VÄSTERVIKS KOMMUN

Kommunens revisorer

2021-09-15

Till
Kommunfullmäktige för kännedom
Kommunstyrelsen

Granskning av efterlevnad av dataskyddsförordningen (GDPR)

Ernst & Young AB (EY) har på uppdrag av de förtroendevalda revisorerna genomfört en granskning av kommunens nämnder, med kommunstyrelsen som ansvarig nämnd, med avseende på personuppgiftshantering. Granskningen syftade till att ge en *övergripande* förståelse av huruvida Västerviks kommun bedriver ett ändamålsenligt arbete med dataskyddsförordningen (the General Data Protection Regulation, GDPR) och i vilken utsträckning som de åtgärder som förordningen stipulerar uppfylls.

Granskningen utgår från EY:s ramverk för personuppgiftshantering gentemot dataskyddsförordningen för kommunala verksamheter. Ramverket består av 12 områden vilka bedöms från en skala från 1 (*begynnande*) till 5 (*optimerad*).

Baserat på den analys och granskning som genomförts bedöms Västerviks kommuns nämnder samt kommunstyrelsen ha en genomsnittlig mognadsgrad på 2,53 av 5,00. Mognadsgraden är strax under genomsnittet för vad EY generellt observerar i en offentlig verksamhet av liknande storlek och karaktär. Detta innebär att kommunen har en bit kvar att nå upp till en nivå som rekommenderas av EY, givet den stora mängd personuppgifter och känsliga personuppgifter som hanteras.

Mot bakgrund av granskningens iakttagelser rekommenderas kommunstyrelsen att:
Styrning och styrande dokument

- Upprätta en övergripande informationssäkerhetspolicy
- Upprätta riktlinjer och anvisningar för dataskyddsarbetet utifrån policyn
- Etablera en rutin för uppföljning av kommunens nämnder, för att säkerställa att nämnderna efterlever den policy och de regler som har fastställts

Granskning och rapportering

- Implementera en granskningsplan för att utvärdera och säkerställa att alla verksamheter lever upp till relevanta krav inom personuppgiftshantering
- Etablera en formell rutin för verksamheterna att dokumentera samt kontinuerligt rapportera resultatet av arbetet med personuppgifter till ledningsnivå på kommunen
- Fastställa ett rapporteringskrav gällande frekvens och innehåll som rapporteringen till kommunstyrelse ska utgå ifrån

Riskhantering

- Etablera en metod samt rutin för att vid återkommande tillfällen bedöma risker i personuppgiftshanteringen
- Att samtliga nämnder implementerar rutiner samt en ansvarsfördelning som säkerställer att konsekvensbedömningar utförs i de fall då riskanalyserna visar på höga integritetsrisker för den registrerade
- Genomföra konsekvensbedömningar inför varje ny behandling av personuppgifter inom verksamheten, samt vid regelbundna tillfällen

Utbildning och medvetenhet

- Implementera en utbildnings- samt informationsplan som inkluderar regelbundna interna utbildningar inom dataskyddsförordningen
- Implementera en rutin för regelbunden uppföljning för att säkerställa att alla anställda tar del av utbildningarna
- Etablera en rutin för att kontinuerligt uppdatera utbildningsmaterialet för att säkerställa att alla anställda inom verksamheten är medvetna om dataskyddsförordningens krav på personuppgiftshantering.

Vi ställer oss bakom granskningens slutsatser och rekommendationer och överlämnar härmed granskningen för kännedom. Vi önskar svar på rapportens rekommendationer samt vilka åtgärder ni planerar att vidta senast 10 december 2021.

För Västerviks kommuns revisorer

Britt-Louise Åberg Källmark
Ordförande

Lennart Petersson
Vice ordförande

Bilaga: Granskningsrapport – Granskning av efterlevnad av dataskyddsförordningen (GDPR).

VÄSTERVIKS KOMMUN

Kommunens revisorer

2021-09-15

Till
Västerviks Bostads AB
Tjustfastigheter AB

Granskning av efterlevnad av dataskyddsförordningen (GDPR)

Ernst & Young AB (EY) har på uppdrag av lekmannarevisorerna genomfört en granskning av Västerviks Bostads AB och Tjustfastigheter AB med avseende på personuppgiftshantering. Granskningen syftade till att ge en övergripande förståelse av huruvida de båda bolagen bedriver ett ändamålsenligt arbete med dataskyddsförordningen (the General Data Protection Regulation, GDPR) och i vilken utsträckning som de åtgärder som förordningen stipulerar uppfylls.

Granskningen utgår från EY:s ramverk för personuppgiftshantering gentemot dataskyddsförordningen för kommunala verksamheter. Ramverket består av 12 områden vilka bedöms från en skala från 1 (*begynnande*) till 5 (*optimerad*).

Baserat på den analys och granskning som genomförts bedöms Västerviks Bostads AB och Tjustfastigheter AB ha en genomsnittlig mognadsgrad på 2,93 av 5,00. Mognadsgraden är strax över genomsnittet för vad EY generellt observerar i en offentlig verksamhet av liknande storlek och karaktär. Det är en mognadsgrad som är något lägre än vad EY rekommenderar, givet den mängd personuppgifter som hanteras.

Mot bakgrund av granskningens iakttagelser rekommenderas Västerviks Bostads AB och Tjustfastigheter AB att:

Granskning

- Implementera en granskningsplan för att kontinuerligt utvärdera och säkerställa att relevanta krav på hantering av personuppgifter uppfylls
- Kontinuerligt analysera behov av granskning och uppföljning inom dataskydds- och informationssäkerhetsarbetet

Utbildning

- Etablera en rutin för att kontinuerligt utbilda anställda inom integritetsfrågor samt kontrollera att alla anställda framgångsrikt slutför utbildningarna
- Implementera rutiner för att kontinuerligt uppdatera utbildningsmaterialet
-

Riskhantering

- Upprätta en rutin för att återkommande bedöma risker kopplade till sin personuppgiftshantering

Vi ställer oss bakom granskningens slutsatser och rekommendationer och överlämnar härmed granskningen för kännedom. Vi önskar svar på rapportens rekommendationer samt vilka åtgärder ni planerar att vidta senast 30 november 2021.

Britt-Louise Åberg Källmark
Lekmannarevisor

Sven Öberg
Lekmannarevisor

Lennart Petersson
Lekmannarevisor

Ivar Svensson
Lekmannarevisor

Anders Helderud
Lekmannarevisor

Bilaga: Granskningsrapport – Granskning av efterlevnad av dataskyddsförordningen (GDPR).

2021-09-15

Till
Västervik Miljö och Energi AB
Västerviks Kraft-Elnät AB

Granskning av efterlevnad av dataskyddsförordningen (GDPR)

Ernst & Young AB (EY) har på uppdrag av lekmannarevisorerna genomfört en granskning av Västervik Miljö och Energi AB och Västerviks Kraft-Elnät AB med avseende på personuppgiftshantering. Granskningen syftade till att ge en *övergripande* förståelse av huruvida de båda bolagen bedriver ett ändamålsenligt arbete med dataskyddsförordningen (the General Data Protection Regulation, GDPR) och i vilken utsträckning som de åtgärder som förordningen stipulerar uppfylls.

Granskningen utgår från EY:s ramverk för personuppgiftshantering gentemot dataskyddsförordningen för kommunala verksamheter. Ramverket består av 12 områden vilka bedöms från en skala från 1 (*begynnande*) till 5 (*optimerad*).

Baserat på den analys och granskning som genomförts bedöms Västervik Miljö och Energi AB och Västerviks Kraft-Elnät AB ha en genomsnittlig mognadsgrad på 2,79 av 5,00. Mognadsgraden är en genomsnittlig mognadsgrad jämfört med vad EY generellt observerar i en offentlig verksamhet av liknande storlek och karaktär. Det är dessutom en siffra i linje med vad EY anser kan förväntas av bolaget, givet den ringa mängd känsliga personuppgifter som hanteras.

Mot bakgrund av granskningens iakttagelser rekommenderas Västervik Miljö och Energi AB och Västerviks Kraft-Elnät AB att:

Granskning

- Vidareutveckla den interna kontrollen avseende personuppgiftshantering och implementera en granskningsplan för att kontinuerligt utvärdera och säkerställa att relevanta krav på personuppgiftshanteringen uppfylls

Utbildning

- Etablera en rutin för att kontinuerligt utbilda anställda inom dataskyddsförordningen
- Implementera rutiner som säkerställer att internutbildningar uppdateras över tid

Hantering av leverantörsrelationer

- Arbeta vidare för att upprätta PUB-avtal med alla leverantörer där det är relevant
- Upprätta en dokumenterad rutin för att regelbundet granska personuppgiftsbiträden

Vi ställer oss bakom granskningens slutsatser och rekommendationer och överlämnar härmed granskningen för kännedom. Vi önskar svar på rapportens rekommendationer samt vilka åtgärder ni planerar att vidta senast 30 november 2021.

Britt-Louise Åberg Källmark
Lekmannarevisor

Sven Öberg
Lekmannarevisor

Lennart Petersson
Lekmannarevisor

Ivar Svensson
Lekmannarevisor

Anders Helderud
Lekmannarevisor

Bilaga: Granskningsrapport – Granskning av efterlevnad av dataskyddsförordningen (GDPR).

2021-09-15

Till
Västervik Resort AB

Granskning av efterlevnad av dataskyddsförordningen (GDPR)

Ernst & Young AB (EY) har på uppdrag av lekmannarevisorerna genomfört en granskning av Västervik Resort AB med avseende på personuppgiftshantering. Granskningen syftade till att ge en övergripande förståelse av huruvida de båda bolagen bedriver ett ändamålsenligt arbete med dataskyddsförordningen (the General Data Protection Regulation, GDPR) och i vilken utsträckning som de åtgärder som förordningen stipulerar uppfylls.

Granskningen utgår från EY:s ramverk för personuppgiftshantering gentemot dataskyddsförordningen för kommunala verksamheter. Ramverket består av 12 områden vilka bedöms från en skala från 1 (*begynnande*) till 5 (*optimerad*).

Baserat på den analys och granskning som genomförts bedöms Västervik Resort AB ha en genomsnittlig mognadsgrad på 2,19 av 5,00. Mognadsgraden är en mognadsgrad strax under genomsnittet för vad EY generellt observerar i en offentlig verksamhet av liknande storlek och karaktär. Detta innebär också att bolaget har en bit kvar för att nå upp till en nivå som rekommenderas av EY, givet den mängd personuppgifter som hanteras av bolaget.

Mot bakgrund av granskningens iakttagelser rekommenderas Västervik Resort AB att:

Organisation och kontroll

- Dokumentera en formell, informationssäkerhetsspecifik organisationsstruktur med tillhörande roller samt en tydlig ansvarsfördelning för att minimera risker för personberoende samt för överarbetsbelastning
- Avsätta resurser för att utveckla arbetet med integritetsfrågor och dataskydd

Behandling av personuppgifter

- Upprätta ett dokumenterat register över alla personuppgifter som hanteras i bolaget
- Upprätta dokumenterade rutiner för att säkerställa att personuppgifter endast behandlas för deras ursprungliga ändamål, informationsklassning samt gallring av personuppgifter, exempelvis i form av en dokumenthanteringsplan.

Riskhantering

- Ta fram en metod samt rutin för att kontinuerligt kunna bedöma integritetsrisker kopplade till personuppgiftsbehandlingen

- Implementera rutiner samt en ansvarsfördelning för att genomföra konsekvensbedömningar inom organisationen

Vi ställer oss bakom granskningens slutsatser och rekommendationer och överlämnar härmed granskningen för kännedom. Vi önskar svar på rapportens rekommendationer samt vilka åtgärder ni planerar att vidta senast 30 november 2021.

Britt-Louise Åberg Källmark
Lekmannarevisor

Sven Öberg
Lekmannarevisor

Lennart Petersson
Lekmannarevisor

Ivar Svensson
Lekmannarevisor

Anders Helderud
Lekmannarevisor

Bilaga: Granskningsrapport – Granskning av efterlevnad av dataskyddsförordningen (GDPR).

Västerviks kommun

Granskning av efterlevnad dataskyddsförordningen (GDPR)

Augusti 2021

Ernst & Young AB
111 47 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Sammanfattning

EY har på uppdrag av Västervik kommuns förtroendevalda revisorer genomfört en granskning av kommunens nämnder, med kommunstyrelsen som ansvarig nämnd, såväl som de kommunala bolagen Västervik Miljö och Energi AB, Västerviks Kraft-Elnät AB, Västervik Resort AB, Västerviks Bostads AB samt Tjustfastigheter AB med avseende på personuppgiftshantering. De ovan nämnda bolagen hänvisas hädanefter till samlingsbegreppet ”de helägda bolagen”.

Granskningens syfte är att ge en *övergripande* förståelse av huruvida Västerviks kommun och dess helägda bolag bedriver ett ändamålsenligt arbete med dataskyddsförordningen (the General Data Protection Regulation, GDPR) och hur väl man uppfyller de åtgärder som förordningen stipulerar.

En översiktlig granskning av 12 olika områden med utgång i EY:s ramverk för personuppgiftshantering gentemot dataskyddsförordningen för kommunala verksamheter har genomförts under februari 2021 till juli 2021. Enligt metoden bedöms kommunens mognadsgrad enligt 116 punkter på en ordinarie skala från 1 (*begynnande*) till 5 (*optimerad*) inom de respektive 12 områdena. Analysen har baserats på intervjuer med identifierade nyckelpersoner i kommunen och dess helägda bolags personuppgiftssäkerhetsarbete, samt genomgång av insamlad styrdokumentation i kommunen och bolagen.

Baserat på den analys och granskning som genomförts bedöms objekten ha följande genomsnittliga mognadsgrader:

- Västerviks kommuns nämnder genom kommunstyrelsen: 2,53 av 5,00

2,53 är en mognadsgrad strax under genomsnittet för vad EY generellt observerar i en offentlig verksamhet av liknande storlek och karaktär. Detta innebär att kommunen har en bit kvar att nå upp till en nivå som rekommenderas av EY, givet den stora mängd personuppgifter och känsliga personuppgifter som hanteras.

- Västervik Miljö & Energi AB & Västerviks Kraft-Elnät AB: 2,79 av 5,00

Mognadsgraden 2,79 är en genomsnittlig mognadsgrad jämfört med vad EY generellt observerar i en offentlig verksamhet av liknande storlek och karaktär. Det är dessutom en siffra i linje med vad EY anser kan förväntas av bolaget, givet den ringa mängd känsliga personuppgifter som hanteras.

- Västervik Resort AB: 2,19 av 5,00

2,19 är en mognadsgrad strax under genomsnittet för vad EY generellt observerar i en offentlig verksamhet av liknande storlek och karaktär. Detta innebär också att bolaget har en bit kvar för att nå upp till en nivå som rekommenderas av EY, givet den mängd personuppgifter som hanteras av bolaget.

- Västervik Bostads AB & Tjustfastigheter AB: 2,93 av 5,00

Mognadsgraden 2,93 är strax över genomsnittet för vad EY generellt observerar i en offentlig verksamhet av liknande storlek och karaktär. Det är en mognadsgrad som är något lägre än vad EY rekommenderar, givet den mängd personuppgifter som hanteras.

På en övergripande nivå rekommenderar EY således att nämnderna jobbar vidare med att etablera tydliga processer och riktlinjer kring hur arbetet med granskning och kontroll ska genomföras. Detta för att säkerställa att verksamheterna lever upp till relevanta krav inom

Ernst & Young AB
111 47 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

personuppgiftshantering. Vidare rekommenderas det även att etablera en formell rutin för att dokumentera, samt kontinuerligt rapportera resultatet av arbetet med personuppgifter. Slutligen rekommenderar EY även att kommunen jobbar vidare med utbildning och kunskapsspridning på en övergripande nivå. Detta genom att implementera utbildningsplaner med planlagda och regelbundna aktiviteter kopplade till dataskyddsförordningen.

Ernst & Young AB
111 47 Stockholm
Besöksadress:
Hamngatan 26

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Innehållsförteckning

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

1. Inledning

1.1. 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. Andra syften med dataskyddsförordningen är att modernisera dataskyddsdirektivets regler från 1995 och att anpassa dessa till det nya digitala samhället.

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:

- Både offentliga och privata institutioner skall kunna beläggas med sanktioner utefter samma bedömningskriterier (upp till 10 MSEK för offentliga verksamheter beroende på överträdelsens allvarlighetsgrad).
- Obligatorisk överträdelseanmälan rörande personuppgiftsincidenter skall göras till den lokala tillsynsmyndigheten inom 72 timmar efter att incidenter har uppdagats.
- Individer har rätt till ersättning i form av skadestånd till följd av överträdelser av förordningen av en personuppgiftsansvarig eller ett personuppgiftsbiträde.

Datainspektionen är den tillsynsmyndighet som ansvarar för uppföljning och kontroll av att lag och förordning efterlevs. I oktober 2018 publicerade Datainspektionen en ”sammanställning av resultatet från granskning av dataskyddsombud”. Granskningen omfattade såväl offentlig som privat sektor. Det konstateras att det är en marginell skillnad i efterlevnaden av reglerna mellan myndigheter och privata aktörer. Inga primärkommuner ingick i granskningen. Av totalt 66 tillsynsärenden beslutade inspektionen att ge reprimander i 57 fall. I två fall fick tillsynsobjekten ett föreläggande och sju fall avslutades utan åtgärd. Datainspektionen har också inlett andra inspektioner inom ramen för dataskyddsförordningens efterlevnad.

Då Västerviks kommun med dess verksamheter samt de kommunala bolagen hanterar stora mängder personuppgifter, har de förtroendevalda revisorerna i Västerviks kommun beslutat att genomföra en helhetsgranskning av kommunens arbete med personuppgiftshantering med hänsyn till dataskyddsförordningen (GDPR).

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

1.2. Syfte och revisionsfrågor

Syftet med granskningen är att ge en *övergripande* förståelse av huruvida Västerviks kommun och dess helägda bolag bedriver ett ändamålsenligt arbete med dataskyddsförordningen och hur kommunens mognad ser ut i uppfyllelse av de åtgärder som förordningen stipulerar. Granskningen ska svara på följande tre revisionsfrågor:

- Arbetar Västerviks kommun ändamålsenligt för att uppfylla de krav och regleringar för personuppgiftshantering som har införts i och med dataskyddsförordningen (GDPR)?
- Är Västerviks kommuns policyer och riktlinjer ändamålsenliga för att uppnå regelefterlevnad med avseende på dataskyddsförordningen (GDPR)?
- Har Västerviks kommun ändamålsenlig kontroll och uppföljning av arbetet med dataskyddsförordningen (GDPR)?

1.3. Avgränsning

De iakttagelser och rekommendationer som presenteras i denna rapport baseras enbart på den information som inhämtats under intervjuer och genom granskning av erhållna dokument, såsom riktlinjer, rutiner och policyer. Granskningen är begränsad till arbetet som Västervik kommun bedriver på central nivå och kommunens nämnder eller kommunalägda bolag utöver Västervik Miljö och Energi AB, Västerviks Kraft-Elnät AB, Västervik Resort AB, Västerviks Bostads AB samt Tjustfastigheter AB har således inte granskats i ytterligare detalj. Ingen teknisk analys har genomförts och inga stickprov på efterlevnad har tagits.

1.4. Metod

Granskningens syfte har adresserats genom intervjuer med identifierade nyckelpersoner i kommunen och dess helägda bolags informationssäkerhetsarbeten samt genomgång av relevant dokumentation (se *Bilaga 2: Dokumentförteckning*). Granskningen är utförd mot god praxis och med utgångspunkt i EY:s metod för granskning av mognadsgrad gentemot dataskyddsförordningen.

Metoden består av ett ramverk med 116 frågor. Dessa frågor är kategoriserade över 12 områden kopplade till dataskyddsförordningen och täcker in de områden som är väsentliga utifrån ett internkontrollperspektiv för att bedöma eventuella avvikelser och risker kopplat till brister i personuppgiftshanteringen. Besvarandet av frågorna som innefattas av ramverket sker genom arbetsmöten med GDPR-specialister från EY. Våra 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 både direkt kopplade till krav från förordningen och indirekt kopplade genom att täcka exempelvis 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 viktigt att inte enbart granska huruvida enskilda kontroller är på plats och enskilda krav är täckta; det är även av stor vikt att säkerställa att styrning och uppföljning av regeluppfyllnad sker systematiskt.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

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 områdes färgkod visar en genomsnittlig mognadsgrad som beräknas över alla krav som ingår i området. Respektive krav har inte viktats. Mognadsgraden per område indikerar vilka områden som har störst förbättringsbehov, men på grund av genomsnittsberäkningen kan till exempel ett område med grön färgkod ändå sakna viktiga kontroller. Granskningens huvudsakliga värde ligger i dess observationer och rekommendationer som beskrivs i en bredare kontext i själva granskningsrapporten.

Inledningsvis har underlag såsom policyer, strategi- och styrdokument och dylikt samlats in för att analyseras. Därefter höll EY:s GDPR-specialister totalt fyra arbetsmöten med ansvariga inom kommunen samt respektive bolag (se *Bilaga 1: Förteckning över intervjuade funktioner*). Under arbetsmötena avhandlades samtliga 12 områden. Efter att EY analyserat resultatet av arbetsmötena sammanställdes ett rapportutkast som faktagranskades av de intervjuade. EY genomförde sedan justeringar och uppdateringar av rapporten som även kvalitetssäkrades av EY:s verksamhetsrevisorer, varefter de förtroendevalde revisorerna på kommunen erhöll en slutlig rapport med övergripande rekommendationer för fortsatt arbete.

Tidsplanen för arbetet såg ut enligt följande:

- Februari 2021 – Förberedelser, planering och insamling av dokumentation.
- Mars 2021 – juni 2021 – Dokumentanalys, utförande av arbetsmöten (2021-03-03, 2021-03-08, 2021-03-11 samt 2021-03-15), granskning av kompletterande dokumentation och uppföljningsfrågor, färdigställande av rapport samt faktagranskning av kommunen och bolagen.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

- Augusti 2021 – Kvalitetssäkring av EY:s verksamhetsrevisorer och slutgiltig presentation för kommunens förtroendevalda revisorer.

Västervik Miljö och Energi AB samt Västerviks Kraft-Elnät AB granskades som en enhet, vilket även gjordes för Västervik Bostads AB samt Tjustfastigheter AB. Detta var ett gemensamt beslut mellan EY och verksamheterna som baserades på att de separata bolagen styrs och agerar som en enhet inom frågor relaterade till dataskyddsförordningen.

1.5. Definitioner

Se bilaga 3.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

2. Västerviks kommun

2.1. Bedömning

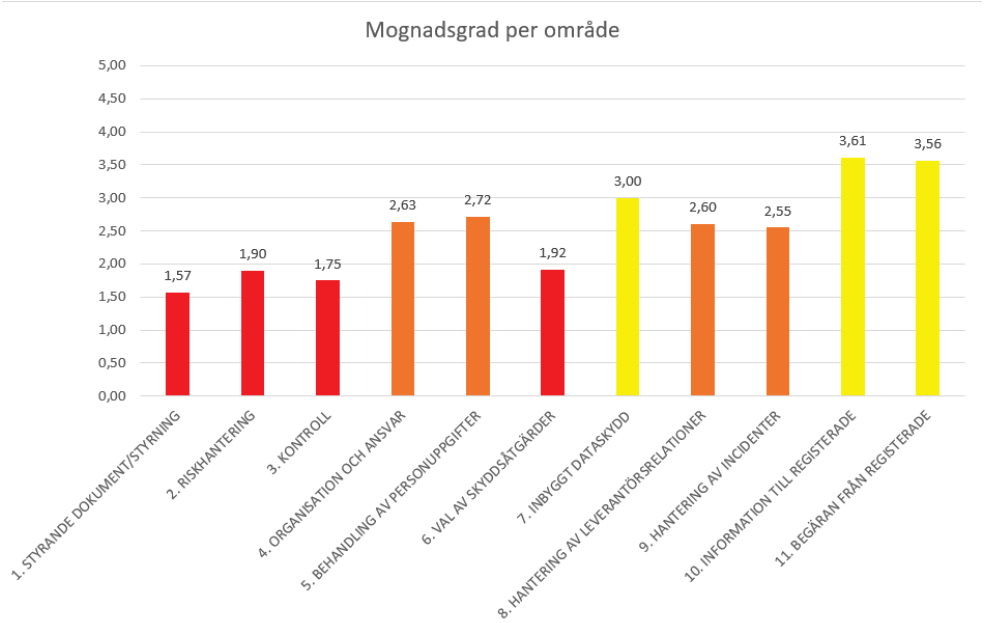
Baserat på utförd granskning konstateras att Västerviks kommun och dess verksamheter har en mognadsgrad strax under genomsnittet inom personuppgiftshantering, jämfört med vad EY generellt observerar i en offentlig verksamhet av motsvarande storlek och karaktär. Kommunens mognadsgrad uppnår en summa av 2,53, vilket även är en lägre mognadsgrad än vad EY rekommenderar för en kommun likt Västerviks kommun som hanterar en stor mängd personuppgifter och känsliga personuppgifter.

Det finns goda ambitioner inom organisationen att arbeta med integritetsfrågor och dataskydd, samt en god kunskap om dataskyddsförordningen och dess krav. Trots detta finns det brister inom styrningen av personuppgiftsarbetet från kommunens sida. Det saknas exempelvis styrdokument kring arbetet med personuppgifter inom organisationen som är uppdaterade i enlighet med dataskyddsförordningen. Det finns dessutom en utvecklingspotential inom styrningen med avseende på kontrollområdet. Detta då det i dagsläget inte finns någon etablerad granskningsplan över hur arbetet med personuppgifter efterlever dataskyddsförordningen i kommunens verksamheter.

Västerviks kommun rekommenderas att i ett första skede upprätta styrdokument som inkluderar behandling av personuppgifter enligt dataskyddsförordningens krav. Detta för att möjliggöra att processer och riktlinjer för riskhantering, utbildning och granskning kan implementeras konsekvent genom hela kommunen.

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

Figur 2: Mognadsgrad per område

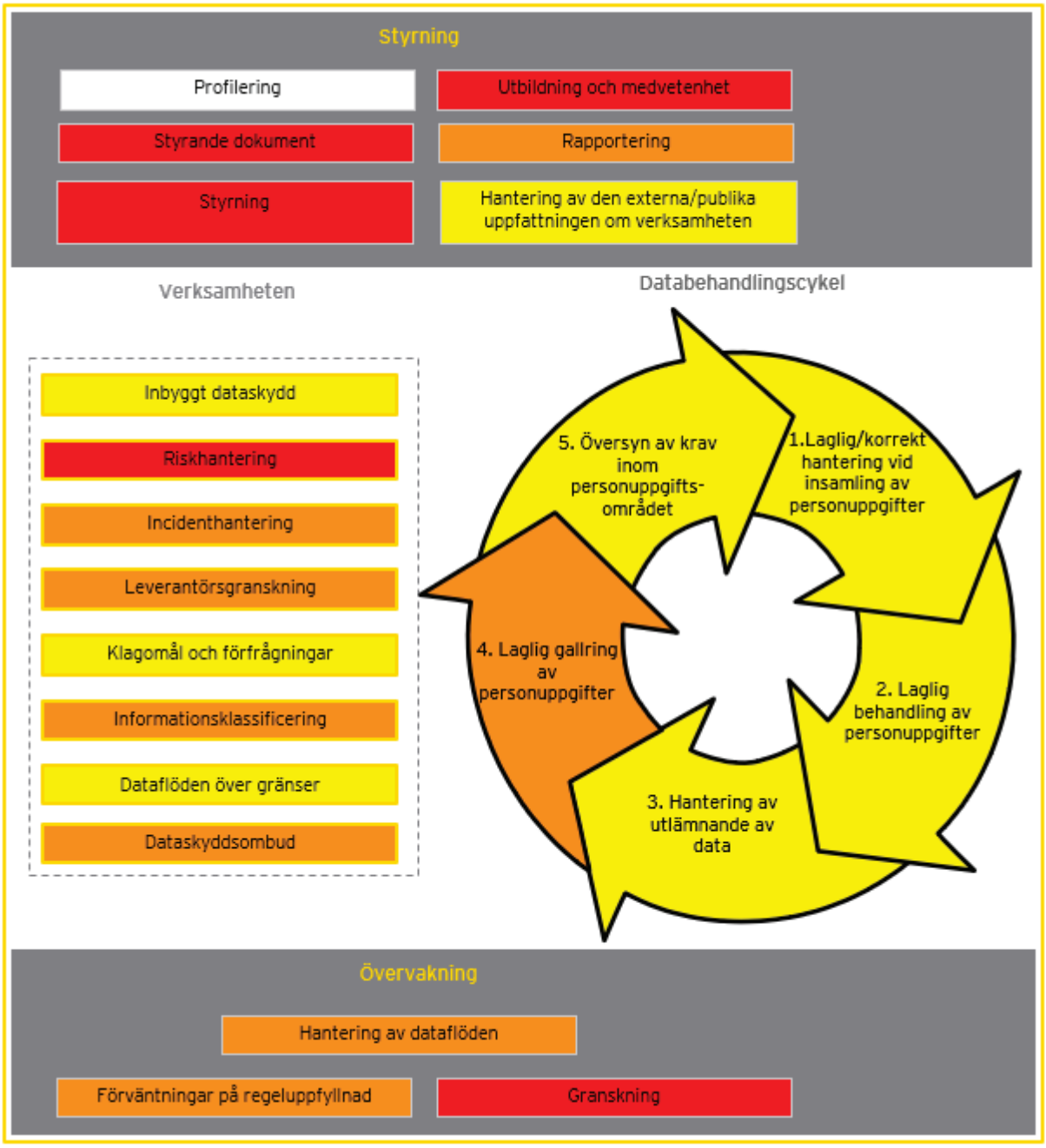


Nivå 5 representerar hög mognadsgrad medan nivå 1 representerar låg mognadsgrad.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Figur 3: 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.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

2.2. 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	Inom Västerviks kommun finns det en säkerhetspolicy som uttrycker kommunfullmäktiges övergripande viljeriktning för kommunkoncernens arbete med informationssäkerhet. Informationssäkerhetsinstruktioner fastställdes av kommunstyrelsen 2013. Instruktionerna är inte uppdaterade sedan dess och är därmed inte uppdaterade i enlighet med dataskyddsförordningen. Kommunen saknar i dagsläget en informationssäkerhetspolicy. Respektive nämnd samt helägt bolag inom kommunen är personuppgiftsansvariga för deras verksamheter och ska följa koncerngemensamma policyer och riktlinjer, samt ansvarar för efterlevnaden av dessa i respektive verksamhet. Det är upp till respektive verksamhet att ta fram lokala instruktioner kring personuppgiftshantering anpassade efter deras verksamhet. I dagsläget saknas övergripande instruktioner eller riktlinjer för hantering av personuppgifter i enlighet med dataskyddsförordningen inom kommunkoncernen. Det pågår dock ett arbete med att ta fram dessa. Kommunen har utsett en informationssäkerhetssamordnare som har ett koncerngemensamt samordningsansvar för dataskydd och informationssäkerhet. Kommunen har rekommenderat samtliga nämnder och bolag att följa de koncerngemensamma riktlinjerna. Västerviks kommun skapade inför dataskyddsförordningens införande i maj 2018 en gemensam samordningsgrupp med syftet att stötta kommunens nämnder, förvaltningar och bolag med arbetet kring dataskyddsförordningen. Samordningsgruppen leds av kommunens informationssäkerhetssamordnare och involverar respektive dataskyddsombud för varje nämnd samt bolag. Samordningsgruppen möts tre till fyra gånger per halvår.	Västerviks kommun saknar en informationssäkerhetspolicy som är uppdaterad i enlighet med dataskyddsförordningen. Det saknas övergripande instruktioner eller riktlinjer beträffande hanteringen av personuppgifter i enlighet med kraven i dataskyddsförordningen. Lokala rutiner gällande personuppgiftsbehandling har tagits fram inom vissa bolag samt nämnder, men det saknas tydliga krav, uppföljning samt samordning för arbete med lokala rutiner från kommunens sida.	1,57

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Riskhantering	Västerviks kommun genomför koncernövergripande risk- och sårbarhetsanalyser vid varje ny mandatperiod. Analysen ses över av samtliga nämnder och bolag årligen samt vid behov. Metoden säkerställer dock inte i dagsläget att risker som kan finnas i samband med hantering av personuppgifter analyseras. Inom kommunen finns en medvetenhet kring riskerna kopplade till behandlingen av personuppgifter, och informella riskbedömningar görs löpande vid behov. Det saknas en dokumenterad rutin för att genomföra konsekvensbedömningar innan en ny behandling av personuppgifter påbörjas i verksamheten.	Det saknas rutiner för att genomföra kontinuerliga riskanalyser kring arbetet med integritetsrisker i kommunens verksamhet och IT-system. Det saknas metod och ansvar för att genomföra konsekvensbedömningar innan verksamheten startar en ny typ av behandling.	1,90
Kontroll	Västerviks kommun har valt ett arbetssätt som innebär att ett dataskyddsombud (DSO) utses per nämnd och bolag. Notera att bolagen Västervik Miljö & Energi AB samt Västerviks Kraft-Elnät AB har ett gemensamt DSO. Detta gäller även för Västerviks Bostads AB samt TjustFastigheter AB. Alla verksamheter samt helägda bolag har i dagsläget ett utsett dataskyddsombud, eller en roll med liknande arbetsuppgifter. Uppdraget innebär att respektive DSO är kontaktperson gentemot IMY i enlighet med GDPR. Informationssäkerhetssamordnaren genomförde under 2019 en koncerngemensam nulägesanalys över arbetet kring dataskyddsförordningen. Utifrån nulägesanalysen tog man fram en aktivitetsplan för att nå önskat resultat. Det planeras i dagsläget inte att genomföras en återkommande analys av verksamheten. Kommunens informationssäkerhetssamordnare har kontinuerlig kontakt med respektive DSO genom möten med samordningsgruppen för arbetet med dataskyddsförordningen. Det sker ingen formell rapportering från respektive nämnd eller bolag kring arbetet med personuppgifter till kommunstyrelsen. Det är upp till varje enskild verksamhet att avgöra huruvida de vill genomföra interna granskningar kring arbetet med dataskyddsförordningen.	Västerviks kommun har ingen fastslagen granskningsplan eller internkontrollfunktion som följer upp att kommunens förvaltningar samt bolag hanterar personuppgifter i enlighet med dataskyddsförordningen. En formell rutin för rapportering från respektive förvaltning och bolag till kommunstyrelse samt krav som sådan rapportering ska utgå ifrån har inte förankrats.	1,75

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Organisation och ansvar	Det finns en dokumenterad organisation- samt ansvarsfördelning kring informationssäkerhetsarbetet i kommunen, denna ansvarsfördelning inkluderar dock inte specifikt arbete med dataskyddsförordningen. Exempelvis saknas tydliga riktlinjer kring ansvaret gällande implementation, uppföljning samt rapportering av arbetet med personuppgifter för varje nämnd och bolag. Kunskapsnivån inom dataskyddsförordningen samt Integritetsskyddsmyndighetens befogenheter upplevs som god i allmänhet inom kommunens verksamheter. 2019 genomfördes en nulägesanalys av arbetet med integritetsfrågor och dataskydd i verksamheten. Det framkom då att det finns brister inom bemanning av arbetet med dataskyddsfrågor. Vissa dataskyddsombud har uppgett att de vid vissa tillfällen nedprioriterar arbetet på grund av andra uppgifter eller ansvar som de har. I vissa fall har inte dataskyddsombudet enbart en rådgivande roll, utan granskar även till viss del arbetet denne själv har implementerat.	Det saknas en komplett kommunövergripande ansvarsfördelning kring arbetet med dataskyddsförordningen. Det är inte säkerställt inom alla förvaltningar att deras dataskyddsombud har tillräckligt med resurser för att genomföra sitt arbete, samt inte har några intressekonflikter kring andra uppgifter och ansvar.	2,63
Behandling av person-uppgifter	Inom Västerviks kommun rekommenderas nämnder samt bolag att upprätta en registerförteckning med hjälp av en systemleverantör, men vissa förvaltningar och bolag har valt att skapa en egen typ av registerförteckning. Respektive verksamhet ansvarar för att registerförteckningen är komplett. Respektive DSO ansvarar för sammanställning av registerförteckning. Kommunen undersökte under 2019 hur arbetet med registerförteckningar fortlöper i verksamheten. Det visade sig då att avsaknaden av styrande dokument kring hanteringen av personuppgifter har försvårat arbetet med att föra personuppgiftsregister. Det saknas en rutin för att säkerställa att de olika verksamheterna arbetar med en registerförteckning i enlighet med dataskyddsförordningen, exempelvis för att kontrollera om förteckningarnas fullständighet eller riktighet över tid. Det finns inga koncernövergripande riktlinjer för hur man ska arbeta med gallring inom respektive verksamhet i Västerviks kommun. Det är upp till varje enskild verksamhet inom kommunen att arbeta med gallring av personuppgifter.	Det finns inga formella rutiner för hur man inom kommunen ska arbeta med registerförteckningar samt följa upp deras riktighet över tid. Det saknas rutiner eller kontroller som säkerställer att personuppgifter i respektive förvaltning endast behandlas för de ändamål som de samlades in för och sedan anonymiseras, raderas eller gallras inom rätt tidsram.	2,72

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Val av skydds-åtgärder	Man arbetar i kommunen med att ta fram en ny informationshanteringsplan som ska omfatta informationsklassning av personuppgifter. Det finns i dagsläget dock inte någon metod eller något verktyg för att regelbundet genomföra informationsklassificering. Västerviks kommun distribuerar information samt utbildningar inom integritetsfrågor och dataskydd till samtliga anställda inom kommunkoncernen via intranätet. Utbildningarna är inte obligatoriska, och det saknas en rutin för att överse huruvida anställda genomför utbildningarna. Kommunens HR-avdelning arbetar i dagsläget med att ta fram en internutbildning inom informationssäkerhet samt dataskyddsförordningen för nyanställda i chefspositioner. Kommunen uppmanar alla anställda att genomföra utbildningar inom dataskyddsförordningen, men det är upp till respektive förvaltning samt bolag att genomföra ytterligare utbildningar med de anställda inom deras verksamhet. Kommunen arbetar för att ta fram en informations- och utbildningsplan som inkluderar arbetet med personuppgifter.	En rutin för att säkerställa att samtlig strukturerad och ostrukturerad information blir klassificerad har inte implementerats. Det saknas en rutin för att säkerställa att anställda regelbundet tar del av interna utbildningar om dataskyddsförordningen. Västerviks kommun saknar en informations- och utbildningsplan som inkluderar arbetet med personuppgifter i enlighet med dataskyddsförordningen.	1,92
Inbyggt dataskydd	Västerviks kommun arbetar med lagring- samt uppgiftsminimering i enlighet med respektive förvaltningar samt bolags gallringsrutiner. Inom kommunen använder man i vissa fall sekretessavtal vid exempelvis höga systembehörigheter från leverantörer eller externa konsulter. Det finns inga dokumenterade rutiner för att genomföra tester eller uppföljning av behörighetsstrukturer i kommunens IT-system som hanterar personuppgifter.	Det saknas omgivande tester och uppföljning av behörighetsåtkomster i IT-system.	3,00

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Hantering av leverantörs-relationer	Västerviks kommun har tagit fram en koncerngemensam mall för PUB-avtal som baseras på en mall från SKR samt bilaga. Mallen distribueras via intranätet. Man planerar att arbeta fram en ny systemförvaltningsmodell inom kommunen som ska inkludera granskning av leverantörer och deras efterlevnad av dataskyddsförordningen. Det saknas i dagsläget en rutin för att säkerställa att man inom kommunen har upprättat PUB-avtal med alla relevanta leverantörer, samt rutiner för att säkerställa att personuppgiftsbiträden agerar i enlighet med dataskyddsförordningen över tid. Vissa förvaltningar använder IT-system som har datalagring i tredje land. Det saknas kommungemensamma instruktioner för hur verksamheterna ska säkerställa att datalagringen har en tillräcklig skyddsnivå.	Det saknas en rutin för att säkerställa att det finns PUB-avtal med alla relevanta leverantörer. Det saknas en rutin för att säkerställa att personuppgiftsbiträden långsiktigt agerar i linje med dataskyddsförordningen. I dagsläget finns det ingen koncerngemensam riktlinje för att säkerställa att datalagring i tredje land har en tillräcklig skyddsnivå.	2,60
Hantering av incidenter	Västerviks kommun arbetar med att ta fram en rutin för rapportering av personuppgiftsincidenter. Rutinen omfattar hur en incident ska utredas, bedömas, rapporteras och kommuniceras, men är i skrivande stund ej beslutad. Incidentrapportering sker via intranätet för de förvaltningar samt bolag som väljer att använda kommunens riktlinje. Det finns inga etablerade rutiner på plats som kontrollerar att de interna instruktionerna eller rutinerna gällande personuppgiftsincidenter efterlevs. Västerviks kommun har upprättat ett register över personuppgiftsincidenter som omfattar alla incidenter som rapporterats från kommunens förvaltningar. Kommunens bolag ansvarar för att dokumentera deras incidenter inom respektive verksamhet.	En rutin för att granska efterlevnaden av rutinerna gällande personuppgiftsincidenter saknas.	2,55

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Information till registrerade	Det finns en koncerngemensam dokumenterad mall för att informera registrerade om verksamhetens behandling av personuppgifter. Mallen distribueras på intranätet. På kommunens hemsida erbjuds även registrerade utförlig information kring hur behandlingen av personuppgifter ska ske. Västerviks kommun har etablerat en blankett för insamling samt återkallande av samtycke, vars utformning säkerställer att samtycket är distinkt, tydligt samt bygger på en aktiv handling som inte är ihopblandat med andra samtycken. Man har inte etablerat en dokumenterad rutin för hur verksamheten kommunicerar med registrerade vid förändringar av kommunens hantering av personuppgifter.		3,61
Begäran från registrerade	Det finns överlag en direkt och tydlig kontaktväg för registrerade via kommunens hemsida för att framföra förfrågningar och klagomål. Kommunen har uppgett kontaktuppgifter till dataskyddsombuden för samtliga verksamheter. Kommunen har tagit fram en lokal rutin för förvaltningarna att hantera en begäran av en registrerad. Kommunen erbjuder registrerade hos förvaltningarna att använda en E-tjänst för att begära ett registerutdrag. Registrerade identifierar sig med Bank-id för att använda E-tjänsten. Det finns ingen koncerngemensam rutin för att hantera begäran från registrerade. Kommunens bolag hanterar begäran om registerutdrag samt begäran om rättelse i enlighet med deras lokala rutiner.	Det saknas dokumenterade rutiner kring begäran från registrerade som kan användas av samtliga förvaltningar och bolag, och det sker ingen uppföljning huruvida respektive bolag har etablerat lokala rutiner.	3,56
Profilering	Beslut som enbart grundar sig på automatiserad behandling av registrerade förekommer inte.	N/A	N/A

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

2.3. Övergripande rekommendationer

Då iakttagelser har identifierats inom flera delar av ramverket har EY valt att presentera fyra övergripande rekommendationer och förslag på åtgärder för de främsta riskerna inom Västervik kommuns dataskydd och informationssäkerhetsarbete. Rekommendationerna är rangordnade i prioritetsordning men EY rekommenderar att samtliga förslag åtgärdas inom 12 månader.

Styrning och styrande dokument

För att säkerställa att alla bolag samt nämnder inom Västerviks kommun arbetar i enlighet med dataskyddsförordningen bör Västerviks kommunstyrelse fokusera på att ta fram en övergripande informationssäkerhetspolicy. Utifrån denna policy kan kommunen skapa en strategi med ett tydligt syfte för arbetet med integritetsfrågor och dataskydd som är förankrat från kommunfullmäktige, ända ner till de operativa verksamheterna. Kommunen rekommenderas därefter att fokusera på att ta fram riktlinjer och anvisningar för dataskyddsarbetet utifrån policyn, som täcker in alla relevanta delar inom dataskyddsförordningen. EY rekommenderar även att Västerviks kommunstyrelse ska etablera en rutin för uppföljning av kommunens nämnder, för att säkerställa att de efterlever den policy och de regler som har fastställts.

Granskning och rapportering

En begränsad uppföljning av informationssäkerhetsarbetet inom kommunens verksamheter medför en viss risk att verksamheternas dagliga arbete skiljer sig från det sätt som kommunen anvisar samt tror att arbetet bedrivs på. Därför rekommenderas Västerviks kommunstyrelse att implementera en granskningsplan för att utvärdera och säkerställa att alla verksamheter lever upp till relevanta krav inom personuppgiftshantering. Man rekommenderas även att etablera en formell rutin för verksamheterna att dokumentera samt kontinuerligt rapportera resultatet av arbetet med personuppgifter till ledningsnivå på kommunen. Exempelvis skulle detta kunna ske genom att man säkerställer att arbetet med dataskydd och integritetsfrågor integreras i internkontrollarbetet. För att säkerställa att uppföljning av dataskyddsförordningen utförs och kommuniceras till ledningen, rekommenderas kommunstyrelsen att fastställa ett rapporteringskrav gällande frekvens och innehåll som rapporteringen till kommunstyrelse ska utgå ifrån.

Riskhantering

Riskhantering syftar till att utvärdera hur Västerviks kommun identifierar samt minskar integritetsrisker i sin verksamhet och i sina IT-system. Därmed rekommenderas kommunstyrelsen att etablera en metod samt rutin för att vid återkommande tillfällen bedöma risker med deras personuppgiftshantering. Utifrån dessa riskanalyser bör informationsskydd för respektive identifierad integritetsrisk etableras för att säkerställa ett adekvat dataskydd inom kommunen. Samtliga nämnder rekommenderas att implementera rutiner samt en ansvarsfördelning som säkerställer att konsekvensbedömningar utförs i de fall då riskanalyserna visar på höga integritetsrisker för den registrerade, samt att man vid dessa tillfällen söker råd hos Integritetsskyddsmyndigheten. Konsekvensbedömningar rekommenderas att genomföras inför varje ny behandling av personuppgifter inom verksamheten, samt vid regelbundna tillfällen för att säkerställa att verksamheten minimerar nya eller förändrade risker.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Utbildning och medvetenhet

Kommunstyrelsen rekommenderas att implementera en utbildnings- samt informationsplan som inkluderar regelbundna interna utbildningar inom dataskyddsförordningen. Kommunen distribuerar i dagsläget utbildningar inom integritetsfrågor samt dataskydd till anställda via sitt intranät, men rekommenderas även att implementera en rutin för regelbunden uppföljning för att säkerställa att alla anställda tar del av utbildningarna. Man rekommenderas att etablera en rutin för att kontinuerligt uppdatera utbildningsmaterialet för att säkerställa att alla anställda inom verksamheten är medvetna om dataskyddsförordningens krav på personuppgiftshantering. Uppdaterade utbildningar eller dokumentation skulle vara lämpliga att inkludera vid kommunens möten med samordningsgruppen för dataskyddsförordningen, då respektive ansvarigt dataskyddsombud kan säkerställa att alla anställda inom deras verksamheter tar del av utbildningsmaterialet.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

3. Västervik Miljö och Energi AB samt Västerviks Kraft-Elnät AB

3.1. Bedömning

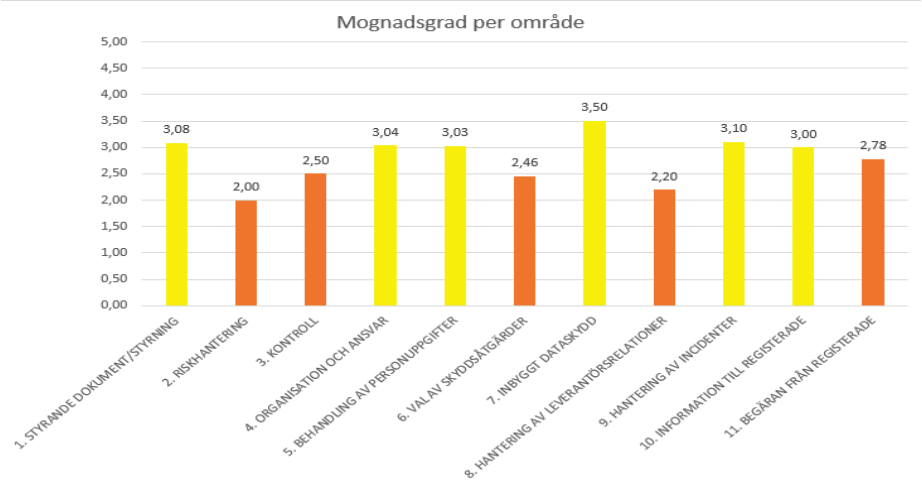
Västervik Miljö och Energi AB samt Västerviks Kraft-Elnät AB granskades som en enhet, då bolagen i det dagliga arbetet styrs och uppfattas som ett och samma. Detta beslut fattades i enighet mellan EY och utsedda representanter för respektive bolag.

Baserat på utförd granskning konstateras det att bolaget ligger på en genomsnittlig mognadsgrad i jämförelse med vad EY har observerat av andra bolag av liknande karaktär. Den genomsnittliga mognadsgraden på 2,79 bedöms av EY vara ändamålsenlig med tanke på mängden, samt känslighetsgraden, av personuppgifter som företaget hanterar. Det framgår att de ansvariga inom bolagen har arbetat på ett ambitiöst sätt med dataskyddsfrågor och bolagsledningen visar på ett intresse för dessa frågor då man relativt nyligen genomförde en internkontroll inom personuppgiftshantering.

Bolagen ämnar arbeta utefter ISO27001-standarden med kontinuerlig uppföljning och utveckling av informationssäkerhetsarbetet, vilket inkluderar arbetet med dataskydd och personuppgiftshantering. Inom detta arbete har de självständigt arbetat med personuppgiftshantering och tagit fram lokala instruktioner som täcker många av dataskyddsförordningens områden. Bolagen rekommenderas att fortsatt implementera och dokumentera rutiner och kontroller, främst inom utbildning och medvetenhet, arbetet med registerförteckningen, PUB-avtal samt intern granskning.

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

Figur 4: Mognadsgrad per område

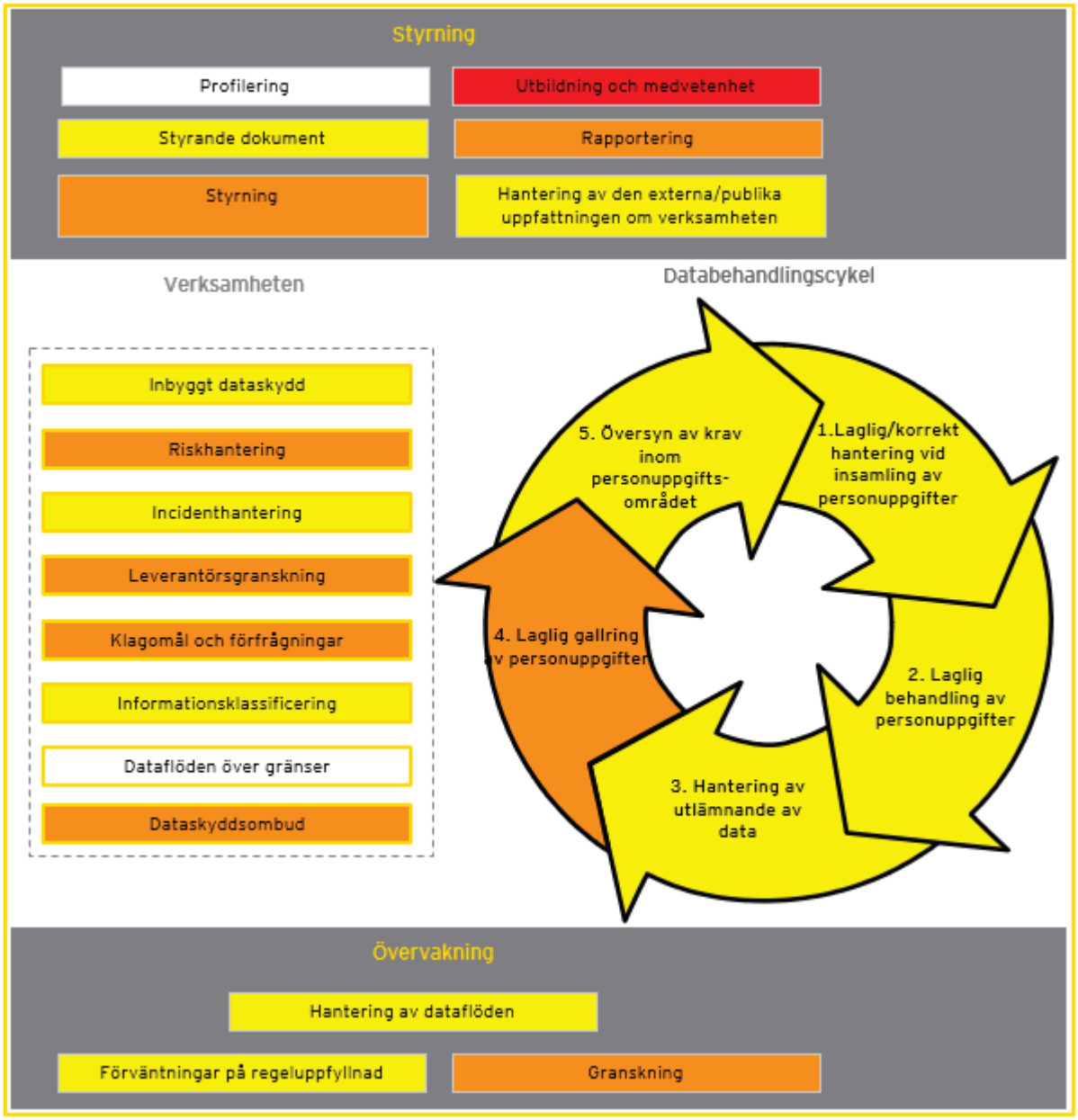


Nivå 5 representerar hög mognadsgrad medan nivå 1 representerar låg mognadsgrad.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Figur 5: 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.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

3.2. Nuläge och iakttagelser

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

Tabell 2: Observationer inom de 12 områdena

Område	Nuläge	Iakttagelser	Mognad
Styrande dokument/ styrning	Bolagen har tagit fram en informationssäkerhetspolicy som reviderades senast 2021. Policyn granskas och uppdateras vid behov, men minst en gång per år av bolagsstyrelsen. Bolagen har skapat en instruktion som beskriver hur man ska hantera personuppgifter inom bolagen. Instruktionerna granskas minst en gång var 18e månad av dokumentets godkännare. Det finns ingen rutin för att följa upp hur instruktionerna efterlevs i praktiken.		3,08
Riskhantering	Bolagen har en tydlig rutin för att genomföra årliga riskanalyser i bolagens verksamhet och IT-system. Denna rutin säkerställer dock inte att integritetsrisker analyseras regelbundet som del utav arbetet med riskanalyser. En riskanalys kring arbetet med integritetsfrågor och dataskydd genomfördes dock under 2020. Det finns ingen dokumenterad rutin för konsekvensbedömningar, däremot arbetar man inom bolaget kontinuerligt med att bedöma nya risker som kan uppstå för de registrerade med de befintliga behandlingarna samt inför nya behandlingar. Detta sker exempelvis i samband med de årliga genomgångarna av registerförteckningen. Bolaget har analyserat befintliga behandlingar av personuppgifter och kommit fram till att det inte finns något behov av att genomföra strukturerade konsekvensbedömningar.	Det saknas en dokumenterad rutin som säkerställer att integritetsrisker i bolagets verksamhet och IT-system analyseras kontinuerligt. Det saknas en fastställd och dokumenterad rutin för att genomföra konsekvensbedömningar innan en ny typ av behandling startas.	2,00

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Kontroll	Bolagen fattar årligen beslut om aktuella kontrollpunkter för nästkommande års internkontrollarbete. Riskbedömningen görs löpande av tjänstemän vartefter kontroller och granskningsintervall fastställs och utvärderas årligen. Av bolagens internkontrollplaner finns 4 kontrollpunkter avseende GDPR som utvärderades och avrapporterades till kommunstyrelsen i samband med 2020 års avrapportering. Kontrollpunkterna återfinns fortsatt i riskanalysen och kontrolleras i enlighet med fastställd kontrollplan. Rapportering till bolagsstyrelsen kring dataskyddsarbetet i bolagen sker alltså bland annat genom en årlig internkontroll, i de fall då bolagsstyrelsen valt att kontrollen ska omfatta dataskyddsfrågor. Personuppgiftshantering granskas ibland som en del av internkontrollarbetet då bolagsstyrelsen valt ut området för granskning. Men ingen specifik granskningsplan för arbetet med personuppgiftshantering existerar i dagsläget som säkerställer att organisationen kontinuerligt uppfyller relevanta krav på hantering av personlig information. Det finns inga dokumenterade rutiner för att bistå Integritetsskyddsmyndigheten med efterfrågad dokumentation.	Det saknas en specifik granskningsplan för arbetet med personuppgiftshantering som säkerställer att bolagen kontinuerligt uppfyller relevanta krav på personuppgiftshantering.	2,50
Organisation och ansvar	Bolagen har utsett ett dataskyddsombud (DSO), och det finns tydligt definierade roller och ansvar kopplat till arbetet med dataskydd och informationssäkerhet. DSO har god kunskap inom dataskyddsförordningen samt integritetsskyddsmyndighetens befogenheter. DSO arbetar med både dataskyddsfrågor samt andra arbetsuppgifter. DSO har en rådgivande roll i organisationen men utför även visst operativt arbete och implementation kring dataskyddsfrågor som denne sedan ska granska.	Bolagen har inte säkerställt att DSO enbart har en rådgivande position, utan DSO granskar även till viss del arbetet som denne har varit med och implementerat.	3,04

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Behandling av person-uppgifter	Bolagen har genomfört en kartläggning av sina behandlingsprocesser av personuppgifter, dokumenterad som en registerförteckning. Bolagen har dokumenterat en instruktion kring hur arbetet med registerförteckningen ska bedrivas. Ansvaret för registerförteckningens riktighet och fullständighet över tid åligger systemägarna, som ska gå igenom förteckningen årligen. Det saknas dock i dagsläget en rutin som säkerställer att arbetet med registret granskas och att instruktionen efterlevs. Under 2020 genomfördes en internkontroll av registerförteckningen som visade att vissa personuppgifter i registret inte var komplett analyserade eller uppdaterade. Bolagen har två separata dokumenthanteringsplaner för både Västervik Miljö och Energi AB samt Västervik Kraft-Elnät AB. En gallringsplan är fastställd i dokumenthanteringsplanen men en rutin för att säkerställa att personuppgifter gallras inom de angivna tidsramarna saknas. Bolagen uppger att de inte hanterar några känsliga personuppgifter.	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 och sedan anonymiseras, raderas eller gallras inom rätt tidsram.	3,03
Val av skydds-åtgärder	Bolagen har tagit fram en lokal instruktion som informerar hur anställda ska arbeta i enlighet med dataskyddsförordningen. Instruktionerna innehåller definitioner av personuppgifter samt känsliga personuppgifter som återspeglar dataskyddsförordningens definitioner väl. Instruktionerna finns tillgängliga för alla anställda i det IT-baserade ledningssystemet. Betydande ändringar och nyheter kommuniceras löpande, eller vid behov, av kvalitets- och miljöansvarig. Under våren 2018 genomförde bolagen en utbildningsinsats inom integritetsfrågor och dataskydd för alla anställda. I utbildning och introduktion av alla nyanställda ingår hantering av personuppgifter också som en viktig del. Bolagen diskuterar att ta fram en internutbildning inom dataskyddsförordningen för anställda i chefspositioner. Det saknas dock en rutin för regelbunden utförande, uppföljning eller uppdatering av utbildning.	Det finns i dagsläget inte en dokumenterad process som säkerställer att internutbildningar inom dataskyddsförordningen uppdateras och genomförs regelbundet av de anställda.	2,46

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Inbyggt dataskydd	Bolagen ställer krav på vilka säkerhetsfunktioner system ska innehålla vid upphandlingar. Kommunen håller dessutom på att ta fram standardiserade krav på ”privacy by design” med syftet att säkerställa att inbyggt dataskydd finns som krav vid upphandling av samtliga nya IT-system. Efterlevnad av krav följs upp i de kontinuerliga möten som hålls med systemleverantörer. Dataskyddsombudet har översyn över vilka användare som har behörighet till de IT-system som lagrar personuppgifter och utför behörighetskontroller på ad-hoc basis. Lagrings- och uppgiftsminimering sker kontinuerligt på ett informellt sätt. Dock försöker man etablera ett standardiserat arbetssätt kring detta. Lagringsminimering sker även enligt gallringsrutiner som är fastställda i dokumenthanteringsplanerna. Bolagen genomförde under 2020 en internkontroll kring uppgiftsminimering där man genom stickprov fastställde att inga icke nödvändiga personuppgifter hade insamlats.	Det saknas en fastställd rutin för att regelbundet kontrollera att behörighetsnivåer inom IT-system är lämpliga, exempelvis genom periodisk granskning.	3,50
Hantering av leverantörs-relationer	En mall för PUB-avtal tillhandahållen av SKR används för att skriva avtal med flertalet leverantörer. Bolagen har tagit fram utförliga instruktioner för hur ett PUB-avtal ska skrivas, samt när det är nödvändigt att upprätta. Stickprov har under en internkontroll genomförd under 2020 visat att det i dagsläget eventuellt saknas PUB-avtal med vissa leverantörer. I dagsläget sker ingen strukturerad och formell uppföljning eller kontroll kring hur information behandlas och lagras i praktiken hos berörda leverantörer. Frågorna kan dock diskuteras och analyseras ad hoc som en del av de kontinuerliga träffar som hålls tillsammans med systemleverantörer. Bolagen lagrar ingen data i tredje land.	Det saknas eventuellt kompletta PUB-avtal för vissa leverantörer där det vore relevant. En dokumenterad rutin för att säkerställa att personuppgiftsbiträden långsiktigt och regelbundet agerar i linje med dataskyddsförordningen saknas.	2,20

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Hantering av incidenter	Det finns lokala instruktioner för hur personuppgiftsincidenter ska identifieras samt rapporteras via incidentshanteringsverktyg. Dessa instruktioner finns tillgängliga för alla anställda via incidentrapporteringsverktyget. Det är upp till den enskilde anställde att rapportera en eventuell incident. Två biträdande säkerhetsskyddschefer är åtgärdsansvariga för incidenter och dessa avgör, i samråd med DSO och linjechefer, om en incident ska rapporteras vidare till Integritetsskyddsmyndigheten. Då inga incidenter hittills har identifierats i verksamheten, saknas etablerade rutiner som kontrollerar att de interna instruktionerna gällande incidentrapportering efterlevs.	En rutin för att granska efterlevnaden av instruktionerna gällande personuppgiftsincidenter saknas.	3,10
Information till registrerade	Bolagen har säkerställt att de via sin hemsida lämnar utförlig information till de registrerade om hur deras personuppgifter behandlas. Det saknas en dokumenterad process för hur bolagen ska kommunicera med registrerade vid en eventuell förändring av personuppgiftsbehandling eller vid en inträffad personuppgiftsincident. Vid de enskilda fall när bolagen samlar in personuppgifter via samtycke, sker detta med hjälp av en samtyckesblankett som säkerställer att samtycket sker genom en aktiv handling på ett distinkt och tydligt sätt som inte är ihopblandat med andra samtycken. Det saknas i dagsläget en dokumenterad rutin för hur registrerade kan återkalla sitt samtycke.	Det saknas en process för hur bolagen kan kommunicera med registrerade vid en eventuell förändring i behandlingen av personuppgifter eller vid en incident.	3,00
Begäran från registrerade	Det finns en tydlig kontaktväg för registrerade att framföra förfrågningar eller klagomål via bolagens hemsida eller direktkontakt med kundservicegruppen via e-post eller telefon. Bolagen har etablerat en dokumenterad rutin för att hantera en begäran från en registrerad, samt rutiner för att säkerställa identiteten på den registrerade vid begäran. Det finns inga fastställda rutiner för hantering av förfrågningar gällande felaktiga, inte längre nödvändiga, eller gällande radering av personuppgifter.	Det saknas en rutinbeskrivning avseende hanteringen av inkommen begäran från registrerad om rättelse, radering och begränsning av personuppgifter.	2,78
Profilering	Beslut som enbart grundar sig på automatiserad behandling av registrerade förekommer inte.	N/A	N/A

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

3.3. Övergripande rekommendationer

Iakttagelser av varierande vikt har identifierats inom flera delar av ramverket. EY har valt att presentera de mest relevanta övergripande rekommendationerna för Västervik Miljö och Energi AB samt Västerviks Kraft-Elnät AB och förslag på åtgärder för de främsta riskerna inom dataskydds- och informationssäkerhetsarbetet. EY rekommenderar att samtliga förslag åtgärdas inom 12 månader.

Granskning

En alltför begränsad uppföljning av Västervik Miljö och Energi AB och Västerviks Kraft-Elnät AB:s informationssäkerhetsarbete medför risk att den dagliga informationshanteringen avviker från de rutiner bolagen anvisar till. Bolagen har visat en förståelse för detta då man under 2020 har genomfört en internkontroll inom sitt arbete med personuppgiftshantering. Bolagen rekommenderas att vidareutveckla detta arbete, och implementera en granskningsplan för att kontinuerligt utvärdera och säkerställa att man uppfyller relevanta krav på personuppgiftshantering.

Utbildning

Västervik Miljö och Energi AB och Västerviks Kraft-Elnät AB rekommenderas att etablera en rutin för att kontinuerligt utbilda anställda inom dataskyddsförordningen, för att säkerställa att alla anställda är medvetna om vikten av, samt deras ansvar, när det gäller integritetsfrågor och dataskydd. Vidare rekommenderas bolagen att implementera rutiner som säkerställer att internutbildningar uppdateras över tid.

Hantering av leverantörsrelationer

Västervik Miljö och Energi AB och Västerviks Kraft-Elnät AB rekommenderas att arbeta vidare för att upprätta PUB-avtal med alla leverantörer där det är relevant. Vidare rekommenderas bolagen att upprätta en dokumenterad rutin för att regelbundet granska deras personuppgiftsbiträden för att säkerställa att de agerar enligt PUB-avtal och dataskyddsförordningens krav, då bolagen är ansvariga för integriteten av de personuppgifter som tillhandahålls leverantörer.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

4. Västervik Resort AB

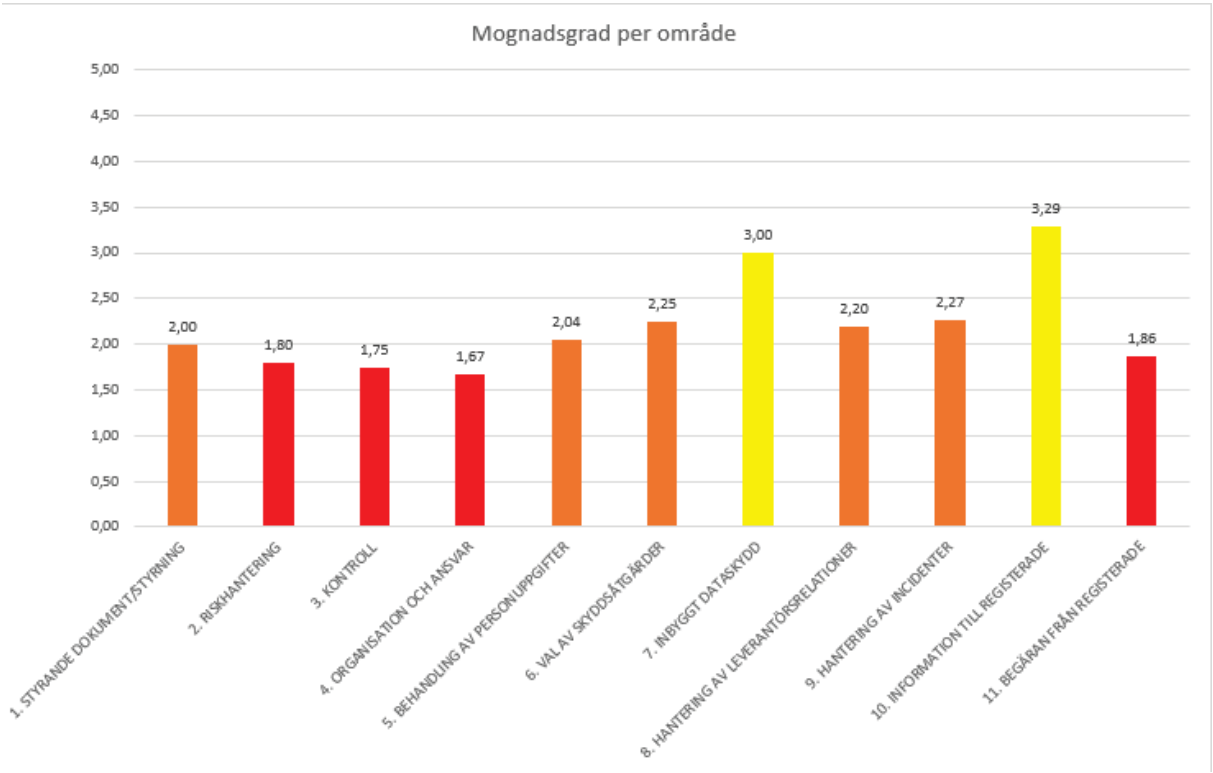
4.1. Bedömning

Baserat på utförd granskning konstateras att Västervik Resort AB har en mognadsgrad strax under genomsnittet inom personuppgiftshantering, jämfört med vad EY generellt observerar i en offentlig verksamhet av motsvarande storlek och karaktär. Bolagets mognadsgrad uppnår en summa av 2,19, vilket är en lägre mognadsgrad än vad EY rekommenderar för ett bolag av liknande storlek och hantering av personuppgifter.

Bolaget visar en god förståelse för vikten av information till registrerade i enlighet med dataskyddförordningen och arbetar på ett ändamålsenligt sätt med samtycke från registrerade.

Då det saknas en tydligt dokumenterad organisation samt ansvarsfördelning inom arbetet med informationssäkerhet och personuppgiftshantering, rekommenderas bolaget i första hand att dokumentera en formell, informationssäkerhetsspecifik organisationsstruktur med tillhörande roller samt en tydlig ansvarsfördelning. Vidare rekommenderas bolaget att fortsätta utveckla arbetet med integritetsfrågor genom att exempelvis upprätta en registerförteckning över bolagets personuppgiftsbehandlingar samt en rutin för att kontinuerligt analysera integritetsrisker relaterade till bolagets arbete med personuppgifter.

Figur 6: Mognadsgrad per område

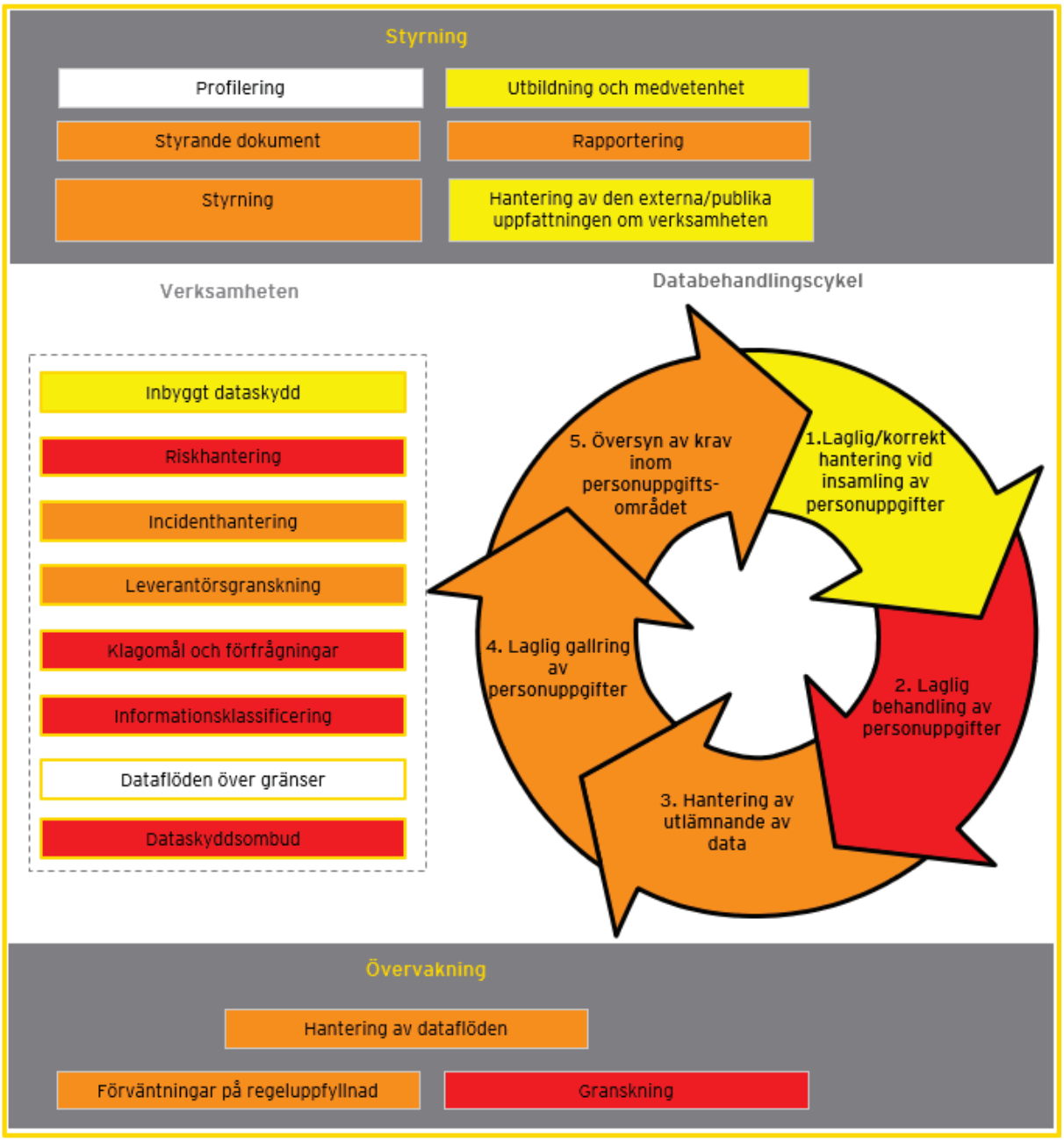


Nivå 5 representerar hög mognadsgrad medan nivå 1 representerar låg mognadsgrad.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Figur 7: 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.

Notering: för kategorin dataskyddsombud beror den röda markeringen på en otydlig ansvarsfördelning samt bristande förutsättningar att utöva sina uppgifter och inte på befattningshavaren och dennes kompetens.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

4.2. Nuläge och iakttagelser

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

Tabell 3: Observationer inom de 12 områdena

Område	Nuläge	Iakttagelser	Mognad
Styrande dokument/ styrning	Bolaget har dokumenterat processen för att hantera personuppgifter i verksamheten i form av flödeskartor. Man har inte tagit fram någon ytterligare dokumentation kopplat till styrning, då man följer Västervik kommuns styrdokument. Det saknas rutiner för att följa upp hur arbetet med personuppgiftshantering går inom bolaget. Brister och förbättringsområden har inte analyserats formellt eller dokumenterats.	Det saknas dokumenterade rutiner beträffande hanteringen av personuppgifter i enlighet med kraven från dataskyddsförordningen.	2,00
Riskhantering	Två gånger om året genomför bolagsledningen riskanalyser av verksamheten i enlighet med en mall för riskanalyser tillhandahållen av Västerviks kommun. Bolaget har vid vissa tillfällen bedömt risker kopplade till hanteringen av personuppgifter, men det finns ingen rutin för att göra kontinuerliga riskanalyser kring integritetsrisker. Man saknar en fastställd metod för att genomföra konsekvensbedömningar innan bolaget startar en ny typ av behandling av personuppgifter. Man genomför vissa konsekvensbedömningar på en informell operativ nivå i det dagliga arbetet och förlitar sig dessutom på kommunens bedömningar när de gäller de IT system som drivs av dem. Dock saknas det en dokumenterad rutin för att säkerställa att konsekvensbedömningar utförs då bolaget startar en ny behandling eller kontinuerligt vid behov.	Det saknas dokumenterade rutiner för att genomföra kontinuerliga riskanalyser kring arbetet med integritetsrisker i bolagets verksamhet och IT-system. Det saknas en dokumenterad rutin för att säkerställa att konsekvensbedömningar genomförs innan bolaget startar en ny typ av behandling.	1,80

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Kontroll	Bolaget har en utsedd kontaktperson till Integritetsskyddsmyndigheten. Det finns ingen formell rutin för att bistå Integritetsskyddsmyndigheten med efterfrågad information eller för att rapportera personuppgiftsincidenter. Bolaget använder sig av Västervik kommuns riktlinjer för incidenthantering. Kontaktpersonen som är ansvarig för personuppgiftsarbetet inom bolaget ska rapportera status för dataskyddsarbetet i bolaget till informationssäkerhetssamordnare på Västerviks kommun. I dagsläget har bolaget inte en fastslagen granskningsplan för att utvärdera och säkerställa att man uppfyller relevanta krav på hantering av personuppgifter.	Det saknas en formell rutin för att bistå Integritetsskyddsmyndigheten med efterfrågad information. Det finns hittills ingen tydligt fastställd granskningsplan eller kontinuerlig internkontrollsplan för dataskyddsfrågor.	1,75
Organisation och ansvar	Det saknas dokumentation kring organisation och ansvarsfördelning inom bolaget kopplat till integritetsfrågor och dataskydd. Bolaget har utsett en kontaktperson som ingår i kommunens nätverk för dataskyddsombud, där denna tar del av information samt nyheter kring arbetet med personuppgifter inom kommunen. Då bolagets kontaktperson arbetar med liknande arbetsuppgifter som ett dataskyddsombud, har denne god kunskap inom dataskyddsförordningen. Kontaktpersonen arbetar huvudsakligen heltid på en tjänst inom bolagets högsta ledning. Bolaget har inte försäkrat sig om att deras kontaktperson har allt stöd som krävs för att säkerställa att de uppgifter som fastställs i dataskyddsförordningen utförs.	Det saknas i dagsläget en tydlig ansvarsfördelning inom bolaget som säkerställer att arbetet med personuppgifter kan bli oberoende granskat. Bolaget har inte försäkrat sig om att kontaktpersonen för arbetet med personuppgifter har tillräckligt med stöd i form av tid och resurser för att utföra sina uppgifter relaterade till integritetsfrågor.	1,67
Behandling av person-uppgifter	Bolaget saknar i dagsläget ett dokumenterat register över de personuppgifter man hanterar. Bolaget har ingen rutin på plats för att säkerställa att personuppgifterna endast behandlas för de ändamål de ursprungligen samlades in för. Man har lokala rutiner för gallring av personuppgifter, men det finns ingen dokumenterad instruktion för hur detta ska genomföras. Ansvarig för dataskyddsfrågor inom bolaget samt receptionsansvarig har genomfört stickprov för att säkerställa att gallring genomförs, och har vid dessa stickprov inte upptäckt några brister.	Ett dokumenterat register över alla personuppgifter bolaget hanterar saknas. Det saknas rutiner som säkerställer att personuppgifter endast behandlas för de ändamål som de samlades in för och sedan anonymiseras, raderas eller gallras inom rätt tidsram.	2,04

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Val av skydds-åtgärder	Bolaget har ingen etablerad rutin eller metod för att genomföra informationsklassificering av personuppgifter. Bolaget uppvisar en förståelse för betydelsen av känsliga personuppgifter då man har etablerat ett tankesätt att personuppgifter i allmänhet ska hanteras varsamt. Personen som är ansvarig för dataskyddsfrågor i bolaget genomför årligen en utbildning med bolagets anställda där information kring dataskyddsförordningen inkluderas. Efter utbildningen signerar de anställda ett dokument som visar att de tagit del av informationen. De som inte kan delta vid utbildningstillfället får ta del av utbildningen via e-mail.	En metod och rutin för att genomföra klassificering av strukturerad såväl som ostrukturerad information och dokumentation saknas.	2,25
Inbyggt dataskydd	Bolaget har rutiner för att ta bort användare direkt efter avslutad anställning. Ansvarig för dataskyddsfrågor samt receptionsansvarig ansvarar för att enbart behöriga användare har åtkomst till de system som hanterar personuppgifter och har rutiner för att kontrollera detta. Lagrings- och uppgiftsminimering för befintliga system sker i enlighet med befintliga gallringsrutiner.	Bolaget saknar en dokumenterad rutin för att kontrollera behörighetsstrukturer, exempel på detta kan vara periodiska granskningar av höga behörigheter.	3,00
Hantering av leverantörs-relationer	Bolaget använder en mall tillhandahållen av SKR för PUB-avtal. Man har upprättat PUB-avtal med flertalet leverantörer, och arbetar för att upprätta det med samtliga leverantörer där det vore relevant. Uppföljning och kontroll kring hur information behandlas och hanteras sker i en begränsad utsträckning och finns inte dokumenterat, men man har kontinuerlig kontakt med leverantören av bolagets bokningssystem. Bolaget anser att man har en god insyn i deras verksamhet och hur de arbetar med personuppgifter.	Det finns inte kompletta PUB-avtal med vissa leverantörer där det vore relevant.	2,20
Hantering av incidenter	Bolaget har en lokal rutin för att hantera personuppgiftsincidenter. Incidenter ska rapporteras till bolagets kontaktperson för personuppgiftsarbetet som följer Västerviks kommuns riktlinjer för incidenthantering. Incidenter rapporteras via intranätet. Man har inte identifierat några personuppgiftsincidenter, därmed saknas det rutiner för att säkerställa att processen följs i praktiken.	Det saknas rutiner för att följa upp hur väl instruktionerna för incidenthantering efterlevs i bolaget.	2,27

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Information till registrerade	Bolaget har tagit fram en integritetspolicy som de delger via sin hemsida. Policyn riktar till sig registrerade och beskriver hur bolaget behandlar personuppgifter. Policyn revideras senast under mars 2021. Bolaget har tydliga rutiner för hur samtycke ska inhämtas och dokumenteras. Alla samtycken lagras i bokningssystemet vid bokningstillfället. Det finns rutiner för att återkalla ett samtycke från en registrerad. Det finns i dagsläget ingen dokumenterad rutin för hur bolaget kommunicerar med de registrerade vid personuppgiftsincidenter eller vid en förändring av bolagets hantering av personuppgifter.	En rutin för hur bolaget kommunicerar möjliga förändringar i hur man hanterar personuppgifter eller incidenter som berör registrerade saknas.	3,29
Begäran från registrerade	På bolagets hemsida anges postadressen som kontaktväg för registrerade. Det finns inga kontaktuppgifter till en ansvarige för dataskyddsfrågor på hemsidan. Klagomål och förfrågningar från registrerade brukar komma till receptionen som kopplar in bolagets kontaktperson om så är nödvändigt. Det finns ingen lokal rutin för att hantera en begäran från registrerade. Om en eventuell begäran görs, är det ansvarige för dataskyddsfrågor som ansvarar för att hantera den.	Det finns inte en tydlig, dokumenterad kontaktväg för de registrerade till bolagets ansvarige för personuppgifter. Det saknas dokumentation som beskriver hur man ska hantera en begäran från registrerade.	1,86
Profilering	Beslut som enbart grundar sig på automatiserad behandling av registrerade förekommer inte.	N/A	N/A

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

4.3. Övergripande rekommendationer

Iakttagelser av varierande vikt har identifierats inom flera delar av ramverket. EY har valt att presentera de mest relevanta övergripande rekommendationerna för Västervik Resort AB och förslag på åtgärder för de främsta riskerna inom dataskydds- och informationssäkerhetsarbetet. Rekommendationerna är rangordnade i prioritetsordning men EY rekommenderar att samtliga förslag åtgärdas inom 12 månader.

Organisation samt kontroll

Västervik Resort AB rekommenderas att dokumentera en formell, informationssäkerhetsspecifik organisationsstruktur med tillhörande roller samt en tydlig ansvarsfördelning för att minimera risker att vara för personberoende, samt för överarbetsbelastning. Det saknas i dagsläget resurser för att bolaget ska kunna genomföra ett adekvat och oberoende dataskyddsarbete. Bolaget rekommenderas därför att avsätta resurser för att utveckla arbetet med integritetsfrågor och dataskydd, så att man kan genomföra grundläggande gap-analyser för att identifiera utvecklingsområden, utveckla rutiner och processer utifrån detta, samt granska efterlevnaden av rutinerna i bolaget.

Behandling av personuppgifter

Västervik Resort AB rekommenderas att upprätta ett dokumenterat register över alla de personuppgifter som hanteras, för att leva upp till de krav som ställs i dataskyddsförordningen. I samband med detta rekommenderas bolaget att upprätta dokumenterade rutiner för att säkerställa att personuppgifter endast behandlas för deras ursprungliga ändamål, informationsklassning samt gallring av personuppgifter, exempelvis i form av en dokumenthanteringsplan.

Riskhantering

Riskhantering syftar till att utvärdera hur bolagen identifierar och minskar integritetsrisker i sin verksamhet och i sina IT-system. Västervik Resort AB rekommenderas att ta fram en metod samt rutin för att kontinuerligt kunna bedöma integritetsrisker kopplade till sin personuppgiftsbehandling. Bolaget rekommenderas även att implementera rutiner samt en ansvarsfördelning för att genomföra konsekvensbedömningar inom organisationen.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

5. Västerviks Bostads AB samt Tjustfastigheter AB

5.1. Bedömning

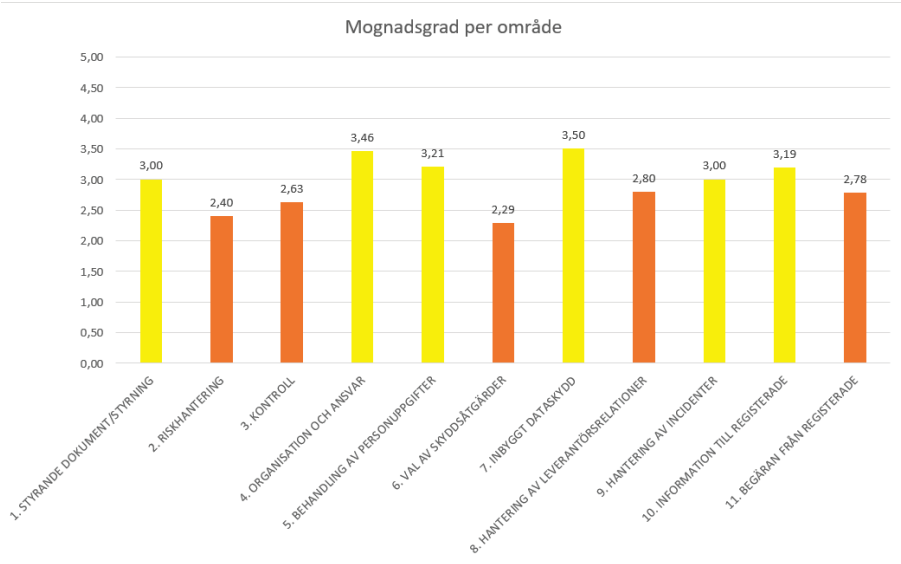
Västerviks Bostads AB samt Tjustfastigheter AB granskades som en enhet. Detta då bolagen i det dagliga arbetet med dataskyddsförordningen styrs och uppfattas som ett bolag. Detta beslut fattades i enighet mellan EY och utsedda representanter för respektive bolag.

Baserat på utförd granskning konstateras bolagen ligga strax över genomsnittet i jämförelse med andra bolag av liknande karaktär och storlek inom deras arbete med informationssäkerhet och personuppgiftshantering. Den genomsnittliga mognadsgraden på 2,93 bedöms dock av EY vara något lägre än rekommenderat med tanke på mängden, samt känslighetsgraden, av personuppgifter som företaget hanterar. Ett ambitiöst arbete med integritets- samt dataskyddsfrågor har styrts från bolagsledningen genom organisationen. Detta exemplifieras av att bolaget i skrivande stund redan påbörjat arbeta med de rekommendationer och observationer som framkommer av denna rapport.

Bolagen har på ett självständigt sätt arbetat med personuppgiftshantering, främst genom att ta fram en väl dokumenterad systemförvaltningsplan som i flera avseenden motsvarar dataskyddsförordningens krav på personuppgiftshantering. Bolagen rekommenderas att fortsätta arbetet med att implementera en granskningsplan för att säkerställa efterlevnaden av dataskyddsförordningen, utveckla rutiner och ställa krav inom utbildning och medvetenhet, samt arbeta ytterligare med riskanalyser specifikt gällande personuppgiftshantering.

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

Figur 8: Mognadsgrad per område

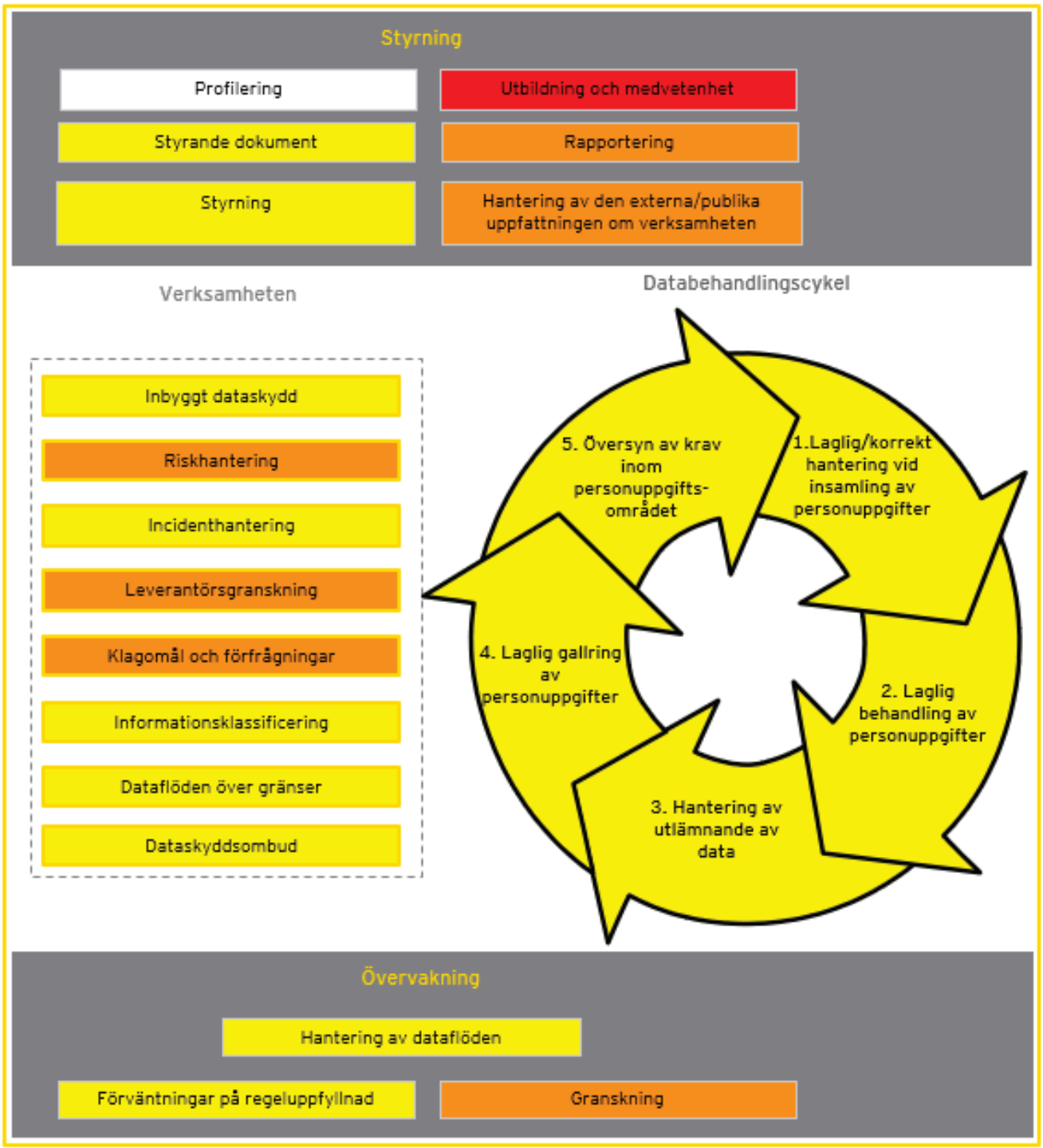


Nivå 5 representerar hög mognadsgrad medan nivå 1 representerar låg mognadsgrad.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Figur 9: 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.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

5.2. Nuläge och iakttagelser

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

Tabell 4: Observationer inom de 12 områdena

Område	Nuläge	Iakttagelser	Mognad
Styrande dokument/ styrning	Bolagen uppger att man följer kommunens koncerngemensamma styrdokument, och har därmed inte tagit fram en lokal informationssäkerhetspolicy som omfattar behandling av personuppgifter. Bolagen har dock etablerat en systemförvaltningsplan som granskas och revideras löpande men minst två gånger per år av förvaltningsorganisationen. Systemförvaltningsplanen omfattar riktlinjer kring flera av dataskyddsförordningens områden som informationsklassificering, risk- och sårbarhetsanalyser, laglig behandling av personuppgifter samt incidenthantering. Det finns ingen dokumenterad och etablerad rutin för att kontinuerligt följa upp hur arbetet med systemförvaltningsplanen går i praktiken.		3,00
Riskhantering	Bolagen utför årligen risk- samt sårbarhetsanalyser inom Bolagens IT-miljö samt IT-system i samband med en internkontroll. En etablerad metod används för att genomföra riskanalyser, och man använder metoden för att bedöma IT- och informationssäkerhetsrelaterade risker i Bolagen. Metoden täcker ibland in integritetsrisker men detta sker ad hoc och inte enligt en dokumenterad rutin.	Det saknas en dokumenterad rutin som säkerställer att integritetsrisker i bolagets verksamhet och IT-system analyseras kontinuerligt.	2,40
Kontroll	Bolagen har utsett ett dataskyddsombud (DSO) som är kontaktperson gentemot Integritetsskyddsmyndigheten. Det saknas i dagsläget en formell rutin för att bistå Integritetsskyddsmyndigheten med information. DSO genomförde på eget initiativ under januari 2021 en intern granskning av arbetet med personuppgifter inom bolagen, som rapporterades till bolagsledningen. Granskningen omfattade personuppgiftsincidenter, interninformation samt utbildningsbehov. Utöver denna rapport finns ingen fastslagen granskningsplan för att kontinuerligt utvärdera och säkerställa att man uppfyller relevanta krav på hantering av personuppgifter i bolagen.	Bolagen har ingen fastslagen granskningsplan eller internkontrollfunktion med fokus på att arbetet med personuppgifter är i enlighet med dataskyddsförordningens krav.	2,63

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Organisation och ansvar	Bolagen har tydligt definierade roller samt ansvar kopplade till arbetet med dataskydd och integritetsfrågor, samt påvisar generellt sett en god kunskap inom dataskyddsförordningen samt Integritetsskyddsmyndighetens befogenheter. Dataskyddsombudet (DSO) arbetar främst med andra uppgifter inom bolagen, men upplever sig ha tillräckligt med resurser för att kunna utföra de arbetsuppgifter som fastställts i dataskyddsförordningen. Verksamhetsutvecklaren arbetar för att ta fram lokala riktlinjer och dokument kring hanteringen av personuppgifter, men DSO är även till viss del involverad i detta. Detta arbete är dock relativt begränsat, och DSO har främst en rådgivande roll i bolagen.		3,46
Behandling av person-uppgifter	En registerförteckning har etablerats vars riktighet och tillgänglighet över tid kontinuerligt kontrolleras av bolagens dataskyddsombud. Det saknas en dokumenterad rutin för att över tid säkerställa att personuppgifter endast behandlas för de ändamål som de ursprungligen samlades in för. Bolagen har skapat lokala dokumenthanteringsplaner som även omfattar gallringsplaner. Det finns även dokumenterade instruktioner för hur gallring ska genomföras.	Det saknas rutiner som säkerställer att personuppgifter endast behandlas för de ändamål som de samlades in för.	3,21
Val av skydds-åtgärder	Bolagen har tagit fram en digital färdplan, där man dokumenterat sina IT-system samt kartlagt dataflöden och klassificerat personuppgifter som lagras i IT-systemen. Man höll vid införandet av dataskyddsförordningen i maj 2018 en obligatorisk utbildning inom dataskydd och integritetsfrågor för alla anställda. Det har inte skett några obligatoriska utbildningar sedan dess, men man distribuerar interna utbildningar inom dataskyddsförordningen via intranätet som man uppmanar anställda att ta del av. Då det inte finns några krav på de anställda att genomföra utbildningarna saknar man en process som säkerställer att anställda regelbundet tar del av utbildningarna.	En rutin för att säkerställa att samtlig ostrukturerad information blir klassificerad har inte implementerats. Bolagen har inte etablerat en process som säkerställer att alla anställda regelbundet tar del av internutbildningar om dataskyddsförordningen.	2,29

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Inbyggt dataskydd	Man har dokumenterade rutiner för behörighetshantering i känsliga IT-system. Årligen genomför man inom bolagen en kontroll av behörighetsstrukturer i system som behandlar personuppgifter för att säkerställa att exempelvis anställda som slutat har fått sitt användarkonto gallrat. Lagringsminimering sker enligt de befintliga gallringsrutinerna. Det saknas en dokumenterad rutin för att arbeta med uppgiftsminimering.	En formell rutin eller plan för lagrings- och uppgiftsminimering kan förtydligas i de fall som dokumenthanteringsplanen inte är tillämplig.	3,50
Hantering av leverantörs-relationer	Det finns ett dokumenterat register över alla leverantörer samt huruvida man har upprättat ett PUB-avtal med dem eller inte. Man uppger att man har upprättat PUB-avtal med sina största leverantörer, men att man i vissa fall saknar PUB-avtal med leverantörer. Man arbetar för att ta fram PUB-avtal med samtliga relevanta leverantörer. Bolagen saknar rutiner som regelbundet säkerställer att personuppgiftsbiträden hanterar personuppgifter i enlighet med dataskyddsförordningen. Man utför ingen granskning av arbetet med personuppgifter hos leverantörer eller underleverantörer. Bolagen har viss datalagring i tredje land, men har säkerställt att leverantörens skyddsnivå är tillräcklig då de arbetar i enlighet med dataskyddsförordningen.	Det saknas kompletta PUB-avtal för vissa leverantörer där det vore relevant. En rutin för att regelbundet säkerställa att personuppgiftsbiträden långsiktigt agerar i linje med dataskyddsförordningen saknas.	2,80
Hantering av incidenter	Det finns lokala rutiner för incidentrapporteringen inom bolagen. Alla incidenter relaterade till personuppgifter i bolagen dokumenteras i ett incidentsregister. Dataskyddsombudet är ansvarig för att rapportera incidenter till Integritetsskyddsmyndigheten inom 72 timmar om så är nödvändigt. Det saknas en dokumenterad rutin för att informera drabbade individer av en personuppgiftsincident. Två incidenter har hittills identifierats, och dataskyddsombudet var involverad vid båda dessa tillfällen. Det saknas etablerade rutiner som kontrollerar att de interna instruktionerna gällande incidentrapportering efterlevs.	En rutin för att granska efterlevnaden av instruktionerna gällande personuppgiftsincidenter saknas.	3,00

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Information till registrerade	Bolagen har en utförlig information över sin behandling av personuppgifter för registrerade på sin hemsida. Man har tagit fram en lokal mall för hur man ska informera registrerade om bolagens behandling av personuppgifter. Samtycke som laglig grund används i vissa fall för bolagens marknadssystem. Samtycket dokumenteras i systemet och den registrerade kan själv logga in och återkalla sitt samtycke via 'Mina sidor'. Bolagen har en kommunikationsansvarig som hanterar eventuell kommunikation med media. Det finns ingen dokumenterad rutin för hur man kommunicerar med de registrerade om förändringar i hur man hanterar deras personuppgifter.	Det saknas en process för hur man kommunicerar möjliga förändringar i hur man hanterar personuppgifter som berör registrerade.	3,19
Begäran från registrerade	Bolagen har dokumenterat en lokal rutin för att hantera en begäran från en registrerad. Rutinen säkerställer att man kontrollerar identiteten på den registrerade. Då man hittills inte har tagit emot en begäran om registerutdrag har man inte heller genomfört någon kvalitetskontroll av registerutdragen. Man har inte etablerat en rutin för att hantera förfrågningar gällande felaktiga, inte längre nödvändiga eller radering av personuppgifter. Det finns en tydlig kontaktväg för registrerade via bolagens hemsida, där man förutom generella kontaktuppgifter även uppger dataskyddsombudets kontaktuppgifter. Företaget har dessutom tagit fram en blankett som kan användas av de registrerade om de vill skicka in förfrågningar gällande felaktiga, inte längre nödvändiga, eller radering av personuppgifter.	Det saknas en rutin för hantering av förfrågningar gällande felaktiga, inte längre nödvändiga, eller radering av personuppgifter.	2,78
Profilering	Beslut som enbart grundar sig på automatiserad behandling av registrerade förekommer inte.	N/A	N/A

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

5.3. Övergripande rekommendationer

Iakttagelser av varierande vikt har identifierats inom flera delar av ramverket. EY har valt att presentera de mest relevanta övergripande rekommendationerna för Västervik Bostads AB samt Tjustfastigheter AB och förslag på åtgärder för de främsta riskerna inom dataskydds- och informationssäkerhetsarbetet. Rekommendationerna är rangordnade i prioritetsordning men EY rekommenderar att samtliga förslag åtgärdas inom 12 månader.

Granskning

Västervik Bostads AB samt Tjustfastigheter AB:s dataskyddsombud genomförde under året en intern granskning av arbetet med personuppgifter i organisationen. Bolagen rekommenderas att arbeta vidare med granskningar av detta slag, främst genom att implementera en granskningsplan för att kontinuerligt utvärdera och säkerställa att man uppfyller relevanta krav på hantering av personuppgifter. Genom att exempelvis integrera dataskyddsarbetet i den årliga internkontrollen som genomförs, skulle man även få en formell rutin för att dokumentera och rapportera resultatet till ledningsnivå. I slutfasen av revisionen har arbetet med att implementera en granskningsplan påbörjats. Bolagen rekommenderas därmed att fortsätta detta arbete och kontinuerligt analysera behov av granskning och uppföljning inom dataskydds- och informationssäkerhetsarbetet.

Utbildning

Västervik Bostads AB samt Tjustfastigheter AB har visat på goda ambitioner att sprida kunskap samt medvetenhet inom organisationen genom att uppmana anställda att ta del av de internutbildningar inom dataskyddsförordningen som finns på kommunens intranät. Då det inte har skett någon obligatorisk utbildning sedan införandet av dataskyddsförordningen 2018, rekommenderas bolagen att etablera en rutin för att kontinuerligt utbilda anställda inom integritetsfrågor samt kontrollera att alla anställda framgångsrikt slutför utbildningarna. Bolagen rekommenderas även att implementera rutiner för att kontinuerligt uppdatera utbildningsmaterialet. I slutfasen av revisionen har arbetet med att implementera en rutin för utbildning redan påbörjats. Bolagen rekommenderas därmed att fortsätta detta arbete och kontinuerligt analysera utbildningsbehov inom dataskydd- och informationssäkerhet.

Riskhantering

Västervik Bostads AB samt Tjustfastigheter AB rekommenderas att ta fram en rutin för att återkommande bedöma risker kopplade till sin personuppgiftshantering. I dagsläget används en metod för riskanalys kring informationssäkerhet, men bolagen rekommenderas att arbeta vidare med dessa och specifikt fokusera på att genomföra riskanalyser samt konsekvensbedömningar av deras personuppgiftshantering.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Revisionsfrågor

Revisionsfrågorna besvaras utifrån granskningen som helhet, det vill säga Västerviks kommuns kommunala verksamheter samt de helägda bolagen, i en sammanvägd bedömning. I de fall bedömningen i något väsentligt skiljer sig mellan de helägda bolagen och de kommunala verksamheterna noteras detta i förklaringen nedan. I den sammanlagda bilden har dessa skillnader dock inte ansetts kunna påverka den totala bedömningen då det övergripande och slutgiltiga ansvaret för efterlevnad av dataskyddsförordningen ligger på kommunstyrelsen.

Färgkod	Förklaring
	Revisionsfråga uppfylls ej
	Revisionsfråga uppfylls delvis
	Revisionsfråga uppfylls

Revisionsfråga	Svar	
Arbetar Västerviks kommun ändamålsenligt för att uppfylla de krav och regleringar för personuppgiftshantering som har införts i och med dataskyddsförordningen (GDPR)?	På en övergripande nivå anses Västerviks kommun delvis arbeta ändamålsenligt med dataskyddsförordningen. Genomgående uppvisar kommunen ambition och kunskap inom frågorna rörande dataskyddsförordningen. Det finns dock områden som bör förbättras innan arbetet kan beskrivas som ändamålsenligt, exempelvis relaterat till granskning, utbildning och styrning.	

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Är Västerviks kommuns policyer och riktlinjer ändamålsenliga för att uppnå regelefterlevnad med avseende på dataskyddsförordningen (GDPR)?	På en övergripande nivå anses Västerviks kommuns policyer och riktlinjer vara delvis ändamålsenliga. Flertalet relevanta policyer och riktlinjer finns redan på plats, och några är dessutom under utveckling i skrivande stund. Kommunen och bolagen jobbar i många frågor tillsammans för att etablera standardiserade rutiner i hela kommunen. Dock saknas det en central och uppdaterad informationssäkerhetspolicy som kommunens arbete med att ta fram riktlinjer och anvisningar för dataskyddsarbetet kan utgå från. Vidare saknas vissa relevanta riktlinjer, exempelvis relaterat till arbetet med granskning och utbildning.	
Har Västerviks kommun ändamålsenlig kontroll och uppföljning av arbetet med dataskyddsförordningen (GDPR)?	På en övergripande nivå anses Västerviks kommun ej arbeta ändamålsenligt med kontroll och uppföljning. Svaret grundas i att samtliga bolag samt kommunen ej arbetar strukturerat med att granska och kontrollera efterlevnaden av dataskyddsförordningen. Exempelvis har ingen granskningsplan skapats eller efterlevts i något av objekten. Vidare kan även arbetet med leverantörsuppföljning generellt förbättras. En begränsad uppföljning av informationssäkerhetsarbetet inom kommunen medför en risk att verksamheternas dagliga arbete skiljer sig från det sätt som kommunen anvisar samt tror att arbetet bedrivs på.	

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

6. Slutsatser

Granskningens syfte har varit att ge en övergripande förståelse för huruvida Västerviks kommun och dess helägda bolag bedriver ett ändamålsenligt arbete med dataskyddsförordningen (the General Data Protection Regulation, GDPR) och hur väl man uppfyller de åtgärder som förordningen stipulerar. I besvarandet av revisionsfrågorna bedöms Västerviks kommun och helägda bolag i relation till andra offentliga organisationer av liknande storlek och karaktär. Granskningen har resulterat i följande resultat:

- Västerviks kommuns nämnder genom kommunstyrelsen: 2,53 av 5,00

2,53 är en mognadsgrad strax under genomsnittet för vad EY generellt observerar i en offentlig verksamhet av liknande storlek och karaktär. Detta innebär att kommunen har en bit kvar att nå upp till en nivå som rekommenderas av EY, givet den stora mängd personuppgifter och känsliga personuppgifter som hanteras.

- Västervik Miljö & Energi AB & Västerviks Kraft-Elnät AB: 2,79 av 5,00

Mognadsgraden 2,79 är en genomsnittlig mognadsgrad jämfört med vad EY generellt observerar i en offentlig verksamhet av liknande storlek och karaktär. Det är dessutom en siffra i linje med vad EY anser kan förväntas av bolaget, givet den ringa mängd känsliga personuppgifter som hanteras.

- Västervik Resort AB: 2,19 av 5,00

2,19 är en mognadsgrad strax under genomsnittet för vad EY generellt observerar i en offentlig verksamhet av liknande storlek och karaktär. Detta innebär också att bolaget har en bit kvar för att nå upp till en nivå som rekommenderas av EY, givet den mängd personuppgifter som hanteras av bolaget.

- Västervik Bostads AB & Tjustfastigheter AB: 2,93 av 5,00

Mognadsgraden 2,93 är strax över genomsnittet för vad EY generellt observerar i en offentlig verksamhet av liknande storlek och karaktär. Det är en mognadsgrad som är något lägre än vad EY rekommenderar, givet den mängd personuppgifter som hanteras.

På en övergripande nivå rekommenderar EY att kommunen jobbar vidare med att etablera tydliga processer och riktlinjer kring hur arbetet med granskning och kontroll ska genomföras. Detta för att säkerställa att kommunen samt bolagen lever upp till relevanta krav inom personuppgiftshantering. Vidare rekommenderas det även att etablera en formell rutin för att dokumentera, samt kontinuerligt rapportera, resultatet av arbetet med personuppgifter. Slutligen rekommenderar EY även att kommunen jobbar vidare med utbildning och kunskapsspridning på en övergripande nivå. Detta genom att implementera utbildningsplaner med planlagda, och regelbundna, aktiviteter kopplade till dataskyddsförordningen.

Stockholm den 2021-08-10

Helena Törnqvist, Partner, EY

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

7. Bilaga 1: Förteckning över intervjuade funktioner

7.1. Västerviks kommun

- DSO för respektive nämnd
- Informationssäkerhetssamordnare
- Säkerhetschef
- IT-chef
- Samordnare för IT samt infrastruktur
- Kommunstyrelsens förvaltning
- Barn- och utbildningsförvaltning
- Socialförvaltning
- Miljö och byggnadsförvaltningen

7.2. Västervik Energi och Miljö AB samt Västervik Kraft-Elnät AB

- DSO
- Säkerhetschef

7.3. Västervik Resort AB

- DSO/Marknadschef

7.4. Västervik Bostads AB samt Tjustfastigheter AB

- VD
- Verksamhetsutvecklare
- DSO
- Ekonomichef
- IT-stöd
- Marknadsstöd

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

8. Bilaga 2: Dokumentförteckning

8.1. Västerviks kommun

- Säkerhetspolicy
- Riktlinjer till säkerhetspolicy
- Informationssäkerhetsinstruktioner Användare
- Informationssäkerhetsinstruktioner Utveckling, förvaltning drift
- Handlingsplan GDPR
- Rapport Nuläge dataskyddsförordningen Västerviks kommunkoncern 2019
- Personuppgiftsincidenter Västerviks kommun
- Västerviks kommun IT- och informationssäkerhetsgranskning april 2020
- Missiv granskning av IT- och informationssäkerhet
- Bilaga 1 Revision IT- och informationssäkerhet
- Beslut att utse dataskyddsombud – Miljö- och byggnadsförvaltningen
- GDPR presentation kontorsmöte – Miljö- och byggnadsförvaltningen
- Register över personuppgiftsbehandlingar – Miljö- och byggnadsförvaltningen
- Beslut att utse dataskyddsombud – Socialförvaltningen
- Register över personuppgiftsbehandlingar – Socialförvaltningen
- Beslut om att utse dataskyddsombud – kommunstyrelsen
- Beslut om att utse dataskyddsombud – valnämnden
- Beslut om att utse dataskyddsombud – överförmyndarnämnden
- Beslut om att utse dataskyddsombud – kommunens revisorer
- Mall – personuppgiftsbiträdesavtal svensk version
- Mall – personuppgiftsbiträdesavtal engelsk version
- Mall – samtyckesmall
- Mall – Återkalla samtycke
- Mall – information till den registrerade
- Blankett – begäran om registerutdrag enligt dataskyddsförordningen
- Blankett – begäran om rättigheter enligt dataskyddsförordningen
- Rutin – begäran om registerutdrag
- Process – hantera begäran om registerutdrag
- Utbildningsmaterial – Politikerutbildning 18 mars 2019 (utbildningen erbjöds till samtliga förtroendevalda politiker)
- Register över personuppgiftsbehandlingar - Kommunstyrelsen 2021-03-01
- Register över personuppgiftsbehandlingar - Valnämnden 2021-03-01
- Register över personuppgiftsbehandlingar - Överförmyndarnämnden 2021-03-01
- Register över personuppgiftsbehandlingar - kommunens revisorer 2021-03-01
- Beslut att utse dataskyddsombud – Barn- och utbildningsförvaltningen
- Datainspektionens mottagningsbekräftelse
- Principer och rättslig grund för personuppgiftsbehandling
- Flöde tillåten personuppgiftsbehandling
- GDPR – e-posthantering
- E-postkontakt med leverantörer – PuB
- Rättlig grund för personuppgiftsbehandling
- Folder GDPR skolor
- Bildpublicering och GDPR – samtycke bilder
- GDPR för förskolan
- GDPR för skola
- Folder GDPR för gymnasiet

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

- GDPR för gymnasiets personal
- Registerförteckning personuppgiftsbehandlingar – barn- och utbildningsförvaltningen
- 15 Nya dataskyddsförordningen
- Enkla grunder i dataskydd

8.2. Västervik Miljö och Energi AB samt Västerviks Kraft-Elnät AB

- Begäran om registerutdrag med personuppgifter (GDPR-instruktion) V.1 2019-03-19
- Hur skyddar vi personuppgifter och arbetar med integritetsskydd (GDPR-instruktion) V.3 2021-02-15
- Offentlighet och sekretess, utlämnande av allmän handling - Riktlinjer för Västervik Miljö & Energi AB V.6 2020-03-20
- Personuppgiftbiträdesavtal, s.k. PUB-avtal – hur gör vi (GDPR-instruktion) V.3 2021-01-26
- Så skyddar vi dina personuppgifter – ”skärmklipp” från www.vmeab.se
- Dokumenthanteringsplan för Västervik Miljö & Energi AB – Beslutad av bolagsstyrelsen 2019-01-23
- Dokumenthanteringsplan för Västerviks Kraft Elnät AB – Beslutad av bolagsstyrelsen 2019-01-23
- Informationssäkerhetspolicy för Västervik Miljö & Energi AB V.2 Fastställd av bolagsstyrelsen 2019-05-28 (tas upp för översyn av bolagsstyrelsen på möte 2021-02-22)
- Informationssäkerhetspolicy för Västerviks kommun 2011-08-01
- Säkerhetspolicy 2019–2022 för Västerviks kommunkoncern 2019-09-23
- Riktlinjer till säkerhetspolicy 2019–2022 för Västerviks kommunkoncern 2019-06-18
- Riktlinjer för säkerhetsarbetet i kommunkoncernen 2013-01-14
- Informationssäkerhetsinstruktion för användare inom Västerviks kommunkoncern 2013-12-20
- Informationssäkerhetspolicy – Västerviks Miljö & Energi AB 2021-02-22 ver 2
- Internkontrollplan 2020 - fastställd av bolagsstyrelsen 2019 – VMEAB
- Redovisning av internkontroll GDPR 2020 VMEAB - Arbetsmaterial inför styrelsemöte 2021-03-12
- Reglemente för intern kontroll med tillämpningsanvisningar.pdf

8.3. Västervik Resort AB

- GDPR
- Handlingsplan GDPR grund
- Hantering av GDPR_ISO
- Informationssäkerhet utveckling fortvaltning drift 2013
- Informationssäkerhetsinstruktioner Användare 2013
- INTEGRITETSPOLICY-VÄSTERVIK-RESORT-2021
- KPMGs rapport ang DSF 2020-09-25 Nybro kommun
- Rapportera en personuppgiftsincident
- Riktlinjer till säkerhetspolicy 2019–2022
- Rutin hantering av personuppgiftsincident 0.1
- Skylt gdpr info
- Säkerhetspolicy-2019-2022-kf190923
- Säkerställning av GDPR_ISO
- Särskilt formulär för dokumentation av personuppgiftsincident

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

- Tillägg integritetspolicy

8.4. Västerviks Bostads AB samt Tjustfastigheter AB

- 1.0 Systemförvaltningsorganisation Momentumfamiljen, Bostadsbolaget
- 2.0 Systemförvaltningsplan Momentumfamiljen, Bostadsbolaget
- 2.1 System- och aktivitetslista v 1.0 Momentumfamiljen, Bostadsbolaget
- Dataskyddsombud _ Mottagningsbekräftelse daterad 2018-06-27
- Gallringsplan Momentum PM & Marknadssystemet
- Gallringsrutin Personal
- Granskningsrapport
- Handlingsplan GDPR 2018-06-05
- Informationsmall behandling av personuppgifter_webb
- Informationssäkerhet utveckling forvaltning drift 2013
- Informationssäkerhetsinstruktioner Användare 2013
- Instruktion PUB-avtal
- Introduktion av nyanställd och vikarier
- Plan Byggservice
- Plan Direktion Bolagsledning
- Plan Drift
- Plan Marknad Ekonomi
- Plan Marknad
- Plan Personal Löner
- Plan Teknik-byggande
- Plan Uthyrning
- Rapport Nuläge dataskyddsförordningen Västerviks kommunkoncern hösten 2019
- Registerförteckning vbab
- Riktlinjer till säkerhetspolicy 2019-2022
- Rutin begäran av registerutdrag
- Rutin personuppgiftsincident
- Rutin System medarbetare slutar
- Sammanställning incidenter 2019-2021
- Säkerhetspolicy-2019-2022-kf190923
- Utdrag ur Digital färdplan Bostadsbolaget

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

9. Bilaga 3: 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.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

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.