Granskningsrapport 2023
Genomförd på uppdrag av revisorerna
Maj 2023

Granskning av efterlevnaden av dataskyddsförordningen (GDPR)

Laholms kommun

Building a better working world

Innehåll

1. Sammanfattning

EY har på uppdrag av revisorerna i Laholms kommun granskat om det bedrivs ett ändamålsenligt arbete med dataskyddsfrågor inom kommunstyrelsen respektive barn- och ungdomsnämnden.

Vår sammanfattande bedömning är att kommunstyrelsen och barn- och ungdomsnämnden delvis säkerställt en grundläggande struktur för arbetet med efterlevnaden av GDPR men att följsamheten till rutiner och arbetssätt inte motsvarar intentionerna. Vidare bedömer vi att systematiken i hur arbetet bedrivs och uppföljningen av arbetet behöver stärkas. Inom den parallella granskningen av dataskyddsarbetet inom Laholmshem och AB och Kommunfastigheter i Laholm AB framgår otydligheter kring vilka beslut som ska fattas och kännedom om beslut kring styrdokumentation.

Bedömningen är att det krävs förändringar för att åstadkomma en god efterlevnad av dataskyddsförordningen. Vi har i vår bedömning tagit hänsyn till de personuppgifter som styrelsen/nämnden hanterar och att dessa i flera fall är att betrakta som känsliga, särskilt gäller detta delar av personalområdet och elevhälsoområdet. Ett bristande dataskyddsarbete riskerar att förutom ekonomisk skada i form av sanktionsavgifter från tillsynsmyndigheter också orsaka förtroendeskada hos invånare och personligt lidande hos de registrerade om personuppgifter exempelvis sprids.

När det gäller uppföljning av arbetet till nämnd och kommunstyrelsen är bedömningen att det inte genomförs tillräckliga kontroller och styrelsen/nämnden tar inte heller del av någon återrapportering. Den som är personuppgiftsansvarig, i detta fall styrelse/nämnd, kan överlåta den faktiska behandlingen av personuppgifter men personuppgiftsansvaret kan aldrig överlåtas. Den personuppgiftsansvariga har ett generellt ansvar att, utifrån de integritetsrisker som finns med behandlingen, genomföra lämpliga tekniska och organisatoriska åtgärder. Detta för att säkerställa och visa att behandlingen utförs i enlighet med dataskyddsförordningen. Vår bedömning är att de granskade organen brister i förhållande till detta ansvar.

Inom ramen för granskningen har vi gjort följande iakttagelser:

- Kommunen har ett dataskyddsombud som delas med Hylte och Falkenbergs kommun.
- De granskade organen har antagit de riktlinjer som finns för Laholms kommun och som riktar sig till alla verksamheter och kommunala bolag.
- Registerförteckningar över behandlingar finns men de är i flera fall inte kompletta.
- Det finns rutiner för incidenthantering och totalt har 22 incidenter anmälts inom de båda organens verksamheter under 2020-mars 2023.

Utifrån granskningsresultatet rekommenderas kommunstyrelsen och barn- och ungdomsnämnden att:

- Se över och uppdatera styrdokument inom dataskyddsområdet.
- Färdigställa registerförteckning som lever upp till lagens krav.
- Säkerställa att PUB-avtal upprättas samt dokumentera överväganden och beslut om att ej upprätta PUB-avtal.
- Säkerställa att all personal har den kunskap om dataskydd som krävs inkl. kunskap om incidenthantering.
- Säkerställa att nämnder och styrelser regelbundet tar del av återrapportering om arbetet med dataskydd.

Utifrån granskningsresultatet rekommenderar vi kommunstyrelsen att:

- Tydliggöra i ägardirektiven vilka styrande dokument inom informationssäkerhet och dataskydd som Laholmshem AB och Kommunfastigheter i Laholm AB ska följa.
- Säkerställa att bolagens styrelser antar och arbetar efter de styrande dokumenten.

2. Inledning

2.1. Bakgrund

Dataskyddsförordningen (GDPR, The General Data Protection Regulation) trädde i kraft den 25 maj 2018. Europaparlamentets och rådets dataskyddsförordning (EU) 2016/679 gäller i hela EU och ersatte i Sverige den äldre personuppgiftslagen (PUL) från 1998. Det främsta syftet med dataskyddsförordningen är att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter.

I jämförelse med PUL ställer dataskyddsförordningen högre krav på företag och organisationers interna kontroll kopplat till hanteringen av personuppgifter. Vid överträdelse av förordningens artiklar föreligger skärpta sanktioner, exempelvis kan kommuner beläggas med sanktioner och obligatorisk incidentanmälan rörande personuppgiftsincidenter skall göras till den lokala tillsynsmyndigheten inom 72 timmar efter att incidenter har uppdagats. Vidare har individer rätt till ersättning i form av skadestånd till följd av överträdelser av förordningen av en personuppgiftsansvarig eller ett personuppgiftsbiträde.

Då Laholms kommun med dess verksamheter hanterar stora mängder personuppgifter, har de förtroendevalda revisorerna i Laholms kommun beslutat att genomföra en granskning av kommunens arbete med personuppgiftshantering utifrån bestämmelserna i dataskyddsförordningen (GDPR).

2.2. Syfte och revisionsfrågor

Syftet med granskningen är att bedöma om Laholms kommun säkerställer ett ändamålsenligt dataskyddsarbete. Granskningen svarar på följande revisionsfrågor:

- Har kommunen tydligt definierade roller och ansvar inom området dataskydd?
- Finns det registerförteckningar över personuppgiftbehandlingar?
- Har det förekommit incidenter, finns det rutiner för incidentrapportering och har dessa rutiner följts?
- Finns det rutiner för hantering av personuppgifter som omfattar exempelvis begäran om registerutdrag, rättelse av uppgifter och radering av uppgifter?
- Genomförs kontroll, uppföljning och återrapportering av Laholms kommuns dataskyddsarbete?

2.3. Genomförande och avgränsning

Granskningen omfattar kommunstyrelsen och barn- och ungdomsnämnden. Granskningen har skett genom dokumentstudier och intervjuer, för en fullständig lista med intervjuade, se kapitel 6 Källförteckning. Därtill har ett urval om totalt sex

personuppgiftsincidenter granskas (tre per styrelse/nämnd) för att bedöma om hanteringen följer lagar och rutiner. För bedömning se bilaga 2, Stickprovsresultat.

2.4. Revisionskriterier

Granskningens bedömningar utgår från följande revisionskriterier. För att läsa mer om revisionskriterierna, se bilaga 1.

- Kommunallagen (2017:725)
- Dataskyddsförordningen (GDPR)
- Laholms kommuns "Policy för informationssäkerhet och personuppgiftshantering"

3. Organisation och styrning

I avsnittet redovisas iakttagelser och bedömning om kommunen har tydligt definierade roller och ansvar inom området dataskydd och om det finns rutiner för hantering av personuppgifter som omfattar exempelvis begäran om registerutdrag, rättelse av uppgifter och radering av uppgifter. Vi redovisar också om det har upprättats registerförteckningar över de personuppgiftsbehandlingar som genomförs.

Revisionskriterier

Enligt dataskyddsförordningens fjärde artikel framgår att 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.

Av dataskyddförordningen framgår även att personuppgiftsansvarige och personuppgiftsbiträdet ska utnämna ett dataskyddsombud om behandlingen genomförs av en myndighet eller ett offentligt organ.

Dataskyddsförordningens 30:e artikel sätter krav på att varje personuppgiftsansvarig (och dess företrädare) ska föra ett register över behandling som utförts under dess ansvar. Vidare anges i förordningens art 15-18 bland annat att den registrerade har rätt att ta del av vilka uppgifter som finns registrerade, rätt till radering och rättelse.

I dataskyddsförordningens 28:e artikel framgår att den som behandlar personuppgifter för personuppgiftsansvarigs räkning benämns personuppgiftsbiträde. I samma artikel framgår att när uppgifter behandlas av personuppgiftsbiträdet å den personuppgiftsansvarigas räkning ska hanteringen regleras genom avtal.

3.1. Iakttagelser organisation samt roller och ansvar

3.1.1. Kommunövergripande

Av *Policy för informationssäkerhet och personuppgiftshantering* (beslutad av kommunfullmäktige januari 2022) framgår att ansvaret för informationssäkerhet och personuppgiftshantering följer verksamhetsansvaret. Detta innebär att den som är ansvarig för en viss verksamhet även ansvarar för informationssäkerheten och personuppgifter inom verksamhetsområdet. I förlängningen innebär detta att respektive nämnd är personuppgiftsansvarig, vilket även redovisas i

kommunstyrelsen och nämndernas *Riktlinje för behandling av personuppgifter*[1]. Av riktlinjerna framgår att det är personuppgiftsansvarigs uppgift att:

- Se till och kunna visa att dataskyddsprinciperna efterlevs i alla stadier av behandlingen av personuppgifter.

Av *Riktlinje för behandling av personuppgifter* framgår vidare att respektive nämnd beslutar om personuppgiftssamordnare (PUS). PUS är operativt ansvarig för GDPR för verksamheten samt agerar stöd till verksamheten genom att vara sakkunnig i dataskyddsfrågor. I flertalet nämnder finns även registerförtecknare med uppgift att föra register över verksamhetens behandlingar och agera som PUS förlängda arm i verksamheterna.

Av riktlinje framgår att kanslichef tillika är processägare för informationssäkerhetsprocessen. Processägaren har till uppgift att utveckla och förbättra processen, hålla styrdokument och riktlinjer aktuella samt tillhandahålla juridisk kompetens. Processägaren sammankallar forum för personuppgiftsfrågor där PUS och dataskyddsombudet ingår.

Dataskyddsombudet ska enligt riktlinjen informera och ge råd till nämnd och anställda om skyldigheterna enligt lag. Dataskyddsombudet ska även övervaka att lagen följs avseende fungerande rutiner och åtgärder, ansvarstilldelning, information, utbildning och granskning, samt samarbeta och vara kontaktperson gentemot Datainspektionen[2]. Dataskyddsombud agerar även kontaktperson till de registrerade.

Dataskyddombudet ska vara gemensamt för alla nämnder och styrelser i Laholms kommun. Av kommunstyrelsens beslut kring dataskyddsombud 2018-05-15 uppmanas respektive nämnd och bolag att utse samma person till dataskyddsombud för sin verksamhet. Av beslut framgår även att dataskyddsombud delas mellan kommunerna Falkenberg, Hylte och Laholm. Kostanden fördelas utifrån invånarantal och Laholms kommun står för ca 0,3 heltidstjänst. Totalt bistår dataskyddsombudet cirka 35 personuppgiftsansvariga i de olika kommunerna.

Personuppgiftssamordnarens, personuppgiftsansvarigs, processägare och dataskyddsombudets ansvar och uppgifter framgår inte i den övergripande styrande dokumentationen utan behandlas i den riktlinje som varje enskild nämnd och kommunstyrelsen antar.

Av riktlinjen framgår att de upprättade styrdokument ska prövas en gång per mandatperiod. Enligt intervju sker ingen uppföljning av nämndernas styrdokument eller aktualitet från kommunstyrelsen.

---

[1] Respektive nämnd och kommunstyrelsen antar sin egen riktlinje. Inom ramen för granskningen har vi tagit del av kommunstyrelsens riktlinje (beslutad 2018-02-13) och barn- och ungdomsnämndens riktlinje (beslutad 2018-02-28). Det är identisk information i riktlinjerna.

[2] Datainspektionen bytte 1 januari 2021 namn till Integritetsskyddsmyndigheten.

3.1.2. Kommunstyrelsen

Av *Policy för informationssäkerhet och personuppgiftshantering* framgår att kommunstyrelsen har det övergripande ansvaret för informationssäkerhetsarbetet. I ansvaret åligger det kommunstyrelsen att upprätta en organisation kring informationssäkerhet som fungerar som stöd till kommunens förvaltningar för att uppfylla informationssäkerhetsansvaret och ett korrekt hanterande av personuppgifter. Kommunstyrelsen har även ansvaret att upprätta nämndsövergripande reglementen, instruktioner och anvisningar.

Enligt *Riktlinje för behandling av personuppgifter i Laholms kommun, kommunstyrelsens verksamhetsområde*, är kommunstyrelsen personuppgiftsansvarig för de personuppgiftsbehandlingar som avser kommunstyrelsens verksamhet. Det framgår även att personuppgiftssamordnare ska utses av kommunstyrelsen. Registerförtecknare utses av verksamheten och kanslichef innehar rollen som processägare.

Inom ramen för granskningen har vi tagit del av kommunstyrelsens beslut att utse personuppgiftssamordnare.

3.1.3. Barn- och ungdomsnämnden

Barn- och ungdomsnämnden har även de antagit *Riktlinjer för behandling av personuppgifter i Laholms kommun, barn- och ungdomsnämndens verksamhetsområde*. Då de är likalydande för både kommunstyrelsen och barn- och ungdomsnämnden återges de inte igen. Inom ramen för granskning har vi tagit del beslut av barn- och ungdomsnämnden där både personuppgiftssamordnare (beslut 2018-05-22) och dataskyddsombud (beslut 2018-05-30) utsetts.

Enligt beslut från barn- och ungdomsnämnden 2018-05-22 framgår att nämnden har tre utsedda funktioner som personuppgiftssamordnare. Av intervju framgår att en av dessa slutade för cirka fyra år sedan och att tjänsten inte återbesatts. Vid intervjuerna framkommer att nämnden avser att inte ha mer än två personuppgiftssamordnare. Beslutet har däremot inte uppdaterats.

Utöver två personuppgiftssamordnare finns cirka 15 registerförtecknare. Enligt intervju är registerförtecknares uppgift att agera PUS förlängda arm i verksamheterna. Det framgår vid intervju att administrativ personal på skolorna i regel är registerförtecknare. För den administrativa personalen finns regelbundna samverkansmöten där GDPR kan vara en del. Däremot finns inget nätverk eller regelbundna träffar mellan PUS och registerförtecknare. Av intervju framgår även att registerförtecknare inte registrerar registerförteckning. Detta åligger PUS. I uppdraget ingår snarare att uppmärksamma på behovet av att upprätta eller uppdatera registerförteckningen.

3.2. Iakttagelser rutiner

Av *Riktlinje för behandling av personuppgifter* framgår att det är processägarens uppgift att utveckla och förbättra processen, hålla styrdokument och riktlinjer aktuella samt tillhandahålla juridisk kompetens.

För kommunen finns flertalet rutiner. Bland annat finns upprättade rutiner vad gäller registerutdrag, rutin för e-post, riktlinje för publicering av bilder film och ljud, samt rutiner för incidenthantering.

Det framgår vid intervju att gällande rutiner bör ses över. Bland annat hänvisar riktlinje från 2018 till Datainspektion, som numera bytt namn till Integritetsskyddsmyndigheten. Vidare är flera av de rutiner vi tagit del av inte daterade och det framgår inte vem som fattat beslut om rutinen varpå det inte tydligt framgår aktualitet och status.

För Laholms kommun finns kommunövergripande *Rutin för begäran av registerutdrag (odaterad).* Det framgår bland annat att den nämnd/kommunstyrelsen som får in en begäran om registerutdrag ansvarar för att föra vidare förfrågan och sammanställa samt skicka ut informationen. Information kring radering av uppgifter berörs i flera av rutinerna. Däremot finns ingen tydlig dokumenterad rutin kring detta. Det framförs att frågor kring radering styrs bland annat av lagar och planer om registrering och gallring av allmänna handlingar. Av intervju framgår att det är ovanligt att begäran om registerutdrag eller radering inkommer.

Av intervju framgår att dokumenthanteringsplanerna reglerar vad som gäller för gallring. Det framgår att det inte sker några systematiska kontroller av att gallring sker men att mycket uppgifter och handlingar gallras i samband med att det lämnas till centralarkivet.

3.3. Iakttagelser registerförteckningar och PUB-avtal

3.3.1. Kommunövergripande

Registerförteckning upprättas i systemstödet Draftit. I systemstödet ska ansvarig för behandlingen, risk samt ändamålet med personuppgiftsbehandlingen anges. Det ska bland annat även dokumenteras vilka uppgifter som behandlas samt vilken rättslig grund som finns för behandlingen.

Inom ramen för granskningen har vi tagit del av Laholms kommuns registerförteckning. I förteckning finns drygt 250 behandlingar upptagna[3]. Av registerförteckning framgår att cirka 60 procent av behandlingarna inte har

[3] Med behandling av personuppgifter menas i princip allting som går att göra med personuppgifterna. Det kan till exempel vara att samla in, registrera, lagra, samköra eller skriva ut uppgifterna. Personuppgiftsansvariga och personuppgiftsbiträden är skyldiga att föra ett register över sina behandlingar. Vad som ska finnas med i registret beskrivs i artikel 30 i dataskyddsförordningen.

riskbedömts. Vidare är mer än 75 procent under bearbetning och registreringen inte slutförd. Enligt uppgift ställer verktyget där registerförteckningar registreras krav som inte bedöms relevanta för alla registerförteckningar.

Av registerförteckning framgår att en majoritet av förteckningarna är från 2018. Av intervju framgår att riskbedömningen tillkommit efter 2018 vilket ligger bakom att flertalet behandlingar inte riskbedömts. Den senast registrerade behandlingen är från 2021. Av intervju framgår att arbetet med registerförteckning stannat av under senare tid. Det framgår att registerförteckning är under utveckling och att det pågår en diskussion kring på vilken nivå behandlingar ska registreras.

Av intervju framgår att kommunen har som ambition att ta ställning till upprättande av personuppgiftsbiträdesavtal[4] (PUB-avtal) redan vid upphandling och att kommunen vill följa SKR:s standard kring PUB-avtal. Det framgår däremot vid intervju att det saknas PUB-avtal för flera av kommunens centrala system, exempelvis diariesystemet Ciceron. Enligt intervju vill inte företagen som hanterar systemen skriva på SKR:s avtal då det finns olika uppfattningar om hur ansvaret ska regleras och vilka kontroller som ska genomföras samt vem som ska stå för kostnader förknippade med dylika kontroller.

Vidare finns ingen dokumenterad rutin var eller hur överväganden om personuppgiftsansvarsfrågor ska dokumenteras som vid tillfällen när det anses att PUB-avtal inte är nödvändigt. Exempelvis om det inte är frågan om en ansvarig biträdes situation utan att båda parter är personuppgiftsansvariga. Diskussioner som förs dokumenteras inte vilket gör att det i efterhand inte går att ta del av överväganden eller beslut om att inte upprätta PUB-avtal.

3.3.2. Kommunstyrelsen

Av kommunstyrelsens internkontrollplan 2022 framgår att PUB-avtal ska kontrolleras. Detta ska genomföras en gång per halvår. Vid uppföljning för 2022 framgår att det gjorts en sökning på avtal som registrerats andra halvåret inom kommunstyrelsens diarium. Under andra halvåret 2022 har ett PUB-avtal registrerats gällande IT-plattformen Infocaption. Vi noterar dock att denna behandling inte återfinns i registerförteckningen.

Det framgår även av uppföljning av internkontrollplan att det upprättats ett ramavtal med Tele 2 vad gäller operatörs- och växeltjänster men att det inte identifierats något PUB-avtal för ramavtalet. Inte heller denna behandling återfinns i registerförteckningen. Kontrollen visar även att det saknas PUB-avtal för Visma Ciceron, Vismas ekonomisystem och för Infracontroll.

Som åtgärd framgår att arbetet med att upprätta biträdesavtal inom kommunstyrelsens verksamhetsområde behöver återupptas samt att

[4] Enligt Dataskyddsförordningen behöver personuppgiftsbiträdesavtal ingås när personuppgiftsbiträde behandlar personuppgifter åt den personuppgiftsansvariga.

personuppgiftssamordnare behöver utses[5]. Vidare framgår att det finns behov av informations- och utbildningsinsatser till verksamheterna. Enligt uppföljningen behöver det även finnas samverkan med upphandlingsenheten för att sprida information om behovet av PUB-avtal i samband med upphandlingar.

3.3.3. Barn och ungdomsnämnden

Av intervju framgår att arbetet med registerförteckning delvis stannat av. Det framgår att nämnden tidigare registrerade alla behandlingar men att det numera görs stötvisa insatser. Registreringarna som förtecknas sker utifrån övergripande processer. Det saknas helt registreringar för till exempel appar som används vid undervisning. Det framgår vid intervju att det upplevs som svårt att hålla koll på samtliga verktyg som används vid undervisning och att det därför inte ser någon registrering av dessa behandlingar. Vid sakgranskning framförs att registreringar ska ske på övergripande nivå och att det tidigare skedde för mindre behandlingar detta uppges vara anledningen till att registerförteckningen inte är fullständig.

Av intervju framgår att även barn- och ungdomsnämnden saknar PUB-avtal för vissa tjänster och system.

3.4. Bedömning

Det är vår bedömning att kommunen delvis har definierade roller med tydlig ansvarsfördelning. Det framgår i respektive styrelse/nämnds riktlinjer vilka roller som respektive styrelse/nämnd förväntas inneha. Dock saknas denna information i det kommunövergripande styrdokument vilket innebär att nämnder och styrelser potentiellt kan fatta olika beslut kring dataskyddsombud, personuppgiftsansvar samt vad respektive nämnds uppgift är kopplat till GDPR. Inom den parallella granskningen av dataskyddsarbetet inom Laholmshem AB och Kommunfastigheter i Laholm AB framgår otydligheter kring vilka beslut som ska fattas och kännedom om besluten.

Vidare noterar vi att styrdokumenten i flera fall bör uppdateras eftersom de bland annat refererar till Datainspektionen, som numera heter Integritetsskyddsmyndigheten. Vidare saknar flera dokument, datum och uppgift om när och vem som fastställt dokumenten. Detta innebär att det inte tydligt framgår aktualitet och status. Intrycket förstärks av att fler av rutinerna innehåller kommentarer och markeringar som tyder på att det är en arbetsversion och inte ett slutgiltigt och beslutat dokument. Vidare har de inte prövats föregående mandatperiod i enighet med vad riktlinjen förskriver. För barn- och ungdomsnämnden kan det konstateras att beslut om PUS inte uppdaterats sedan förändringen av antalet PUS; från tre till två.

[5] Personuppgiftssamordnare utsågs av kommunstyrelsen 2023-03-14.

Bedömningen är att det finns skriftliga rutiner för begäran om registerutdrag. Däremot noterar vi att det inte finns någon sammanställd rutin kring rättelse även om det framgår olika rutiner att detta ska göras.

Vi bedömer att det inom kommunstyrelsens ansvarsområde enbart delvis finns registerförteckningar som lever upp till lagstiftningens krav. Vi grundar vår bedömning på att arbetet påbörjats men ej slutförts, likaså att flera av registreringarna är ofullständiga. Vi ser det som allvarligt att ansvaret för personuppgifter inte finns tydliggjort genom PUB-avtal för flera av kommunens centrala system så som Ciceron. Vi menar vidare att processen för övervägande kring personuppgiftsansvarsfrågor bör förtydligas och att överväganden bör dokumenteras. Ett dokumenterat övervägande skulle kunna tydliggöra varför det inte funnits behov av att upprätta ett PUB-avtal.

Även för barn- och ungdomsnämnden bör arbetet med registerförteckning utökas, särskilt avseende de behandlingar av barn- och elevers personuppgifter som sker inom ramen för undervisningen. Vi bedömer att det finns risk för att organisationen kan gå miste om iakttagelser i verksamheterna då registerförtecknarna främst är administrativ personal. De behandlingar som görs inom ramen för undervisningen bedöms därför inte fångas i dagsläget i tillräcklig utsträckning.

4. Incidenter och uppföljning

I avsnittet redovisas iakttagelser och bedömning avseende om det förekommit incidenter och hur dessa i så fall har hanterats. Vidare redovisas iakttagelser och bedömning avseende kontroll, uppföljning och återrapportering av Laholms kommuns dataskyddsarbete.

Revisionskriterium

Kommunallagens 6 kap 6 § anger att nämnder och styrelser inom sitt ansvarsområde ska se till att verksamheten bedrivs i enlighet med Kommunfullmäktiges mål och riktlinjer, samt i enlighet med lagar och författningar som gäller för verksamheten.

Enligt artikel 33 i Dataskyddsförordningen framgår att vid en personuppgiftsincident ska den personuppgiftsansvarige utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till den tillsynsmyndighet som är behörig. Om anmälan till tillsynsmyndigheten inte görs inom 72 timmar ska den åtföljas av en motivering till förseningen.[6]

4.1. Iakttagelser incidenthantering

Incidenthanteringsprocess

Incidenthanteringsprocessen är dokumenterad i ett flödesschema. Processen inleds med en felanmälan till IT-avdelningen. Felanmälan skickas sedan vidare till en gemensam brevlåda för kommunens personuppgiftsansvariga. Därefter hanteras anmälan av den berörda verksamhetens personuppgiftsansvarig. När ärendet är identifierat som en incident registreras detta av lämplig personuppgiftsansvarig i kommunens ärendehanteringssystem, Ciceron[7]. I Ciceron finns vägledning till fortsatt arbete runt incidenten.

Enligt uppgift ska kommunens incidenthanteringsprocess revideras under 2023. Förslaget till den reviderade incidenthanteringsprocessen inkluderar ett förtydligande vid underrättelse till de registrerade som är drabbade. Revideringen inkluderar även förtydligande kring vem som ska informeras vid incident och på vilket sätt. Förslag till revidering berör även uppföljning och vidtagna åtgärder vid incident. Av intervju framgår även att ärendehanteringssystemet ska ses över och att en ny e-tjänst ska införas. Ambitionen är att förenkla incidenthanteringsprocessen inom kommunen.

---

[6] Anmälan ska göras om det inte är osannolikt att personuppgiftsincidenten medför risk för fysiska personers fri- och rättigheter. Övervägande sker genom bedömning.

[7] Ciceron är en webbaserad molnlösning och är ett verktyg för kommunens ärende- och informationshantering av allmänna handlingar.

Incidenthanteringsbok

Av incidenthanteringshandboken framgår att intervall och form för den sammanställda rapporten av incidenter återstår att definieras. Av intervju framkommer att så inte skett och att handboken nu ska revideras bland annat i syfte att matcha den nya e-tjänsten.

I nuvarande handbok finns en definition av vad en personuppgiftsincident är[8]. Definitionen följs av att incidenten ska meddelas till Datainspektionen[9] inom 72 timmar från upptäckten om personuppgiftsincidenten kan medföra en risk för de registrerade. Det framkommer även att en incident som inte medför risker för den registrerade inte behöver anmälas till myndighet men beslutet att inte rapportera incidenten vidare ska motiveras och dokumenteras.

Handboken reglerar vem som kan anmäla en incident och vem ärendet ska hanteras av. Det framgår att alla i organisationen som upptäcker en incident ska anmäla den i kommunens IT-verktyg, eller att en personuppgiftssamordnare rapporterar incidenten till IT-service.

Det framkommer i handboken att incidenter ska sammanställas med jämna mellanrum i en sammanställd rapport som kommuniceras vidare till kommunledning, processägare och nämnder. De föreslagna åtgärderna ska följas upp för att säkerställa att önskat resultat uppnåtts.

Av protokoll under 2022 för kommunstyrelsen respektive barn- och ungdomsnämnden framgår att styrelse/nämnd inte tagit del av någon sammanställning.

Manual för handläggning av personuppgiftsincidenter

I kommunen finns en manual för handläggning av personuppgiftsincidenter. Denna syftar till att vara ett guidande verktyg för hur en personuppgiftsincident ska genomföras och dokumenteras. I manualen framförs att varje PUS har i uppgift att se efter den gemensamma brevlådan två gånger under en arbetsdag.

4.1.1. Stickprov incidenter

Inom ramen för granskningen har stickprov genomförts av kommunstyrelsens och Barn- och ungdomsnämndens hantering av personuppgiftsincidenter. Syftet med stickproven är att kontrollera om de åtgärder som vidtagits tillfredställande utifrån lagen och kommunens egna föreskrifter och riktlinjer. Detta inkluderar i vilken utsträckning bedömning och anmälan sker och vilka åtgärder som vidtas.

Under 2020 fram till 2023 registrerades totalt 22 personuppgiftsincidenter från kommunstyrelsens respektive barn- och utbildningsnämndensansvarsområde, sex

[8] Personuppgiftsincident är en oönskad händelse, eller avvikelse från normala rutiner som riskerar informationens konfidentialitet, riktighet och tillgänglighet.

[9] Numera Integritetsskyddsmyndigheten

inom kommunstyrelsen och sexton inom barn- och ungdomsnämnden. Flest incidenter rapporterades under 2022 då tre incidenter anmäldes inom kommunstyrelsens ansvarsområde och sju incidenter anmäldes inom barn- och ungdomsnämndens ansvarsområde.

Antal incidenter	2020	2021	2022	2023 (t.o.m. feb)
Totalt KS och BUN	6	4	10	2
Kommunstyrelsen	1	1	3	1
Barn- och ungdomsnämnden	5	3	7	1

Av samtliga 22 personuppgiftsincidenter under 2020-2023, har tre från kommunstyrelsen och tre från barn- och ungdomsnämnden valts ut. Inom ramen för stickprovskontrollen har dokumentation som berör respektive ärende granskats. Beaktade delar i stickprovskontrollen tar sin utgångspunkt i dataskyddsförordningens regler och skrivelser. Följande kontrollmoment har ingått i bedömningen:

- Ärendebeskrivning
- Riskbedömning
- Rapportering till Integritetsskyddsmyndigheten, IMY
- Rapportering inom 72h efter vetskap om incidenten och eventuell motivering till försening.
- Information till de drabbade och utsträckningen de kommer/ inte kommer informeras
- Underrättelse från personuppgiftsbiträde till personuppgiftsansvarig efter vetskap om incidenten
- Beskrivning av personuppgiftsincidenten innehållande antal registrerande, kategorier av och ungefärligt antal personuppgiftsposter
- Kontaktuppgifter för lämplig kontaktpunkt
- Beskrivning av konsekvenserna
- Vidtagna åtgärder

I bilaga 2 finns en utförlig utvärdering av kontrollmomenten som ingår i stickprovskontrollen.

För samtliga personuppgiftsincidenter dokumenteras en övergripande beskrivning av incidenten och antal registrerade som berörts. Dokumentationen av incidenterna är kortfattade och innehåller kortfattade rader och stycken i mailkontakt och vid registrering.

Vid samtliga utvalda stickprov framgår att incidenter genomgått en riskbedömning. Det framgår däremot inte av dokumentationen vad bedömningen grundas på.

Vid fyra av sex stickprovskontroller är incidenteten rapporterad till IMY. De två resterande incidenter har behandlats internt. Vid ett av fallen genomfördes en bedömning av kommunstyrelsen i samråd med dataskyddsombudet att incidenten inte skulle rapporteras vidare till IMY. Motivering till varför incidenten inte rapporterades vidare går inte att utläsa av dokumentationen. Däremot framgår att konsekvenserna av incidenten bedömdes som obetydlig för de registrerade. Detta mot bakgrund av att de som tog del av personuppgifterna redan hade tillgång till uppgifterna. Incidentens allvarlighetsgrad bedömdes vara *obetydlig*. För incidenten i barn- och ungdomsnämnden gjordes en intern anmälan och enligt dokumentation framkommer inte varför incidenten inte rapporterats vidare.

Tre av sex incidentrapporteringar från kommunstyrelsen och barn- och ungdomsnämnden rapporterades inte inom 72 timmar. Förklaring till sen rapportering i barn- och ungdomsnämnden uppges bero på osäkerhet om Laholms kommun tillhörde de drabbade av incidenten.

Ingen av incidenterna som granskats har rapporterats vidare till de registrerade. Kortfattade motiveringar beskriver anledningarna för respektive incident. I tre fall har kommunen inte tagit ställning till om underrättelse till berörda parter krävts, två anses inte medföra risk för personers fri- och rättigheter och en incident saknar motivering.

Vidare framkommer att tre incidenter inträffade hos och upptäcktes av personuppgiftsbiträdet. Två av incidenterna upptäcktes internt inom kommunstyrelsen. Utifrån dokumentationen framgår det inte hur ett av tre incidenter för barn- och ungdomsnämnden upptäcktes.

Samtliga incidenter har ett uppskattat antal berörda registrerade och till vilken kategori dessa tillhör. I fem av sex fall anges även vilka potentiella konsekvenser incidenten kan resultera i. Den sjätte anses inte medföra konsekvenser. I samtliga fall har namn på kontaktuppgifter för lämplig kontaktpunkt angetts.

Det framgår vidare av dokumentation från stickprovskontrollen att verksamheterna i samtliga fall har vidtagit åtgärder för incidenten. Exempel på åtgärder är polisanmälan, nedstängning av tjänster, radering av personuppgifter och upprättad kontakt med verksamhet som bidragit till incidenten. En incident från kommunstyrelsen avviker i detta fall där inga åtgärder vidtagits. I ett fall för barn- och ungdomsnämnden inväntar nämnden svar från personuppgiftsbiträdet. Vidare arbete med åtgärder för att förhindra att liknande art av händelse upprepar sig är inte angivet i dokumentationen.

Vid intervju framgår att alla vägledande dokument finns på kommunens hemsida men att mer kommunikation hade möjliggjort att informationen kommer ut i verksamheterna. Detta går även att utläsa i ett av stickproven från kommunstyrelsen då det i åtgärderna efterfrågar allmänna informationsinsatser för hanteringen av personuppgifter i hela organisationen, samt att ett verktyg för säker e-post är önskvärt.

Sammanfattningsvis bedöms två stickprov var för både kommunstyrelsen och barn- och ungdomsnämnden som delvis tillfredställande. Ett av kommunstyrelsens

respektive ett av barn- och ungdomsnämndens stickprov bedöms som tillfredställande.

4.2. Iakttagelser kontroll och uppföljning

I *Riktlinjen för behandling av personuppgifter i Laholms kommun, kommunstyrelsens verksamhetsområde* anges att en behandling av personuppgifter får genomföras om en lämplig teknisk och organisatorisk säkerhet vidtagits för behandlingen. Vidare fastställs att säkerheten ska baseras på genomförda informationssäkerhetsklassningar och riskanalyser. I riktlinjen uppges även att införandet och tillämpning av rutiner ska genomföras för att:

- Kontinuerligt testa, undersöka och visa på effektiviteten av införda säkerhetsåtgärder

Det framgår inte vid intervjuer att dessa tester faktiskt genomförs.

Kommunstyrelsens uppföljning av intern kontroll från andra halvåret 2022 behandlades av kommunstyrelsen 2023-02-14. Uppföljningen innehåller två kontrollmoment som rör ärendehantering och informationssäkerhet kopplat till GDPR.

Det första kontrollområdet avser sekretess och skydd av handlingar. Momentet omfattade granskning av rätt skydd av handlingar. Utifrån stickprov på handlingar som registrerades under året identifierades två handlingar som innehöll personuppgifter (personnummer) som inte var skyddade. Detta åtgärdades genom att skydda uppgifterna. Det framgår inga ytterligare åtgärder.

Det andra kontrollområdet avsåg granskning av upprättade och registrerade personuppgiftsbiträdesavtal i kommunstyrelsens diarium. Se tidigare beskrivning under kapitel 3.3 Iakttagelser registerförteckningar och PUB-avtal.

Även barn- och utbildningsnämndens interna kontroll från 2022 omfattar upprättande av personuppgiftsbiträdesavtal för förvaltningsgemensamma digitala tjänster. Kontrollen genomförs en gång per halvår genom en avstämning av att PUB-avtal tecknats i samband med ingående avtal. PUB-avtal saknades vid ett av tre upprättade avtal.

Dataskyddsombudet genomförde en granskning under 2019 som syftade till att få en bild av kommunens nämnder och styrelsers efterlevnad av GDPR. Granskningen syftade även till att bedöma om det fanns utpekade roller med särskilt ansvar för arbetet. Syftet var även att få en bild över kompetensen hos funktioner med särskilt ansvar för personuppgiftshantering och om det fanns en lösning för säker digital kommunikation.

Det framgår vid intervju att dataskyddsombudet presenterat rapporten för vissa nämnder/verksamheter inom kommunen. Det har inte genomförts någon uppföljning av rekommendationerna eller någon ytterligare granskning. Utifrån dokumentation och intervjuer framkommer att kommunstyrelsen och barn- och ungdomsnämnden inte genomför några övriga uppföljningar eller kontroller inom

Building a better working world

området, utöver den interna kontrollen återgiven ovan. Vid sakgranskning framkommer att dataskyddsombudet på olika sätt stöttar verksamheten i arbetet med GDPR samt följer upp risker som uppdagas. Kommunstyrelsen och nämnden tar däremot inte del av information kring arbetet som bedrivs.

4.3. Iakttagelser utbildning

Vid intervju framkommer att utbildning till nämnder inom området för GDPR ges vid varje ny mandatperiod. Nämnderna informeras om ansvarsområde och deras roll för området. Vidare framkommer att kommunstyrelsen ger ut viss datorbaserad utbildning kopplat till GDPR. Vid intervju uppges att en del informationsinsatser från kommunstyrelsen utfördes under 2018 till samtliga anställda i verksamheterna. Det framförs därtill att det inte skett någon uppföljning eller vidare kompetensutveckling till medarbetare efter informationsinsatserna 2018.

4.4. Bedömning

Bedömningen är att det inte finns en tillräcklig uppföljning, kontroll och återrapportering av incidenter inom varken kommunstyrelsen eller barn- och ungdomsnämnden. Det finns ett brett underlag av material för området men materialet innehåller otydligheter och kommunikationen ut till verksamheterna bedöms inte som tillräcklig. Kommunikationen kring policys, rutiner och riktlinjer behöver stärkas för att undvika en underrapportering av incidenter och okunskap på området. Stickprovskontrollen visar att det delvis finns en tillfredställande dokumentation vid incidenthantering. Att flera stickprov saknar beskrivning av åtgärder, konsekvens samt att drabbade inte blivit kontaktade förstärker intrycket av att ytterligare arbete krävs.

Vidare bedömer vi att kommunstyrelsen respektive barn- och ungdomsnämnden inte tar del av återrapportering av vare sig incidenter, förebyggande arbete eller kontroll av efterlevnad i tillräcklig utsträckning. Nämnden bör utifrån sitt ansvar som personuppgiftsansvarig, regelbundet ta del av information om hur arbetet bedrivs. Det är positivt att GDPR hanteras inom ramen för den interna kontrollen däremot bedömer vi att återrapporteringen kring den interna kontrollen inte fullt ut är tillräcklig. De avvikelser som iakttagits inom ramen för intern kontroll bör beskrivas tydligare och åtgärder vidtas i större utsträckning. Vidare behandlar den interna kontrollen enbart mindre avgränsade delar av arbetet med personuppgifter och efterlevnaden av dataskyddsförordningen och en samlad uppföljning finns inte. Detta bedöms som en brist.

5. Slutsats

Vår sammanfattande bedömning är att kommunstyrelsen och barn- och ungdomsnämnden delvis säkerställt en grundläggande struktur för arbetet med efterlevnaden av GDPR men att följsamheten till rutiner och arbetssätt inte motsvarar intentionerna. Vidare bedömer vi att systematiken i hur arbetet bedrivs och uppföljningen av arbetet behöver stärkas.

Bedömningen grundar sig på att det delvis finns definierade roller inom området. Det kan även konstateras att det finns registerförteckningar samt rutiner för bland annat registerutdrag. På samtliga av dessa områden krävs dock fortsatt arbete för att uppfylla dataskyddslagen och interna styrdokument.

De kommunala styrdokument som reglerar ansvarsområdet innehåller otydligheter och är i flera fall inte uppdaterade. Kommunen bör överväga riktlinjer på kommunövergripande nivå då det i dagsläget finns risk att nämnder och styrelser potentiellt kan fatta olika beslut kring dataskyddsombud, personuppgiftsansvar samt vad respektive nämnds uppgift är kopplat till GDPR. Inom den parallella granskningen av dataskyddsarbetet inom Laholmshem och AB och Kommunfastigheter i Laholm AB framgår otydligheter kring vilka beslut som ska fattas och kännedom om besluten.

Vidare görs bedömningen att registerförteckningar inte är fullständiga. Vi bedömer det som allvarligt att ansvaret för personuppgifter inte finns tydliggjort, i form av PUB-avtal, för flera av kommunens centrala system.

Uppföljning, kontroll och återrapportering av incidenter inom kommunstyrelsen och barn- och ungdomsnämnden bedöms inte som tillräcklig vilket bland annat grunder sig i en inte tillräcklig kommunikation ut till verksamheterna. Kommunikationen kring policys, rutiner och riktlinjer behöver stärkas eftersom vi ser att det finns risk för underrapportering av incidenter. Vidare menar vi att styrelsen och barn- och ungdomsnämnden bör utifrån sitt ansvar som personuppgiftsansvarig, regelbundet ta del av information om hur arbetet bedrivs. Styrelsen/nämnden är alltid enligt lagen personuppgiftsansvarig, något som inte förändras av att man exempelvis utser dataskyddsombud eller datasskyddssamordnare. Styrelsen/nämnden behöver därför regelbundet ta del av information om hur arbetet bedrivs. Utbildning i början av en mandatperiod är ett grundläggande inslag detta ansvar men långt ifrån tillräckligt.

Revisionsfråga	Svar
▸ **Har kommunen tydligt definierade roller och ansvar inom området dataskydd?**	Kommunen har delvis definierade roller och ansvar inom området dataskydd.

▸ **Finns det registerförteckningar över personuppgiftbehandlingar?**	Det finns registerförteckningar men de lever enbart delvis upp till lagstiftningens krav. Vi bedömer att kommunen inledde ett arbete i samband med att GDPR trädde i kraft men att arbete sedan tappat fart och inte slutförts. Vidare bedömer vi det som allvarligt att ansvaret för personuppgifter inte finns tydliggjort, i form av PUB-avtal, för flera av kommunens centrala system.
▸ **Har det förekommit incidenter, finns det rutiner för incidentrapportering och har dessa rutiner följts?**	Det har under 2020–2022 förekommit totalt 22 incidenter i kommunen men flera intervjuade uppger att det sannolikt finns en underrapportering. Kommunen har inte haft någon samlad eller dokumenterad information till medarbetare om incidenter vilket såklart bedöms påverka kunskapen hos medarbetare och i förlängningen hur många incidenter som anmäls. En ny e-tjänst är på gång under våren 2023. Av de rapporterade incidenterna visar våra totalt sex stickprov att två av dessa hanterats tillfredställande. Fyra har hanterats på ett delvis tillfredställande sätt.
▸ **Finns det rutiner för hantering av personuppgifter som omfattar exempelvis begäran om registerutdrag, rättelse av uppgifter och radering av uppgifter?**	Delvis. Det finns skriftliga rutiner för begäran om registerutdrag. Gällande rättelse och radering finns inte specifika rutiner utan frågan om radering styrs bland annat av lagar och planer om registrering och gallring av allmänna handlingar.
▸ **Genomförs kontroll, uppföljning och återrapportering av Laholms kommuns dataskyddsarbete?**	Nej. Det är vår bedömning att styrelse och nämnd inte tar del av återrapportering av vare sig incidenter, förebyggande arbete eller kontroll av efterlevnad i tillräcklig utsträckning. Det är positivt att den interna kontrollen under 2022 omfattat PUB-avtal men vår bedömning är det inte tydligt framgår åtgärder vid brister samt att det även finns andra risker förknippade med personuppgiftshantering som den interna kontrollen inte omfattat.

Utifrån granskningsresultatet rekommenderas kommunstyrelsen och barn- och ungdomsnämnden att:

- Se över och uppdatera styrdokument inom dataskyddsområdet.
- Färdigställa registerförteckning som lever upp till lagens krav.

- Säkerställa att PUB-avtal upprättas samt dokumentera överväganden och beslut om att ej upprätta PUB-avtal.
- Säkerställa att all personal har den kunskap om dataskydd som krävs inkl. kunskap om incidenthantering.
- Säkerställa att nämnder och styrelser regelbundet tar del av återrapportering om arbetet med dataskydd.

Utifrån granskningsresultatet rekommenderar vi kommunstyrelsen att:

- Tydliggöra i ägardirektiven vilka styrande dokument inom informationssäkerhet och dataskydd som Laholmshem AB och Kommunfastigheter i Laholm AB ska följa.
- Säkerställa att bolagen styrelser antar och arbetar efter de styrande dokumenten.

Laholm den 16 maj 2023

Hanna Ericsson	Victor Klügel	Ellen Wikström
EY	*EY*	*EY*

6. Källförteckning

Intervjuade funktioner

- Dataskyddsombud för Laholms kommun
- Barn- och ungdomsnämndens presidium
  - Ordförande
- Kommunstyrelsens förvaltning
  - Kommundirektör
  - Kanslichef
- Barn- och ungdomsnämndens förvaltning
  - Förvaltningschef
  - Skoljurist tillika personuppgiftssamordnare för BUN
  - Nämndsekreterare tillika personuppgiftssamordnare för BUN

Analyserade dokument

- Handbok incidenthantering – Personuppgiftsincidenter för PUS. 2018
- Incidenthanteringsprocess. Analys för incident.
- Kommunstyrelsens rapport av intern kontroll. 2022
- Kommunstyrelsens och barn- och ungdomsnämndens informationsblanketter.
- Manual handläggning av personuppgifter
- Policy för informationssäkerhet och personuppgiftshantering. 2022-01-25
- Registerförteckning från Draftit. Laholms kommun, 2023-02-06
- Riktlinjer för behandling av personuppgifter i Laholms kommun, barn- och ungdomsnämndens verksamhetsområde. 2018-02-28
- Riktlinjer för behandling av personuppgifter i Laholms kommun, kommunstyrelsens verksamhetsområde. 2018-02-13.
- Rutin för begäran av registerutdrag.
- Rutin för e-post, Laholms kommun. 2018-04-05
- Riktlinje för publicering av bilder, filmer och ljud på personer i kommunens kommunikationskanaler. 2021-05-11.
- Utredningsblankett personuppgiftsincident

Bilaga 1. Revisionskriterium

Kommunallagen (2017:725)

Det är enligt 6 kap. 1 § styrelsens uppgift att leda och samordna förvaltningen av kommunens angelägenheter och ha uppsikt över övriga nämnders och eventuella gemensamma nämnder. Kommunstyrelsen ska, enligt 6 kap. 2 §, uppmärksamt följa de frågor som kan inverka på kommunens utveckling och ekonomiska ställning.

Kommunallagens 6 kap 6 § anger att nämnderna inom sitt ansvarsområde ska se till att verksamheten bedrivs i enlighet med Kommunfullmäktiges mål och riktlinjer, samt i enlighet med lagar och författningar som gäller för verksamheten.

Dataskyddsförordningen

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.

I enlighet med dataskyddförordningens 5:e artikel ska behandling av personuppgifter uppfylla ett antal grundläggande principer, så som (a) laglighet, korrekthet och öppenhet, (b) insamlingenav uppgifterna ska ändamålsbegränsas med andra ord; samlas in för särskilda, uttryckligat angivna och berättigade ändamål och inte senare behandlas på ett sätt som går emot dessa ändamål. (c) Behandlingen av personuppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas, *uppgiftsminimering*. (d) behandlingen ska inneha korrekthet och (e) de får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas, *lagringsminmering*. Personuppgifterna ska slutligen behandlas med integritet och konfidentialitet och den personuppgiftsansvarige innehar en ansvarsskyldighet att följande punkter efterlevs.

Av dataskyddförordningen framgår även att personuppgiftsansvarige och personuppgiftsbiträdet ska utnämna ett dataskyddsombud om behandlingen genomförs av en myndighet eller ett offentligt organ. I ett förtydligande på Integritetsskyddsmyndighetens (IMY) webbplats framgår att kommunala eller landstingsägda bolag inte är att betrakta som ett offentligt organ. Om de i sin kärnverksamhet regelbundet, systematiskt och i stor omfattning övervakar enskilda personer eller om de i sin kärnverksamhet behandlar känsliga personuppgifter eller uppgifter om brott i stor omfattning måste de dock likväl utse ett personuppgiftsombud. Även organisationer som *inte* måste ha ett dataskyddsombud rekommenderas av IMY att organisationer utser ett

dataskyddsombud, även om de inte måste, om de utför arbetsuppgifter av allmänt intresse. [10]

Dataskyddsförordningens 30:e artikel sätter krav på att varje personuppgiftsansvarig (och dess företrädare) ska föra ett register över behandling som utförts under dess ansvar. Vidare anges i förordningens art 15-18 bland annat att den registrerade har rätt att ta del av vilka uppgifter som finns registrerade, rätt till radering och rättelse.

Enligt artikel 33 i dataskyddsförordningen framgår *att v*id en personuppgiftsincident ska den personuppgiftsansvarige utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till den tillsynsmyndighet som är behörig. Om anmälan till tillsynsmyndigheten inte görs inom 72 timmar ska den åtföljas av en motivering till förseningen.

Laholms kommuns "Policy för informationssäkerhet och personuppgiftshantering"

Laholms kommuns policy för informationssäkerhet och personuppgiftshantering är antagen i kommunfullmäktige i januari 2022 och gäller från och med 1 februari 2022. Den riktar sig till alla verksamheter och kommunala bolag i kommunen. Policyn innefattar informationssäkerhet med syfte att skapa och upprätthålla rutiner och skydd av informationstillgångar så att informationen är tillgänglig när den behövs, är korrekt och inte manipulerad eller förstörd och att informationen endast är tillgänglig för behöriga personer. Detta för att informationen kommunen hanterar ska vara korrekt. Genom att säkerställa en korrekt hantering av information i kommunen skapas förtroende och tillit för kommuninvånare, näringsliv och andra organisationer gentemot kommunen.

Policyn ska vidare fungera som ett stöd i kommunens arbete att identifiera hot, sårbarhet, risker och upprättande av risk- och sårbarhetsanalyser vid kommunens behandling av information. Därtill ska policyn möjliggöra processer för att genomföra åtgärder för att reducera hot, sårbarhet samt risker till en acceptabel nivå.

Det är kommunstyrelsen som ansvarar för att bibehålla dokumentets aktualitet. Detta innefattar all hantering av informationstillgångar i kommunen oberoende av karaktär, form eller miljö. Kommunstyrelsen ansvarar även för upprättande av reglementen, instruktioner och anvisningar. Därtill är det förvaltningschef eller motsvarande som ansvarar för utformningen av att konkreta regler och anvisningar är utformade på ett säkert sätt och att dessa sprids i organisationen.

I policyn finns även riktlinjer för roller och ansvar, däribland att verksamheterna ansvarar för dess informationssäkerhet och personuppgifter inom verksamheten.

[10]https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/dataskyddsombud/maste-ni-utse-ett-dataskyddsombud/

Slutligen ska kommunfullmäktige minst en gång per mandatperiod undersöka om styrdokumentet är aktuellt. Om så inte är fallet ska detta upphävas, revideras eller sammanföras med annat styrdokument vid behov.

Bilaga 2. Stickprovsresultat

Tabell 1. Stickprov kommunstyrelsen

Datum	2023-01-15	2022-11-15	2021-09-23
Ärendebeskrivning	Personuppgiftsincident, KPA pension, användare har tillfälligt kunnat komma åt andras uppgifter. Anmält till IMY	Personuppgiftsincident 2022-11-14, personuppgifter skickade med e-post av misstag	Personuppgiftsincident, Protokoll från Nämnden för överförmyndare i samverkan som innehåller personuppgifter, publicerades av misstag på webben. IMY har avslutat ärendet.
Finns det en angiven riskbedömning av incidenten och dokumentation av denna?	Riskbedömningen beskrivs som begränsad.	Ja, i egen anmälan	Riskbedömningen beskrivs som begränsad.
Rapporterad till IMY? Om nej riskbedömning?	Ja.	Nej, bedömes av dataskyddsombudet att intern anmälan var tillräcklig.	Ja.
Rapportering inom 72 h efter vetskap om incidenten? Om nej, motivering till förseningen?	Nej. Incidenten rapporterades av KPA 13 januari 2023, dataskyddsombudet vidarebefordrade rapporten till Laholms kommuns kanslichef 15 januari. Därefter beslutades att anmäla incidenten. Laholm rapporterade inom 72 h.	Nej. Upptäcktes 221110, anmäldes 221114 och rapporterades till dataskyddsombudet 221115.	Ja.
Är de drabbade informerade? Om inte, kommer de informeras?	Nej, har inte tagit ställning om de drabbade ska informeras eller ej.	Nej. Incidenten medför inte hög risk för personers	Nej. Det framgår inte varför drabbade inte informerats.

		fri- och rättigheter.	
Underrättelse från personuppgiftsbiträdet till personuppgiftsansvarige efter vetskap om incidenten?	Ja.	Intern händelse.	Intern händelse.
Har personuppgiftsincidenten beskrivits utförligt? – (berörda antal registrerade - kategorier av och ungefärligt antal personuppgiftsposter)	Ja. Dokument innehållande vissa personuppgifter för anställda/tidigare anställda hos er, felaktigt tillgängliggjorts på KPA Mina sidor. Incidenten uppstod i samband med migrering av information mellan två system. Dokumenten omfattar uppgifter från åren 2010, 2011, 2012 innehållande: Namn, personnummer, utbetalat pensionsbelopp.	Ja. En person begärde ut fakturor från ett antal olika bolag. I begäran var bolagen angivna med organisationsnummer. Ett av bolagen var enskild firma varför organisationsnumret var samma som personnumret. Skickat personnummer i ett e-postmeddelande. Inträffade pga. mänskliga faktorn, fel i det enskilda fallet.	Ja. Obehörigt röjande genom felaktigt utskick av mejl/brev/sms. Registratorn registrerar utdrag från protokoll med paragraf, anslagsbevis och rapport gällande delårsrapport utan att kolla hela filen förutom första sida, anslagsbevis och paragraf. Mellan paragraf och rapport var hela protokoll som innehåller personuppgifter med. Handlingen lämnas i sin helhet till pressen. Totalt påverkades 1-10 uppgifter.
Förmedlat namn på och kontaktuppgifter för lämplig kontaktpunkt?	Ja.	Ja.	Ja.

Beskrivning av konsekvenserna?	Ja. Registrerade i fråga förlorar kontrollen över de egna personuppgifterna.	Inga konsekvenser. De som fick del av personuppgiften hade redan tillgång till den.	Den registrerade förlorar kontrollen över de egna personuppgifterna. Skadat anseende. Förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt.
Vidtagna åtgärder?	Beslut fattades omedelbart att stänga ner berörda delar av den tjänst som omfattades av incidenten. När incidenten blev känd skapades omedelbart en arbetsgrupp för att utvärdera och analysera incidenten. Felet är rättat. Fortsatt efterarbete med incidenten pågår.	Inga åtgärder har vidtagits. Önskan om allmänna informationsinsatser allmänt om hanteringen ev. personuppgifter i hela organisationen. Verktyg för säker e-post är önskvärt.	Ja, kontaktat pressen och bett dem radera personuppgifter. Uppgifterna borttagna från verksamhetssystemet.
Bedömning:	Tillfredställande.	Delvis tillfredställande.	Delvis tillfredställande.

Tabell 2. Stickprov Barn- och ungdomsnämnden

Datum	2023-01-15	2022-11-15	2021-09-23
Ärendebeskrivning	Obehörig åtkomst: Någon inom eller utanför organisationen har tagit del av information som den saknade behörighet till.	Obehörig åtkomst: Någon inom eller utanför organisationen har tagit del av information som den saknade behörighet till.	Utskrift av elevers närvaro/frånvaro har skrivits ut på felaktig skrivare.
Finns det en angiven riskbedömning av incidenten och	Riskbedömningen beskrivs som mycket allvarlig.	Riskbedömningen beskrivs som begränsad.	Riskbedömningen beskrivs som begränsad.

dokumentation av denna?			
Rapporterad till IMY? Om nej riskbedömning?	Ja.	Ja.	Nej. Ingen motivering går att utläsa.
Rapportering inom 72 h efter vetskap om incidenten? Om nej, motivering till förseningen?	Ja.	Nej. Oklarhet i om Laholm kommun tillhörde de drabbade. Dessa uppgifter bekräftades av Skola24 den 4 januari per telefon.	Ja.
Är de drabbade informerade? Om inte, kommer de informeras?	Nej. Har inte tagit ställning.	Nej. Har inte tagit ställning.	Nej. Incidenten medför inte risk för personers fri- och rättigheter.
Underrättelse från personuppgiftsbiträdet till personuppgiftsansvarige efter vetskap om incidenten?	Ja. Incidenten upptäcktes via personuppgiftsbiträdet.	Ja. Incidenten upptäcktes via personuppgiftsbiträdet.	N/A
Har personuppgiftsincidenten beskrivits utförligt? – (berörda antal registrerade - kategorier av och ungefärligt antal personuppgiftsposter)	Ja. Berörda personuppgifter är angivna. En misstanke kring händelseförloppet finns. Berörda registrerade grupper: Anställda, användare, barn, skolelever i förskola, grundskola, gymnasium. Varför incidenten inträffade och det berörda antalet av personuppgifter är okänt.	Ja. I samband med en uppdatering av systemet Skola24 går något fel. Risk har funnits att personuppgifter har visats mot fel person vid inlogg av elev och vårdnadshavare i mobilapp Skola24 (inte webbtjänst). Under perioden 17 december - 19 december har det funnits risk för att felaktiga personuppgifter har visats vid inloggning. Oklart i vilken omfattning detta har skett, d.v.s. hur många av elever och	Ja. Beskrivning: Utskrift av elevers närvaro/frånvaro har skrivits ut på felaktig skrivare. Går ej att härleda var ifrån utskriften kommer. 101–1000 registrerade påverkades av incidenten. Obehörigt röjande: Personuppgifter har spridits på

	Typ av berörda personuppgifter är angivna.	vårdnadshavare som har loggat in i appen under aktuell period. 1–10 registrerade påverkades. Berörda registrerade grupper: Anställda hos den personuppgiftsansvarige, användare av den personuppgiftsansvariges tjänster, skolelever i förskola, grundskola eller gymnasium. Personuppgifter som incidenten drabbat är angiven.	ett felaktigt sätt. Obehörig åtkomst: Någon inom eller utanför organisationen har tagit del av information som de saknade behörighet till. Berörda personuppgifter: För- och efternamn.
Förmedlat namn på och kontaktuppgifter för lämplig kontaktpunkt?	Ja.	Ja.	Delvis. Namn är angivet.
Beskrivning av konsekvenserna?	Den registrerade förlorar kontrollen över de egna personuppgifterna.	Den registrerade förlorar kontrollen över de egna personuppgifterna.	Den registrerade förlorar kontrollen över de egna personuppgifterna. Liknande incidenter kan inträffa igen.
Vidtagna åtgärder?	Applikationen har stängts ned. Personuppgiftsbiträdet har gjort en polisanmälan avseende dataintrånget. Ett varningsbrev har skickats till Zenbase, där de uppmanas att omgående ta ner hemsidan och att personuppgifterna däri destrueras. Personuppgiftsbitr	Kontakt har tagits med Skola24 för att få klarhet i vad som hänt och i vilken omfattning som registrerade i Laholms kommun är drabbade. Saknas information till Skola24. Oklart om fel användare har tagit del av tidigare registrerad frånvaro. Skola24 har lovat att återkomma om detta. Det är klargjort att	Kontakt med chef för elevhälsan då det bedöms troligt att utskrifterna kom från denna enhet.

	ädet undersöker eventuella öppna läckage och kommer genomföra justeringar under natten om så krävs. Webbplatsen zenbase.se stängdes ner. Personuppgiftsbitr ädet har lokaliserat personen bakom sajten som har stängts av från Vklass.	incidenten endast gäller modulen frånvaro/närvaro, alltså inte omdömen.	
Bedömning:	Tillfredställande.	Delvis tillfredställande.	Delvis tillfredställande.