesavtal (PUB-avtal) med leverantörer. Kommunstyrelsen har i dagsläget ingen uppföljning av nämndernas uppföljning av leverantörers efterlevnad. Det finns en mall för PUB-avtal, baserad på SKR:s mall. Det är upp till respektive systemförvaltare och systemägare att följa upp leverantörers efterlevnad. Kommunstyrelsen granskar i form av stickprov baserat på klassificering av informationen.	Det finns inga centralt definierade rutiner för hur kommunen ska arbeta med behörighetskontroller i deras IT-system.	
Val av skydds-åtgärder	Det finns kommungemensamma rutiner för klassificering av system och information men respektive verksamhet kan välja att frångå framtagna rutiner om de motiverar varför. Dessa rutiner finns dokumenterade i rutinen för systemsäkerhet, *” Rutin för inventering och klassificering av informationstillgångar i Malmö stad”.* Bedömning av informationens skyddsbehov görs utifrån dess krav på tillgänglighet, riktighet, sekretess/konfidentialitet och spårbarhet. För varje informationsmängd ska det genomföras en informationsklassificering. Som en del av klassningsprocessen ingår det att identifiera typ av personuppgifter. Klassificering ska genomföras under hela informationens livscykel vilket inkluderar nyanskaffning samt ny hantering och förändrad behandling av data. Det finns ingen beskrivning av vad som anses	Rutinen för klassificering av informationstillgångar behöver utvecklas och kompletteras med tydligare instruktioner med avseende på ostrukturerad data.	2,33

	vara strukturerad och ostrukturerad information utan klassificering av informationstillgångar avser all information oberoende av i vilken form den förekommer. I Malmö stads ärendehandbok beskrivs vad som avses med känsliga personuppgifter enligt dataskyddsförordningen. Kommunstyrelsen anordnar inga obligatoriska utbildningar inom informationssäkerhet och dataskydd för de anställda, men de rekommenderas att genomgå den utbildning som finns. Malmö stad har således inte säkerställt att samtliga anställda får den dataskyddsutbildning de behöver. Det finns inga rutiner som säkerställer att utbildningar förblir aktuella över tid. Kommunstyrelsen har ett stadsövergripande ansvar för att följa upp att respektive nämnd har en systematik för genomförande av utbildning men huvudansvaret för genomförandet ligger på respektive nämnd. Respektive förvaltning kan arbeta på olika sätt och stadskontorets uppgift är främst att stödja och hjälpa till med att genomföra önskad utbildning. Enligt intervjuade på stadskontoret finns det på Malmö stads intranät en utbildning inom informationssäkerhet som är tillgänglig för samtliga anställda inom kommunen. Utbildningen erbjuds som webbutbildning samt fysiskt på plats. Innan Covid-19 pandemin anordnades det två gånger om året en introduktionsdag för nyanställda där bland annat informationssäkerhet behandlades. Introduktionen av nyanställda ses över för tillfället där utbildning inom dataskydd och informationssäkerhet kan komma att bli ett obligatoriskt moment. Vi intervju uppgavs att dataskydd åtminstone brukar nämnas vid introduktion av nyanställda. Historiskt sett har ingen obligatorisk utbildning inom dataskydd erbjudits utöver ett verktyg som köptes in där anställda fick en länk till dataskyddsfrågor via e-post. Enligt de intervjuade ska en gedigen utbildningsinsats ha genomförts kopplat till Malmö stads Instagram-	Det har inte säkerställts att samtliga anställda får tillräckligt med utbildning kopplat till dataskyddsförordningen.	

	konto. Gällande GDPR specifikt har DSO anordnat en bred utbildning inom staden och vid behov inom dataskyddsnätverket. DSO har erbjudit utbildningar till olika nyckelpersoner och yrkesgrupper (chefsbefattningar, systemförvaltare, informationssäkerhetssamordnare, arkivarier, registratorer m.fl.) beroende på behov. Stadsjuristerna erbjuder enligt de intervjuade kontinuerliga utbildningar utifrån förvaltningarnas förfrågningar och behov. En före detta dataskyddssamordnare ska ha utbildat anställda inom GDPR. Det finns dock ingen dokumenterad och fastställd plan för utbildningsinsatser. Det finns inget centralt utbildningsverktyg i Malmö stad. Ett flertal plattformar används vilket medför att utbildningar är svårt att följa upp samlat. Respektive nämnd kan använda olika typer av utbildningsformer och plattformar.	Kommunstyrelsen saknar en dokumenterad och fastställd utbildningsplan som definierar hur utbildning inom dataskydd ska bedrivas löpande, samt i samband med nyanställning.	
Inbyggt dataskydd	I Malmö stads ärendehandbok beskrivs det att en handling kan registreras med en sekretessmarkering i ärendehanteringssystemet för att begränsa åtkomst till handlingen. Markeringen fungerar som en extra varning så att en person som försöker begära ut en handling blir informerad om att denne inte bör klicka vidare. Enligt intervjuade nyckelpersoner genererar systemstödet för informationsklassificering en kravlista på både organisatoriska och tekniska krav. I *”Riktlinjer för behandling av personuppgifter i Malmö stad”* framgår det att varje behandling av personuppgifter ska ske i enlighet med gällande lagstiftning samt efterleva vissa grundläggande principer där uppgiftsminimering och lagringsminimering ingår. Principerna skall dokumenteras vid klassificering för att kunna påvisa efterlevnad. Verksamheterna ska använda integritetsvänliga tekniker, åtkomstbegränsning och inbyggt dataskydd. Det ska finnas skriftliga rutiner och dokumentation som visar att kraven på		3,00

	dataskydd som standard och inbyggt dataskydd efterlevs. Det finns dock ingen dokumentation som visar på hur efterlevnad säkerställs.		
Hantering av leverantörs-relationer	Kommunstyrelsen har centralt för kommunen tagit fram en mall för PUB-avtal baserat på SKR:s förlaga. Enligt dataskyddsförordningen ska ett skriftligt PUB-avtal tecknas med personuppgiftsbiträden och det ska framgå av registerförteckningen om ett sådant avtal är upprättat. Kommunstyrelsen ges inte insyn i respektive nämnds lista över leverantörer utan hänvisar till respektive verksamhets dataskyddssamordnare för att besvara huruvida PUB-avtal finns för samtliga leverantörer. För nya leverantörer ska PUB-avtal finnas på plats då det är ett krav vid upphandling. Det är respektive systemförvaltare och systemägare som ansvarar för att föra en dialog om efterlevnad med leverantörerna. Det finns dock inga dokumenterade rutiner för hur efterlevnad säkerställs över tid. I *”Riktlinjer för behandling av personuppgifter i Malmö stad”* framgår att den personuppgiftsansvarige ska säkerställa att behandling uppfyller kraven i dataskyddsförordningen genom t.ex. kontroller och kravställning, men det finns ingen dokumentation över hur sådana kontroller går till. Det framkommer att det förekommer datalagring utanför EU. Det saknas kommungemensamma instruktioner för hur verksamheterna ska säkerställa att datalagringen har en tillräcklig skyddsnivå. Malmö stad ställer krav på leverantörer vid upphandling av ny leverantör och eventuella avsteg från kraven skall dokumenteras.	Det saknas dokumenterade rutiner för att säkerställa att personuppgiftsbiträden och leverantörer uppfyller och agerar i enlighet med dataskyddsförordningen över tid.	2,70
Hantering av incidenter	Vid incidenter tillämpas de centralt framtagna *”Rutin för handläggning av*		2,64

	personuppgiftsincident" för rapportering. Rutinen vänder sig till medarbetare och chefer. Respektive nämnd kan ta fram egna rutiner om så behövs och det är respektive verksamhet som ansvarar för att dokumentera de incidenter som uppkommit inom den egna verksamheten. Enligt rutinen ska en incident anmälas till närmsta chef eller via ett systemstöd. Det finns även en mall för anmälan kallad *"Blankett för anmälan om personuppgiftsincident".* Rutinen beskriver att dataskyddssamordnaren avgör om ärendet ska meddelas vidare till DSO och att DSO ska kontaktas senast 24 timmar efter konstaterad incident för att bedöma om anmälan ska göras till IMY. Enligt intervjuade nyckelpersoner får DSO alltid en kopia på ärenden från IMY. Exempelvis i det fall IMY väljer att inleda tillsyn. I *"Rutin för handläggning av personuppgiftsincident"* ingår att informera de som berörs av personuppgiftsincidenten i de fall incidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. I de fall det sker en större incident som behöver kommuniceras till allmänheten beror processen på om incidenten är stadsövergripande eller för en nämnd. Enligt intervjuade nyckelpersoner kan det antingen hanteras genom den centrala kommunikationsavdelningen eller via samverkan mellan stadskontoret och berörd förvaltning. Enligt *"Riktlinjer för behandling av personuppgifter i Malmö stad"* ska det finnas tillräckliga skriftliga rutiner för att upptäcka, rapportera, utreda och hantera personuppgiftsincidenter i enlighet med dataskyddsförordningen. Enligt intervjuade ska detta ha omfattats av kommunstyrelsens interna kontroll 2021. DSO kan enligt uppgift följa upp incidenthanteringen om denne anser att det är viktigt.	Kommunstyrelsen har inte säkerställt att den definierade incidenthanteringsrutinen efterlevs i praktiken. Det interna kontrollmomentet är inte tillräckligt för att säkerställa detta.	

Information till registrerade	Enligt centralt framtagna *”Riktlinjer för personuppgiftsbehandling i Malmö stad”* ska det säkerställas att den registrerade informeras om behandlingen i enlighet med dataskyddsförordningen. Enligt intervjuade nyckelpersoner ska alla samordnare ha fått utbildning i hur man hanterar informationsskyldigheten och det ska finnas mallar för att lämna information i enlighet med artikel 12, 13 och 14. Det finns även en sida för personuppgiftshantering på webben där det finns kontaktuppgifter för allmänna frågor och information om tillvägagångssätt för hur registrerade kan utöva sina rättigheter. Enligt intervjuade nyckelpersoner ingår de flesta behandlingarna inom ramen för en viss lagstiftning eller allmänt intresse. Inom Malmö stad är det rekommenderat att inte stödja sig på samtycke inom offentlig verksamhet, men i de fall en verksamhet väljer att använda en blankett för samtycke måste det även finnas en rutin för hur man visar upp att samtycket är giltigt och att det kan upphöra. I undantagsfall är det informationsägare och samordnare som ansvarar för att ta fram rätt rutin för samtycke och att säkerställa efterlevnad enligt dataskyddsförordningen. Enligt *”Användning av bilder och filmer i Malmö stad”* finns det kommunövergripande mallar för samtycke och modellavtal som kan användas av alla nämnder. Samtycke tas tillbaka genom skriftligt meddelande till Kommunstyrelsen.		3,07
Begäran från registrerade	Det finns stadsövergripande rutiner för begäran om registerutdrag och hantering av personuppgiftsbehandling, vilket inkluderar rättelse, radering, begränsning, dataportabilitet och invändning. En begäran kan inkomma på flera sätt, exempelvis via e-tjänst, e-post, skriftlig begäran, telefon eller besök. Vid användning av e-tjänst sker identitetskontroll via bank-id. I övriga fall kontrolleras den registrerades legitimation.		2,88

	”Lathund – tjänster: Personuppgifter hos kommunen” innehåller instruktioner för hur en handläggare använder e-tjänsten för att hantera förfrågningar från registrerade. Resultatet av handläggningen kan meddelas direkt via plattformen eller via post. Däremot saknas tydliga instruktioner för hur rutinerna för hantering av begäran från registrerade hanteras i praktiken. Exempelvis framgår det ej vem som ansvarar för respektive steg, hur man kommer fram till att en registrerad har rätt till begränsning eller vilka tekniska åtgärder som kan vidtas för att säkerställa att uppgifter begränsas Registrerade kan även fylla i en blankett för begäran om registerutdrag och hantering av personuppgiftsbehandling. Blanketten skickas till Malmö stads reception för handläggning och den registrerade kan därefter hämta ut handlingen i receptionen eller få den skickad till sig med rekommenderat brev. Enligt intervjuade nyckelpersoner verkar det i dagsläget inte förekomma några behandlingar om begäran av begränsning av personuppgifter.	Det saknas tydliga instruktioner för hur begäran från registrerade ska hanteras i praktiken.	
Profilering	Beslut som enbart grundar sig på automatiserad behandling av registrerade förekommer inte under kommunstyrelsen.		N/A

5.2. Servicenämnden

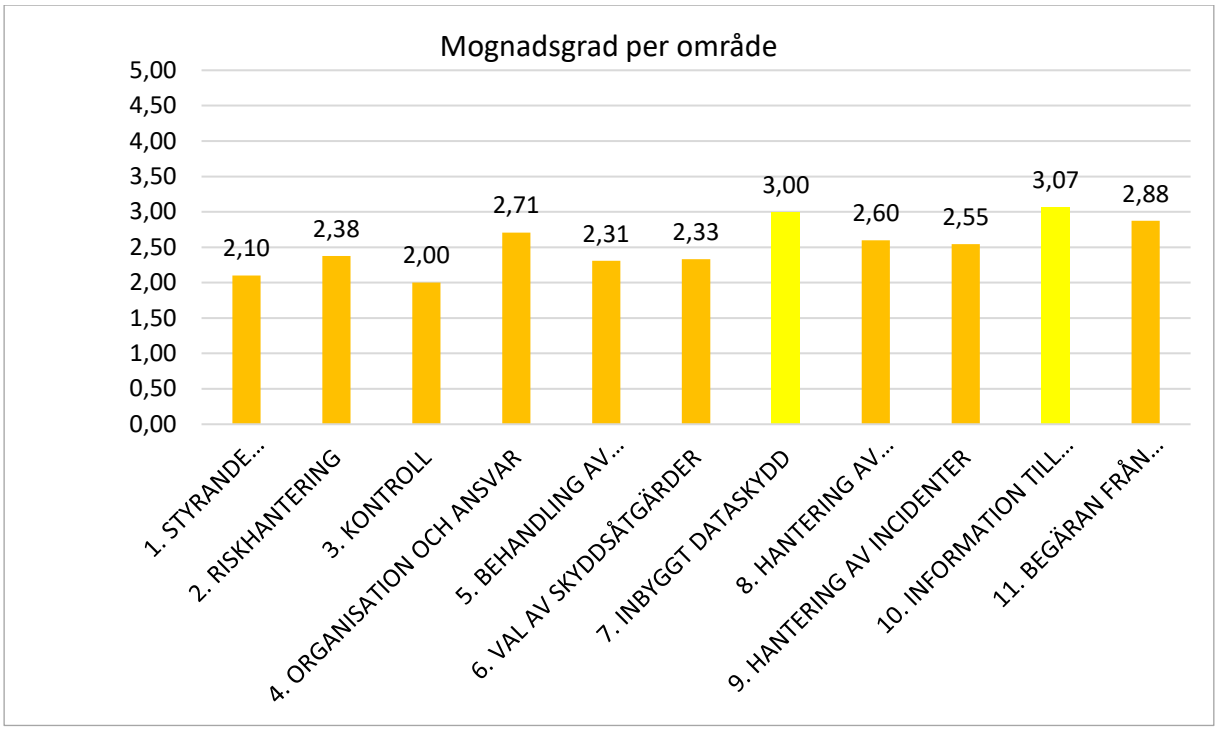
Baserat på granskningen konstateras att servicenämnden har en mognadsgrad strax under genomsnittet för personuppgiftshantering jämfört med vad EY generellt observerar i en offentlig verksamhet av motsvarande storlek och karaktär. Servicenämndens mognadsgrad uppnår en summa av 2,47 av 5,00. Det är vår bedömning att mognadsgraden är låg sett till kommunens storlek, riskbild samt den mängd personuppgifter som nämnden är ansvarig för.

Det är vår bedömning att servicenämnden behöver stärka sitt dataskyddsarbete. Vi noterar att det finns en god förståelse för vikten av att genomföra riskanalyser och konsekvensbedömningar. Likaså vikten av att utbilda sin personal inom dataskyddsfrågor. Samtidigt som nämnden uppvisar goda ambitioner finns det i dagsläget ett flertal förbättringsområden relaterat till dataskyddsarbetet. Serviceförvaltningen har enligt vår mening inte tillräckligt med resurser för att bedriva ett önskvärt och ändamålsenligt dataskyddsarbete. Detta framförallt avseende det kontinuerliga riskhanteringsarbetet och granskningen av regelverkens efterlevnad. Nämnden bör säkerställa att det genomförs riskanalyser kopplat till samtliga IT-system, samt konsekvensbedömningar för de behandlingar där det anses vara relevant.

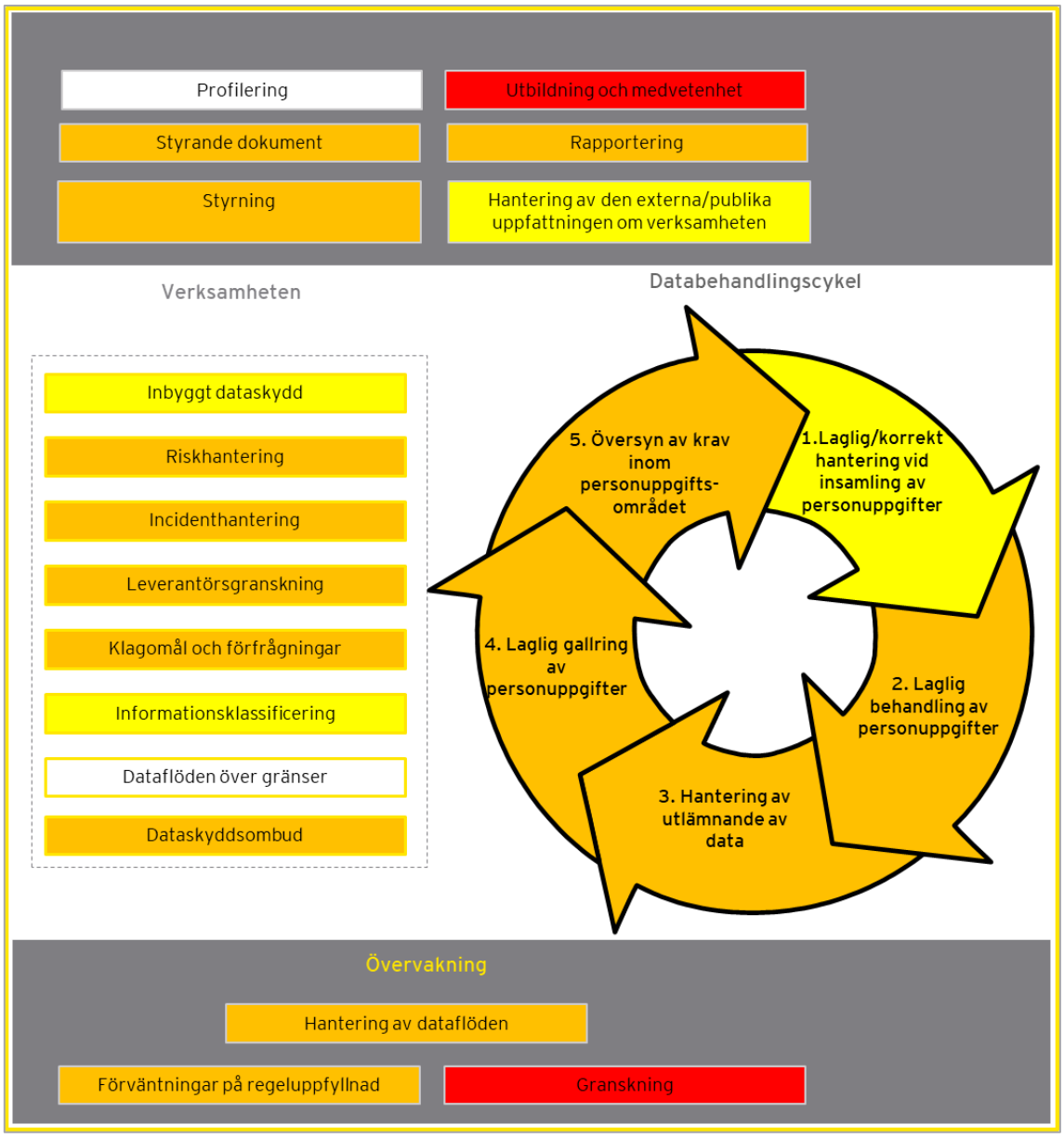
Översiktsbilderna nedan redovisar kommunens mognadsgrad för de 12 huvudområden som granskats, samt nedbrutet på 22 underområden.

Nivå 5 representerar hög mognadsgrad medan nivå 1 representerar låg mognadsgrad. Mognadsgrad beskrivs på en standardiserad skala enligt nedan:

1. Begynnande – Det finns ingen dokumentation eller uppföljning, händelser hanteras ad hoc.
2. Upprepbar – Viss grundläggande dokumentation finns, men denna kan variera mellan olika enheter och vara bristfällig i sin omfattning och tillämpning.
3. Definierad – Det finns dokumenterade processer och dessa tillämpas i stor mån genom hela organisationen.
4. Förvaltad – Förutom väl dokumenterade processer som tillämpas i hela organisationen, finns det dessutom ett system för uppföljning.
5. Optimerad – Baserat på uppföljningen finns också rutiner för kontinuerlig förbättring och uppdatering av processer och ramverk.



Figur 3: Mognadsgrad per område



Figur 4: Grafisk överblick av mognadsgrad per område (notera att de 12 huvudområdena är uppdelade i ytterligare detalj)

5.2.1. Nuläge och iakttagelser

Nedan följer en beskrivning av den övergripande nulägesbild och iakttagelser per område som har identifierats under granskningens utförande.

Område	Nuläge	Iakttagelser	Mognad
Styrande dokument/ styrning	Servicenämnden utgår till huvudsak från de kommungemensamma riktlinjerna för behandling av personuppgifter och informationssäkerhet. Nämnden tillämpar även stadens gemensamma arkivhandbok samt den lathund som finns gällande begäran om registrerades rättigheter. Därutöver har Servicenämnden även utarbetat egna styrdokument i de fall de använder ett annorlunda arbetssätt än de kommungemensamma, samt när de har sett ett behov av komplettering eller justering. De har också en egen kompletterande arkivredovisning. Servicenämnden ansvarar för att uppdatera sina egna rutiner och instruktioner. Enligt intervjuade har nämnden uppdaterat sina riktlinjer med jämna mellanrum gällande det de lagrar och delar, samt baserat på feedback från medarbetare och förändrade rekommendationer från IMY. Revidering av dokument sker vid behov eller enligt definierade revideringsintervaller. De dokument som har tagit fram ska revideras vid behov. Enligt intervjuade nyckelpersoner från serviceförvaltningen används främst eget material för utbildning. Enligt intervjuade nyckelpersoner på serviceförvaltningen kommuniceras konsekvenser av att inte följa gällande rutiner och riktlinjer. De behandlar exempelvis konsekvenser för både de egna och andra verksamheter samt vad som kan drabba medborgarna.	Servicenämnden har till del anpassat kommungemensamma styrdokument. Däremot inte i tillräcklig utsträckning och med tillräcklig systematik för att anses vara tillräckligt. Det saknas en dokumenterad rutin som genom regelbunden revidering säkerställer att styrande dokument förblir uppdaterade och riktiga över tid.	2,10
Risk-hantering	Servicenämnden saknar en fungerande systematik för att säkerställa att riskanalyser och konsekvensbedömningar utförs regelbundet. Riskanalyser utförs inför nya	Det är inte säkerställt att riskanalyser, konsekvensbedömningar och handlingsplaner förblir uppdaterade och riktiga över tid.	2,38

	behandlingar och för nya system. Det saknas en systematik för att kontinuerligt granska efterlevnad för befintliga och äldre system. Enligt intervjuade nyckelpersoner på Serviceförvaltningen har det funnits viss resursbrist, vilket har inneburit att riskanalyser inte har kunnat utföras för samtliga system, eller till den grad som anses önskvärt.	Det är inte säkerställt att det finns tillräckligt med resurser för att genomföra riskanalyser och konsekvensbedömningar enligt dokumenterade rutiner.	
Kontroll	Servicenämnden har inte genomfört någon oberoende granskning av arbetet med informationssäkerhet och dataskydd. Däremot har intern kontroll genomfört en informationssäkerhetsgranskning under 2021 och under 2022 kommer ytterligare en att ske med fokus på åtkomst till system och lokaler. Personuppgiftsincidenthantering har granskats som en del av den interna kontrollen men det har inte skett någon generell granskning av efterlevnad av dataskyddsförordningen och det finns ingen granskningsplan utöver intern kontroll. Resultaten från genomförda granskningar rapporteras till nämnden. Representanter för förvaltningen har enligt uppgift kontinuerliga möten med systemägare och systemförvaltare för att granska efterlevnad av rutiner där IT- och informationssäkerhetssamordnaren påtalar vikten av handlingsplaner och riskanalyser. Ett formulär används för när personuppgiftsbehandling påbörjas. Tidigare har de gått igenom registerförteckningar två gånger om året för att kontrollera om de är kompletta. På grund av för stor arbetsbörda görs det inte längre.	Det saknas en specifik granskningsplan för arbetet med personuppgiftshantering som säkerställer att Servicenämnden kontinuerligt uppfyller kraven inom dataskyddsförordningen.	2,00
Organisation och ansvar	Nätverk med dataskyddskoordinatorer fungerar som en kanal för att nå ut med information. Serviceförvaltningens dataskyddssamordnare har kontaktpersoner på respektive		2,71

	verksamhet inom förvaltningen, men IT- och informationssäkerhetssamordnaren saknar kontaktpersoner för arbetet med informationssäkerhet. Serviceförvaltningens IT- och informationssäkerhetssamordnare har ansvar för mer än 40 system varav ett flertal är föråldrade. Nämnden kan dessutom komma att involveras i arbetet med ytterligare ett 30-tal andra system, men detta är fortfarande i en tidig fas. Av intervjuer framkommer att det upplevs råda viss kompetens- och resursbrist samt att det saknas fullt stöd från ledningsgruppen gällande arbetet med dataskydd och informationssäkerhet.	Det är inte säkerställt att det finns tillräckligt med resurser för att genomföra önskvärt arbete inom dataskydd och informationssäkerhet.	
Behandling av person-uppgifter	Enligt intervjuade nyckelpersoner på serviceförvaltningen hanteras en begränsad mängd känsliga personuppgifter. Liksom kommunstyrelsen och i enlighet med Malmö stads kommunövergripande riktlinjer försöker servicenämnden att undvika användning av samtycke i största möjliga mån. Samtyckesblanketter används när bilder och filmer används för presentation på intranätet eller vid marknadsföring av verksamheten. Behandlingsgrund för personuppgiftsbehandling ska framgå av registerförteckningen. Enligt intervjuade nyckelpersoner på serviceförvaltningen är det koordinatorerna inom respektive verksamhet som ansvarar för att kontrollera att registerförteckningar är kompletta. Dataskyddssamordnaren agerar stöd till koordinatorerna och kontaktar förvaltningens avdelningar två gånger per år för att säkerställa att uppdateringar och kompletteringar av registerförteckningen görs. Utvecklingssekreteraren utför dock inga stickprov eller kontroller för att säkerställa att registerförteckningen är komplett, men ska enligt uppgift få in svar på nya personuppgiftsbehandlingar med jämna		2,31

	mellanrum. I dagsläget förs registerförteckningen i Excel. Servicenämnden tar hjälp av en arkivarie i arbetet med register- och arkivförteckning. Arkivarien utför gallring vid förfrågan. Det utförs ingen systematisk granskning av verkställande av gallringar. Det finns äldre system som saknar inbyggd funktionalitet för gallring men för nya system ställs det krav på att system ska passa in i nämndens arkiv- och gallringsplan. Rutiner för hur behörigheter ska skapas, gås igenom och avslutas finns inte för samtliga system. Det ska finnas en rutin för att avsluta behörigheter men det förekommer fall där behörigheter inte avslutats i tid. Avseende ärendehanteringssystemet är det upp till en så kallad superanvändare att tillse att avslut sker.	Det saknas en dokumenterad rutin för uppföljning av registerförteckningens riktighet och fullständighet över tid. Det saknas dokumenterade rutiner och/eller kontroller som säkerställer att personuppgifter endast behandlas för de ändamål som de samlades in för. Det saknas dokumenterade rutiner som säkerställer att gallring av personuppgiftsbehandlingar verkställs inom satt tidsram. Det saknas en dokumenterad rutin för hur behörighetskontroller ska genomföras i servicenämndens IT-system.	
Val av skydds-åtgärder	Informationsklassificering sker inför upphandling eller uppgradering av system. Liksom på central nivå genereras en kravlista beroende på klassificeringen där åtgärder baseras på de risker som ses. Det saknas dock en dokumenterad process för att identifiera och klassificera ostrukturerad information. Systemförvaltare ska arbeta löpande med informationsklassificering där IT- och informationssäkerhetssamordnaren påtalar om så inte är fallet. I dagsläget saknas det en utbildningsplan. Det pågår enligt uppgift en dialog om att ta fram en övergripande plan. Ett förslag utarbetades i början på 2021. I samband med att GDPR infördes anordnades obligatoriska utbildningar inom GDPR för samtliga anställda. I dagsläget är utbildningarna inte tvingande. Enligt intervjuade är dock gensvaret bra. Det uppges finnas en förståelse för allvaret av	Rutinen för klassificering av informationstillgångar behöver utvecklas och kompletteras med tydligare instruktioner med avseende på ostrukturerad data. Det finns i dagsläget ingen dokumenterad plan som säkerställer att utbildningar inom dataskyddsförordningen genomförs regelbundet av de anställda.	2,33

	GDPR och informationssäkerhet. Brister i utförandet är främst kopplat till kompetensbrist. Enligt de intervjuade har förvaltningen en funktion med sammanhållande uppgift för hela verksamhetens utbildning. Det finns två så kallade utbildningsblock där en fokuserar på daglig hantering av GDPR och en annan för personuppgifter. Det anordnas även utbildningar baserat på vad verksamheterna och ledningsgrupperna efterfrågar. Det utarbetas enligt uppgift för tillfället en introduktionsutbildning där varje nyanställd ska få ta del av de två utbildningsblocken. Det finns önskemål om att utöka delarna som avser GPDR i den befintliga utbildningen. Utvecklingssekreteraren hör av sig till verksamheter för att stämma av om utbildning efterfrågas.	Servicenämnden har inte säkerställt att samtliga anställda får tillräckligt med utbildning kopplat till dataskyddsförordningen.	
Inbyggt dataskydd	Servicenämnden har inte tillsett att det finns systemstöd som underlättar kryptering eller som genererar varningsmeddelanden, bortsett från en rutin för vad som inte får skannas till Outlook. Det finns till exempel inget inbyggt stöd för att rapportera okrypterade meddelanden som incidenter eller något stöd som varnar om användning av personuppgifter.	Det saknas en dokumenterad rutin för hur systemägare ska utföra behörighetskontroller i Servicenämndens IT-system.	3,00
Hantering av leverantörs-relationer	Den kommungemensamma mallen för PUB-avtal, baseras på SKRs mall. Delegationsordningen styr vem som har rätt att skriva under avtalen. Upphandling av nya system godkänns inte om inte IT- och informationssäkerhetssamordnaren har kontrollerat krav på informationssäkerhet och dataskydd. Det saknas dock en rutin för att granska efterlevnad över tid. PUB-avtal tecknas med nya leverantörer. Det saknas dock PUB-avtal för vissa system. Detta beror bland annat på att vissa äldre system saknar leverantörer och att vissa system inte behandlar personuppgifter.	Servicenämnden saknar en rutin för att säkerställa att leverantörer lever upp till definierade kravställningar inom dataskyddsarbetet över tid.	2,60

	Enligt de intervjuade granskas att leverantörer levererar avtalad tjänst. I samband med Privacy Shield-domen gick nämnden genom sina system i syfte att kontrollera att inga leverantörer har lagringsplatser utanför EU. Bortsett från ett fåtal Microsoft-tjänster ska enligt de intervjuade ingen leverantör ha lagring utanför EU. Nämnden har enligt uppgift tagit fram egna styrdokument för vad som gäller för Microsofts tjänster, skanning, kopiering och USB-minnen. En informationssäkerhetsmatris anger vilka typer av personuppgifter som får lagras i Microsoft 365.		
Hantering av incidenter	De kommungemensamma rutinerna för hantering av personuppgiftsincidenter används inte. Istället har egna rutiner utarbetats. Det framförs att den lokala rutinen utarbetades som ett snabbare och enklare tillvägagångssätt. Rutinen ingår som en del av avvikelserapporteringen där det är möjligt att specificera om det rör sig om en personuppgiftsincident. Tillvägagångssättet är detsamma oavsett om det är en personuppgiftsincident eller incident av annat slag. Rapporter förmedlas till förvaltningens koordinator som i sin tur kontaktar dataskyddssamordnaren för bedömning av hur allvarlig incidenten är och om anmälan till IMY bör göras. Skriftligt beslut om anmälan tas av verksamhetschefen i enlighet med delegationsordningen. Det är dock inte säkerställt om rutinen efterlevs i praktiken. Alla incidenter sparas och diarieförs. Enskilda frågor rapporteras uppåt till berörd chef. Dessutom ges en översikt av bland annat hur många personuppgiftsincidenter som förekommit under året i samband med en årlig avvikelserapport. Malmö stads DSO involveras vid allvarligare incidenter. Incidenter av mindre allvarlig karaktär hanteras på egen hand,	Servicenämnden har inte säkerställt att den definierade incidenthanteringsrutinen efterlevs i praktiken.	2,55

Information till registrerade	Egna samtyckesblanketter har upprättats gällande ljud, bild och film, där lagringstid, ändamål och rättigheten att dra tillbaka samtycke framgår. Bilder samlas in tillsammans med underskrift och dokumenteras i det kommungemensamma ärendehanteringssystemet.		3,07
Begäran från registrerade	Nämnden tillämpar de kommungemensamma rutinerna avseende begäran om registerutdrag och hantering av personuppgiftsbehandlingar. Det är koordinatorerna inom respektive verksamhet som kontrollerar om en person förekommer i verksamhetens system. Det framförs att koordinatorer har en egen dokumenterad rutin för den praktiska hanteringen. Denna är dock inte officiellt fastställd eller att anse som styrande. Enligt intervjuade har endast begäran om registerutdrag inkommit. Således har rutinen inte testats vid exempelvis begäran om radering. Begäran om radering och dataportabilitet beskrivs vara svåra att fullt ut tillmötesgå på grund av lagar kopplat till exempelvis arkivering.	Det saknas en officiell rutin för hur begäran från registrerade ska hanteras i praktiken. Inofficiella rutiner riskerar att skapa personberoenden.	2,88
Profilering	Servicenämnden använder inte profilering.		N/A

5.3. Gymnasie- och vuxenutbildningsnämnden

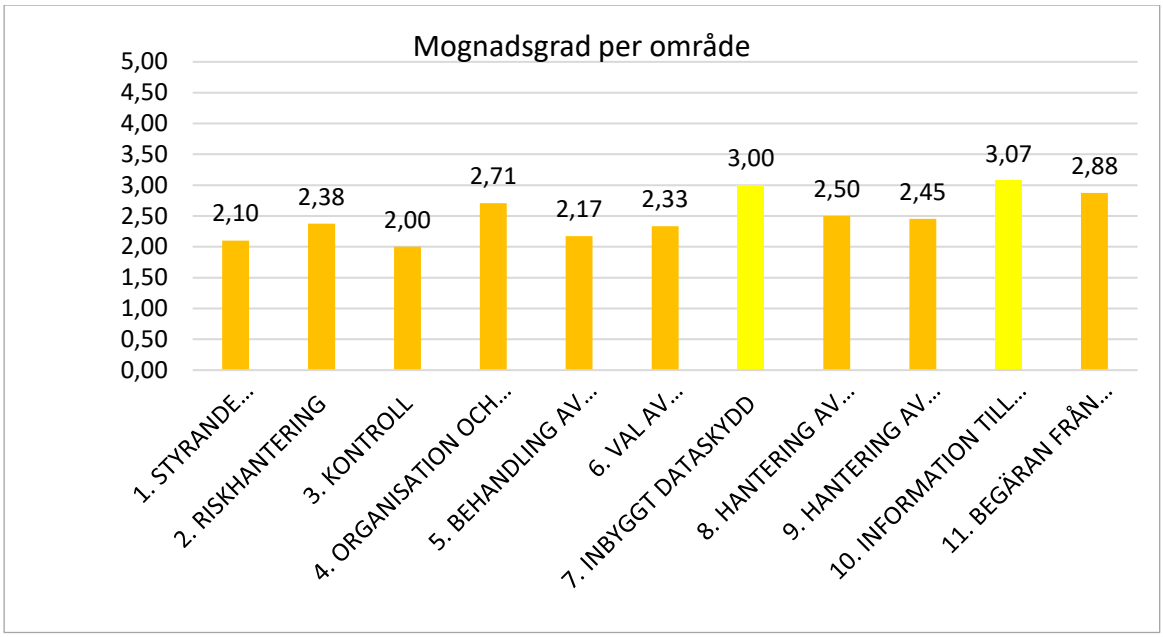
Av granskningen konstateras att gymnasie- och vuxenutbildningsnämndens mognadsgrad är strax under genomsnittet för personuppgiftshantering jämfört med vad EY generellt observerar i en offentlig verksamhet av motsvarande storlek och karaktär. Gymnasie- och vuxenutbildningsnämnden mognadsgrad uppgår till 2,42 av 5,00. Det är vår bedömning att mognadsgraden är låg sett till kommunens storlek, riskbild samt den mängd personuppgifter som nämnden är ansvarig för.

Det är vår bedömning att gymnasie- och vuxenutbildningsnämnden behöver stärka sitt dataskyddsarbete. Nämnden behöver däri förbättra arbetet med att anpassa kommungemensamma styrdokument och rutiner till den egna verksamheten samt säkerställa dess efterlevnad. Det finns även ett behov av att se över rutinerna för incidenthantering då det inte är säkerställt att de efterlevs i praktiken. Nämnden har enligt vår mening inte säkerställt att samtliga behandlingar finns dokumenterade i registerförteckningen samt att de förblir riktiga över tid. Det har även identifierats att riskanalyser och konsekvensbedömningar inte har kunnat utföras enligt dokumenterad rutin. Nämnden bör också tillse att registerförteckningen är komplett, samt att risk- och konsekvensbedömningar sker systematiskt och enligt dokumenterade rutiner. Det är avslutningsvis vår bedömning att nämnden inte säkerställt att förvaltningen har de nödvändiga resurserna för att bedriva ett önskvärt och ändamålsenligt dataskyddsarbete.

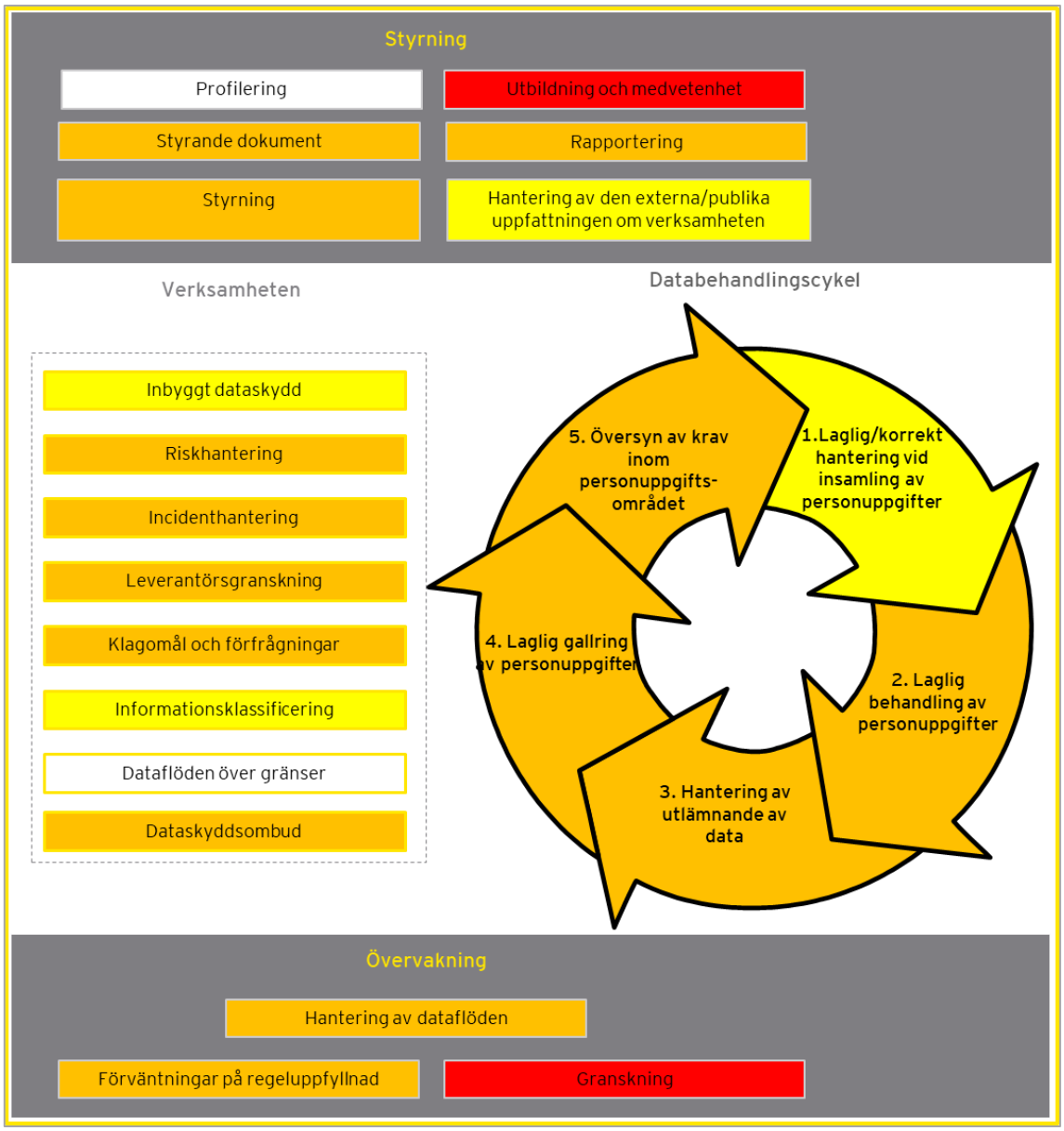
Översiktsbilderna nedan redovisar kommunens mognadsgrad för de 12 huvudområden som granskats, samt nedbrutet på 22 underområden.

Nivå 5 representerar hög mognadsgrad medan nivå 1 representerar låg mognadsgrad. Mognadsgrad beskrivs på en standardiserad skala enligt nedan:

1. Begynnande – Det finns ingen dokumentation eller uppföljning, händelser hanteras ad hoc.
2. 2. Upprepbar – Viss grundläggande dokumentation finns, men denna kan variera mellan olika enheter och vara bristfällig i sin omfattning och tillämpning.
3. Definierad – Det finns dokumenterade processer och dessa tillämpas i stor mån genom hela organisationen.
4. Förvaltad – Förutom väl dokumenterade processer som tillämpas i hela organisationen, finns det dessutom ett system för uppföljning.
5. Optimerad – Baserat på uppföljningen finns också rutiner för kontinuerlig förbättring och uppdatering av processer och ramverk.



Figur 5: Mognadsgrad per område



Figur 6: Grafisk överblick av mognadsgrad per område (notera att de 12 huvudområdena är uppdelade i ytterligare detalj)

Mognadsgraden beskrivs enligt den standardiserade skalan med respektive färgkod. De områden som inte var tillämpliga för granskningen är vita.

5.3.1. Nuläge och iakttagelser

Nedan följer en beskrivning av den övergripande nulägesbild och iakttagelser per område som har identifierats under granskningens utförande.

Område	Nuläge	Iakttagelser	Mognad
Styrande dokument/ styrning	Gymnasie- och vuxenutbildningsnämnden förlitar sig till stor del på de kommungemensamma styrdokument och rutiner gällande riktlinjer för dataskydd, personuppgiftsbehandlingar, informationssäkerhet, riskanalyser, registrerades rättigheter samt incidenthantering. Nämnden förlitar sig på att kontinuerliga genomgångar av dokument sker centralt. Det finns ingen dokumenterad process för att anpassa kommungemensamma styrdokument till nämndens verksamheter. Enligt intervjuade förekommer viss anpassning av kommungemensamma dokument, exempelvis för rutiner som finns tillgängliga på intranätet.	Gymnasie- och vuxenutbildningsnämnden har inte anpassat kommungemensamma styrdokument till den egna verksamheten. Det saknas en dokumenterad rutin som säkerställer att styrande dokument förblir uppdaterade och riktiga över tid.	2,10
Risk-hantering	Gymnasie- och vuxenutbildningsnämnden följer kommungemensamma riktlinjer gällande riskhantering. Vid nyanskaffning av system används det kommungemensamma klassificeringsprotokollet och systemstöd för att generera de krav som ställs på systemet. Vid nyanskaffning av system eller vid ny personuppgiftsbehandling utförs någon form av riskanalys och regelrätt konsekvensbedömning men det sker ingen uppföljning eller kontroll som säkerställer att riskanalyser görs regelbundet. Enligt intervjuade finns det omfattande eftersläpningar relaterat till personuppgiftsbehandlingar. Detta på grund av att uppföljning av konsekvensbedömningar ej har genomförts. Likaså själva genomförandet av konsekvensbedömningar vid nyanskaffning av system/ny behandling av personuppgifter. Det är upp till respektive chef/informationsägare att kontakta dataskyddssamordnaren för att genomföra en konsekvensbedömning. Därefter genomför dataskyddssamordnaren en bedömning tillsammans med chefen/informationsägaren. Enligt ramverket för konsekvensbedömningar kan även Malmö	Gymnasie- och vuxenutbildningsnämnden har inte säkerställt att riskanalyser och konsekvensbedömningar sker utifrån dokumenterad rutin.	2,38

	stads DSO eller stadsjurister involveras. I de fall en bedömning resulterar i en mycket hög risk sker samråd med DSO och eventuellt IMY.		
Kontroll	Nämnden genomför i dagsläget inte någon egen uppföljning, internkontroll, av arbetet med dataskydd. Respektive systemägare ska säkerställa att det finns rutiner för behörighetskontroller till nämndens IT-system. Enligt intervjuade har det utarbetats en rutin för behörighetstilldelning. Många av de rutiner som tillämpas har från början utarbetats av grundskolenämnden. Behörighetshantering är ett fokusområde för stadens interna kontroll och enligt intervjuade sker årliga genomgångar av behörigheter. Det saknas rutiner för att rapportering till styrelse/nämnd om status för dataskyddsarbetet. Ledningsgruppen på förvaltningen involveras enligt uppgift vid större incidenter. Den interna kontrollplanen återrapporteras till nämnden.	Gymnasie- och vuxenutbildningsnämnden saknar en granskningsplan för internkontroll som säkerställer efterlevnad av dataskyddsförordningen.	2,00
Organisation och ansvar	Gymnasie- och vuxenutbildningsnämnden har ett eget nätverk för dataskyddsfrågor. Detta utöver det kommungemensamma nätverket. Arbetet inom nätverket beskrivs vara mer av ett kontaktnät än grunden för ett systematiskt arbete. Det anses finnas ett behov att stärka det interna nätverket samt införa tätare samarbete. Gymnasie- och vuxenutbildningsnämnden har en informationssäkerhetssamordnare som arbetar centralt på förvaltningen. Denne deltar i det kommungemensamma nätverket för informationssäkerhet tillsammans med andra samordnare. Förvaltningens dataskyddssamordnare arbetar i stor utsträckning med dataskyddssamordning. Nämnden har delegerat beslut om registrerades rättigheter och incidenthantering till sektions- eller enhetscheferna. Vid intervju uppges att varje skola har en administrativ chef		2,71

	som har i uppgift att hantera registerutdrag och incidenter. Enligt de intervjuade finns det tillräckligt med stöd i staden för att inhämta och upprätthålla god kunskap inom informationssäkerhet och dataskydd. Utöver stöd i centrala styrdokument och rutiner kan de även vända sig till stadens DSO, stadsjurister eller informationssäkerhetsansvarig vid eventuella frågor inom området. Däremot har de inte haft tillräckligt med resurser och tid för att utföra dataskyddsarbetet i önskvärd utsträckning. Resursbristen har lyfts med förvaltningsledningen. Detta har resulterat i en projektanställd dataskyddssamordnare. Dennes anställning ska utvärderas nästa år. En informationssäkerhetssamordnare tillsattes sommaren 2021 (del av tjänst).	Det saknas tillräckliga resurser för att utföra önskat dataskydds- och informationssäkerhetsarbete.	
Behandling av person-uppgifter	Gymnasie- och vuxenutbildningsnämnden hanterar en stor mängd personuppgifter men enligt de intervjuade är de flesta uppgifterna inte känsliga. Det finns säkerhetsklassade system som förvaltas gemensamt med andra nämnder och ett antal andra system där känsliga uppgifter förekommer, exempelvis inom HR. Dataskyddssamordnaren har i uppgift att säkerställa att registerförteckningen är riktig och komplett över tid. En inventering genomfördes inför dataskyddsförordningens inträde i maj 2018. Det saknas dock en process för att säkerställa att förteckningen förblir komplett över tid. Det uppges vara målsättningen att föra in alla registerförteckningar i det kommungemensamma systemstödet. Vid anskaffning av IT-system ställs krav på att systemet inte ska behandla mer personuppgifter än nödvändigt. Det saknas systematik för uppföljning av dess efterlevnad. Anonymisering eller pseudonymisering av data görs ej som regel. Det framförs i sakkontrollen	Det saknas en definierad process för att säkerställa att registerförteckningen förblir riktig och komplett över tid.	2,17

	att flera av de nuvarande systemen inte möjliggör detta. Flera av nämndens system har stöd för automatisk och löpande gallring av uppgifter. För de system där automatisk gallring saknas har systemägaren i uppgift att tillse att gallring sker. Det saknas rutin för hur systemägaren ska gallra. Nämnden gör ingen uppföljning för att säkerställa att systemägare verkställer gallring. Gallringsfrist framgår av den kommungemensamma arkivhandboken och nämndens arkivredovisning. I dagsläget har det stadsgemensamma dokument- och ärendehanteringssystemet ingen gallringsfunktion. En modul för gallring ska enligt uppgift implementeras under 2022. Den digitala lärmiljön har en gallringsfunktion (90 dagar).	Det saknas rutin för att säkerställa att gallring utförs enligt definierad rutin.	
Val av skydds-åtgärder	Informationssäkerhetssamordnaren leder och samordnar arbetet med att informationsklassificera nya system och behandlingar. Ansvaret ligger hos respektive verksamhet. Klassificering ska ske under systemets hela livscykel och olika funktioner kan vara involverade vid olika tillfällen. Baserat på resultaten från klassificeringen och riskanalyserna genereras en kravlista på olika skyddsåtgärder som ska implementeras. Nämnden genomförde vid årsskiftet 2020/2021 punktinsatser för utbildning inom dataskydd och GDPR för chefer och rektorer. Dels en mer djupgående utbildning med sektionschefer (2019), dels en mer generell för all administrativ personal inom förvaltningen. Nämnden saknar systematik för utbildning av nyanställda. Det finns enligt uppgift information på intranätet samt en checklista där den nyanställdes chef ansvarar för att se till att det som ska göras vid nyanställning verkställs. I dagsläget saknas det e-tjänst för utbildning. Enligt de intervjuade finns en intention om att arbeta mer aktivt med utbildning framöver.	Rutinen för klassificering av informationstillgångar behöver utvecklas och kompletteras med tydligare instruktioner med avseende på ostrukturerad data. . Nämnden har inte säkerställt att samtliga anställda får den utbildning de behöver kopplat till dataskyddsförordningen. Det saknas en dokumenterad plan för utbildningar kopplat till arbetet med dataskyddsfrågor.	2,33

	Detta förutsatt att tillräckliga resurser finns tillgängliga.		
Inbyggt dataskydd	Vid klassificering av system specificeras eventuella krav på inbyggt dataskydd. Enligt de intervjuade finns det inbyggt dataskydd i nämndens system.	Det saknas en dokumenterad rutin för hur systemägare ska utföra behörighetskontroller i gymnasie- och vuxenutbildningsnämndens IT-system.	3,00
Hantering av leverantörs-relationer	Nämnden tecknar PUB-avtal med leverantörer. Det saknas dock en rutin för att följa upp leverantörers efterlevnad. Enligt de intervjuade ska PUB-avtal finnas för samtliga leverantörer och punktinsatser har genomförts för att säkerställa att datalagring inte sker utanför EU. Enligt de intervjuade är utgångspunkten att all lagring ska ske inom EU/EES. I de fall det finns stöd för överföring, exempelvis genom standardklausuler, får lagring ske utanför dessa gränser. PUB-avtal tecknas av kommunstyrelsen för kommungemensamma system där nämnden undertecknar en bilaga. Detta gäller specifikt för den stadsgemensamma plattformen för e-tjänster. Hanteringen kan se annorlunda ut för andra system. Exempelvis att PUB-avtal tecknas centralt med fullmakt från berörda nämnder. Det finns en rutin på intranätet som specificerar att samordnare och DSO ska involveras i upphandlingsprocessen. Enligt rutinen ska klassificering av hanterad information att genomföras, samt en aktiv bedömning av huruvida en risk och sårbarhetsanalys ska genomföras.	Gymnasie- och vuxenutbildningsnämnden saknar rutin för att säkerställa att leverantörer lever upp till definierade kravställningar inom dataskyddsarbetet.	2,50
Hantering av incidenter	Incidenter rapporteras antingen via Malmö stads gemensamma system eller direkt till ansvarig chef. Enligt de intervjuade är det vanligare att rapportera till chef än via systemet. Ansvarig chef tar därefter kontakt med förvaltningens dataskyddssamordnare som tillsammans med ansvarig chef fyller i en incidentrapport. Det saknas system för att kan		2,45

	hantera både anmälan och dokumentation/uppföljning av incident. Det kan rapporteras i Agera. Enligt uppgift rapporteras incidenter alltid till DSO för kännedom. DSO konsulteras också vid allvarligare incidenter. Nämnden ansvarar själva för att anmäla incidenter till IMY men kan ta stöd från DSO om så behövs. Det ingår i rutinen för hantering av incidenter att informera berörda enligt upprättad mall. Det har identifierats att dokumentationen behöver stärkas t.ex. i en tjänsteanteckning. Information till berörda ges muntligen. Under granskningsmötet framkom att den dokumenterade rutinen behövde revideras för att motsvara den faktiska hanteringen.	Gymnasie- och vuxenutbildningsnämnden har inte säkerställt att tillräcklig information loggas i samband med incidentrapportering. Gymnasie- och vuxenutbildningsnämnden har inte säkerställt att den definierade rutinen för incidenthantering efterlevs i praktiken.	
Information till registrerade	Gymnasie- och vuxenutbildningsnämnden har upprättat en samtyckesblankett samt egna rutiner vid insamling av foto och film i pedagogisk verksamhet. Enligt de intervjuade är det endast i dessa sammanhang som samtycke används.		3,07
Begäran från registrerade	De kommungemensamma e-tjänsterna ”begär registerutdrag” och ”begär radering, rättelse, begränsning, överflytt och invändningar” tillämpas av nämnden. Vid begäran om radering av uppgifter kontaktar ansvarig chef förvaltningens dataskyddssamordnare som om kontaktar ansvarig chef. Beslutet är delegerat till sektionschef/enhetschef. Vid behov involveras även DSO. Det finns centrala rutiner för hantering av begäran från registrerade, men det saknas tydliga instruktioner för hur rutinerna för hantering av begäran från registrerade appliceras i praktiken. Exempelvis framgår det ej vem som ansvarar för respektive steg, hur man kommer fram till att en registrerad har rätt till begränsning eller vilka tekniska åtgärder som kan vidtas för att säkerställa att uppgifter begränsas.	Gymnasie- och vuxenutbildningsnämnden saknar tydliga instruktioner för hur begäran från registrerade hanteras i praktiken..	2,88

Profilering	Gymnasie- och vuxenutbildningsnämnden använder inte personuppgifter för marknadsföring eller profilering.		N/A

5.4. Funktionsstödsnämnden

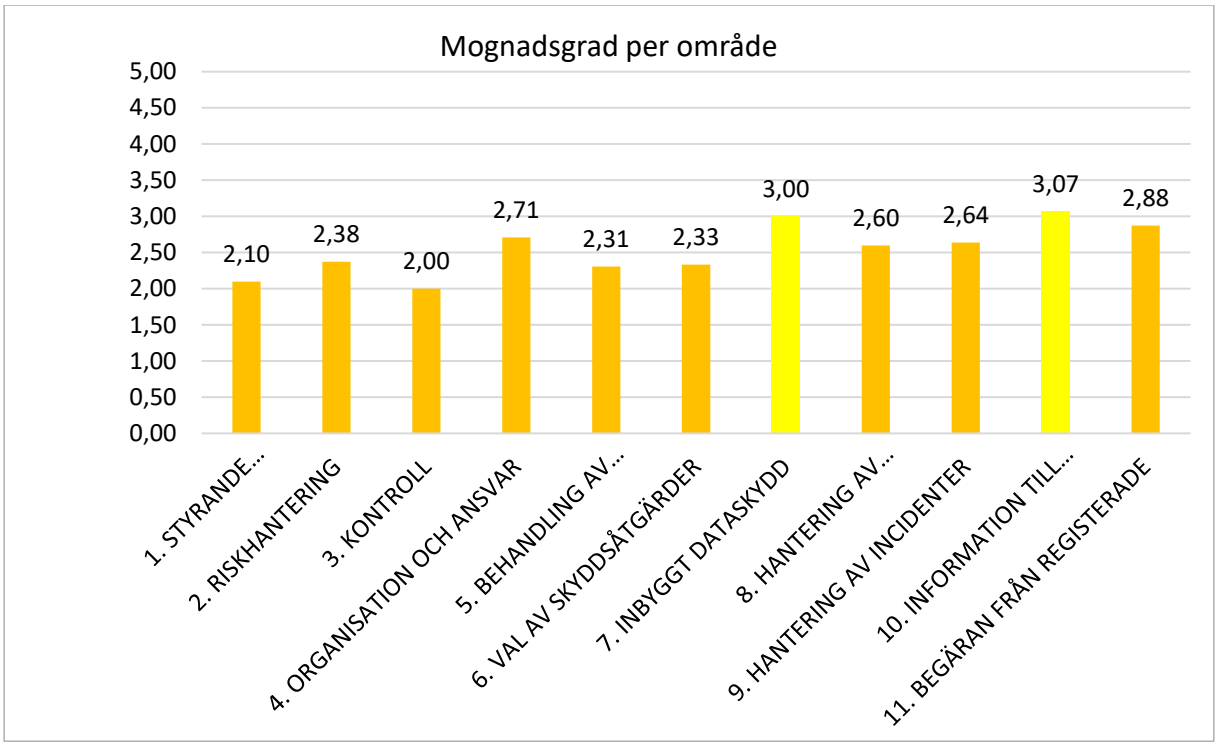
Av granskning konstateras att funktionsstödsnämnden har en mognadsgrad strax under genomsnittet för personuppgiftshantering jämfört med vad EY generellt observerar i en offentlig verksamhet av motsvarande storlek och karaktär. Funktionsstödsnämndens mognadsgrad uppnår en summa av 2,47 av 5,00. Det är vår bedömning att mognadsgraden är låg sett till kommunens storlek, riskbild samt den mängd personuppgifter som nämnden är ansvarig för.

Det är vår bedömning att funktionsstödsnämnden behöver stärka sitt dataskyddsarbete. Nämnden har enligt vår mening inte i tillräcklig utsträckning anpassat kommungemensamma styrdokument och rutiner för den egna verksamheten, eller säkerställt dess efterlevnad. Det är därtill av vikt att nämnden tillser att riskanalyser och konsekvensbedömningar genomförs enligt dokumenterade rutiner. Likaså att registerförteckningen är komplett samt förblir riktig över tid. Det finns enligt vår bedömning ett behov av att se över rutinen för incidenthantering då det inte är styrkt att den efterlevs i praktiken. Slutligen är det vår bedömning att nämnden inte säkerställt att förvaltningen har de nödvändiga resurserna för att bedriva ett ändamålsenligt dataskyddsarbete.

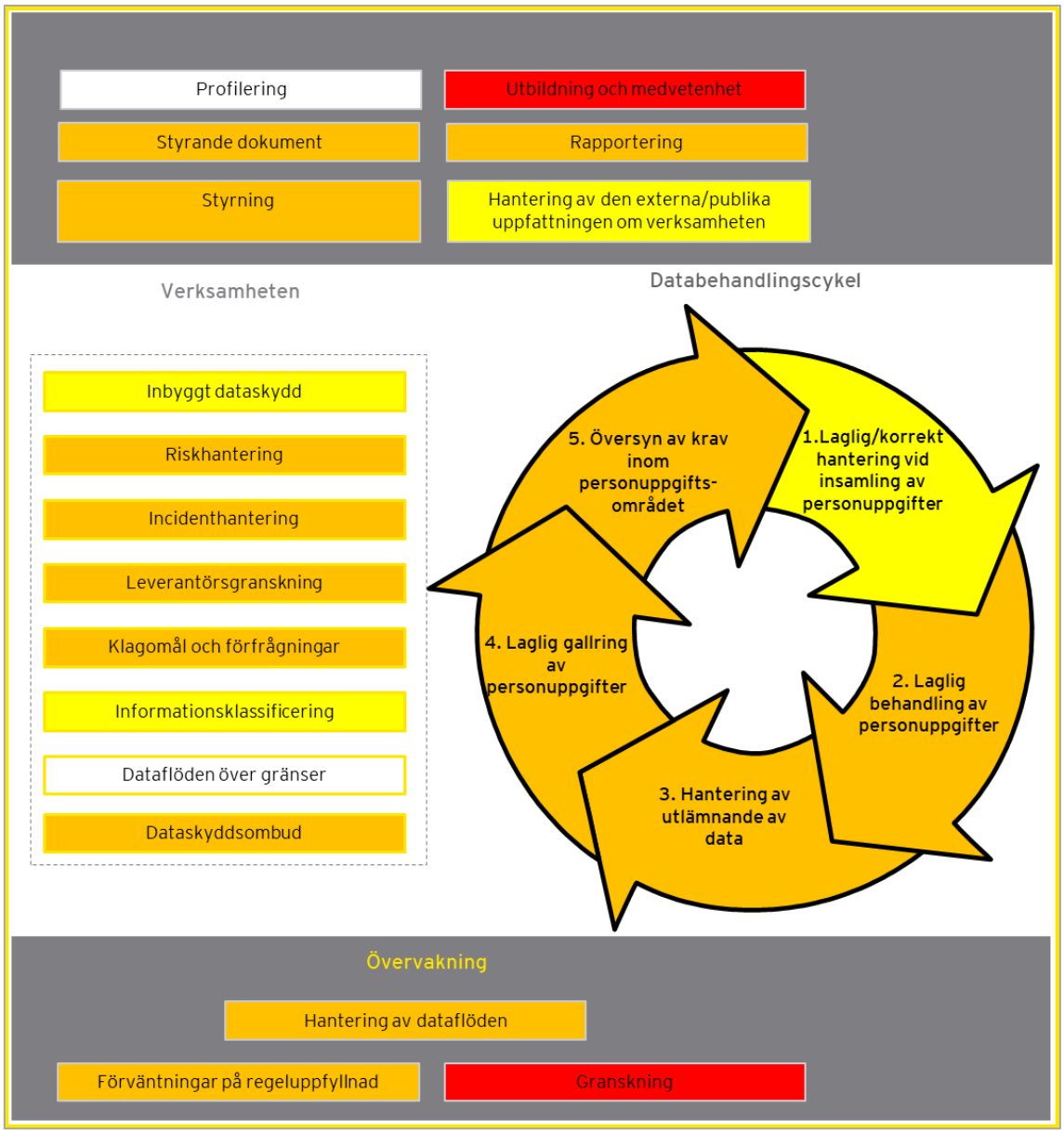
Översiktsbilderna nedan redovisar kommunens mognadsgrad för de 12 huvudområden som granskats, samt nedbrutet på 22 underområden.

Nivå 5 representerar hög mognadsgrad medan nivå 1 representerar låg mognadsgrad. Mognadsgrad beskrivs på en standardiserad skala enligt nedan:

6. Begynnande – Det finns ingen dokumentation eller uppföljning, händelser hanteras ad hoc.
7. 2. Upprepbar – Viss grundläggande dokumentation finns, men denna kan variera mellan olika enheter och vara bristfällig i sin omfattning och tillämpning.
8. Definierad – Det finns dokumenterade processer och dessa tillämpas i stor mån genom hela organisationen.
9. Förvaltad – Förutom väl dokumenterade processer som tillämpas i hela organisationen, finns det dessutom ett system för uppföljning.
10. Optimerad – Baserat på uppföljningen finns också rutiner för kontinuerlig förbättring och uppdatering av processer och ramverk.



Figur 7: Mognadsgrad per område



Figur 8: Grafisk överblick av mognadsgrad per område (notera att de 12 huvudområdena är uppdelade i ytterligare detalj)

Mognadsgraden beskrivs enligt den standardiserade skalan med respektive färgkod. De områden som inte var tillämpliga för granskningen är vita.

5.4.1. Nuläge och iakttagelser

Nedan följer en beskrivning av den övergripande nulägesbild och iakttagelser per område som har identifierats genom granskningen.

Område	Nuläge	Iakttagelser	Mognad
Styrande dokument/ styrning	Funktionsstödsnämnden förlitar sig till stor del på kommungemensamma styrdokument kopplat till behandling av personuppgifter och informationssäkerhet, samt riktlinjer och rutiner kopplat till riskhantering, arkiv- och ärendehantering, personuppgiftsbiträdesavtal, personuppgiftsincidenter, registrerades rättigheter och utlämnande av personuppgifter. Nämnden har till viss del egna rutiner kopplat till de generella riktlinjerna men har inte antagit ytterligare policys. Det sker ingen strukturerad granskning av efterlevnad av styrdokument kopplat till dataskyddsarbetet. Viss granskning genomförs sporadiskt, exempelvis journalgranskning med medicinskt ansvariga, kollegial granskning för att kontrollera att dokumentation sker på korrekt sätt sker, samt loggranskning i vissa system.	Funktionsstödsnämnden har inte säkerställt att styrdokument är anpassade för den egna verksamheten. Det saknas en dokumenterad rutin som säkerställer att styrande dokument förblir uppdaterade och riktiga över tid.	2,10
Risk-hantering	Funktionsstödsnämndens riskhantering utgår från kraven som genereras av klassificeringssystemet. Skyddsåtgärder införs baserat på resultatet från klassificeringen. Det genomförs ingen renodlad riskanalys utifrån ett dataskyddsperspektiv. Det är dock en ingående komponent i de årliga analyserna samt en del av strukturen för klassificeringen. Enligt de intervjuade saknas rutiner för loggar och skyddade personuppgifter som möjliggör identifiering och minimering av risker. Det finns en behovs- och riskö̈versikt avseende behörighetstilldelning som specificerar vad som händer vid för snäv eller för bred åtkomst beroende på befattning. Funktionsstödsnämnden genomför enligt de intervjuade konsekvensbedömningar inför nya eller förändrade behandlingar. Dock genomförs inte strukturerade eller regelbundna	Funktionsstödsnämnden saknar en dokumenterad rutin för hur	2,38

	genomgångar av befintliga behandlingar i syfte att säkerställa deras riktighet. Det saknas också en definierad rutin för hur konsekvensbedömningar ska genomföras.	konsekvensbedömningar ska genomföras.	
Kontroll	Det sker viss uppföljning av arbetet med dataskydd och informationssäkerhet. Funktionsstödsnämnden saknar dock en fastslagen granskningsplan i syfte att säkerställa dataskyddskyddsförordningens efterlevnad. Det har historiskt sett inte genomförts någon kontinuerlig granskning av det övergripande dataskyddsarbetet. Däremot genomförs vissa interna kontroller. Det har upprättats en aktivitetsplan. Enligt aktivitetsplanen lyfts granskning som ett förbättringsområde. Informationssäkerheten har granskats sporadiskt som en del av den interna kontroll.	Det saknas en dokumenterad granskningsplan som med regelbundenhet säkerställer dataskyddsförordningens efterlevnad. Det har ej genomförts strukturerade och regelbundna granskningar av efterlevnaden av dataskyddsförordningen.	2,00
Organisation och ansvar	Funktionsstödsnämnden har roller kopplade till dataskyddsarbetet. Det anses trots detta saknas tillräckligt med resurser för att hantera allt arbete som behöver utföras. Det uppges finnas ett behov av en tydligare systematik för att följa upp arbetet. Nämnden har under pandemin uppmärksammat ett ökat behov av resurser för arbetet med informationssäkerhet och dataskydd. Risker kopplade till de område som är i behov av utökade resurser har lyfts med nämnden. De har dock inte brutits ned i konkreta steg eller handlingsplaner. Enligt de intervjuade finns det en god dialog med nämnden och en plan för att utöka budgeten för dataskyddsarbetet under 2022. Förvaltningen samverkar med DSO genom att delta i nätverksträffar och söka stöd hos DSO i samband med incidenter. Kommunstyrelsen har de två senaste åren haft två olika vikarierande DSO. Tillgängligheten och arbetssättet har varierat. Detta har i sin tur	Funktionsstödsnämnden saknar tillräckliga resurser för att utföra önskat dataskydds- och informationssäkerhetsarbete. Kommunstyrelsen har inte säkerställt att DSO har möjlighet att ge	2,71

	resulterat i att nämnden inte alltid fått det stöd som de efterfrågat. Informationssäkerhetssamordnaren och dataskyddssamordnaren har utöver dessa roller även andra arbetsuppgifter inom förvaltningen. I samband med att GDPR infördes fanns det dedikerade arbetsgrupper med uppgift att utarbeta styrdokument och riktlinjer. Bland annat utarbetade dessa registerförteckningar och informationsmaterial.	funktionsstödsnämnden det stöd som efterfrågas.	
Behandling av person-uppgifter	Funktionsstödsnämnden använder den kommungemensamma e-tjänsten för att på begäran lämna ut personuppgifter. Den registrerades identitet säkerställs via bank-id. I de fall begäran görs via blanketter skickas utdrag via rekommenderat brev. Funktionsstödsnämnden tillämpar även de kommungemensamma rutinerna för samtycke, vilka framförallt används vid insamling av bilder och liknande information. Funktionsstödsnämnden hanterar omfattande personuppgifter kopplat till anställda och brukare. Uppgifter förekommer dels i fysiskt arkiv på grund av lagkrav om förvaring av original, dels i IT-system. Avvikelse- och journalhantering förs digitalt. HR-system och avvikelsesystem är fristående och synkroniseras inte automatiskt med varandra. Funktionsstödsnämnden har tidigare fört sin registerförteckning i en excel-fil. Numera förs registerförteckning genom det kommungemensamma systemstödet. Vid upprättande av en ny behandling frågar dataskyddssamordnaren om hur registret eller behandlingen är tänkt att användas samt informerar om vikten av laglig grund. Information om personuppgiftsbehandling finns även på intranätet. Periodiska granskningar i syfte att säkerställa att registerförteckningar är riktiga och kompletta över tid görs inte. Påminnelser om att		2,31

	uppdatera förteckningar sker ej regelbundet utan endast ad hoc. Det finns arkivbestämmelser och rutiner för hur och när gallring ska genomföras. Vissa system har stöd för automatisk gallring. Om sådant stöd saknas förlitar sig nämnden på rutinerna enligt arkivbestämmelserna. Det saknas systematik för att dokumentera granskning av förteckningar. Enligt de intervjuade förekommer det troligtvis ingen anonymisering av data gällande brukare. Däremot förekommer det viss anonymiserad statistik för att följa upp delar av förvaltningens arbete. Det finns planer på att införa pseudonymisering genom kundnummer istället för personnummer. Funktionsstödsnämnden har inte genomfört djupare analyser av dataflöden. Kravställning vid upphandling av system finns upprättat. Enligt de intervjuade hålls uppföljningsmöten varje kvartal eller oftare beroende på leverantörens storlek, dock ej med specifikt fokus på dataskydd.	Funktionsstödsnämnden saknar en definierad rutin för att säkerställa att registerförteckningar är komplett och förblir riktig över tid. Funktionsstödsnämnden saknar en dokumenterad process för att säkerställa att gallring utförs enligt definierad rutin.	
Val av skydds-åtgärder	Funktionsstödsnämnden skiljer på känsliga och vanliga personuppgifter som en del av klassificeringsarbetet där typ av personuppgift anges i både klassificeringsprotokoll och klassificeringssystem. För klassificering av strukturerad information används både protokoll och system. Protokollet liknar till stor del systemet men innehåller mer information. Enligt de intervjuade genomförs ingen klassificering av ostrukturerad data. De har historiskt sett inte haft full insyn i vilka ostrukturerade data som innehas. Dataskyddssamordnaren är involverad vid klassificering av nya system och kontaktas av anställda på avdelningarna vid eventuella förändringar. När GDPR infördes genomfördes en utbildningsinsats i genom att dataskyddssamordnare informerade om GDPR för verksamheterna. Det finns en introduktionsutbildning där GDPR ingår och en checklista för nyanställda där	Rutinen för klassificering av informationstillgångar behöver utvecklas och kompletteras med tydligare instruktioner med avseende på ostrukturerad data .	2,33

	informationssäkerhet ingår. Enligt de intervjuade är en ny film om informationssäkerhet på väg där delar av GDPR ingår. I november 2021 planerade (vid tidpunkten då denna granskning genomfördes) funktionsstödsnämnden att genomföra en informationssäkerhetsutbildning med inslag av GDPR. Det kommer däri finnas möjlighet att följa upp vilka som har slutfört utbildningen. Ambitionen är att utbildningarna ska vara obligatoriska men detta är inte fastställt. Det finns ingen dokumentation eller uppföljning som styrker att utbildningar är obligatoriska samt att anställda har fått den utbildning de behöver.	Funktionsstödsnämnden har inte säkerställt att samtliga anställda får den utbildning de behöver kopplat till dataskyddsförordningen. Det saknas en dokumenterad plan för hur funktionsstödsnämnden ska arbeta med utbildningar kopplat till dataskyddsfrågor.	
Inbyggt dataskydd	Informationssäkerhetssamordnare och dataskyddssamordnare har tagit hjälp av en stadsjurist för utformandet av behörighetstilldelning. Det är sektionschefen på respektive verksamhet som har i uppgift att lägga till och avsluta personalens behörigheter. Det finns en rutin för behörighetsansökan till vissa system. Det saknas dock en dokumenterad rutin för samtliga system avseende hur behörighetskontroller ska utföras. Det genomförs i dagsläget ingen periodisk genomgång av IT-behörigheter. Det saknas tillräckliga resurser för detta. Däremot förekommer vissa periodiska granskningar av behörigheter, exempelvis en månatlig stickprovskontroll för loggranskning av journaler för att kontrollera att rätt brukare finns på rätt ställe. Efter 90 dagars inaktivitet låser sig systemet. Då kontaktas verksamhetschefer för att genomföra kontrollen. För de system som saknar inbyggd kontroll är det verksamhetschefens uppgift att kontrollera att rätt person har rätt behörighet. Journalsystemet har begränsad åtkomst. Beroende på yrkeskategori och verksamhet tilldelas olika typer av behörigheter. Under pandemin uppstod en ökad systemadministration vilket de intervjuade ser som ett tecken på att behörigheterna fungerar	Det saknas en dokumenterad rutin för hur behörighetskontroller ska utföras i samtliga IT-system inom Funktionsstödsnämnden. Periodiska granskningar av behörigheter utförs ej för samtliga system.	3,00

	som de ska. För IT-drift och systemförvaltning ges en normal behörighet för vanlig åtkomst och en speciell behörighet som endast används för att genomföra förändringar i systemet.		
Hantering av leverantörs-relationer	Enligt de intervjuade finns PUB-avtal för samtliga upphandlade system. En inventering av nämndens leverantörer utfördes i samband med att GDPR trädde i kraft. Detta sker enligt de intervjuade regelbundet. Däremot saknas tydliga rutiner som säkerställer att personuppgiftsbiträden hanteras på ett sätt som innebär att dataskyddsförordningen efterlevs över tid. Nämnden använder ett system för att bygga flöden där uppdatering eller tillägg av en process leder till klassificering. Därmed sker en indirekt automatisk revidering av PUB-avtalen. Medarbetare med roller inom dataskydd och informationssäkerhet involveras i tidigt skede vid upphandling. För de system som Funktionsstödsnämnden själv ansvarar för sker ingen datalagring utanför EES/EU.	Funktionsstödsnämnden saknar en rutin för att säkerställa att leverantörer lever upp till definierade kravställningar inom dataskyddsarbetet över tid.	2,60
Hantering av incidenter	Funktionsstödsnämnden följer de kommungemensamma rutinerna för hantering av incidenter. Incidenter rapporteras tillika i det kommungemensamma systemet. Incidenter kan därtill fångas upp i ytterligare system inom nämnden. Medarbetare kan enligt rutin rådgöra med dataskyddssamordnaren om en incident är en personuppgiftsincident eller ej. Detta innebär att dataskyddssamordnaren ofta involveras redan innan incidenten har rapporterats i det kommungemensamma systemet. Samråd sker med ansvarig chef vid allvarliga incidenter. Förvaltningsdirektören involveras för att bedöma om incidenten ska anmälas till IMY. Vid allvarliga incidenter rapporterar förvaltningsdirektören till nämnden. Enligt de intervjuade finns det rutiner för hur en incident ska utredas. Interna rapporter sparas i nämndens arkivsystem. Det är dock inte säkerställt att rutinen efterlevs i praktiken.	Funktionsstödsnämnden har inte säkerställt att den definierade	2,64

	Informationssäkerhetssamordnaren och dataskyddssamordnaren informeras oftast om incidenter i ett tidigt skede. Dataskyddssamordnaren och informationssäkerhetssamordnaren diskuterar förslag på åtgärdsplaner för att förhindra att en incident händer igen.	incidenthanteringsrutinen efterlevs i praktiken.	
Information till registrerade	Funktionsstödsnämnden tillämpar samtyckesblanketter vid insamling av ljud och bild som berör barn. Vårdnadshavare får information om insamlingens syfte vid ansökan om insats. Blanketter och information finns på hemsidan och omfattas av lagstiftning kopplat till Hälso- och sjukvårdslagen (HSL) samt lagen om särskilt stöd (LSS). Vid större incidenter och kriser har DSO i uppgift att föra kriskommunikation avseende dataskyddsfrågor. Kommunikationsavdelningen inom kommunstyrelsens verksamhetsområde kan erbjuda stöd när det gäller kriskommunikation. Funktionsstödsnämnden förlitar sig på kommunstyrelsens personal för jour utanför normal arbetstid.		3,07
Begäran från registrerade	Funktionsstödsnämnden utgår från de kommungemensamma riktlinjerna gällande hantering av personuppgiftsbehandlingar och rutiner för begäran från registrerade. Nämnden använder den kommungemensamma e-tjänsten samt blanketter. Ibland inkommer förfrågningar via e-post och brev. Varje gång en begäran om radering inkommer görs en enskild prövning. Det är trots detta inte mycket information som får raderas, men samtycke kan dras in direkt. Det finns centrala rutiner för hantering av begäran från registrerade, men det saknas tydliga instruktioner för hur rutinerna för hantering av begäran från registrerade appliceras i praktiken. Exempelvis framgår det ej vem som ansvarar för respektive steg, hur man kommer fram till att en registrerad har rätt till begränsning eller vilka tekniska åtgärder som kan vidtas för att säkerställa att uppgifter begränsas.	Funktionsstödsnämnden saknar tydliga instruktioner för hur begäran från registrerade hanteras i praktiken.	2,88

Profilering	Funktionsstödsnämnden använder inte profilering i dagsläget.		N/A

Bilaga 2: Förteckning över intervjuade funktioner

5.6. Stadskontoret

- Avdelningschef, stadskontoret
- Dataskyddsombud
- Strategisk samordnare-informationssäkerhet
- Stadsjurist, IT och informationssäkerhet
- Stadsjurist, stadskontoret

5.7. Serviceförvaltningen

- IT- och informationssäkerhetssamordnare.
- Utvecklingssekreterare/Dataskyddssamordnare

5.8. Gymnasie- och vuxenutbildningsförvaltningen

- Dataskyddssamordnare
- Kanslichef för nämndkansli
- Utvecklingssekreterare

5.9. Funktionsstödsförvaltningen

- Chef, strategiska avdelningen
- Dataskyddssamordnare
- Enhetschef, Systemförvaltning och utveckling
- IT- och informationssäkerhetssamordnare.

6. Bilaga 3: Dokumentförteckning

6.1. Kommunstyrelsen

- Arkivredovisning 2021-211.pdf
- Begäran om registerutdrag (personuppgifter) (1).docx
- Begäran om rättelse, radering, begränsning, dataportabilitet eller invändning.pdf
- Beslutad ärendehandbok 4.0 2020-09-24.pdf
- Bilaga 1 - Blankett för anmälan om personuppgiftsincident.docx
- Bilaga 2 - Detaljerade bestämmelser och exempel på incidenter.pdf
- Dataskyddsförordningen - Program del 2 - Roller och ansvar.pdf
- dataskyddskrav.xlsx
- Försättsblad till registerutdrag (personuppgifter).docx
- GDPR - Malmö stads förhållningssätt för bilder och filmer.pdf
- GDPR info-presentation.pptx
- IT-system på STK.xlsx
- Klassningsmatris.JPG
- Krav utifrån lagstiftning GDPR.xlsx
- Kravlista nivå 1 Mindre viktig.xls
- Kravlista nivå 2-Viktig.xls
- Kravlista nivå 3-Mycket viktig.xls
- Intern rättsakt - när en nämnd hanterar personuppgifter åt en annan nämnd.docx
- Lathund Personuppgifter hos kommunen - handläggning NR.docx
- Mall för modellavtal (på engelska) - Bild och film.docx
- Mall för personuppgiftsbiträdesavtal - In English.docx
- Mall för personuppgiftsbiträdesavtal - Instruktion - In English.docx
- Mall för personuppgiftsbiträdesavtal- instruktion (1).docx
- Mall för personuppgiftsbiträdesavtal.docx
- Mall för samtycke - Bild och film.docx
- Mall för samtycke (på engelska) - Bild och film.docx
- Protokoll för invent och klass ver 2021-07-13.pdf
- Riktlinjer för behandling av personuppgifter i Malmö stad - KS den 2 maj 2018.pdf
- Riktlinjer för infosäk ver 2019 BESLUTAD KSAU.pdf
- Rutin för handläggning av personuppgiftsincident.pdf
- Rutin för hantering av personuppgiftsbiträdesavtal tecknade för kommungemensamma lösningar (2).docx
- Rutin för systemsäk ver 7.0 191029.pdf
- Rutiner för begäran om begränsning av behandling.pdf
- Rutiner för begäran om dataportabilitet.pdf
- Rutiner för begäran om radering.pdf
- Rutiner för begäran om registerutdrag.pdf
- Rutiner för rättelse av personuppgifter.pdf
- Överenskommelse om servicenivå för kommungemensam tjänst.docx
- §24 KS AU Utseende av dataskyddsombud(2290817).pdf

6.2. Servicenämnden

- Förteckning över sidor med processer kopplade till serviceförvaltningens GDPR.docx
- Informationssäkerhet serviceförvaltningen utbildningsunderlag.pdf
- Infosäk på Serviceförvaltningen version sept 2020.pptx
- Mall GDPR-utbildning.pptx
- Mall för att registrera personuppgiftsbiträdesavtal.pdf
- Mall för registrering av begäran enligt dataskyddsförordningen (GDPR).pdf
- Mall för registrering av personuppgiftsincident i Platina.pdf
- PUBA för interna överenskommelser
- Registerförteckning HR Service.xlsx
- Registerförteckning HR-avdelningen.xlsx
- Registerförteckning ITD 20210906.xlsx
- Registerförteckning ITS.xlsx
- Registerförteckning Kommunteknik.xlsx
- Registerförteckning Kommuntjänster.xlsx
- Registerförteckning Kontaktcenter.xlsx
- Registerförteckning Skolrestauranger.xlsx
- Registerförteckning Staben.xlsx
- Registerförteckning Stadsfastigheter.xlsx
- Riktlinjer för lagring och delning av sekretess och personuppgifter.pdf.xlsx
- Rutin för skanning av sekretess och personuppgifter.pdf.xlsx
- Utskriftsversion av informationssäkerhetsmatris.pdf.xlsx

6.3. Gymnasie- och vuxenutbildningsnämnden

- GVF Rutiner för foto och film i pedagogisk verksamhet.docx
- GVF Rutiner gällande registrerades rättigheter.docx
- Samtycke foto och film GYVUX.docx

6.4. Funktionsstödsnämnden

- Arkivredovisning för funktionsstödsnämnden.pdf
- Bilaga Behovs- och riskö̈versikt för FSF avseende behörighetstilldelning.pdf
- Funktionsstödsnämndens delegationsordning, version 2.7 (FSN-2018-1147).pdf
- Information om GDPR.pdf
- Information+till+patient+om+personuppgiftshantering+2018-10-12.pdf
- Rutin för behörighetstilldelning till system som hanterar patientuppgifter.pdf
- rutin för hantering av allmänna handlingar.pdf
- Rutin för journalföring och behandling av personuppgifter.pdf
- Rutin för skanning, gallring och arkivering av patientjournaler 2021.pdf
- Rutin för åtkomst och loggranskning av HSL-journal.pdf
- Rutiner för behörighetsansökan till Lifecare-Procapita 19-02-26.pdf
- Utlämnande av journalhandling (FSF).pdf

7. Bilaga 4: Definitioner

Behandling: Med behandling menas varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte, t.ex. insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring.

Dataskyddsombud (DSO): Myndigheter och offentliga organ är skyldiga att utse dataskyddsombud. Dataskyddsombudets uppgifter är bland annat att informera och ge råd inom den egna organisationen om vilka skyldigheter som gäller enligt såväl förordningen som nationella bestämmelser. Ombudet ska också bevaka att dessa regler följs och ge råd om den konsekvensbedömning avseende dataskydd som ska göras enligt förordningen. Slutligen ska ombudet fungera som kontaktpunkt för dataskyddsmyndigheten och samarbeta med denna.

EU/EES: EU står för den Europeiska unionen och EES för Europeiska Ekonomiska Samarbetsområdet. I EU ingår följande länder Belgien, Bulgarien, Cypern, Danmark, Estland, Finland, Frankrike, Förenade Kungariket, Grekland, Irland, Italien, Lettland, Litauen, Luxemburg, Malta, Nederländerna, Polen, Portugal, Rumänien, Slovakien, Slovenien, Spanien, Sverige, Tjeckien, Tyskland, Ungern, Österrike. I EES ingår utöver länderna i EU även Island, Liechtenstein och Norge.

Förhandssamråd: Om man vid en konsekvensbedömning bedömer att behandlingen skulle leda till en hög risk om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken måste man samråda med Integritetsskyddsmyndigheten.

Informationsklassning: Klassning av organisationens informationstillgångar enligt i riktlinjer dokumenterade regler med avseende på informationens sekretess, riktighet och tillgänglighet.

Informationssäkerhet: Berör i huvudsak säkerhetsfrågor som berör information, oberoende av system, eller plattformar.

Konsekvensanalys: Innan man inleder en behandling av personuppgifter som kan leda till en hög risk för integritetsintrång till exempel ett omfattande register med känsliga personuppgifter, måste man bedöma konsekvenserna för de registrerade (konsekvensbedömning).

Känslig personuppgift: Exempel på känsliga personuppgifter är ras och etniskt ursprung, politisk åsikt, religiös eller filosofisk övertygelse, biometriska och genetiska data,

medlemskap i fackförening, hälsa eller uppgifter om fysisk persons sexualliv eller sexuell läggning.

Personuppgift: Med personuppgift avses all slags information som direkt eller indirekt kan hänföras till en fysisk levande person, d.v.s. medborgare, anställda m.fl. Exempel på personuppgifter är namn, personnummer, telefonnummer, bank- och kontouppgifter, IP-adress, försäkringsnummer m.m.

Personuppgiftsansvarig: Med personuppgiftsansvarig avses en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.

Personuppgiftsbiträde: Med personuppgiftsbiträde avses en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för personuppgiftsansvarigs räkning.

Personuppgiftsincident: En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Policy och instruktion: Avser dokumentation av rutiner på ett eller annat sätt. I denna rapporten görs ingen skillnad på om dokumentationen är antagen på politisk eller tjänstemannanivå.

Profilering: Varje form av automatisk behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar.

Pseudonymisering: Behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används. De kompletterande uppgifterna ska förvaras separat och vara föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person.

Register: En strukturerad samling av samtliga personuppgiftsbehandlingar som företas inom verksamheten.

Registrerad: Med registrerad avses den enskilde vars personuppgifter behandlas.

Samtycke: Med samtycke avses varje slag av frivillig, specifik, informerad och otvetydig viljeyttring från den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne.

Tillsynsmyndighet: En oberoende offentlig myndighet som är utsedd av en medlemsstat. I Sverige är Integritetsskyddsmyndigheten tillsynsmyndighet.

Tredje land: Med tredje land avses ett land som inte är medlem i EU eller EES. En överföring till tredje land är när personuppgifter som behandlas i ett EU- eller EES-land görs tillgängliga i ett land utanför EU/EES-området. Exempelvis när personuppgifter i ett datoriserat register skrivs ut och skickas i pappersform eller när personuppgifter skickas via e-post. Personuppgifter får föras över endast om det finns en adekvat skyddsnivå i mottagarlandet eller om det finns särskilda garantier för att uppgifterna och de registrerades rättigheter skyddas.

Tredje part: Med tredje part avses en fysisk eller juridisk person, offentlig myndighet, institution eller organ som inte är den registrerade, den personuppgiftsansvarige, personuppgiftsbiträdet eller de personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar är behöriga att behandla personuppgifterna.