



Strategi för arbetet med ledning och styrning av dataskyddet i Lomma kommun

I syfte att skydda enskildas grundläggande rättigheter och skyldigheter, avseende deras rätt till skydd av personuppgifter i enlighet med GDPR och tillhörande svenska lagar och övriga författningar, arbetar Lomma kommun med dataskydd enligt följande struktur.

Mål

Målet är att myndigheternas behandling av personuppgifter ska omfatta följande principer för behandling:

- Laglighet, öppenhet och korrekthet
- Uppgifterna behandlas för särskilda uttryckligt angivna och berättigade ändamål
- Insamlingen är uppgiftsminimerad
- Uppgifterna är korrekta och nödvändigt uppdaterade
- Personuppgifterna förvaras endast under den tid som är nödvändig
- Uppgifterna behandlas på ett sätt som säkerställer uppgifternas integritet och konfidentialitet. Uppgifterna ska skyddas mot obehörig eller otillåten behandling och mot förlust, förstöring och skada genom olyckshändelse

Personuppgifter ska endast behandlas om

- den enskilde lämnat sitt samtycke,
- behandlingen är nödvändig för att fullgöra avtal,
- behandlingen är nödvändig för att fullgöra rättslig förpliktelse ,
- behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för annan fysisk person eller
- behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning

Särskilda kategorier av personuppgifter ska endast behandlas enligt undantagen i artikel 9. 2 a,b,c,e,f,g,h eller j, i Dataskyddsförordningen och förutsatt att regleringen i Dataskyddslagen 3 kap 2-8 §§ i Dataskyddslagen är uppfyllda, d.v.s. framförallt med stöd av:

- den registrerade lämnat sitt samtycke,
- att behandlingen är nödvändig för att den registrerade ska kunna fullgöra sina skyldigheter och utöva sina rättigheter inom arbetsrätten och på områdena social trygghet och socialt skydd

- att behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse, utifrån kriterierna i Dataskyddslagen 3kap 3§.
- att behandlingen är nödvändig för hälso- och sjukvård och social omsorg, enligt Dataskyddslagen 3 kap 5 §
- att behandlingen är nödvändig för arkivändamål av allmänt intresse eller statistiska ändamål eller
- behandlingen rör personuppgifter som på ett tydligt sätt har offentliggjorts av den registrerade

Struktur för ansvarsfördelningen i organisationen

Personuppgiftsansvarig

Varje nämnd är, enligt GDPR, personuppgiftsansvarig och ska kunna visa att principerna och kraven efterlevs.

Nämnden ska se till att dataskyddsprinciperna efterlevs i alla stadier av behandlingen av personuppgifter och ska i förväg bedöma vad principerna innebär i praktiken och hur de ska förverkligas i den egna verksamheten och dessutom dokumentera denna bedömning.

Nämnden ska genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa att kunna visa att personuppgifterna behandlas i enlighet med GDPR. Åtgärderna ska dimensioneras utifrån en riskbedömning. Åtgärderna ska bedömas och ses över regelbundet och uppdateras vid behov.

De datasystem där personuppgifter behandlas ska byggas upp så att de som standard genomför dataskyddsprinciperna.

Nämnden ska fastslå erforderliga skyddsåtgärder. Nämnden ansvarar för att personuppgiftsincidenter anmäles till tillsynsmyndigheten i lagstadgad omfattning.

Dataskyddsombud

Varje nämnd ska utse ett dataskyddsombud. Dataskyddsombudet har en kontrollerande och en rådgivande funktion.

Dataskyddsombudet ska kontrollera att personuppgifter behandlas på ett korrekt och lagligt sätt hos den personuppgiftsansvarige och informera och ge råd om dataskyddsförordningen och angränsande regler. Dataskyddsombudet ska fungera som en kontaktpunkt för tillsynsmyndigheten och för registrerade personer. Ombudet ska ha en självständig roll i organisationen och rapportera till ledningen.

I uppdraget som dataskyddsombud ingår att:

- Vara ett kunskapsstöd inom nämndens ansvarsområde gällande dataskyddsförordningen och annan tillämplig dataskyddslagstiftning.
- Övervaka den interna efterlevnaden av dataskyddsförordningen och annan tillämplig dataskyddslagstiftning.
- Rapportera till organisationens ledning om dataskyddsfrågor och organisationens brister och utvecklingsbehov.
- Tillsammans med sakkunniga inom nämndens ansvarsområde kravställa och arbeta för att införa säkerhetsskyddsåtgärder enligt lagstiftning inom dataskydd.

A.B. L.B.

- Identifiera kompetensutvecklingsbehov, planera och genomföra utbildningar avseende dataskyddsförordningen och angränsande lagstiftning.
- Övervaka den interna efterlevnaden av organisationens strategi för dataskydd.
- Bistå i utredning av misstänkta dataintrång.
- Ge råd vid genomförande av konsekvensbedömning av dataskydd och övervaka genomförandet av den.
- Omvärldsbevakning och nätverkande/kunskapsinhämtning rörande, dataskyddsförordningen och svenska dataskyddslagstiftning och riktlinjer från tillsynsmyndigheten.
- Fungera som kontaktpunkt för tillsynsmyndigheten Integritetsskyddsmyndigheten och vid behov genomföra förhandssamråd.

Den personuppgiftsansvarige ska offentliggöra dataskyddsombudets kontaktuppgifter och meddela dessa till tillsynsmyndigheten.

Den personuppgiftsansvarige ska tillse att dataskyddsombudet har erforderliga resurser för att genomföra uppdraget.

Ansvarsfördelningen på förvaltningarna

Varje förvaltning ska aktivt driva ett självständigt dataskyddsarbete, som inte leds av dataskyddsombudet. På varje förvaltning finns en av förvaltningschefen utsedd arbetsgrupp som initialt ansvarar för inventering av personuppgiftsbehandlingar för respektive myndighet, men som även fortsättningsvis aktivt ska bedriva dataskyddsarbetet inom respektive nämnds ansvar. För varje arbetsgrupp finns en ansvarig tjänsteman. Förvaltningens arbete följs upp av dataskyddsombudet för respektive nämnd.

Sammanhållande och konsultativ roll i förhållande till förvaltningarna har kommunledningskontoret. Kommunledningskontoret bistår också nämnderna vid bedömningar av personuppgiftsincidenter och anmälan av sådana till tillsynsmyndigheten.

Kommunens ledningsgrupp ska löpande informeras om förvaltningarnas dataskyddsarbete.

Redovisning av hur dataskyddsprinciperna förverkligas

Principerna för dataskyddets olika delar bedöms uppfyllas av respektive personuppgiftsansvarig (respektive nämnd) med ledning av styrdokument enligt följande.

- *Principen om laglighet, öppenhet och korrekthet*

Att principen om laglighet, öppenhet och korrekthet ska efterlevas framgår av styrdokumenterna "Strategi för arbetet med ledning och styrning av dataskyddet i Lomma kommun", "Anvisningar om information till den registrerade", "Guidelines för rättelser, radering, hantering vid invändning mot behandling och vid begränsning av behandling", "Plan för tekniskt skydd för personuppgifter", "Plan för organisatoriskt skydd för personuppgifter".

- *Principen om att uppgifterna behandlas enbart för särskilda uttryckligt angivna och berättigade ändamål*

Att principen om att uppgifterna behandlas enbart för särskilda uttryckligt angivna och berättigade ändamål efterlevs framgår av styrdokumentet "Strategi för arbetet med ledning och styrning av dataskyddet i Lomma kommun". Ändamålen dokumenteras i registerförteckning av den personuppgiftsansvarige.

AB. L.B.

- *Behandlingen ska vara uppgiftsminimerad*

Att principen om att behandlingen ska vara uppgiftsminimerad framgår av styrdokumentet "Strategi för arbetet med ledning och styrning av dataskyddet i Lomma kommun".

- *Uppgifterna ska korrekta och nödvändigt uppdaterade*

Att principen om att uppgifterna ska vara korrekta och nödvändigt uppdaterade framgår av styrdokumentet "Strategi för arbetet med ledning och styrning av dataskyddet i Lomma kommun".

- *Förvaras endast under den tid som är nödvändig*

Att principen om att personuppgifterna ska förvaras endast under den tid som är nödvändig framgår av styrdokumentet "Strategi för arbetet med ledning och styrning av dataskyddet i Lomma kommun".

- *Uppgifterna ska behandlas på ett sätt som säkerställer uppgifternas integritet och konfidentialitet*

Att principen om att uppgifterna ska behandlas på ett sätt som säkerställer uppgifternas integritet och konfidentialitet, att uppgifterna ska skyddas mot obehörig eller otillåten behandling och mot förlust, förstöring och skada genom olyckshändelse, framgår av "Plan för tekniskt skydd för personuppgifter" och "Plan för organisatoriskt skydd för personuppgifter".

A.B. L.B.