Granskning av efterlevnad av
Dataskyddsförordningen GDPR
På uppdrag av de förtroendevalda revisorerna
Haninge Bostäder, Tornberget och
utbildningsförvaltningen

Haninge kommun

Granskning av efterlevnad Dataskyddsförordningen GDPR

Mars 2020

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

Sammanfattning

EY har på uppdrag av Haninge kommuns förtroendevalda revisorer genomfört en granskning av kommunens utbildningsförvaltning såväl som de kommunala bolagen Haninge Bostäder AB och Tornberget Fastighetsförvaltnings AB hantering av personuppgifter och efterlevnad av dataskyddsförordningen (The General Data Protection Regulation, GDPR).

Granskningens syfte har varit att ge en övergripande förståelse av huruvida utbildningsförvaltningens, Haninge Bostäder AB:s och Tornbergets Fastighetsförvaltnings AB:s bedriver ett ändamålsenligt arbete med dataskyddsförordningen och hur väl man uppfyller de åtgärder som förordningen stipulerar. Efterlevnaden av dataskyddsförordningen och mognadsgraden har granskats och bedömts enskilt för de tre objekten. Analysen har baserats på intervjuer med identifierade nyckelpersoner i respektive verksamhets personuppgiftssäkerhetsarbete samt genomgång av insamlad styrdokumentation. Analys och iakttagelser har faktagranskats av förvaltningen samt de kommunala bolagen.

En översiktlig granskning av 12 olika områden med utgång i EY:s ramverk för personuppgiftshantering gentemot dataskyddsförordningen för kommunala verksamheter har genomförts under februari till mars 2020. Enligt metoden bedöms de enskilt granskade verksamheternas mognadsgrad enligt 116 punkter på en ordinarie skala från 1 (*begynnande*) till 5 (*optimerad*) inom de respektive 12 områdena. Den genomsnittliga mognadsgraden är baserat på snittet av mognadsgraden för de respektive 12 områdena.

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

- Haninge Bostäder: 2,25 av 5,00
  2,25 är en förhållandevis låg mognadsgrad för ett bostadsbolag, givet bolagets storlek och förhållandevis stora mängd personuppgifter.
- Tornberget: 2,59 av 5,00
  Mognadsgraden 2,59 är i stort i linje med vad som kan förväntas av ett litet fastighetsbolag med få personuppgifter.
- Utbilningsförvaltningen:2,62 av 5,00
  2,62 är en genomsnittlig mognadsgrad för en kommunal förvaltning. Detta innebär dock att man har en bit kvar för att nå upp till en nivå som rekommenderas av EY, givet den stora mängd personuppgifter och känsliga personuppgifter som hanteras inom förvaltningen.

Slutsatserna skiljer sig trots liknade nivå i mognadsgrad då verksamheterna och mängden behandlade personuppgifter skiljer sig åt. Därmed har de granskade enheterna olika riskbilder och således skiljer sig förväntningen på vilken mognadsgrad som kan anses vara tillräckligt bra.

Överlag bedöms mognadsgraden för de tre enskilda verksamheterna vara högst inom organisation och ansvar då man har ett gemensamt dataskyddsombud och liknande ansvarsstruktur. Information till registrerade hade även en relativt hög mognadsgrad i alla verksamheter. Samtliga har en låg mognadsgrad inom kontroll då en fastställd granskningsplan från ledningsnivå inte funnits på plats förrän i februari 2020. DSO har tagit

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

fram ett årshjul för granskning som innefattar samtliga av kommunens verksamheter. Vidare bedömdes alla objekt ha relativt låga mognadsgrader inom riskhantering, val av skyddsåtgärder och leverantörsrelationer.

Det är tydligt att förvaltningen och bolagen lagt ner ett ambitiöst arbete och engagemang för personuppgiftsfrågor och dataskyddsförordningen. Nyckelpersonerna i respektive verksamhet har arbetat målinriktat med att framta rutiner och visar på en medvetenhet kring sin personuppgiftshantering.

De viktigaste gemensamma förbättringspunkterna ligger i att utvärdera om man uppfyller relevanta krav på hantering av personlig information inom samtliga undersökta områden enligt en strukturerad modell för riskanalys. De granskade verksamheterna bör arbeta proaktivt med riskhantering och upprätta rutiner för granskning av efterlevnad. Syftet är att minska risker för ogiltig behandling av personuppgifter såväl som integritetsincidenter inom sin verksamhet såväl som hos leverantörer. Det saknas kontaktväg och rutiner för de granskade verksamheterna att rapportera identifierade brister och åtgärdsförslag inom sitt dataskyddsarbete.

EY rekommenderar kommunstyrelsen att skapa ett rapporteringskrav, med fastställd frekvens och innehåll som kommunala verksamheter kan utgå från, för att säkerställa att uppföljning och granskning av dataskyddsförordningen sker och dokumenteras i samtliga enheter.

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

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

Den nya 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 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 Haninge kommun med dess verksamheter hanterar stora mängder personuppgifter, har de förtroendevalda revisorerna beslutat att genomföra en granskning av efterlevnaden av dataskyddsförordningen i de kommunägda fastighets- och bostadsbolagen, Tornberget och Haninge Bostäder, och i utbildningsförvaltningen.

1.2. Syfte

Syftet med granskningen är att ge en övergripande förståelse av huruvida utbildningsförvaltningen, Haninge Bostäder och Tornberget bedriver ett ändamålsenligt arbete med dataskyddsförordningen och hur deras mognadsgrad ser ut i uppfyllelse av de åtgärder som förordningen stipulerar.

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

1.3. 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 policys. Granskningen är begränsad till arbetet som utbildningsförvaltningen, Haninge Bostäder och Tornberget bedriver och inga andra nämnder, förvaltningar eller kommunalägda bolag har således granskats. 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 den utvalda förvaltningen och bolagens informationssäkerhetsarbete samt genomgång av relevant styrdokumentation (se Avsnitt 7 Bilaga 2: *Dokumentförteckning*). Granskningen är utförd i enlighet med 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.

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

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

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 ett område med grön färgkod exempelvis ändå sakna viktiga kontroller. Granskningens huvudsakliga värde ligger i dess observationer och rekommendationer som beskrivs i en bredare kontext nedan i granskningsrapporten.

Inledningsvis har underlag såsom policyer, strategi- och styrdokument och dylikt samlats in för analys. Därefter höll EYs GDPR-specialister ett arbetsmöte med nyckelpersoner inom respektive granskad verksamhets informationssäkerhetsarbete (se Avsnitt 6 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:

- Januari 2020 – Förberedelser, planering och insamling av dokumentation.
- Februari 2020 – Dokumentanalys, utförande av arbetsmöten (2020-02-03, 2020-02-04 och 2020-02-06), granskning av kompletterande dokumentation och uppföljningsfrågor, färdigställande av rapport, samt faktagranskning av intervjuade nyckelpersoner.
- Mars 2020 – Kvalitetssäkring av EY:s verksamhetsrevisorer och slutgiltig presentation för kommunens förtroendevalda revisorer.

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. Haninge Bostäder AB

Baserat på utförd granskning konstateras att Haninge Bostäder AB, hädanefter benämnt Haninge Bostäder, har en förhållandevis låg mognadsgrad inom personuppgiftshantering, jämfört med vad som kan förväntas av en offentlig verksamhet av motsvarande storlek och karaktär. Som kommunalt bostadsbolag hanterar bolaget relativt stora mängder personuppgifter för såväl hyresgäster som bostadssökande.

De ansvariga inom bolaget har arbetat ambitiöst med dessa frågor och visar intresse och engagemang för dataskyddsfrågorna. Tack vare detta har man nått en bra bit på vägen mot ett effektivt arbete med dataskydd och integritet. Nedan redovisas de områden som behöver förbättras för att öka Haninge Bostäders mognadsgrad.

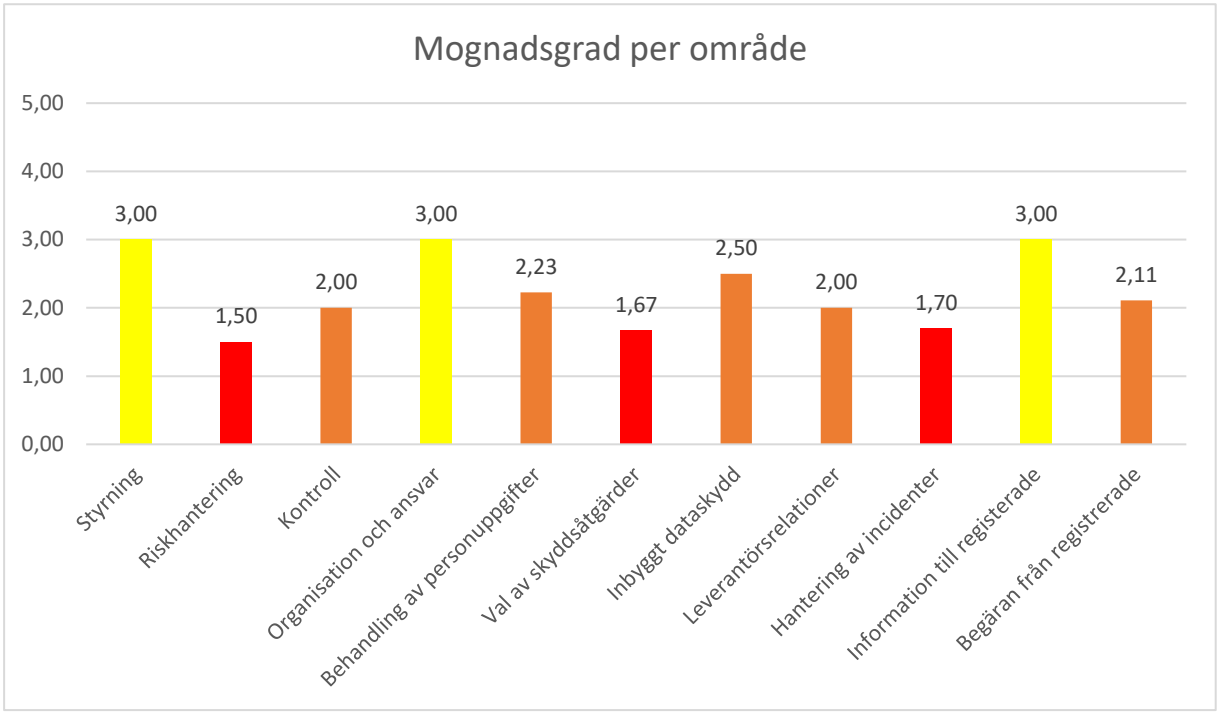
Införandet av dataskyddsförordningen drev digitaliseringen av Haninge Bostäder då man i samband med detta anskaffade ett nytt fastighetssystem för att stärka sin kontroll av informationssäkerhet. Bolaget har däremot inte gjort en strukturerad och dokumenterad analys för att utvärdera om det finns områden där man inte fullt efterlever kraven i dataskyddsförordningen. Den befintliga metoden för riskanalyser är inte utformad för att bedöma personuppgiftsrisker och dess konsekvenser ur en integritetssynpunkt. Haninge Bostäder har i dagsläget ingen fastslagen granskningsplan eller internkontrollfunktion med fokus på att bolagets dataskyddsarbete är i enlighet med dataskyddsförordningens krav. En granskningsplan för 2020 har framtagits av dataskyddsombudet (DSO) för samtliga nämnder, förvaltningar och kommunala bolag. Bolaget har ingen metod för att klassificera strukturerad såväl som ostrukturerad information som underlag till att välja och implementera lämpliga skyddsåtgärder för den information som hanteras. Därtill utförs ingen granskning eller uppföljning av att personuppgiftsbiträden agerar enligt dataskyddsförordningens krav över tid. Personuppgiftsbiträdesavtal har däremot granskats av DSO. Vidare saknas väldokumenterade rutiner för hur man ska bedöma och hantera personuppgiftsincidenter såväl som begäran från registrerade.

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

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

Figur 1: Mognadsgrad per område

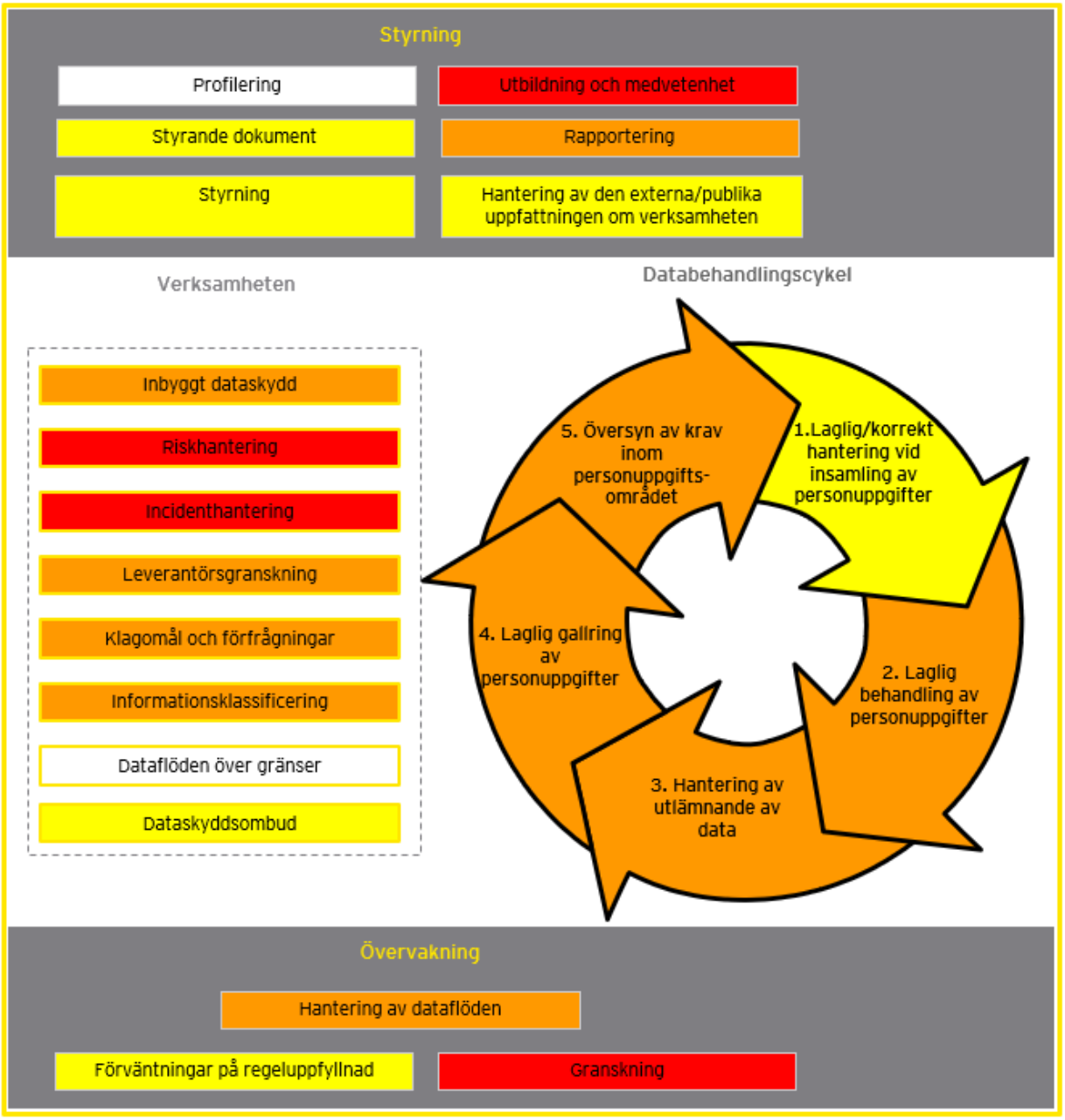


Nivå 5 representerar hög mognadsgrad medan nivå 1 representerar låg mognadsgrad.

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



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

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

2.1. Nuläge och iakttagelser

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

Tabell 1: Observationer inom de 12 områdena

Område	Nuläge	Iakttagelser	Mognad
Styrande dokument/ styrning	Haninge Bostäder anger själva att de inte är bundna att följa alla styrdokument från Haninge kommun men följer i stort de dokument som fastslagits av kommunfullmäktige. Baserat på dessa har bolaget har tagit fram egna styrdokument som beslutats av ledningsgruppen. Bolaget har ett par riktlinjer kopplat till informationssäkerhet och IT men saknar en fastställd informationssäkerhetspolicy. Bolaget anskaffade ett nytt fastighetssystem i samband med införandet av dataskyddsförordningen. I detta stadie gjordes en ostrukturerad analys av områden där man inte levde upp till förordningens krav, varav flertalet områden har lösts allteftersom i samverkan med DSO. En kartläggning av alla affärskritiska processer som innefattar rutinbeskrivningar och hur man förhåller sig till dataskyddsförordningen är i planeringsstadiet. Samtliga anställda genomgick en utbildning inom dataskyddsförordningen i samband med att lagstiftningen trädde i kraft. Utbildningsmaterial finns tillgängligt på bolagets intranät som alla nyanställda går igenom under deras introduktion. DSO har gjort bedömningen att ingen ytterligare utbildningsinsats är nödvändig i dagsläget.	Bolaget saknar en fastställd informationssäkerhetspolicy. Vidare saknar bolaget lokala riktlinjer beträffande hanteringen av personuppgifter för samtliga affärskritiska processer. Haninge Bostäder har inte genomfört en analys enligt en särskild process eller ramverk för att identifiera områden där man inte lever upp till förordningens krav. Därtill saknas uppföljning av analysen samt en åtgärdsplan som innehåller en tidsplan och ansvarsfördelning för att åtgärda de eventuella områden som återstår.	3,0

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	Bolaget använder ett riskhanteringsdokument för att genomföra sina riskanalyser som uppdateras regelbundet. Dessa görs för ekonomi-styrda risker kopplade till finansiering av diverse projekt. Metoden används inte för att bedöma informationsrisker som kan finnas i samband med att verksamheten hanterar personuppgifter. Det framgår däremot att bolaget har en medvetenhet om risker kopplade till personuppgifter och att man har dessa i åtanke. Under våren 2018 arbetade bolaget med en konsult för att se till att man uppfyllde de mest väsentliga kraven som dataskyddsförordningen stipulerar. Hittills har man inte sett något behov att genomföra strukturerad konsekvensbedömning för befintlig behandling av personuppgifter genomförts. Bolaget har beställt en konsekvensanalys av det nya fastighetssystemet som anskaffades vid implementationen av dataskyddsförordningen.	Riskanalyser utförs inte vid återkommande intervaller för integritetsrisker i bolagets verksamhet och IT-system. Det saknas metod och ansvar för att genomföra konsekvensbedömningar innan verksamheten startar en ny typ av behandling.	1,5

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	Kommunens gemensamma DSO är sedan våren 2018 utsedd kontaktperson gentemot Datainspektionen för att svara på eventuella förfrågningar och för att rapportera personuppgiftsincidenter. Det finns inte en väldefinierad eller väldokumenterad process för incidenthantering. Bolagets dataskyddssamordnare har frekvent kontakt med DSO. På samordnaren initiativ har bolaget halvårsavstämningar med DSO för att diskutera eventuella brister som identifieras i verksamheten och aktiviteter för att åtgärda bristerna. DSO har på eget initiativ tagit fram en enskild årsrapport för varje nämnd, förvaltning och bolags dataskyddsarbete som sammanfattar årets framsteg och kommande års fokusområden. DSO granskar personuppgiftsbiträdesavtalen i denna rapport men utöver detta är rapporten av sammanfattande snarare än granskande karaktär. Utöver denna rapport finns ingen fastslagen granskningsplan (exempelvis en revisionsplan) för att utvärdera och säkerställa att man uppfyller relevanta krav på hantering av personlig information. Detta kommer däremot att implementeras för 2020.	Haninge Bostäder har hittills ingen fastslagen granskningsplan eller internkontrollfunktion med fokus på att dataskyddsarbetet är i enlighet med dataskyddsförordningens krav utöver att granska personuppgiftsbiträdesavtalen.	2,0

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	Bolaget har utsett en dataskyddssamordnare samt antagit kommunens DSO. Båda har tydligt definierade roller och ansvar kopplat till bolagets arbete med dataskydd och informationssäkerhet. Dataskyddsombudet rekryterades våren 2018. DSO är i grunden jurist och har tidigare arbetat med dataskydd på en myndighet. DSO har ett kommunövergripande ansvar och upplever sig ha tillräckligt med stöd, sakkunskap och självständighet för att kunna utföra de uppgifter som fastställts i dataskyddsförordningen. DSO gör årsrapport om varje nämnd, förvaltning och bolags status med sitt arbete utefter dataskyddsförordningen. Dock saknas det saknas en etablerad rapporteringsväg både från DSO till bolagsstyrelsen.	Bolaget saknar rutiner för att rapportera till styrelse/nämnd om status för dataskyddsarbetet. En formell väg eller rutin för rapportering från DSO till styrelse/nämnd och krav som sådan rapportering ska utgå ifrån har inte förankrats.	3,0
Behandling av person-uppgifter	Bolaget behandlar främst personuppgifter på avtalsgrund men använder aktivt samtycke för registrering i sin bostadskö. Bolaget behandlar en liten mängd känsliga personuppgifter kopplade till funktionsnedsättning och skyddad identitet bland sina hyresgäster. En rutin för att avpersonifiera personuppgifter för de med skyddad identitet finns. En kartläggning av bolagets behandlingsprocesser av personuppgifter har genomförts, varav en registerförteckning har skapats i Draft-it. Denna uppdateras regelbundet av Dataskyddssamordnaren och granskas årligen av DSO. Bolaget har en fastställd gallringsplan och anonymiserar samt raderar personuppgifter utefter denna tidsplan i forum, bostadskö och kontrakt som utgått. En rutin för att säkerställa att personuppgifter endast lagras inom de tidsramar som gäller givet det angivna ändamålet med behandlingen saknas.	Det saknas 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.	2,23

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	Haninge Bostäder har definierat och dokumenterat vad som menas med ”personuppgifter” och ”känsliga personuppgifter” i sin verksamhet. Däremot genomför bolaget ingen klassificering av strukturerad information på ett sådant sätt att informationen hanteras i enlighet med de krav som dataskyddsförordningen ställer. Likväl utför bolaget ingen klassificering av ostrukturerad data utöver att sekretessklassa viss dokumentation enligt offentlighets- och sekretesslagen. Bolaget gjorde en utbildningsinsats inom dataskydd och integritetsfrågor våren 2018 för alla anställda. Utbildningsmaterialet är inkluderat i introduktionen för alla nyanställda. En regelbunden uppföljning eller uppdatering av utbildningen genomförs inte.	En metod och rutin för att genomföra klassificering av strukturerad såväl som ostrukturerad information och dokumentation saknas. Bolaget har inte etablerat en process som säkerställer att internutbildningar om dataskyddsförordningen uppdateras och genomförs regelbundet av befintliga anställda.	1,67
Inbyggt dataskydd	Verksamheten har genomfört åtgärder (både tekniska och organisatoriska) för att öka säkerheten i sin databehandling. Exempelvis anskaffades ett nytt fastighetssystem våren 2018 för att öka bolagets dataskydd. Fastän ingen strukturerad konsekvensanalys avseende integritetshantering/personuppgifter finns dokumenterad framgår det att bolaget haft dataskydd i åtanke när systemet anskaffades. Lagring- och uppgiftsminimering för befintliga system sker informellt enligt dialog inom säkerhetsteamet och utöver detta enligt dokumenthanteringsplanen. Haninge Bostäder arbetar enligt principen att individer ska ha så lite behörighet som möjligt i sina system. Endast de som behöver tillgång till personuppgifter för att utföra sina arbetsuppgifter ska få ta del av dessa i diverse system. Bolaget utför däremot inga interna kontroller, tester eller uppföljning av sina behörighetsstrukturer.	En formell rutin eller plan för lagrings- och uppgiftsminimering kan förtydligas i de fall dokumenthanteringsplanen inte är tillämplig. Det saknas periodiska granskningar av behörigheter i IT-system.	2,5

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	Haninge Bostäder har flertalet IT-system som behandlar personuppgifter och som tillhandahålls av en extern leverantör i Draft-it. Bolaget har personuppgiftsbiträdesavtal med flertalet leverantörer. Upprättande av personuppgiftsbiträdesavtal som komplement till leverantörskontrakt har upprättats för nya upphandlingar såväl som för befintliga leverantörer. Alla leverantörsavtal samt personuppgiftsavtalen sparas på bolagets server. Uppföljning och kontroll kring hur information behandlas och förvaras i praktiken hos leverantörer saknas. Bolaget har kännedom om vilka personuppgifter som utlämnats till leverantörer genom en registerförteckning i Draft-it. Entreprenörer tilldelas ärenden i en app där får de kontaktuppgifter de behöver för att utföra sitt ärende skickade. Systemleverantörerna har inte tillgång till informationen i bolagets fastighetssystem.	Personuppgiftsbiträdesavtal finns inte med alla externa leverantörer. Det saknas en egen rutin som regelbundet säkerställer att personuppgiftsbiträden långsiktigt agerar i linje med dataskyddsförordningen, varken i upphandlingsfasen eller senare. Det saknas en dokumenterad arbetsmetod som kontrollerar att Personuppgiftsbiträdesavtal uppdateras vid legala eller interna förändringar.	2,0
Hantering av incidenter	Bolaget saknar väldefinierad process för att identifiera, bedöma, följa upp, rapportera eller kommunicera personuppgiftsincidenter då inga incidenter hittills identifierats. Om en incident rapporteras kommer Dataskyddssamordnaren kontakta DSO för vägledning. DSO är ansvarig för att kontakta Datainspektionen inom 72 timmar om nödvändigt.	Haninge Bostäder saknar en tydligt definierad process eller rutin för att identifiera, rapportera, bedöma, avhjälpa och (där så är lämpligt) rapportera integritetsincidenter.	1,70

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	Haninge Bostäder har en dokumenterad rutin för hur registrerade ska informeras kring deras personuppgifter. De hänvisar framför allt till hemsidan där det finns utförlig information. Bolaget använder samtycke endast för sin bostadskö. När samtycke krävs, används formulär vars utformning förutsätter att individernas samtycke bygger på en aktiv handling och är distinkt, tydligt och inte ihopblandat med andra samtycken. Det saknas dokumenterad process för hur verksamheten kommunicerar med de registrerade vid personuppgiftsincidenter eller förändring av bolagets hantering av personuppgifter.	Det saknas en process för hur bolaget kommunicerar möjliga förändringar i hur man hanterar personuppgifter eller incidenter som berör registrerade.	3,0
Begäran från registrerade	Bolaget har en tydlig kontaktväg där registrerade kan framföra förfrågningar och klagomål via sin hemsida. Legitimation uppvisas på plats hos Haninge Bostäder för att få en utskriven kopia av de personuppgifter som bolaget har registrerade. Alternativt kan registret skickas till den begärdas folkbokföringsadress. Bolaget har möjlighet att skriva ut registret i ett maskinläsbart format men ett säkert system där en användare kan ta del av sina personuppgifter finns inte. Det finns inga fastställda rutiner för hantering av förfrågningar gällande felaktiga, inte längre behövande, eller radering av personuppgifter. Vidare har bolaget inte inventerat möjligheten att radera personuppgifter i de system där detta är tillämpligt om en giltig begäran om ”rätten att bli bortglömd” inkommer.	Det finns ingen fastställd rutin för hantering av förfrågningar gällande felaktiga, inte längre behövande, eller radering av personuppgifter. En tydlig ansvarsfördelning och process för att avgöra om en registrerads begäran är ogrundad finns inte dokumenterad.	2,11
Profilering	Haninge bostäder har inget behov av att utföra profilering då automatiserad behandling inte används inom bolaget.	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

2.2. Övergripande rekommendationer

Då flertalet iakttagelser har identifierats inom olika delar av ramverket, har EY valt att presentera sju övergripande rekommendationer och förslag på åtgärder för de främsta riskerna inom bolagets dataskydd och informationssäkerhetsarbete.

Granskning och rapportering

Begränsad uppföljning av bolagets informationssäkerhetsarbete medför risk att dess dagliga informationshantering avviker från sättet som dess rutiner anvisar och man tror att arbetet bedrivs på. Haninge Bostäder rekommenderas därför att implementera en granskningsplan för att utvärdera och säkerställa att man uppfyller relevanta krav på hantering av personlig information samt en formell rutin för att dokumentera och rapportera resultat till ledningsnivå. Kontroller av Haninge Bostäders dataskyddsarbete kan exempelvis integreras i bolagets internkontrollarbete. Kommunstyrelsen rekommenderas även att fastställa ett rapporteringskrav gällande frekvens och innehåll som rapporteringen till styrelse ska utgå från för att säkerställa att uppföljning av dataskyddsförordningen utförs och kommuniceras.

Hantering av leverantörsrelationer

Haninge Bostäder rekommenderas att göra en inventering av samtliga IT-system och tjänster som behandlar personuppgifter och som tillhandahålls till leverantörer. Denna kartläggning kan användas som grund för bolagets arbete med att ingå personuppgiftsbiträdesavtal med externa leverantörer. Bolaget kan exempelvis använda en mall för personuppgiftsbiträdesavtal såsom SKR:s mall och checklista vid upprättandet av personbiträdesavtalen för att kvalitetssäkra att avtalsmallen innehåller relevanta avtalspunkter och krav utifrån dataskyddsförordningen. En sådan checklista kan även användas som underlag till en regelbunden granskning av att personuppgiftsbiträden agerar enligt personuppgiftsbiträdesavtal och förordningens krav, vilket är en rutin som bör fastställas.

Utbildning

Brist på aktiv kommunikation av policys, anvisningar och instruktioner gällande informationssäkerhet medför risk för att bolagets användare besitter otillräcklig kunskap för att på daglig basis hantera bolagets information på ett ändamålsenligt och säkert sätt. EY rekommenderar därför att bolaget tillser att informationssäkerhetsrelaterad dokumentation kommuniceras aktivt till bolagets medarbetare med en bestämd frekvens genom att införa vidareutbildning inom informationssäkerhet och dataskydd. Dessa utbildningar bör regelbundet uppdateras för att säkerställa att nya krav och förhållningssätt kommuniceras till bolagets medarbetare.

Val av skyddsåtgärder

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

Bolaget rekommenderas att genomföra klassificering av strukturerad såväl som ostrukturerad information avseende alla personuppgifter som verksamheten hanterar för att försäkra att information hanteras i enlighet med de krav som dataskyddsförordningen ställer. EY rekommenderar att bolaget använder en metod som exempelvis SKR:s KLASSA för att värdera informationen i verksamhetssystem och ta fram handlingsplaner som identifierar en del av de åtgärder som behöver vidtas för att skydda information.

Inbyggt dataskydd

Haninge Bostäder har behörighetsbegräsningar i sina verksamhetssystem där tilldelning av behörigheter sköts enligt principen att personer bör ha så få rättigheter som möjligt. För att försäkra sig om att inga användare kommer åt information de inte bör ha tillgång till efter avslutad tjänst eller förändrad arbetsroll, rekommenderas bolaget att fastställa en rutin för periodisk granskning av framför allt högre behörigheter i känsliga verksamhetssystem.

Riskhantering

Riskhantering syftar till att utvärdera hur verksamheten identifierar och minskar integritetsrisker i sin verksamhet och i sina IT-system. Bolaget rekommenderas att ta fram en metod och rutin för att bedöma risker kopplade till sin personuppgiftshantering vid återkommande intervaller. Utformningen av informationsskydd för respektive integritetsrisk bör baseras på resultatet från denna analys. I dagsläget saknar bolaget rutiner samt en ansvarsfördelning som säkerställer att konsekvensbedömningar utförs och att man söker råd från Datainspektionen i de fallen där bedömningar visar höga risker ur integritetssynpunkten. EY rekommenderar att konsekvensbedömning görs vid regelbundna intervaller för att säkerställa att man minimerar nya eller förändrade risker.

Incidenthantering

Bolaget rekommenderas att ta fram en väldefinierad process för att identifiera, följa upp, rapportera eller kommunicera personuppgiftsincidenter. Exempelvis kan bolaget upprätta ett internt register över personuppgiftsincidenter som även innehåller en checklista över alla steg och krav man behöver följa enligt dataskyddsförordningen.

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. Tornberget Fastighetsförvaltnings AB

Baserat på utförd granskning konstateras att Tornberget Fastighetsförvaltnings AB, hädanefter benämnt Tornberget, har en mognadsgrad inom personuppgiftshantering som i stort är i linje med vad som kan förväntas av en offentlig verksamhet av motsvarande storlek och karaktär, då bolaget hanterar en liten mängd personuppgifter. Bolaget har färre än tio hyresrätter som hyrs ut till privatpersoner, varför majoriteten av bolagets personuppgifter rör deras egen personal.

De ansvariga inom bolaget har arbetat ambitiöst med dessa frågor och visar intresse och engagemang för dataskyddsfrågorna. Tack vare detta har man nått en bra bit på vägen mot ett effektivt arbete med dataskydd och integritet. Nedan redovisas de områden som behöver förbättras för att öka Tornbergets mognadsgrad.

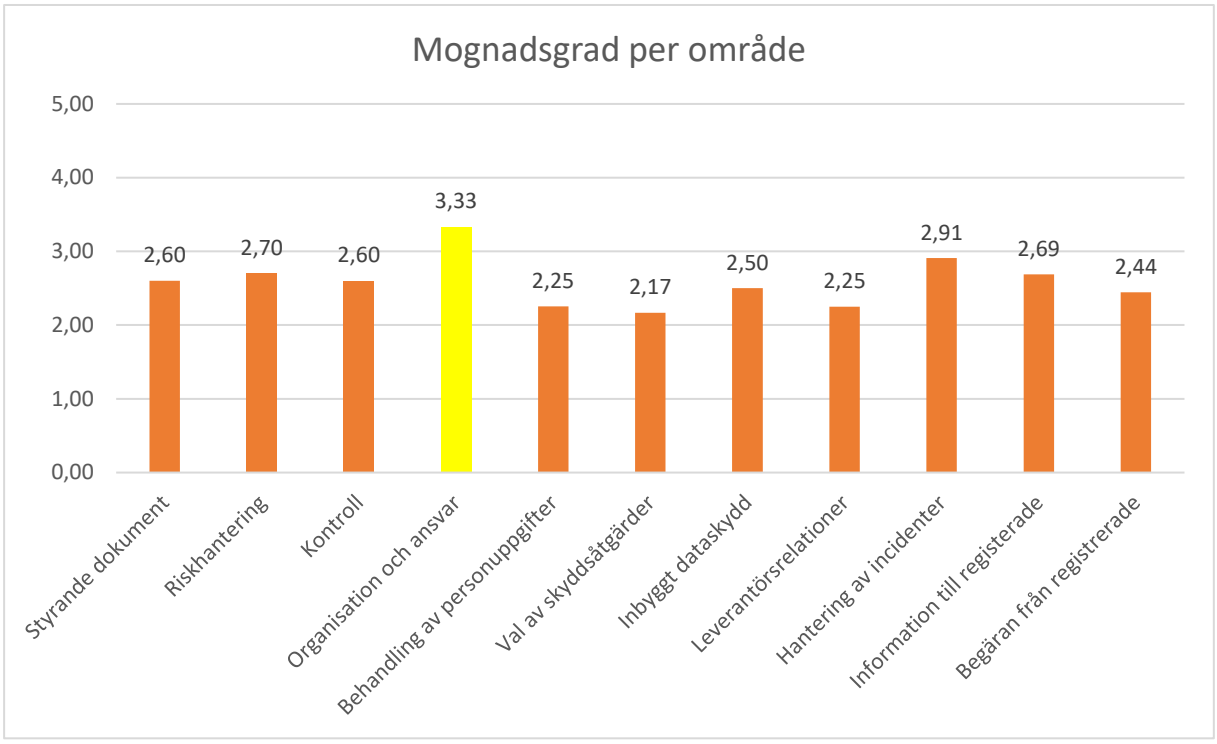
Bolaget rekommenderas bland annat att utföra en strukturerad och dokumenterad analys för att utvärdera om det finns områden inom dataskyddsförordningen där man inte fullt efterlever kraven. Informationsklassificering genomförs inte i dagsläget, dock har en projektgrupp tilldelats uppgiften att framöver klassificera strukturerad information men nyckelpersonerna i bolagets dataskyddsarbete har inte försäkrat sig om att detta projekt kommer genomföras. Bolaget bör även klassificera ostrukturerad information och implementera lämpliga skyddsåtgärder för att skydda den information som hanteras. Det har hittills saknats en fastslagen granskningsplan eller internkontrollfunktion med fokus på att bolagets dataskyddsarbete och behandling av personuppgifter är i enlighet med dataskyddsförordningens krav. En granskningsplan som innefattar Tornberget har framtagits för 2020 av DSO. Tornberget utför inte heller någon granskning eller uppföljning av att personuppgiftsbiträden agerar enligt dataskyddsförordningens krav över tid.

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

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

Figur 3: Mognadsgrad per område

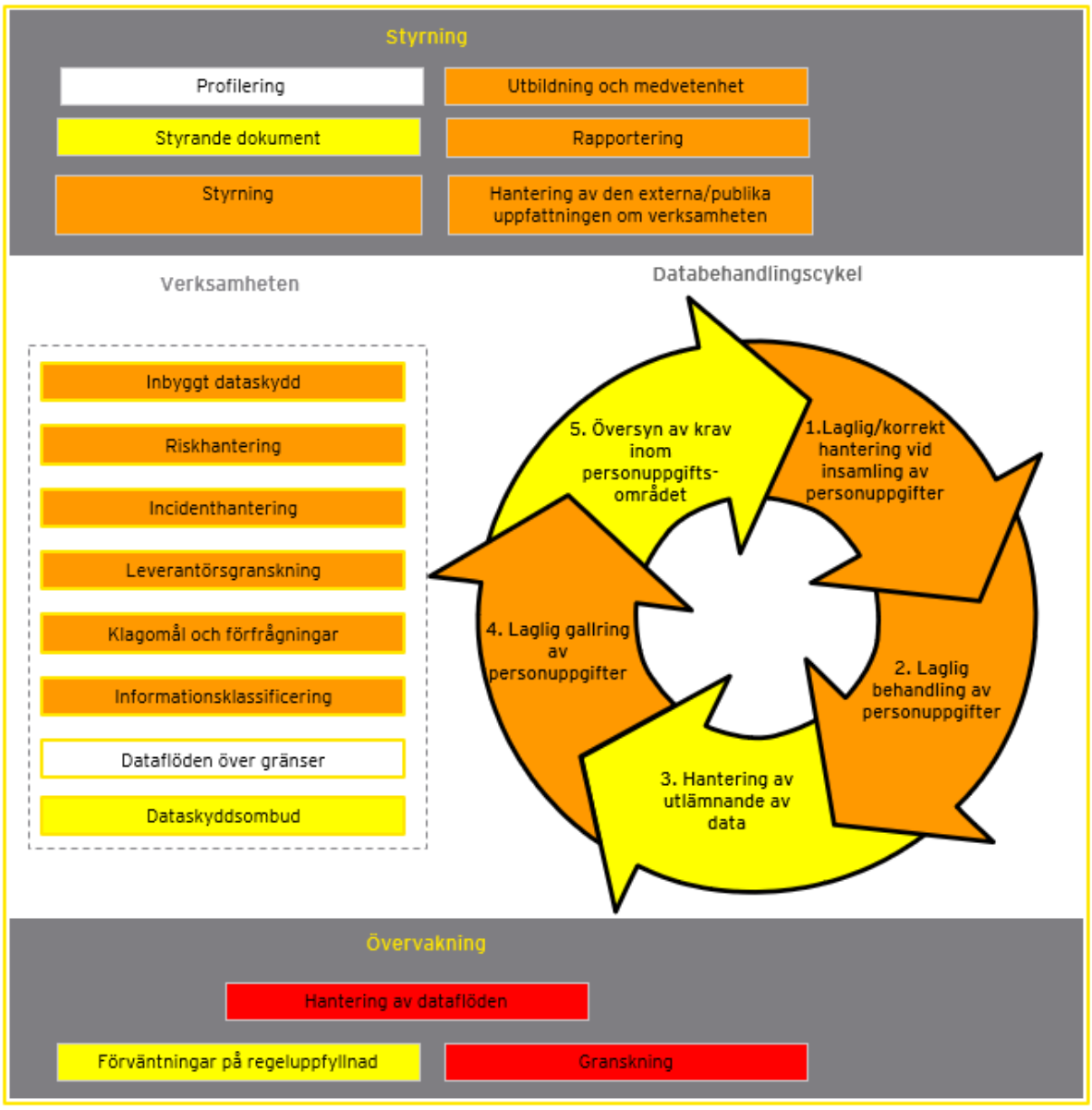


Nivå 5 representerar hög mognadsgrad medan nivå 1 representerar låg mognadsgrad.

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 4: 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

3.1. 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	Tornberget har framtagit flertalet riktlinjer för hur man ska förhålla sig till personuppgiftshantering både internt och externt. Dessa ses över regelbundet genom internrevisioner. Tornberget ska följa Haninge kommuns informationssäkerhetspolicy som inte är uppdaterad utefter dataskyddsförordningen. Bolaget har inte genomfört en analys för att utvärdera om det finns områden inom Dataskyddsförordningen där man inte fullt ut efterlever regelverket. Vid införandet av dataskyddsförordningen utbildades all personal om regelverket. Alla nyanställda ska läsa igenom utbildningsmaterialet och den närmsta chefen har ansvar för att kontrollera att detta fullföljs. Ingen vidareutbildning eller uppföljning av de anställdas kunskap inom dataskyddsförordningen har utförts därefter.	Bolaget saknar en uppdaterad informationssäkerhetspolicy. Vidare saknar bolaget styrdokument beträffande hanteringen av personuppgifter. Tornberget har inte genomfört en strukturerad analys enligt en särskild process eller ramverk. Därtill saknas uppföljning av analysen samt åtgärdsplan med tidsplan och ansvarsfördelning för att åtgärda de eventuella områden som återstår. Bolaget har inte etablerat en process som säkerställer att internutbildningar om dataskyddsförordningen uppdateras och genomförs regelbundet av nyanställda såväl som av befintliga anställda.	2,60
Riskhantering	Tornberget har framtagit en rutin och riktlinjer för hur en riskanalys och konsekvensbedömning ska utföras och bedömas. Baserat på denna analys bestäms en åtgärd för att skydda informationen. Detta utförs för alla behandlingar som ingår i bolagets registerförteckning. En rutin för att uppdatera riskanalyser och konsekvensbedömningar vid återkommande intervaller för att säkerställa att inga nya eller förändrade risker har uppstått som behöver hanteras har inte implementerats.	En rutin för att uppdatera riskanalys och konsekvensbedömning vid återkommande intervaller saknas.	2,70

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	Kommunens gemensamma DSO är utsedd kontaktperson gentemot Datainspektionen för att svara på eventuella förfrågningar och för att rapportera personuppgiftsincidenter. Bolagets dataskyddssamordnare har frekvent kontakt med DSO för rådgivning och vägledning. DSO har på eget initiativ tagit fram en enskild årsrapport för varje nämnd, förvaltning och bolags dataskyddsarbete som sammanfattar årets framsteg och kommande års fokusområden. DSO granskar personuppgiftsbiträdesavtalen i denna rapport men i övrigt är rapporten av sammanfattande snarare än granskande karaktär. Utöver denna rapport finns ingen en fastslagen granskningsplan (exempelvis en revisionsplan) för att utvärdera och säkerställa att man uppfyller relevanta krav på hantering av personlig information, detta planeras däremot att implementeras för 2020.	Bolaget har hittills ingen fastslagen granskningsplan eller internkontrollfunktion med fokus på att dataskyddsarbetet är i enlighet med dataskyddsförordningens krav.	2,60
Organisation och ansvar	Verksamheten har utsett en dataskyddssamordnare samt antagit kommunens DSO. Båda har tydligt definierade roller och ansvar kopplat till bolagets arbete med dataskydd och informationssäkerhet. Därtill finns systemansvariga för respektive IT-system. Dataskyddsombudet rekryterades våren 2018. DSO är i grunden jurist och har tidigare arbetat med dataskydd på en myndighet. DSO har ett kommunövergripande ansvar och upplever sig ha tillräckligt med stöd, sakkunskap och självständighet för att kunna utföra de uppgifter som fastställts i dataskyddsförordningen. DSO gör årsrapport om varje nämnd, förvaltning och bolags status med sitt arbete utefter dataskyddsförordningen. Dock saknas det saknas en etablerad rapporteringsväg både från DSO till bolagsstyrelsen.	Bolaget saknar rutiner för att rapportera till styrelse om status för dataskyddsarbetet.	3,33

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	Bolaget har ett tänk kring sparsam behandling av personuppgifter, som nästintill enbart insamlas på avtalsgrund. En kartläggning av bolagets behandlingsprocesser av personuppgifter har genomförts, varefter en registerförteckning har skapats i Draft-it. Däremot har en kartläggning av dataflöden avseende hur personuppgifter rör sig mellan verksamhetens verksamhetssystem har inte utförts. Det saknas kontroller för riktighet och fullständighet av registerförteckningen. Det saknas exempelvis rutiner eller kontroller på plats för att säkerställa att personuppgifter endast behandlas för de ändamål som de ursprungligen samlades in för eller att uppgifterna raderas, anonymiseras eller gallras inom rätt tidsramar.	En kartläggning av dataflöden avseende hur personuppgifter rör sig mellan verksamhetens verksamhetssystem (inklusive leverantörer) saknas. Det saknas 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.	2,25
Val av skydds-åtgärder	Informationsklassificering görs inte regelmässigt för strukturerad information eller för ostrukturerad information. En projektgrupp har skapats på ledningsnivå för att påbörja en klassificering av strukturerad information i IT-system i KLASSA. Hittills har 3 system blivit klassificerade och arbetet kommer fortsätta under 2020. Utöver den sekretessbedömning som görs i samband med utlämning av offentliga handlingar, saknas en rutin för att genomföra klassificering av ostrukturerad information och dokumentation.	En rutin för att säkerställa att samtlig strukturerad information blir klassificerat har inte implementerats. En metod och rutin för att genomföra klassificering av ostrukturerad information och dokumentation saknas därtill.	2,17

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	Tornberget har upprättat behörighetsgränsningar i sina verksamhetssystem för att styra att användare inte kan ta del av information som de inte har rätt till. Bolaget har däremot ingen rutin för interna kontroller, tester eller uppföljning av sina behörighetsstrukturer. En checklista som inkluderar att inaktivera/ta bort användarkonton för anställda som avslutar sin tjänst finns. Gällande kravet på lagrings- och uppgiftsminimering, finns inga rutiner för gallring utöver det som ingår i bolagets dokumenthanteringsplan. Alla anställda är uppmanade att inte samla in eller lagra mer information än nödvändigt, men det saknas en rutin för att säkerställa att detta efterlevs.	Bolaget utför inga interna kontroller, tester eller uppföljning av tekniska dataskyddsåtgärder. Exempel på detta kan vara periodiska granskningar av höga behörigheter. Det saknas förankrade riktlinjer eller rutiner gällande lagrings- och uppgiftsminimering såväl som regelbunden granskning och gallring av information i IT-system.	2,50
Hantering av leverantörs-relationer	Personuppgiftsbiträdesavtal har tecknats med alla leverantörer. Bolaget utför inte någon form av granskning och godkännande utöver att upprätta personuppgiftsbiträdesavtal, med syfte att säkerställa att leverantören lever upp till kraven i dataskyddsförordningen. Man granskar inte heller att personuppgiftsbiträden följer kraven i dataskyddsförordningen över tid. Leverantörer har inte tillgång till Tornbergets verksamhetssystem eller personuppgifter utöver de kontaktuppgifter som behövs för att leverantör ska kunna hantera en felanmälan.	Det saknas en rutin för att säkerställa att personuppgiftsbiträden långsiktigt agerar i linje med dataskyddsförordningen.	2,25

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	En väldokumenterad lokal rutin för hur personuppgiftsincidenthantering ska utredas, bedömas, rapporteras och kommuniceras har tagits fram. DSO är ansvarig för att rapportera incidenter till Datainspektionen inom 72 timmar om nödvändigt. DSO informerar bolaget om förändringar i lagkrav avseende personuppgiftsincidenter. Man har inte granskat efterlevnaden av sina rutiner då man upplever att de fungerat väl.		2,91
Information till registrerade	Tornberget har utförlig information över sin behandling av personuppgifter för leverantörer, rekrytering, bostadshyresgäster och lokalhyresgäster på sin hemsida. Bolaget samlar nästintill enbart in personuppgifter på avtalsgrund. När samtycke krävs, används blanketter vars utformning förutsätter att individernas samtycke bygger på en aktiv handling och är distinkt, tydligt och inte ihopblandat med andra samtycken. Det framgår hur man återtar sitt samtycke. Det saknas kommunikationsansvarig eller en tydlig process som säkerställer att verksamheten kommunicerar personuppgiftsincidenter eller förändring av bolagets hantering av personuppgifter till de registrerade.	Det saknas en process för hur bolaget kommunicerar möjliga förändringar i hur man hanterar personuppgifter eller incidenter som berör registrerade.	2,69

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

Begäran från registrerade	Tornberget har en väldokumenterad rutin för hur begäran från registrerade hanteras. Det finns en mejladress där registrerade kan framföra förfrågningar och klagomål som DSO ansvarar över. Personuppgiftsregister utlämnas på kommunhuset mot uppvisad legitimation eller skickas till den registrerades folkbokföringsadress. Man erbjuder inget säkert system där registrerade kan ta del av sina personuppgifter. Det finns rutiner för hantering av förfrågningar gällande felaktiga, inte längre behövande, eller radering av personuppgifter, men de är inte utförligt dokumenterade. Vidare har bolaget inte inventerat möjligheten att radera personuppgifter i de system där detta är tillämpligt om en giltig begäran om ”rätten att bli bortglömd” inkommer.	Det saknas en dokumenterad rutin för hantering av förfrågningar gällande felaktiga, inte längre behövande, eller radering av personuppgifter.	2,44
Profilering	Bolaget har inget behov av att utföra profilering då automatiserad behandling inte används inom bolaget.		X

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. Övergripande rekommendationer

Då flertalet iakttagelser har identifierats inom olika delar av ramverket, har EY valt att presentera sex övergripande rekommendationer och förslag på åtgärder för de främsta riskerna inom bolagets dataskydd och informationssäkerhetsarbete.

Granskning och rapportering

Begränsad uppföljning av bolagets informationssäkerhetsarbete medför risk att den dagliga informationshanteringen avviker från sättet som rutiner anvisar och man tror att arbetet bedrivs på. Tornberget rekommenderas därför att implementera en granskningsplan för att utvärdera och säkerställa att man uppfyller relevanta krav på hantering av personlig information såväl som en rutin för att dokumentera och rapportera detta resultat till ledningsnivå. Man bör även fastställa ett rapporteringskrav gällande frekvens och innehåll som rapporteringen ska utgå från för att säkerställa att uppföljning av dataskyddsförordningen utförs och kommuniceras till ledningen.

Utbildning

Brist på aktiv kommunikation av policys, anvisningar och instruktioner gällande informationssäkerhet medför risk att bolagets användare besitter otillräcklig kunskap för att på daglig basis hantera bolagets information på ett ändamålsenligt och säkert sätt. EY rekommenderar därför att Tornberget tillser att informationssäkerhetsrelaterad dokumentation kommuniceras aktivt till kommunens användare med en bestämd frekvens genom att införa vidareutbildning inom integritet och dataskydd. Dessa utbildningar bör regelbundet uppdateras för att säkerställa att nya krav och förhållningssätt kommuniceras till alla medarbetare.

Behandling av personuppgifter

EY rekommenderar att Tornberget gör en kartläggning av dataflöden avseende hur personuppgifter rör sig mellan verksamhetssystem (inklusive leverantörer). Genom att dokumentera de processer och rutiner som är associerade med att hantera hela livscykeln för personuppgifter kan man skapa arbetsflöden för att modifiera användarkonton, samt granska och rapportera personuppgifter. En sådan kartläggning kan underlätta i framtagandet av rutiner för att säkerställa och granska att personuppgifter endast behandlas för de ändamål som de samlades in för och sedan anonymiseras, raderas eller gallras inom rätt tidsram, vilket även bör granskas framöver.

Inbyggt dataskydd

Tornberget har behörighetsbegräsningar i sina verksamhetssystem där tilldelning av behörigheter sköts enligt principen att personer bör ha åtkomst till så få personuppgifter. För att försäkra sig om att inga användare kommer åt information de inte bör ha tillgång till efter

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

avslutad tjänst eller förändrad arbetsroll, rekommenderas bolaget att fastställa en rutin för periodisk granskning av framförallt höga behörigheter i kritiska verksamhetssystem.

Val av skyddsåtgärder

Bolaget rekommenderas att genomföra den påbörjade klassificeringen av strukturerad information, likväl som för ostrukturerad information, för att försäkra att alla personuppgifter hanteras i enlighet med de krav som dataskyddsförordningen ställer. Bolaget kan exempelvis använda KLASSA såsom planerat eller en annan metod för att värdera information och ta fram handlingsplaner som identifierar en del av de åtgärder som bör vidtas för att skydda information i verksamhetssystem.

Leverantörsrelationer

Bolaget rekommenderas att använda en mall som exempelvis SKR:s för personuppgiftsbiträdesavtal vid upprättandet av personbiträdesavtalen för att kvalitetssäkra att avtal innehåller relevanta avtalspunkter och krav utifrån dataskyddsförordningen. En sådan checklista kan även användas som underlag till en regelbunden granskning av att personuppgiftsbiträden agerar enligt personuppgiftsbiträdesavtal och förordningens krav, vilket är en rutin som bör fastställas då bolaget fortfarande är ansvarig 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. Utbildningsförvaltningen

Baserat på utförd granskning konstateras att Utbildningsförvaltningen har en genomsnittlig mognadsgrad inom personuppgiftshantering, jämfört med vad EY generellt observerar i offentlig verksamhet av motsvarande storlek och karaktär. Detta innebär dock att man uppnår en förhållandevis låg mognadsgrad och har en bit kvar för att nå upp till en nivå som rekommenderas av EY, givet den stora mängd personuppgifter och känsliga personuppgifter som hanteras inom förvaltningen.

Förvaltningen rekommenderas i första hand att ta fram en metod och rutin för att bedöma risker kopplade till sin personuppgiftshantering vid återkommande intervaller. Utformningen av informationsskydd för respektive integritetsrisk bör baseras på resultatet från denna analys. Regelbundna integritetsgranskningar för att säkerställa att verksamhetens rutiner, för hur intern rapportering till styrelse och ledning samt extern rapportering till Datainspektionen sker rörande hur verksamheten, lever upp till lagkraven finns inte på plats. Informationsklassificering bör även implementeras då detta varken utförs regelmässigt för strukturerad information eller för ostrukturerad information.

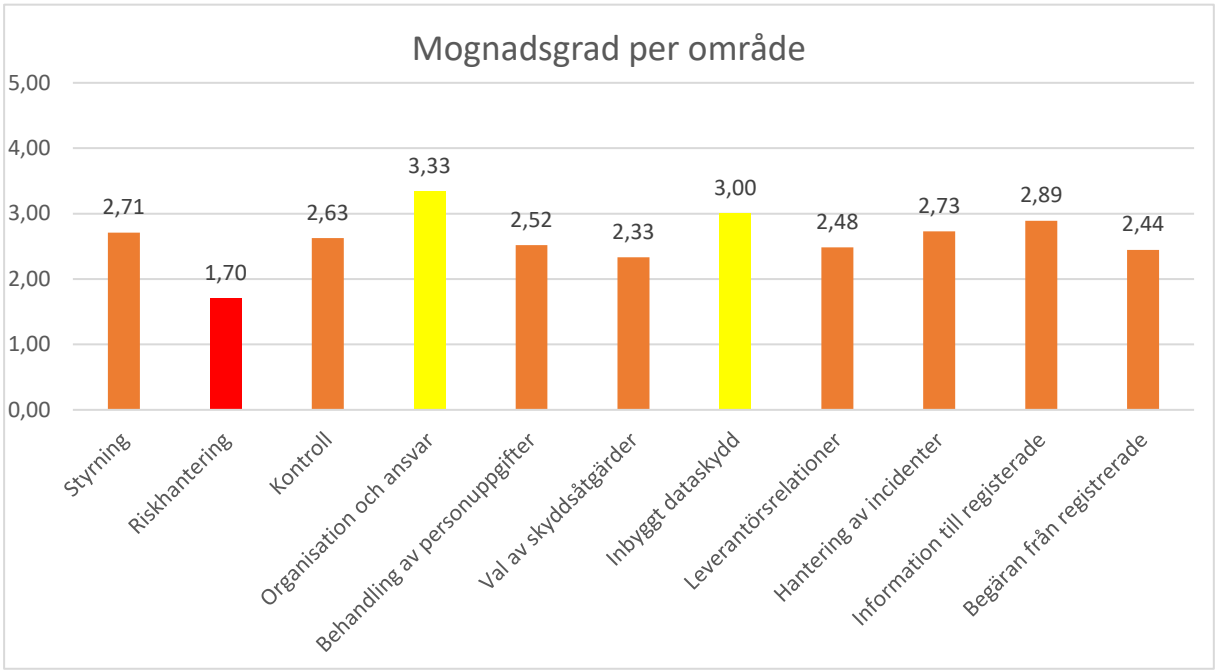
De ansvariga inom förvaltningen har arbetat ambitiöst med dessa frågor och visar intresse och engagemang för dataskyddsfrågorna. Tack vare detta har man nått upp till en genomsnittlig nivå för kommunal verksamhet av liknande karaktär. I följande avsnitt detaljredovisas de områden som behöver förbättras för att öka utbildningsförvaltningens 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

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

Figur 5: Mognadsgrad per område

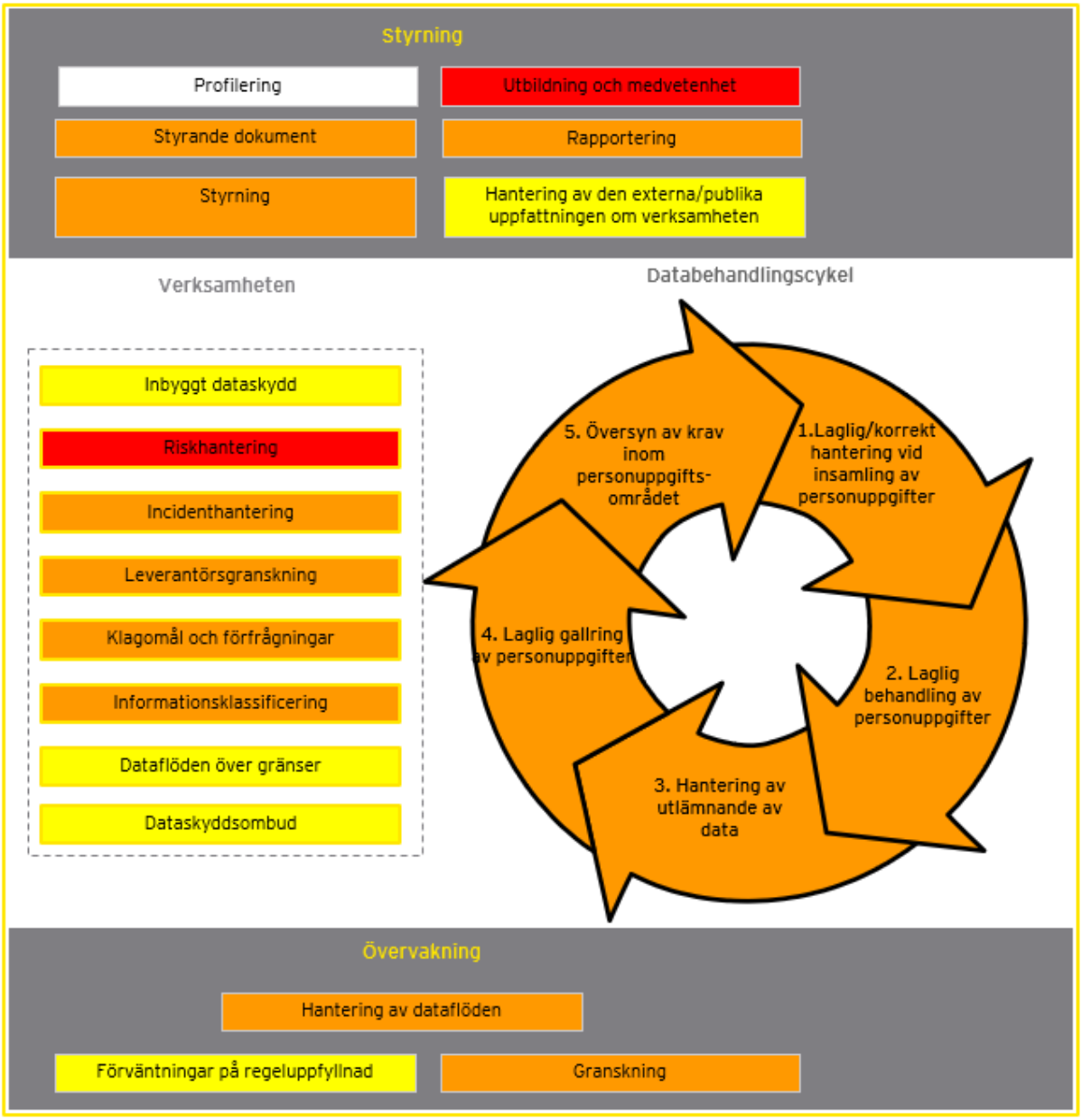


Nivå 5 representerar hög mognadsgrad medan nivå 1 representerar låg mognadsgrad.

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



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

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

4.1. 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	Flertalet styrdokument inklusive kommunens informationssäkerhetspolicy har inte uppdaterats i enlighet med kraven från dataskyddsförordningen. Förvaltningen har tagit fram lokala riktlinjer baserat på kommunens handbok om Dataskyddsförordningen. En grundläggande analys av områden där man inte levde upp till förordningens krav utfördes våren 2018, varav flertalet områden har lösts allteftersom i samverkan med DSO. Förvaltningen genomförde strukturerade utbildningsinsatser kopplat till kraven i dataskyddsförordningen under våren 2018. Alla anställda genomgick en e-utbildning som skickades ut varje vecka under 10 veckors tid såväl som fysiska utbildningsinsatser under maj/juni/september 2018. Fullföljandet av e-utbildningen antas ligga kring 70 %. Utbildningsmaterialet finns på deras intranät. Förvaltningsledarna gick på en ytterligare utbildning i juni 2019. Kommunjuristen har även en grundläggande juridikkurs som kommunens anställda får anmäla sig till där man bland annat trycker på gallring av personuppgifter.	Endast ett fåtal rutiner och policys beträffande hanteringen av personuppgifter i enlighet med kraven från dataskyddsförordningen har dokumenterats, förankrats och kommunicerats i styrdokument på en kommunövergripande nivå. Förvaltningen har inte genomfört en strukturerad analys enligt en särskild process eller ramverk. Därtill saknas uppföljning av analysen samt åtgärdsplan med tidsplan och ansvarsfördelning för att åtgärda de eventuella områden som återstår. Förvaltningen har inte etablerat en process som säkerställer att internutbildningar om informationssäkerhet och dataskydd uppdateras och genomförs regelbundet av nyanställda såväl som av befintliga anställda.	2,71

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	I dagsläget saknas en metod för att genomföra riskanalyser för att bedöma risker som kan finnas i samband med att verksamheten behandlar personuppgifter för de system där förvaltningen är objektägare. Hittills har man endast vid ett tillfälle funnit behov att genomföra konsekvensbedömning. Man har inte haft någon kontakt med Datainspektionen. DSO har varit i kontakt med Draft-it och planerar att införa deras metod för konsekvensanalys under året.	Riskanalyser utförs inte vid återkommande intervaller för integritetsrisker i förvaltningens verksamhet och IT-system.	1,70
Kontroll	Kommunens gemensamma DSO är utsedd kontaktperson gentemot Datainspektionen för att svara på eventuella förfrågningar och för att rapportera personuppgiftsincidenter. Bolagets dataskyddssamordnare har frekvent kontakt med DSO för rådgivning och vägledning. DSO har på eget initiativ tagit fram en enskild årsrapport för varje nämnd, förvaltning och bolags dataskyddsarbete som sammanfattar årets framsteg och kommande års fokusområden. DSO granskar personuppgiftsbiträdesavtalen i denna rapport men i övrigt är rapporten av sammanfattande snarare än granskande karaktär. Utöver denna rapport finns ingen en fastslagen granskningsplan (exempelvis en revisionsplan) för att utvärdera och säkerställa att man uppfyller relevanta krav på hantering av personlig information, detta planeras däremot att implementeras för 2020.	Förvaltningen har i dagsläget ingen fastslagen granskningsplan eller internkontrollfunktion med fokus på att dataskyddsarbetet 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	Förvaltningen har utsett en dataskyddssamordnare samt antagit kommunens DSO. Båda har tydligt definierade roller och ansvar kopplat till bolagets arbete med dataskydd och informationssäkerhet. Dataskyddsombudet rekryterades våren 2018. DSO är i grunden jurist och har tidigare arbetat med dataskydd på en myndighet. DSO har ett kommunövergripande ansvar och upplever sig ha tillräckligt med stöd, sakkunskap och självständighet för att kunna utföra de uppgifter som fastställts i dataskyddsförordningen. DSO gör årsrapport om varje nämnd, förvaltning och bolags status med sitt arbete utefter dataskyddsförordningen. Dock saknas det saknas en etablerad rapporteringsväg både från DSO till bolagsstyrelsen.	En formell väg eller rutin för rapportering från DSO till kommunstyrelsen eller nämnd och krav som sådan rapportering ska utgå ifrån har inte förankrats.	3,33

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	Förvaltningen hanterar en stor mängd personuppgifter såväl som känsliga personuppgifter. En registerförteckning har upprättats där ändamål för insamlingen framgår. Man har dokumenterat dataflöden avseende hur personuppgifter rör sig mellan IT-system i Draft-it och följer upp detta regelbundet. Under granskningen upptäcktes att personuppgifter behandlades för andra ändamål än de samlats in för, och att denna behandling inte fanns upptagen i registerförteckningen. Man håller på att uppdatera instruktionerna för gallring av personuppgifter i samband med införandet av e-arkiv. Gallring utförs men förvaltningen har inte granskat att detta sker ändamålsenligt. Därtill saknar man rutiner för att säkerställa att personuppgifter endast behandlas för de ändamål de samlades in för. Verksamheten utför endast begränsade tester, undersökningar och utvärderingar av effektiviteten hos de tekniska och organisatoriska åtgärder som vidtagits för att garantera säkerheten i behandling av personuppgifter.	Det saknas rutiner för att säkerställa registerförteckningens fullständighet och riktighet över tid. Det saknas 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. Förvaltningen utför begränsade interna kontroller, tester eller uppföljning av tekniska dataskyddsåtgärder.	2,52
Val av skydds-åtgärder	Informationsklassificering görs inte regelmässigt för strukturerad information på dokumentnivå eller för ostrukturerad information. SKR:s KLASSA har använts för att klassificera vissa IT-system. Någon typ av PUL-märkning uppges även finnas i förvaltningens diariesystem. Därtill finns en grundläggande guide för lagring och instruktioner på intranätet kring hur man bör kommunicera i e-post.	En rutin som säkerställer att samtlig strukturerad information blir klassificerat har inte implementerats. En metod och rutin för att genomföra klassificering av ostrukturerad information och dokumentation saknas.	2,33

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	Kommunen har en digital enhet som arbetar med utveckling och säkerhetsåtgärder som tagit fram riktlinjer för vad som ska kravställas vid anskaffning och upphandling av nya system. Det framgår att man har ett tänk kring kravet på lagrings- och uppgiftsminimering inom förvaltningen. Det finns en guide för lagring och en utbildning inom detta kommer äga rum under våren 2020 där alla närvarande även uppmanas gallra sina system.	Förvaltningen utför inga kontroller, tester eller uppföljning av tekniska dataskyddsåtgärder eller behörighetsstrukturer. Det bör som ett minimum finnas rutiner för periodisk granskning av höga behörigheter i känsliga system.	3,00
Hantering av leverantörs-relationer	Förvaltningen har inventerat alla externa IT-system som behandlar personuppgifter och upprättat registerförteckning i Draft-it. Personuppgiftsbiträdesavtal har skapats för alla leverantörer som hanterar förvaltningens personuppgifter. SKR:s inventeringslista i KLASSA används för att säkerställa att relevanta krav och klausuler är integrerade i kontrakt. Förvaltningen reviderar sina avtal utefter SKR revideringar för nya leverantörsavtal. Det finns ingen en rutin för att säkerställa att leverantören lever upp till kraven i dataskyddsförordningen, innan en ny leverantör används, utöver att teckna ett personuppgiftsbiträdesavtal. En rutin för att regelbundet kontrollera att personuppgiftsbiträden hanteras på ett sätt som innebär att dataskyddsförordningen efterlevs över tid är under utveckling av DSO. Förvaltningen använder vissa system som har datalagring utanför EU/EES. För dessa system har förvaltningen skrivit på personuppgiftsbiträdesavtal. Det finns interna riktlinjer som anger att man ska vara restriktiv med personuppgifter i dessa system.	Det saknas en rutin för att säkerställa att personuppgiftsbiträden långsiktigt agerar i linje med dataskyddsförordningen.	2,48

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	En väldokumenterad lokal rutin för hur personuppgiftsincidenthantering ska utredas, bedömas, rapporteras och kommuniceras har framtagits. Ett digitalt system för incidenthantering har även anskaffats. DSO är ansvarig för att rapportera incidenter till Datainspektionen inom 72 timmar om nödvändigt. DSO informerar även bolaget om förändringar i lagkrav avseende personuppgiftsincidenter. Gällande kommunikation till de som drabbats av en personuppgiftsincident så framgår det i lathunden för incidentrapportering att den med störst kunskap ska ansvara för att kontakta dessa. Det finns inga etablerade rutiner på plats som innebär att de interna instruktionerna eller rutinerna gällande personuppgiftsincidenter efterlevs, men DSO har gjort en utvärdering av detta med förbättringsförslag som ska presenteras.	En dokumenterad rutin för att granska efterlevnaden av de interna instruktionerna gällande personuppgiftsincidenter saknas.	2,73

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	Vid insamling av personuppgifter, lämnas utförlig information till den registrerade om hur personuppgifterna kommer användas. När samtycke används för insamling av personuppgifter används blanketter vars utformning förutsätter att individernas samtycke bygger på en aktiv handling och är distinkt, tydligt och inte ihopblandat med andra samtycken. Förvaltningen har däremot inte tydliga rutiner gällande hur de registrerade kan ta tillbaka sina samtycken. Därtill har förvaltningen ingen arbetsmetod för att i efterhand visa att samtycke samlats in från de registrerade. Dataskyddskoordinator är ansvarig för att kommunicera med de registrerade kring hur verksamhetens hantering av personuppgifter kommer förändras framöver, om sådana förändringar planeras. Vid större personuppgiftsincidenter gäller kommunens vanliga rutiner för kommunikationshantering.	En skriftlig rutin som de registrerade kan använda sig av för att ta kunna ta tillbaka sina samtycken saknas. Förvaltningen har inte säkerställt att det i efterhand går att visa att samtycke har samlats in från de registrerade	2,89

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

Begäran från registrerade	Det finns en tydlig kontaktväg via en mejladress där registrerade kan framföra förfrågningar och klagomål. Personuppgiftsregister skickas till folkbokföringsadress eller som ett rekommenderat brev till den registrerade. Det finns rutiner för hantering av förfrågningar gällande felaktiga, inte längre behövande, eller radering av personuppgifter, men de är inte utförligt dokumenterade. Verksamheten är osäker på om man kan skicka personuppgifter till en registrerad eller en ny leverantör i så kallat ”maskinläsbart format”. Man har inte heller ett säkert system där användaren kan logga in och ta del av sina personuppgifter som denne har begärt. Vidare har förvaltningen inte inventerat möjligheten att radera personuppgifter i de system där detta är tillämpligt om en giltig begäran om ”rätten att bli bortglömd” inkommer. I vissa system ska det gå att inaktivera personuppgifter. Observera att för en kommunal förvaltning är det kraftigt begränsat vilka personuppgifter som kan bli bortglömda, då en kommun i många fall är skyldig att behålla dem.	Det saknas möjlighet att få personuppgifter utlämnade i elektroniskt format. Det finns ingen rutin för att följa dataskyddsförordningens krav om en giltig begäran om ”rätt att bli bortglömd” inkommer.	2,44
Profilering	Utbildningsförvaltningen har inget behov av att utföra profilering då automatiserad behandling inte används inom de kommunala verksamheterna.	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

4.2. Övergripande rekommendationer

Då flertalet iakttagelser har identifierats inom olika delar av ramverket, har EY valt att presentera sex övergripande rekommendationer och förslag på åtgärder för de främsta riskerna inom förvaltningens dataskydd och informationssäkerhetsarbete.

Kontroll

Detta område utforskar om verksamheten har någon plan för att granska att hanteringen av personuppgifter sker enligt krav. EY rekommenderar att förvaltningen genomför regelbundna granskningar för att identifiera riskområden eller potentiella brister, så att de kan hanteras och åtgärdas på lämpligt sätt. Genom denna granskning kan man säkerställa att verksamhetens rutiner, för hur intern rapportering till ledning samt extern rapportering till Datainspektionen sker rörande hur verksamheten, lever upp till lagkraven. Man bör även fastställa ett rapporteringskrav gällande frekvens och innehåll som rapporteringen ska utgå från för att säkerställa att uppföljning av dataskyddsförordningen utförs och kommuniceras till ledningen.

Riskhantering

Riskhantering syftar till att utvärdera hur verksamheten identifierar och minskar integritetsrisker i sin verksamhet och i sina IT-system. Förvaltningen rekommenderas att ta fram en metod och rutin för att bedöma risker kopplade till sin personuppgiftshantering vid återkommande intervaller. Utformningen av informationsskydd för respektive integritetsrisk bör baseras på resultatet från denna analys. I dagsläget saknar förvaltningen rutiner samt en ansvarsfördelning som säkerställer att konsekvensbedömningar utförs och att man söker råd från Datainspektionen i de fallen där bedömningar visar höga risker ur integritetssynpunkten. EY rekommenderar att konsekvensbedömning görs vid regelbundna intervaller för att säkerställa att man minimerar nya eller förändrade risker.

Behandling av personuppgifter

För att säkerställa att personuppgifter endast behandlas för de ändamål som de samlades in för och sedan anonymiseras, raderas eller gallras inom rätt tidsram, bör man implementera en rutin för att granska efterlevnaden av de policys och rutiner för dokumenthantering och datalagring som framtagits för att förhindra att detta sker. För att skydda tillgång till personuppgifter i sina IT-system ytterligare bör förvaltningen utföra interna kontroller, tester eller uppföljning av de tekniska dataskyddsåtgärderna och behörighetsstrukturerna som har implementerats.

Val av skyddsåtgärder

Förvaltningen rekommenderas att genomföra klassificeringen av strukturerad såväl som för ostrukturerad information avseende alla personuppgifter som verksamheten hanterar för att

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

försäkra att information hanteras i enlighet med de krav som dataskyddsförordningen ställer. EY rekommenderar att bolaget använder en framtagen modell, som exempelvis SKR:s KLASSA såsom påbörjat, för att värdera informationen i verksamhetssystem och ta fram handlingsplaner som identifierar en del av de åtgärder som behöver vidtas för att skydda information.

Leverantörsrelationer

Utbildningsförvaltningen rekommenderas att ta fram en rutin för att granska att personuppgiftsbiträden agerar enligt personuppgiftsbiträdesavtalet och dataskyddsförordningens krav både vid avtalsskrivande och över tid. Förvaltningen kan exempelvis använda SKR:s checklista vid upprättandet av personbiträdesavtalen som underlag för denna granskning. Därtill bör en rutin för regelbunden granskning av att samtliga personuppgiftsbiträden efterlever dataskyddsförordningen över tid framtas.

Begäran från registrerade

EY rekommenderar att förvaltningen inventerar ifall man kan skicka personuppgifter till en registrerad eller en ny leverantör i så kallat ”maskinläsbart format” inom en månad efter en sådan begäran. Om inte, rekommenderas förvaltningen att se till att detta blir möjligt för att kunna leva upp till kravet på dataportabilitet. Enligt Datainspektionen ska de registrerade få sitt registerutdrag tillhandahållet i elektronisk form ifall begäran lämnats i denna form.

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. Slutsatser

Syftet med granskningen har varit att genomföra en övergripande kartläggning av huruvida Haninge kommun har tillsett att arbetet kring personuppgiftshantering i utbildningsförvaltningen, Haninge Bostäder AB och Tornberget Fastighets AB är i enlighet med dataskyddsförordningen. Förvaltningen och bolagen bedöms i relation till andra offentliga organisationer av liknande storlek i förhållande till antal anställda, övergripande verksamhet samt karaktär och mängd av sin personuppgiftshantering.

- Haninge Bostäder: 2,25 av 5,00
  2,25 är en förhållandevis låg mognadsgrad för ett bostadsbolag, givet bolagets storlek och förhållandevis stora mängd personuppgifter.
- Tornberget: 2,59 av 5,00
  Mognadsgraden 2,59 är i stort i linje med vad som kan förväntas av ett litet fastighetsbolag med få personuppgifter.
- Utbilningsförvaltningen:2,62 av 5,00
  2,62 är en genomsnittlig mognadsgrad för en kommunal förvaltning. Detta innebär dock att man har en bit kvar för att nå upp till en nivå som rekommenderas av EY, givet den stora mängd personuppgifter och känsliga personuppgifter som hanteras inom förvaltningen.

Över lag bedöms mognadsgraden för de tre enskilda verksamheterna vara högst inom organisation och ansvar då man har ett gemensamt dataskyddsombud och liknande ansvarsstruktur. Information till registrerade hade även en relativt hög mognadsgrad i alla verksamheter. Samtliga verksamheter har en låg mognadsgrad inom kontroll då en fastställd granskningsplan från ledningsnivå saknas. Vidare bedömdes alla verksamheter ha relativt låga mognadsgrader inom riskhantering, val av skyddsåtgärder och leverantörsrelationer.

Det är däremot tydligt att förvaltningen och bolagen lagt ner ett ambitiöst arbete och engagemang för personuppgiftsfrågor och dataskyddsförordningen. De granskade verksamheternas dataskyddssamordnare tillsammans med andra nyckelpersoner har arbetat målinriktat med att framta rutiner och visar på en medvetenhet kring sin personuppgiftshantering. Kommunens gemensamma dataskyddsombud har även framtagit en granskningsplan för 2020 för samtliga nämnder, förvaltningar och bolag i kommunen, vilket kommer öka mognadsgraden i samtliga verksamheter då regelbunden granskning, uppföljning och utveckling av rutiner krävs för att uppnå en mognadsgrad över 3,00 inom respektive område.

Gemensamt för de tre granskade enheterna är att den största och viktigaste förbättringspunkter ligger i att analysera vilka brister och förbättringspunkter som finns i personuppgiftshanteringen och därefter baserat på detta ta fram strukturerade planer för att säkerhetsställa att man uppfyller relevanta krav på hantering av personlig information inom i stort sett samtliga undersökta områden. Den begränsade uppföljningen av verksamheternas informationssäkerhetsarbete medför risken att förvaltningens och bolagens dagliga informationshantering avviker från sättet som rutinerna anvisar och man tror att arbetet bedrivs på. Kommunen bör arbeta proaktivt med riskhantering, konsekvensbedömning och informationsklassning samt upprätta rutiner för granskning av efterlevnad för att minska

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

risker för integritetsincidenter och ogiltig behandling av personuppgifter inom sina verksamheter såväl som hos leverantörer.

EY rekommenderar även att kommunstyrelsen fastställer ett rapporteringskrav gällande frekvens och innehåll som rapporteringen till styrelse ska utgå från för att säkerställa att uppföljning av dataskyddsförordningen dokumenteras och rapporteras till ledningsnivå. Utan detta bedömer EY att det kommer bli svårt att skapa tillfredsställande förutsättningar för att bedriva ett ändamålsenligt arbete med personuppgiftshantering på både kort och lång sikt inom kommunen.

Stockholm den 10 mars 2020

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

6. Bilaga 1: Förteckning över intervjuade funktioner

6.1. Haninge Bostäder AB

- VD
- Verksamhetsutvecklare och dataskyddssamordnare
- Dataskyddsombud

6.2. Tornberget Fastighetsförvaltnings AB

- Dataskyddssamordnare
- Registrator
- Fd. Ekonomichef och IT-ansvarig
- HR-konsult
- Dataskyddsombud

6.3. Utbildningsförvaltningen

- Dataskyddsombud
- Kanslichef
- Förvaltningsledare IT-verksamhet
- Dataskyddskoordinator

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 2: Dokumentförteckning

7.1. Haninge Bostäder AB

- Dokumenthanteringsplan, 2019
- Handbok hantering av personuppgifter i enlighet med GDPR, 2018
- Konsekvensanalysmall, 2019
- Draft-it rapport, 2020
- Dataskyddsombudets GDPR rapport för Haninge Bostäder, 2019
- Riktlinjer gällande informationssäkerhet, 2018
- IT-Riktlinjer, 2013

7.2. Tornberget Fastighetsförvaltnings AB

- Dataskyddsombudets GDPR rapport för Tornberget, 2019
- Att tänka på gällande skyddade personuppgifter, 2019
- E-posthantering, 2019
- Incidenthantering register, 2019
- Process för personuppgiftsincidenthantering, 2019
- Personuppgiftsincidentrapporthantering, 2019
- Incidenthantering rapporterade incidenter, 2020
- Tornbergetsriktlinjer för hantering av externa personuppgifter, 2018
- Tornbergetsriktlinjer för hantering av interna personuppgifter, 2018
- Introduktionschecklista för nyanställda, 2019
- Extern kommunikationsplan, 2019
- Intern kommunikationsplan, 2019
- Registerförfrågan – information om utdrag enligt artikel 15 i Dataskyddsförordningen, 2020
- Registerförfrågan mall, 2018
- Svarsmall registerförfrågan utdrag enligt artikel 15 i Dataskyddsförordningen, 2018
- Register över registerförfrågningar, 2018
- Hantering av registerförfrågan process, 2018
- Riskbedömningsmall för konsekvensanalys, 2018
- Modellavtal för samtyckte av bilder, 2019
- Modellavtal för samtyckte av bilder mall, 2018
- Samtycke om användning av bild, 2019
- Samtycke om användning av bildmall, 2018
- Personuppgiftshantering enligt GDPR intranät, 2019
- GDPR utbildning för anställda, 2018
- Informationssäkerhetspolicy för Haninge kommun, 2016

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

7.3. Utbildningsförvaltningen

- Personuppgiftbiträdesavtal följebrev, 2018
- Guide lagring av information, 2019
- Rutiner/tillvägagångsätt personuppgiftsbehandling, 2019
- Riktlinje anskaffning av IT-stöd, 2019
- Information från system/registerförfrågan mall, 2020
- Försättsblad Personuppgiftsutdrag, 2019
- Lathund incidentrapportering, 2018
- Riktlinjer för behandling av personuppgifter, 2018
- Personuppgiftsbiträdesavtal mall, 2018
- Rutin för registerutdrag, 2019
- Så behandlar vi personuppgifter inom gymnasiesär- och gymnasieskolan, 2018
- Så behandlar vi personuppgifter inom förskoleklass, grundsär- och grundskola, 2018
- Så behandlar vi personuppgifter inom förskolan och fritidshemmet, 2018
- Så behandlar vi personuppgifter inom kommunal vuxenutbildning, 2018
- Mall information till registrerad, 2018
- Dataskyddsombudets GDPR rapport för Utbildningsförvaltningen, 2019
- Checklista för behandling av personuppgifter, 2018
- Incidenthantering register, 2019
- Informationssäkerhetspolicy för Haninge kommun, 2016

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 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: 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 Datainspektionen.

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

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

personuppgifter är namn, personnummer, telefonnummer, bank- och kontouppgifter, IP-adress, försäkringsnummer m.m.

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

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

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

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

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

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

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

Registrerad: Med registrerad avses den enskilde vars personuppgifter behandlas.

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

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

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

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.