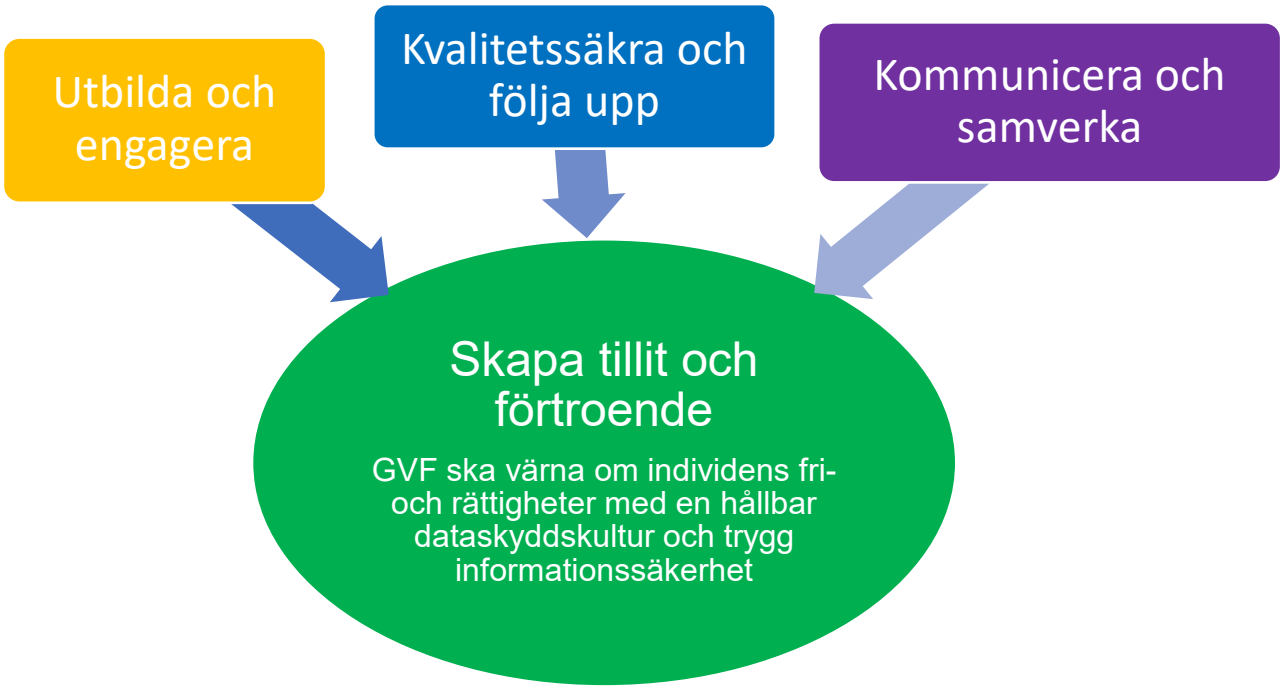
Malmö stad

2023-02-09

Gymnasie- och vuxenutbildningsförvaltningen

Ansvar och organisation för dataskydd och informationssäkerhet



Alla verksamheter måste följa dataskyddsreglerna vid behandling av personuppgifter. Oavsett om det är en offentlig myndighet, ett privat företag, en förening eller någon annan typ av verksamhet.

Dataskyddsreglerna grundar sig i de mänskliga rättigheterna. Alla människor har rätt till respekt för privat- och familjeliv och till skydd av sina personuppgifter. Här kan ni läsa mer om vilka skyldigheter ni har när ni hanterar personuppgifter i er verksamhet.

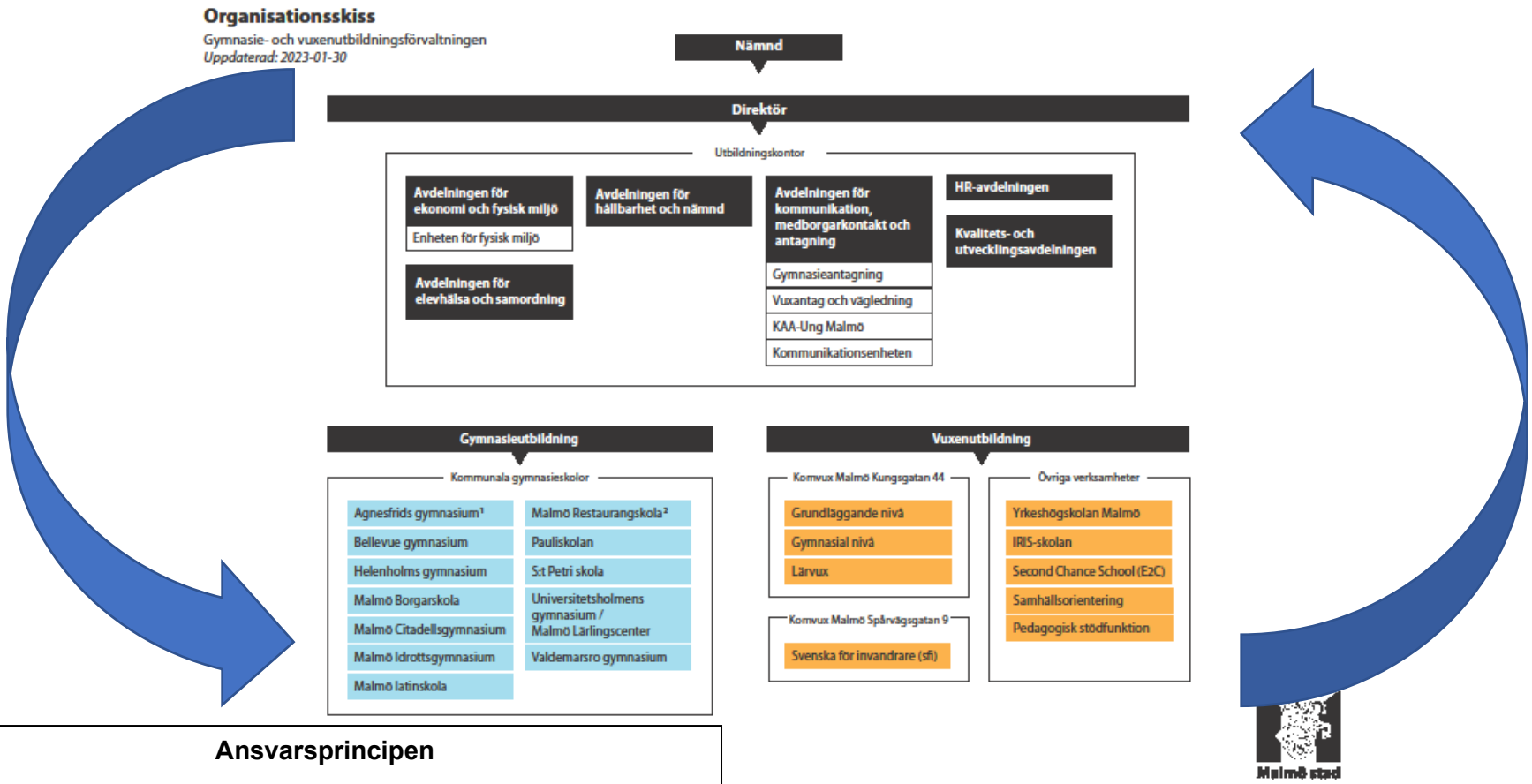
Informationssäkerhetsarbete är att arbeta förebyggande och att kontinuerligt anpassa skyddet utifrån organisationens behov och risker. Då finns informationen tillgänglig när vi behöver den, vi kan lita på att den är riktig och inte manipulerad och att endast behöriga personer får ta del av den.

På Malmö stads sida för Styrdokument | Komin finns följande.
Riktlinjer för behandling av personuppgifter i Malmö stad | Komin
Malmö stads riktlinjer för informationssäkerhet | Komin

Gymnasie- och vuxenutbildningsförvaltningen
Storgatan 20
Postadress: 205 80 Malmö
Telefon: 040-34 30 34
E-post: gyvux@malmo.se
Org.nr: 212000-1124
malmo.se/gvf

Malmö stad

Ansvar för dataskydd och informationssäkerhet



Ansvarsprincipen

Ansvaret för personuppgiftsbehandling och informationshantering och därmed även för dataskydd och informationssäkerheten följer det ordinarie verksamhetsansvaret inom nämndsorganisationen. Detta ansvar gäller från nämnd till enskild medarbetare.

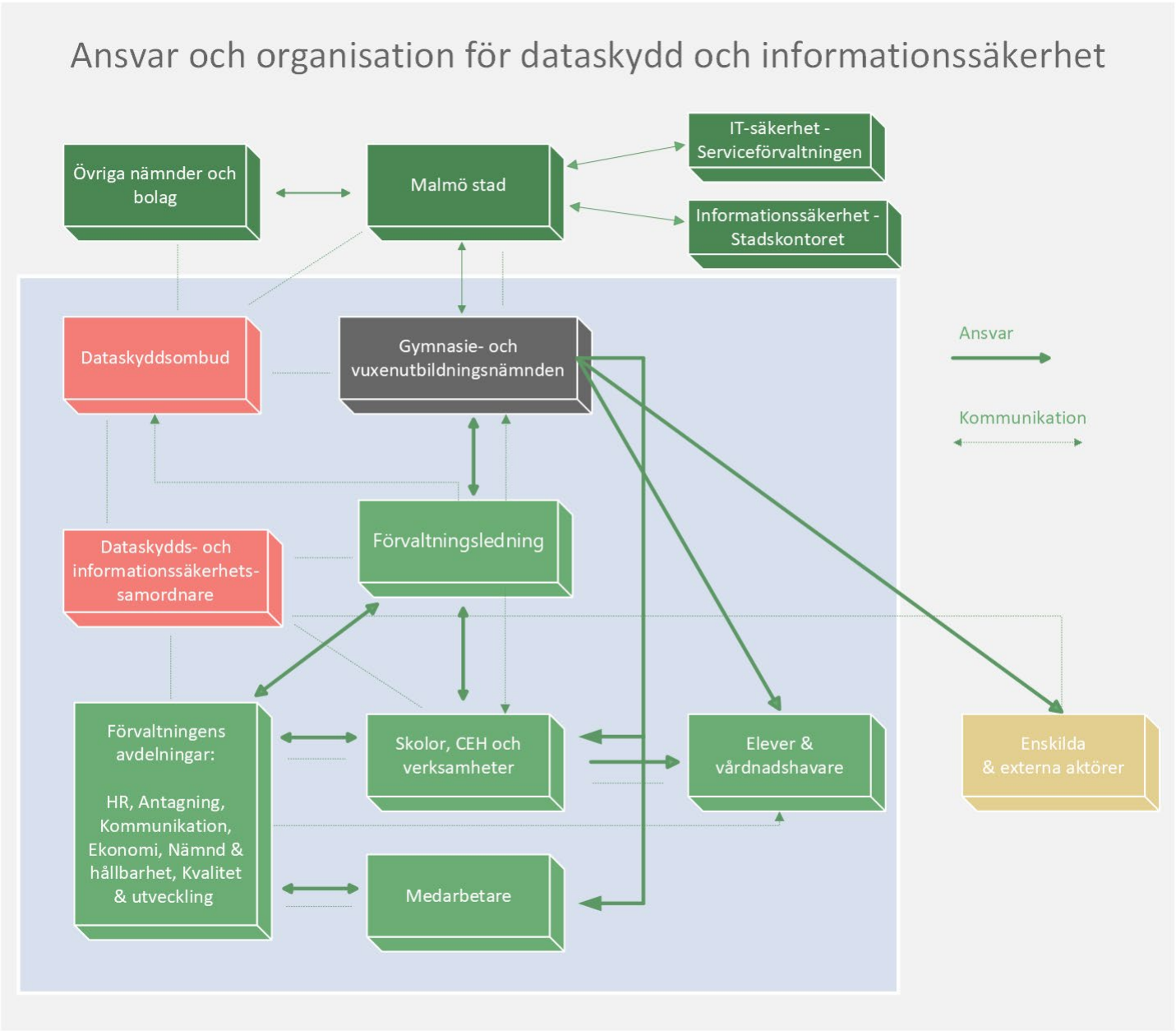
Utöver detta gäller att den som är ansvarig ensamt eller tillsammans med andra för en viss process, projekt eller uppdrag även ansvarig för dataskydd och informationssäkerhet inom sitt ansvarsområde

Ansvar för uppföljning och återrapportering

Medarbetare, chefer och ledning har ett ansvar att följa upp, rapportera brister och åtgärder till nämnden.

Malmö stad

Ansvar och organisation för dataskydd och informationssäkerhet



Malmö stad

Gymnasie- och vuxenutbildningsnämnden är personuppgiftsansvarig

Personuppgiftsansvarig (PuA) är den som ensamt eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.[1] Malmö stads nämnder och helägda bolag är personuppgiftsansvariga för sina respektive verksamhetsområden. Nämnden ansvarar bland annat för följande.

- Är ytterst ansvariga för att personuppgiftsbehandlingen efterlever dataskyddsförordningens krav och ska kunna visa detta.
- Ska bedriva aktivt och strukturerat dataskyddsarbete i enlighet med riktlinjen och tillämplig lagstiftning.
- Ska kunna vis att behandlingen uppfyller dataskyddsförordningens krav genom dokumentation, konsekvensbedömningar och verifierande tester.
- Ska tillse att det finns lämplig organisation på plats som innehar rätt kompetens, tillräckligt med tid och resurser att arbeta med dataskyddsfrågorna kontinuerligt.
- Ska genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen. Den personuppgiftsansvarige skall ta hänsyn till behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter. Dessa åtgärder skall ses över och uppdateras vid behov. Om det står i proportion till behandlingen ska den personuppgiftsansvarige även genomföra lämpliga strategier för dataskydd.[2]
- Ska tillse att anställda är informerade om hur behandling av personuppgifter skall utföras i enlighet med tillämplig dataskyddslagstiftning.
- Ska föra register över personuppgiftsbehandling som utförts under dess ansvar.[3]
- Ska utse dataskyddsombud (DSO) för sina respektive verksamhetsområden och svara för att denne har förutsättningar för att fullgöra sitt uppdrag.

[1] Art. 4 dataskyddsförordningen (EU) 679/2016
[2] S.k. *accountability* (engelska), *ansvarsskyldighet* (svenska), se bl.a. art. 24 dataskyddsförordningen (EU) 279/2016
[3] Art. 30 dataskyddsförordningen (EU) 679/2016

Dataskydd - Ansvar och roller

Beakta alltid att **ansvarsfördelningen** i arbetet kopplat till dataskyddsförordningen är tydligt definierad samt efterlevs i praktiken.

Säkerställ att det finns **tillräckliga resurser** för att utföra ett ändamålsenligt arbete kopplat till dataskyddsförordningen.

Informationsägare

- Den personuppgiftsansvarige ansvarar för att det finns informationsägare för varje personuppgiftsbehandling
- Informationsägaren är tjänstepersonen som tar initiativ för personuppgiftsbehandlingen och har det operativa ansvaret för behandling av personuppgifter inom verksamhetsområdet.
- Informationsägaren ska kunna lämna ytterliga information och besvara i frågor som rör den särskilda personuppgiftsbehandlingen.

Systemägare

- Säkerställer att personuppgiftsbiträdesavtal finns och följs.
- Ansvarar för att säkerställa tekniska och organisatoriska åtgärder i systemet.
- Ansvarar för konsekvensbedömning avseende dataskydd.

Systemförvaltare

- Bistår systemägare och verksamheten avseende tekniska och organisatoriska åtgärder samt konsekvensbedömning.
- Ombesörjer sökning av information vid begäran om registerutdrag samt bistår vid övriga begäranden kring den registrerades rättigheter

Chefsbefattningar

- Chef (oavsett nivå) ansvarar för att sin verksamhet uppfyller kraven på dataskydd.
- Varje chef ansvarar för att deras medarbetare är informerade om hur behandling av personuppgifter ska utföras i enlighet med riktlinjen och tillämplig dataskyddslagstiftning.
- Du som chef ansvarar för informationen i din verksamhet, även kallad informationsägare.
- Du som informationsägare ansvarar för att alla personuppgiftsbehandlingar blir registrerade och hålls uppdaterade över tid.

Medarbetare

- Medarbetare inom nämnden ansvarar för att följa riktlinjer vid behandling av personuppgifter.
- Anställda ska hålla sig informerade om hur behandling av personuppgifter ska utföras i enlighet med dessa riktlinjer och tillämplig dataskyddslagstiftning.

Dataskydds- och informationssäkerhetssamordnare

- Tjänsteperson som samordnar det aktiva dataskydds- och informationssäkerhetsarbetet inom verksamhetsområdet.
- Vara den primära kontaktpunkten inom förvaltningen gällande alla frågor som rör dataskydd och informationssäkerhet.
- Fungera som kontaktyta för dialog om dataskydd och informationssäkerhet mot förvaltningens ledningsgrupp.
- Följa upp inom förvaltningen vidtagna åtgärder.
- Utföra och understödja informationsspridning och utbildning inom förvaltningen.
- Hantera begäran enligt registrerades rättigheter (ex. registerutdrag) inom förvaltningen, i samarbete med verksamheterna.
- Ingå i centralt nätverk för frågor som rör dataskydd och informationssäkerhet.
- Hantera personuppgiftincidenthantering.
- Följa upp PUB-avtal som förvaltningen/verksamheten i egenskap av informationsägare ansvarar för.
- Samordna nätverk och organisation för dataskydds- och informationssäkerhetsfrågor inom förvaltningen.
- Samverka med arkivarie/arkivansvarig i frågor som rör bevarande och gallring samt övriga frågor inom arkivområdet.

Dataskyddsombud (DSO)

- Den personuppgiftsansvarige ska utse ett dataskyddsombud och tillse att denne har tillräckligt med tid och resurser för att fullgöra sitt uppdrag.[4]
- Informera och ge råd till den personuppgiftsansvarig och de anställda om deras skyldigheter enligt tillämplig dataskyddslagstiftning.

[4] Se art. 37 dataskyddsförordningen (EU) 679/2016 för ytterligare information om utnämning av dataskyddsombud. Det är obligatoriskt att utnämna ett dataskyddsombud om behandlingen genomförs av en myndighet eller ett offentligt organ, kärnverksamhet består av behandling som kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning, eller kärnverksamhet består av behandling i stor omfattning av särskilda kategorier av uppgifter enligt art. 9 och personuppgifter som rör fällande domar i brottmål och överträdelser enligt art. 10. Tillsynsmyndigheten rekommenderar att verksamheten utser ett dataskyddsombud, även om de inte måste, exempelvis om de utför arbetsuppgifter av allmänt intresse eller myndighetsutövning.

- Övervaka efterlevnaden av dataskyddsförordningen och den personuppgiftsansvariges strategi för skydd av personuppgifter, inklusive ansvarstilldelning, information till och utbildning av personal som deltar i behandling och tillhörande granskning.
- På begäran ge råd vad gäller konsekvensbedömningen avseende dataskydd och övervaka genomförandet av den enligt artikel 35.
- Samarbeta med tillsynsmyndigheten.
- Fungera som kontaktpunkt för tillsynsmyndigheten i frågor som rör behandling, inklusive förhandssamråd.
- Vid utförandet av sina uppgifter ta vederbörlig hänsyn till de risker som är förknippade med personuppgiftsbehandling, med beaktande av behandlingens art, omfattning, sammanhang och syften.
- Se avsnitt 3.3 i riktlinjen för ytterligare information om dataskyddsombudets roll och ställning.

Informationssäkerhet

Genom god informationssäkerhet i samhället kan man främja[5]

- samhällets effektivitet och kvalitet i informationshantering,
- näringslivets lönsamhet och tillväxt,
- samhällets brottsbekämpning och beredskap mot allvarliga störningar och kriser,
- medborgares fri- och rättigheter samt personliga integritet,
- medborgares och verksamheters förtroende för informationshantering och IT-system.

Informationshantering

Ansvaret för informationssäkerheten ska vara tydligt. All information som Malmö stad äger eller på annat sätt ansvarar för ska behandlas på ett säkert och korrekt sätt. Skyddet av information ska anpassas efter dess skyddsvärde, rådande förutsättningar, hot och risker.

Medarbetare

Alla medarbetare ska ha tillräckliga kunskaper om informationssäkerhet i förhållande till sin roll och arbetsuppgifter. De ska vara säkerhetsmedvetna och ha god kännedom om de hot och risker som finns och hur de kan skydda sig mot dem. Det gäller även konsulter, leverantörer, praktikanter och personuppgiftsbiträden samt andra uppdragstagare som behandlar information för Malmö stads räkning.

Process

Informationssäkerhet ska vara ett integrerat perspektiv och en medveten del av verksamhetens arbetsprocesser och informationshantering. Arbetet ska bedrivas genom ett systematiskt, riskbaserat och långsiktigt perspektiv samt involvera relevanta kompetenser utifrån informationens skyddsvärde och verksamhetens behov.

Teknik

Malmö stads informationssystem ska vara robusta, funktionella och säkra med utgångspunkt i informationens skyddsvärde, riskbild och verksamhetens behov. Detta inkluderar även de informationssystem som Malmö stad köper in.

[5] Vad är informationssäkerhet? (informationssakerhet.se)

Malmö stads ledningssystem för informationssäkerhet och dataskydd (LISD)

Tillsammans så utgör nedan redovisade dokument Malmö stads ledningssystem för informationssäkerhet.

Policy: Malmö stads *Trygghets- och säkerhetspolicy* är ett kommuncentralt styrdokument som beslutats av Kommunfullmäktige. Policyn anger Malmö stads inriktning för allt trygghets- och säkerhetsarbete och reglerar arbetet med trygghet- och säkerhet på alla nivåer i organisationen.
Riktlinje: *Malmö stads riktlinjer för informationssäkerhet* är ett kommuncentralt styrdokument som beslutats av Kommunstyrelsen. Genom att på strategisk nivå reglera ansvar, målsättning och det arbetssätt som gäller för Malmö stads informationssäkerhetsarbete konkretiserar riktlinjen både *Trygghets- och säkerhetspolicyns* samt *Kommunstyrelsens reglemente* styrning beträffande Malmö stads arbete med informationssäkerhet. *Malmö stads riktlinjer för informationssäkerhet* sätter därmed ramarna för hur allt arbete med informationssäkerhet ska bedrivas i Malmö stad. Ramarna för dataskyddsarbetet framgår även av *Riktlinjer för behandling av personuppgifter* i Malmö stad.
Anvisningar: Malmö stads *Anvisningar för informationssäkerhet* är ett samlingsnamn för flera olika områdesspecifika, kommunövergripande styrdokument som beslutas av stadsdirektören. Anvisningarna innehåller konkreta säkerhetsåtgärder som varje förvaltning ska implementera för att efterleva *Malmö stads riktlinjer för informationssäkerhet*.
Stadsövergripande rutiner: Malmö stads *Stadsövergripande rutiner* är ett samlingsnamn för flera olika områdesspecifika rutiner, vägledningar och mallar. De är att betrakta som kommuncentrala styrdokument vilka beslutas av olika tjänstepersoner i Malmö stad. Dessa dokument innehåller mer djupgående beskrivningar och vägledningar hur en säkerhetsåtgärd som beslutats i ovanstående *Anvisningar för informationssäkerhet* ska genomföras.
Förvaltningsanpassade rutiner: *Förvaltningsanpassade rutiner* är ett samlingsnamn för flera olika förvaltningsanapassade rutiner, vägledningar och mallar som kan tas fram och beslutas av respektive förvaltning i de fallen;
1. De *Stadsövergripande rutinerna* inte är nog detaljerade och därmed behöver kompletteras i syfte att verksamhetsanpassa innehållet.
2. Förvaltningen har beslutat om tidsbegränsat avsteg från riktlinje, anvisningar eller stadsövergripande rutiner och är i behov att ta fram egen styrning på området.

Informationssäkerhet - Ansvar

Kommunstyrelsen

Kommunstyrelsen har enligt sitt reglemente det övergripande ansvaret för stadens informationssäkerhet och beslutar om riktlinjer för informationssäkerhet.

Stadsdirektören

Stadsdirektören beslutar om stadsövergripande anvisningar för informationssäkerhet.

Nämnd

Varje nämnd är ansvarig för informationssäkerheten inom sin förvaltning. Nämnden ska tillse att riktlinjen och underliggande styrdokument efterlevs.

Verksamhetsansvarig

- Chef (oavsett nivå) ansvarar för informationssäkerheten inom sin verksamhet.
- Varje chef ansvarar för att deras medarbetare efterlever riktlinjen, har ett riskbaserat arbetssätt samt tillräcklig förståelse och kunskap för att nödvändig informationssäkerhet i verksamheten uppnås. Det inkluderar information och utbildning till medarbetare samt ekonomiskt och säkerhetsmässigt ansvar.

Medarbetare

- Alla medarbetare har ett eget ansvar för verksamhetens informationssäkerhet och ska i sitt eget arbete efterleva gällande styrdokument.
- Varje anställd har en skyldighet att rapportera informationsrelaterade brister och incidenter.

Figur 1 – Systematiskt Informationssäkerhetsarbete hämtad från MSB:s metodstöd.

Gymnasie- och vuxenutbildningsförvaltningens nätverk för dataskydd och informationssäkerhet

På gymnasie- och vuxenutbildningsförvaltningen ska det finnas ett nätverk som arbetar med förvaltningens dataskydds- och informationssäkerhetsfrågor.

Nätverket består av åtminstone en kontaktperson per avdelning och skolenhet samt samordnas av dataskydds- och informationssäkerhetssamordnaren. Nätverkets arbetet syftar till att bland annat identifiera, stödja och följa upp dataskydds- och informationssäkerhetsarbetet så att förvaltningens verksamheter bedrivs i enlighet med gällande regelverk. Detta innefattar bland annat att förvaltningens registerförteckning är korrekt, att vi har ett fungerande incidenthanteringssystem, att vi upprätthåller adekvat dataskydd för våra personuppgifter samt genomför riskanalyser, informationsklassningar och konsekvensbedömningar.

Dataskydds- och informationssäkerhetssamordnaren

- Nätverket samordnas av dataskydds- och informationssäkerhetssamordnaren.
- Samordnaren är förvaltningens kontaktperson i dataskydds- och informationssäkerhetsfrågor inom förvaltningen, mot staden och externa aktörer.
- Samordnaren kallar nätverket till nätverksträffar, planerar dataskyddsnätverkets arbete, introducerar nya kontaktpersoner och håller utbildningar i dataskydd och informationssäkerhet för medarbetare.

Kontaktpersoner för dataskydd och informationssäkerhet

Kontaktpersonen ska i sin verksamhet bland annat.

- Ge stöd till dataskydds- och informationssäkerhetssamordnarens arbete.
- Ge stöd till medarbetare inom den egna verksamheten i dataskydd och informationssäkerhet.
- Inom sin verksamhet uppmärksamma nya personuppgiftsbehandlingar till registerförteckningen samt uppdatera befintliga.
- Delta i informationsklassningar.
- Genomföra årliga kontroller av registerförteckningen enligt årshjul eller efter anmodan från samordnaren.
- Vid upptäckt av en personuppgiftsincident: ge stöd till medarbetare så att dataskydds- och informationssäkerhetssamordnaren informeras.
- Samordna sökningar inom sin verksamhet när dataskydds- och informationssäkerhetssamordnaren får in en begäran om registerutdrag från registrerad/enskild.