Granskning av efterlevnad till
Dataskyddsförordningen GDPR
På uppdrag av de förtroendevalda revisorerna
Upplands-Bro kommun samt Upplands-Brohus

Upplands-Bro Kommun

Granskning av efterlevnad till Dataskyddsförordningen GDPR

December 2019

Building a better working world

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 Upplands-Bro kommuns förtroendevalda revisorer genomfört en granskning av kommunens, dess nämnder, förvaltningar (nämnder och förvaltningar hänvisas hädanefter till samlingsbegreppet ”kommunens verksamheter”) såväl som det kommunala bolaget Upplands-Brohus hantering av personuppgifter. Granskningens syfte har varit att ge en *övergripande* förståelse av huruvida Upplands-Bro kommun och Upplands-Brohus bedriver ett ändamålsenligt arbete med dataskyddsförordningen (The General Data Protection Regulation, GDPR) och hur kommunens mognad ser ut i uppfyllelse av de åtgärder som förordningen stipulerar.

En översiktlig granskning av 12 olika områden med utgång i EYs ramverk för personuppgiftshantering gentemot dataskyddsförordningen för kommunala verksamheter har genomförts under november till december 2019. Enligt metoden bedöms kommunens mognadsnivå i 116 frågor/krav på en ordinarie skala från 1 (*Begynnande*) till 5 (*Optimerad*) inom respektive område. Analysen har baserats på intervjuer med identifierade nyckelpersoner i kommunens och Upplands-Brohus personuppgiftssäkerhetsarbete och genomgång av insamlad styrdokumentation i kommunen och bolaget.

Baserat på den analys och granskning som genomförts bedöms Upplands-Bro kommun ha en förhållandevis låg mognadsgrad på 1,75 av maximalt 5,00. Mognadsgrad 1 innebär begynnande, 3 bedöms vara god praxis (i relation till motsvarande organisationer), och 5 optimerad. Mognadsgraden bedöms vara som högst inom information till registrerade och inbyggt dataskydd. Lägst är mognadsgraden inom kontroll, styrning, riskhantering och hantering av leverantörsrelationer. Analys och iakttagelser har faktagranskats av kommunen, samt Upplands-Brohus.

Kommunens största och viktigaste förbättringspunkter ligger i att upprätta en formaliserad och informationssäkerhetsspecifik organisationsstruktur med tillhörande roller, tydlig ansvarsfördelning. Majoriteten av styrdokument och policys är utdaterade och bör uppdateras för att sätta en struktur i kommunens dataskyddsarbete. Kommunen bör även arbeta proaktivt med riskhantering och upprätta personuppgiftbiträdesavtal med leverantörer för att minska risker för integritetsincidenter och ogiltig behandling av personuppgifter inom sina verksamheter såväl som hos leverantörer. Vidare finns ett behov av att införa styrande rutiner och processer för granskning och uppföljning inom i stort sett samtliga av de 12 undersökta områdena, både för kommunen i helhet och för Upplands-Brohus. Slutligen behöver Upplands-Brohus utföra en analys om ett eget dataskyddsombud behövs och dokumentera ett beslutagande.

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.

Dataskyddsförordningen ställer större krav på företag och organisationers interna kontroll kopplat till hanteringen av personuppgifter och i jämförelse med PUL har även kommit med skärpta sanktioner i händelse av fall där förordningens artiklar inte uppfylls:

- 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 Upplands-Bro kommun, dess nämnder, förvaltningar (nämnder och förvaltningar hänvisas hädanefter till samlingsbegreppet ”kommunens verksamheter”) samt de kommunala bolagen hanterar stora mängder personuppgifter, har de förtroendevalda revisorerna i Upplands-Bro kommun beslutat att en granskning av kommunens verksamheter och bolags arbete relaterat till dataskyddsförordningen är nödvändig. Med bakgrund i ovan har EY genomfört en granskning av Upplands-Bro kommuns och Upplands-Brohus arbete med personuppgiftshantering, med hänsyn till dataskyddsförordningen (GDPR).

1.2. Syfte

Syftet med granskningen är att ge en *övergripande* förståelse av huruvida Upplands-Bro kommun och Upplands-Brohus bedriver ett ändamålsenligt arbete med dataskyddsförordningen och hur kommunens mognad 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 Upplands-Bro bedriver på central nivå och inga av kommunens nämnder, förvaltningar eller kommunalägda bolag utöver Upplands-Brohus har således 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 kommunens och Upplands-Brohus informationssäkerhetsarbete samt genomgång av relevant styrdokumentation (se *Sektion 5*. *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. 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. Besvarandet av frågorna som innefattas av ramverket sker med deltagande av GDPR-specialister från EY. Våra specialister sammanställer svaren och redogör för avvikelser. En bedömning sker också av mognadsgrad inom 12 olika områden i en femgradig skala.

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 t.ex. 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 policys, strategi- och styrdokument och dylikt samlats in för att analyseras. Därefter höll EYs GDPR-specialister ett arbetsmöte med Upplands-Bro kommun där informationssäkerhetsstrateg, dataskyddsombud (tillika kommunjurist), IT-chef deltog och ett med Upplands-Brohus där Ekonomichef och IT-strateg deltog. 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 EYs verksamhetsrevisorer, varefter de förtroendevalde revisorerna på kommunen erhöll en slutlig rapport med övergripande rekommendationer för fortsatt arbete.

Tidsplanen för arbetet såg ut enligt följande:

- Oktober 2019 – Förberedelser, planering och insamling av dokumentation.
- November 2019 – Dokumentanalys, utförande av arbetsmöten (2019-11-04 och 2019-11-07), granskning av kompletterande dokumentation och uppföljningsfrågor, färdigställande av rapport, samt faktagranskning av kommunen.
- December 2019 – Kvalitetssäkring av EYs 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

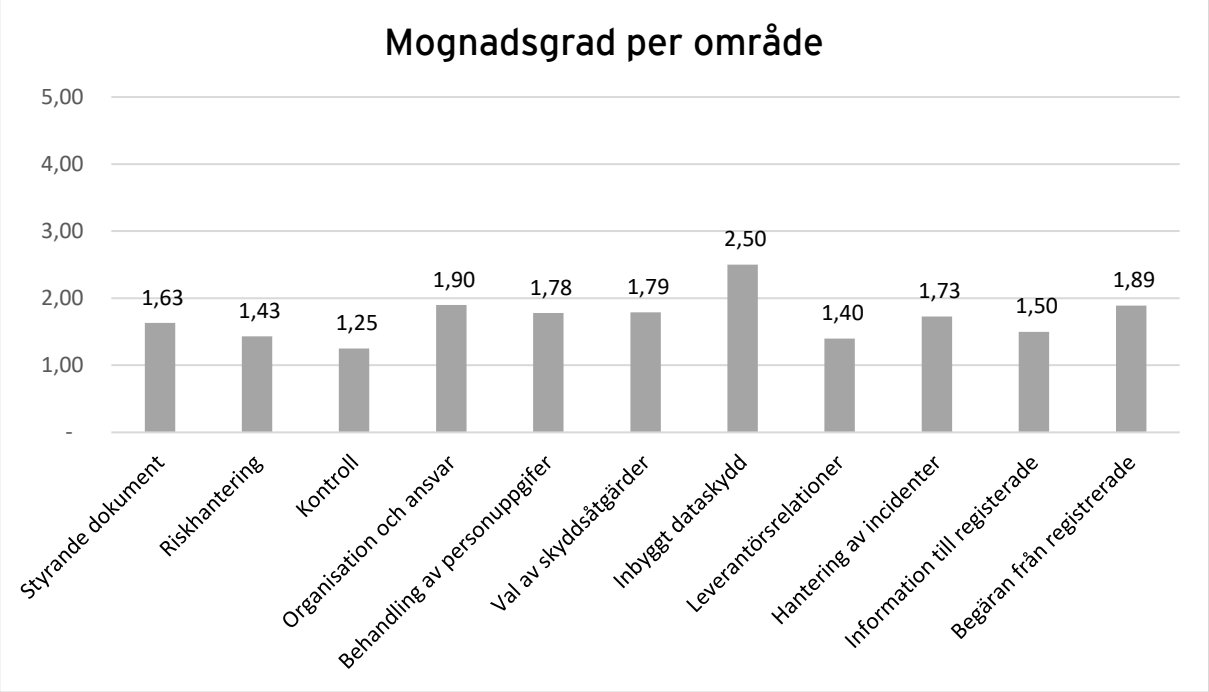
2. Analys

Baserat på utförd granskning konstateras att Upplands-Bro kommun och dess verksamheter, Upplands-Brohus inkluderat, har en förhållandevis låg mognadsgrad inom personuppgiftshantering, jämfört med vad som kan förväntas av en offentlig verksamhet av motsvarande storlek och karaktär.

Det saknas en tydlig organisation och ansvarsfördelning gällande informationssäkerhet och personuppgiftshantering som är förankrad från ledningsnivå. Övergripande strategier som processer och instruktioner för personuppgiftshantering enligt de åtgärder som dataskyddsförordningen stipulerar saknas eller är föråldrade. Styrdokument och rutiner för behandling av personuppgifter enligt dataskyddsförordningen behöver upprättas i första skede för att möjliggöra att processer och riktlinjer för riskhantering och granskning kan implementeras. Kommunen saknar idag en utbyggd organisation med tillräckliga resurser för att lösa de uppgifter som krävs för att öka mognadsgraden.

Översiktsbilderna nedan redovisar kommunens mognadsgrad för de 12 områden som granskats.

Figur 1: Stapeldiagram mognadsgrad per område

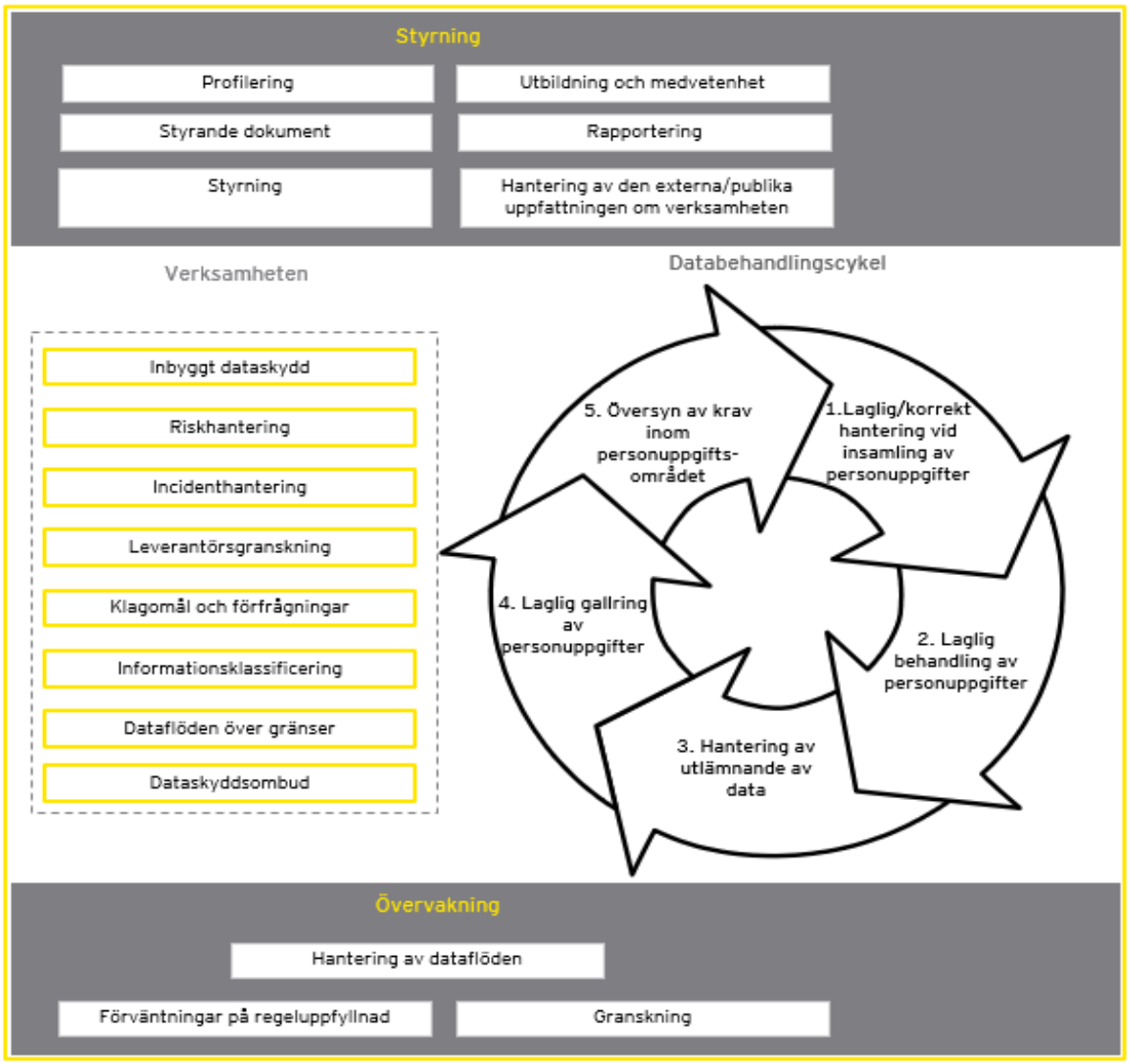


Nivå 5 representerar hög mognadsgrad medan nivå 1 representerar låg mognadsgrad.

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 granskade områden (notera att de 12 huvudområdena är uppdelade i ytterligare detalj)



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	Ett förslag till ett styrdokument och en organisation med tydliga roller, mandat och ansvarsområden beträffande dataskydd och informationssäkerhet framtogs våren 2019. Flertalet styrdokument inklusive kommunens informationssäkerhetspolicy har inte uppdaterats i enlighet med kraven från dataskyddsförordningen. Enligt beslutande regelverk ska de kommunala verksamheterna följa dataskyddsförordningen, men riktlinjer för hur den omsätts i praktiken saknas. Då en rutin för kommunens fortsatta arbete för att fastställa att dataskyddsförordningen efterlevs saknas, har dataskyddsombudet förslagit att enhetscheferna som göra en självutvärdering av verksamhetens anpassning och efterlevnad av förordning, som en initial kartläggning av bristfälliga områden. I övrigt har inga gap-analyser eller åtgärdsplan upprättats.	En formell informationssäkerhetsspecifik organisationsstruktur med tillhörande roller och tydlig ansvarsfördelning inom dataskyddsområdet har inte förankrats eller dokumenteras i styrdokument på en kommunövergripande nivå. 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.	1,63
Riskhantering	Kommunen saknar i dagsläget en tydlig metod eller rutin för att identifiera och minimera integritetsrisker i sin verksamhet och i sina IT-system. Den risk- och sårbarhetsanalys som utförs av kommunens säkerhetsfunktion vart fjärde år är ett potentiellt forum för informationssäkerhet och dataskydd, men dessa risker är inte prioriterade. Vid anskaffning av nya system används SKL:s verktyg KLASSA vid konsekvensbedömning. Ingen strukturerad konsekvensbedömning eller regelbunden riskanalys genomförs för befintlig behandling av personuppgifter. En kartläggning av kommunens behandlingsprocesser av personuppgifter har genomförts, varav en registerförteckning har skapats i systemet Draft-it.	Riskanalyser utförs i regel inte vid återkommande intervaller för integritetsrisker i kommunens verksamhet och IT-system. Det saknas metod och ansvar för att genomföra konsekvensbedömningar innan verksamheten startar en ny typ av behandling. Vidare finns inget ramverk för att utforma informationsskydd utifrån analysens resultat. Kommunens befintliga IT-system har inte gått igenom KLASSA och därför är inte samtliga system riskbedömda enligt en likformig modell.	1,43

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	Dataskyddsombudet är utsedd kontaktperson gentemot Datainspektionen för att svara på eventuella förfrågningar, och för att rapportera personuppgiftsincidenter. I nuläget finns inga formella rutiner på plats för att bistå Datainspektionen med efterfrågad information. Dataskyddsombudet har på eget initiativ framtagit en årsrapport om dataskyddsarbetet till kommunstyrelsen, då en formell rutin eller kanal för rapportering saknas. I den senaste årsrapporten har ombudet inkluderat ett förslag på ett årshjul för rapportering och granskning, då en fastslagen granskningsplan för att utvärdera hur man uppfyller relevanta krav på hantering av personuppgifter saknas i kommunen. Utvecklingen av kontroller av förordningens efterlevnad är fortfarande i planeringsfasen.	En formell rutin för rapportering från skyddsombudet till styrelse/nämnd och krav som sådan rapportering ska utgå ifrån har inte förankrats. Det saknas även en rutin för dataskyddsombudet att följa för att bistå Datainspektionens med information gällande förfrågningar och för att rapportera personuppgiftsincidenter. Kommunen har ingen fastslagen granskningsplan eller internkontrollfunktion med fokus på att dataskyddsarbetet är i enlighet med dataskyddsförordningens krav.	1,25
Organisation och ansvar	Våren 2018 beslutades det att ett gemensamt dataskyddsombud för kommunens verksamheter skulle utses. Då ingen kandidat hittades, utsågs kommunjuristen till dataskyddsombud. Denna tvådelade roll medför att ombudet delvis granskar sitt egna arbete. Ombudet saknar även stöd och resurser, både i form av tid och IT-verktyg, för att kunna övervaka att förordningen efterlevs i kommunens verksamheter. Efterlevnaden har varit särskilt svår att granska då ansvarsfördelningen inte varit tydlig, trots att varje nämnd är personuppgiftsansvariga och ytterst ansvariga för att förordningen efterlevs enligt lagen. Ett förslag över en ny organisation med tydliga roller, mandat och ansvarsområden beträffande dataskydd och informationssäkerhet framtogs under våren 2019.	En strukturerad organisation med tydliga roller och ansvarsområden kopplat till arbetet med personuppgiftshantering enligt dataskyddsförordningen saknas. Man har inte heller försäkrat sig om att dataskyddsombudet inte har några intressekonflikter kring andra uppgifter och ansvar. Kommunen har inte försäkrat sig om att dataskyddsombudet får det stöd och resurser som krävs för att kunna utföra de uppgifter som fastställs i dataskyddsförordningen.	1,9
Behandling av person-uppgifter	Kommunens nämnder och förvaltningar är ansvariga att föra uppdaterade och omfattande register över alla personuppgifter de hanterar i Draft-it. Det saknas däremot kontroller för riktighet och fullständighet av registerförteckningen. Det finns exempelvis inga 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. I dagsläget genomförs inga regelbundna tester, undersökningar eller utvärderingar av de tekniska åtgärder som vidtagits för att garantera säkerheten i behandling av personuppgifter, men regelbundna behörighetskontroller i alla system håller på att utarbetas.	Ändamålet och den rättsliga grunden till behandlingen av personuppgifter är inte dokumenterad för samtliga registrerades personuppgifter. 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. Kommunen utför inga interna kontroller, tester eller uppföljning av tekniska dataskyddsåtgärder eller behörighetsstrukturer.	1,78

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	Kommunen använder SKL:s verktyg KLASSA för att klassificera IT-system utifrån kraven i dataskyddförordningen. Bortsett från informationsklassning av IT-system görs klassning sporadiskt snarare än omfattande inom kommunens verksamheter. Informationsklassificering görs inte regelmässigt för på strukturerad information på dokumentnivå eller för ostrukturerad information. Kommunen tillhandahåller utbildning inom dataskyddsförordningen, förvaltningsrätt och offentlighet- och sekretesslagen. Information om dessa utbildningstillfällen ges till nyanställda vid deras introduktion. Utbildningarna är inte obligatoriska och slutförande följs därför inte upp systematiskt. I övrigt informeras anställda om utbildningstillfällen på kommunens intranät. Generellt är utbildningsnivån inom personuppgiftshanteringen förhållandevis låg.	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. Kommunen har inte etablerat en process som säkerställer att internutbildningar om dataskyddsförordningen uppdateras och genomförs regelbundet av nyanställda såväl som av befintliga anställda.	1,79
Inbyggt dataskydd	SKL:s KLASSA-ramverk används vid nyanskaffning för att bedöma att kommunens databehandling uppfyller kraven för personuppgifter, vilket även resulterar i viss lagrings- och uppgiftsminimering vid ny upphandling. Lagring- och uppgiftsminimering för befintliga system sker informellt- enligt dialog inom säkerhetsteamet då riktlinjer eller rutiner gällande detta inte har förankrats. Kommunen har genomfört vissa åtgärder i sina system för att leva upp till kraven på inbyggt dataskydd i insamlingen, exempelvis har kryptering och varning vid användning av personuppgifter i Office 365 har implementerats. För att begränsa tillgången till personuppgifter i system används säkerhetsgrupper i AD för åtkomst till alla applikationer som driftas internt i kommunen. Dock har flera SaaS-tjänster som inte är kopplade till AD upphandlats, vilket ökar risken för obehörig tillgång till personuppgifter. Regelbundna behörighetskontroller håller på att framtas.	Det finns en generell brist av struktur på informationsförvaltningsområdet då fasta rutiner, kontroller och uppföljning saknas för befintliga IT-system. Det saknas omgivande tester och uppföljning av behörighetsåtkomster i IT-system.	2,50

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	Kommunen tillämpar ansvarsprincipen, vilket innebär att nämnder och förvaltningar själva svarar för att information behandlas och förvaras på ett lämpligt sätt. Då det finns brister i uppföljning och kontroll kring hur detta fungerar i praktiken är kännedomen om vilka personuppgifter som är tillgängliga för eller tillhandahållna till leverantörer relativt låg, för kommunen centralt. Vissa leverantörsavtal ligger kvar i ett gammalt IT-system som inte migrerats korrekt och diarieföreningen är ofullbordad. Vid nya upphandlingar ställer kommunen krav på samverkansforum för att kunna följa upp systemet och att avtalad funktionalitet levereras på ett strukturerat vis. I nuläget finns ett fåtal sådana forum. Uppförande av personuppgiftsbiträdesavtal som komplement till leverantörskontrakt skrivs för nya upphandlingar. För flertalet befintliga system finns personuppgiftsbiträdesavtal med antagande att även gälla utifrån nya förordningar, varför kompletteringar inte alltid har ansetts nödvändiga. SKL:s inventeringslista i KLASSA används för att bedöma om biträdet följer förordningen, men det saknas metoder för att säkerställa att relevanta krav och klausuler är integrerade i kontrakt. Kommunen granskar inte heller att biträden följer kraven i dataskyddsförordningen över tid.	Personuppgiftsbiträdesavtal finns inte till 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 arbetsmetod som kontrollerar att personuppgiftsbiträdesavtal uppdateras vid legala eller interna förändringar.	1,4
Hantering av incidenter	Kommunens dataskyddsombud och informationssäkerhetsstrateg utgår från Datainspektionens rapporterings- och utvärderingsmall för personuppgiftsincidenter, men saknar en tydligt definierad process eller rutin för att identifiera, rapportera, bedöma, avhjälpa och (där så är lämpligt) rapportera integritetsincidenter. Denna ostrukturerade uppföljning är mycket tidskrävande och resulterar i att kommunen har svårt att rapportera incidenter till Datainspektionen inom 72 timmar, vilket är ett krav, om det skulle anses nödvändigt. Utöver lokala systemförvaltningsforum där informationssäkerhet diskuteras, saknas styrning och rutiner som kontrollerar att instruktioner gällande personuppgiftsincidenter efterlevs. Nyckelpersoner inom kommunens dataskyddsarbete misstänker att många personuppgiftsincidenter inte rapporteras då kunskapsnivån om dataskyddsförordningens lagar och förpliktelser varierar inom kommunen.	Kommunen saknar en tydligt definierad process eller rutin för att identifiera, rapportera, bedöma, avhjälpa och (där så är lämpligt) rapportera integritetsincidenter. Styrning och rutiner som säkerställer att kommunens medarbetare har den kunskapsnivå om dataskyddsförordningens lagar och förpliktelser som krävs för att identifiera och rapportera personuppgiftsincidenter fattas.	1,73

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	Kommunhuset använder sig av SKL:s mall för information till den registreras vid insamlingen av personuppgifter och rekommenderar verksamheter att göra detsamma. Kommunen samlar nästintill enbart in personuppgifter på laglig grund. 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: Ett samtycke ska samlas in för varje enskilt användningsområde. Rutiner för att kontrollera att samtycken används på korrekt sätt har inte förankrats. Det finns ingen process för hur verksamheten kommunicerar med de registrerade vid personuppgiftsincidenter eller förändring av kommunens hantering av personuppgifter.	Ändamålet och den rättsliga grunden till behandlingen är inte dokumenterade till alla behandlingar av personuppgifter. Det saknas rutiner och/eller kontroller som säkerställer att personuppgifter endast behandlas för de ändamål som de samlades in för. Det saknas en process för hur kommunen kommunicerar möjliga förändringar i hur man hanterar personuppgifter eller incidenter som berör registrerade.	1,50
Begäran från registrerade	Kommunen har en tydlig kontaktväg där registrerade kan framföra förfrågningar och klagomål via sin hemsida. Rutiner och en säker e-tjänst där den registrerade kan ta del av sina personuppgifter med e-legitimation är under utveckling i dagsläget. I nuläget måste legitimation uppvisas på kommunhuset för att få en utskriven kopia av sina personuppgifter som kommunen har registrerade. För närvarande saknar kommunen möjligheten att extrahera informationen i ett maskinläsbart format. Begäran från registrerade tillhandases kommunens dataskyddsombud och informationssäkerhetsstrateg som hanterar förfrågningarna ad-hoc. Det finns inga fastställda rutiner för hantering av förfrågningar gällande felaktiga, inte längre behövande, eller radering av personuppgifter. Trots att rätten att bli bortglömt är delvis begränsad då personuppgifter är nödvändiga för att kunna fullgöra kommunens myndighetsutövning, finns inga det riktlinjer för att avgöra om den registrerads begäran anses vara ogrundad. Delegationsordningen reglerar däremot vem som får göra bedömningen.	Det finns ingen fastställd rutin för hantering av förfrågningar gällande felaktiga, inte längre behövande, eller radering av personuppgifter. En tydlig ansvarsdelegering och process för att avgöra om en registrerads begäran är ogrundad finns inte dokumenterad.	1,89
Profilering	Kommunen har inget behov av att utföra profilering då automatiserad behandling inte används inom de kommunala verksamheterna.		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

2.2. Övergripande rekommendationer

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

Styrning och styrdokument

För att säkerställa att processer och rutiner beträffande hantering av personuppgifter i enlighet med kraven från dataskyddsförordningen dokumenteras, förankras och kommuniceras på en kommunövergripande nivå rekommenderas Upplands-Bro kommun att uppdatera sin nuvarande informationssäkerhetspolicy från 2010. Policyn bör beskriva syftet med kommunens dataskyddsarbete och innehålla en strategi för kommunens informationssäkerhetsarbete som kan förankras från politisk nivå hela vägen ner i verksamheterna. I nuläget saknas sådana riktlinjer för processer och rutiner beträffande hanteringen av personuppgifter inom i stort sett samtliga av de 12 undersökta områdena från en kommunövergripande nivå. Kommunen rekommenderas även implementera en rutin för att följa upp att verksamheterna efterföljer de regler och policys som är fastställda i styrdokumentet efterlevs.

Organisation och ansvarsfördelning

Den uppdaterade informationssäkerhetspolicyn bör även innehålla en formell, informationssäkerhetsspecifik organisationsstruktur med tillhörande roller och tydlig ansvarsfördelning för att undvika överarbetsbelastning och personberoende. Kommunen bör avsätta resurser specifikt för att utveckla sitt dataskyddsarbete, baserat på rådande situation och hotbild. En tillräckligt stor organisation saknas för att utföra gap-analyser av utvecklingsområden, skapa tillhörande rutiner och processer, och sedan granska efterlevnaden av de processer som implementerats. Upplands-Bro kommun rekommenderas därför även att fastställa en åtgärdsplan inkluderande tidsplan och ansvarig person för att åtgärda eventuella gap där dataskyddsförordningen inte efterlevs.

Granskning och rapportering

Begränsad uppföljning av verksamheternas informationssäkerhetsarbeten medför risk för att nämndernas och förvaltningarnas dagliga informationshantering avviker från sättet som Kommunstyrelseförvaltningen anvisar och tror att arbetet bedrivs på. Kommunen rekommenderas därför att implementera en granskningsplan för att utvärdera och säkerhetsställa att man uppfyller relevanta krav på hantering av personlig information samt en formell rutin för att dokumentera och rapportera resultat till ledningsnivå. Kontroller av kommunens dataskyddsarbete kan exempelvis integreras i kommunens och nämndernas internkontrollarbete. Kommunen 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 till ledningen.

Leverantörsrelationer

Kommunen rekommenderas att göra en ny inventering av samtliga IT-system och tjänster som behandlar personuppgifter och som tillhandahålls till leverantörer. Denna kartläggning kan

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

användas som grund för kommunens fortsatta arbete med att ingå personuppgiftsbiträdesavtal med externa leverantörer. Kommunen rekommenderas att komplettera kontrakt så snart som möjligt för att fastställa rättigheter och skyldigheter enligt dataskyddsförordningens krav. Kommunen kan fortsätta att använda SKL:s mall för personuppgiftsbiträdesavtal och SKL:s checklista vid upprättandet av personbiträdesavtalen för att kvalitetssäkra att avtalsmallen innehåller relevanta avtalspunkter och krav utifrån dataskyddsförordningen. Checklistan 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 kommunens användare besitter otillräcklig kunskap för att på daglig basis hantera kommunens information på ett ändamålsenligt och säkert sätt. EY rekommenderar därför att kommunen tillser att informationssäkerhetsrelaterad dokumentation kommuniceras aktivt till kommunens användare med en bestämd frekvens. Medarbetares bristande medvetenhet är även en mycket vanlig källa till informationssäkerhetsrelaterade incidenter och därför rekommenderas kommunen att följa upp att den obligatorisk utbildning av nyanställda slutförs samt införa vidareutbildning och uppföljning av befintliga medarbetares deltagande. Att ta del av informationssäkerhetspolicyn bör ingå i denna utbildning.

2.3. Upplands-Brohus

Upplands-Brohus har inkluderats i ovanstående analys då nulägesbilden i bolagets efterlevnad av dataskyddsförordningen i stor utsträckning överensstämmer med Upplands-Bro kommun som helhet. Nedan följer en fristående sammanfattning av EYs granskning av Upplands-Brohus.

Upplands-Brohus är ett bostadsföretag som ägs av Upplands-Bro kommun. Bolaget agerar dock självständig vis-a-vis kommunen och har en relativt låg samverkan med resterande kommunala verksamheter. Bolaget har knappt 40 anställda.

Bolaget påbörjade sitt arbete kring nya dataskyddsförordningen under våren 2018 med en introduktionsutbildning för alla anställda. Därefter genomfördes en initial gap-analys av bolagets hantering av personuppgifter utefter dataskyddsförordnings krav. Exempelvis inventerades personuppgiftshantering i IT-system, varav registerförteckningar av personuppgifter och personuppgiftsbiträdesavtal med flertalet leverantörer upprättades. Bolaget har däremot inte implementerat en åtgärdsplan för de gap som identifierades eller etablerat processer som säkerställer att dataskyddsförordningen efterlevs över tid inom bolaget såväl som av leverantörer. Riskanalyser eller konsekvensbedömningar för informationssäkerhet har inte heller genomförts.

En uppdaterad informationssäkerhetspolicy med tillhörande organisationsstruktur och riktlinjer för processer som är utformade i linje med dataskyddsförordningens krav saknas för bolaget. Inget dataskyddsombud har utsetts sedan bolagets avtal om gemensamt dataskyddsombud med kommunens verksamheter löpte ut. En analys eller beslutande om bolaget behöver ett dataskyddsombud har inte utförts. Det är av yttersta vikt att bolaget skapar en formell organisationsstruktur med en tydlig ansvarsfördelning för att säkerställa att granskning av efterlevnad inte faller mellan två ansvarsområden. Bolaget bör även förankra sina informella processer eller tankegångar över hur exempelvis incidenter eller förfrågan bör hanteras i officiella styrdokument och policys, vilka kan användas som grund för interna kontroller av efterlevnad.

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 är restriktivt vid insamling av uppgifter och registrerar som regel inte några känsliga personuppgifter. Personuppgifter ska samlas in på laglig grund, varav registrerade blir väl informerade om hur deras personuppgifter kommer användas och i vilket syfte. Däremot saknas en fastställd plan för att utvärdera och säkerställa att man uppfyller krav på hantering av personlig information. Bolaget har däremot tydliga arkivering- och gallringsrutiner och behörighetsbegränsningar i IT-system för att reducera risken för obehörig behandling av personuppgifter inom verksamheten.

Liksom för Upplands-Bro kommun i helhet ligger bolagets främsta förbättringsområden inom att:

- Dokumentera rutiner och processer beträffande hantering av personuppgifter i styrdokument som är i linje med dataskyddsförordningens krav.
- Fastställa en granskningsplan för att utvärdera och säkerställa att man uppfyller relevanta krav på hantering av personlig information och efterlever de rutiner som har implementerats.
- Framta och dokumentera en formell informationssäkerhetsspecifik organisationsstruktur med tillhörande roller och tydlig ansvarsfördelning.
- Genomföra en analys och ta ett beslut gällande om bolaget behöver ett dataskyddsombud. Om inget ombud anses nödvändigt, ska dennes ansvarsområden fördelas vidare till andra personer i dataskyddsorganisationen.
- Utföra en omfattande inventering av samtliga IT-system och tjänster som behandlar personuppgifter och som tillhandahålls till leverantörer och sedan upprätta personuppgiftsbiträdeskontrakt med alla berörda 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

3. Slutsatser

Syftet med granskningen har varit att genomföra en övergripande kartläggning av huruvida Kommunstyrelsen för Upplands-Bro Kommun har tillsett att arbetet kring personuppgiftshantering är i enlighet med dataskyddsförordningen. Kommunen bedöms i relation till andra offentliga organisationer av liknande storlek i förhållande till antal anställda och övergripande verksamhet. Vår övergripande bedömning är att Upplands-Bro kommun har en förhållandevis låg mognadsgrad, med ett snitt på 1,75, på en femgradig skala. Mognadsgraden bedöms vara som högst inom information till registrerade och inbyggt dataskydd. Lägst är mognadsgraden inom kontroll, styrning, riskhantering och hantering av leverantörsrelationer.

Kommunens största och viktigaste förbättringspunkter ligger i att upprätta en formaliserad och informationssäkerhetsspecifik organisationsstruktur med tillhörande roller, tydlig ansvarsfördelning. Majoriteten av styrdokument och policys är utdaterade och bör uppdateras för att sätta en struktur i kommunens dataskyddsarbete. Kommunen bör även arbeta proaktivt med riskhantering och upprätta personuppgiftbiträdesavtal med leverantörer för att minska risker för integritetsincidenter och ogiltig behandling av personuppgifter inom sina verksamheter såväl som hos leverantörer. Vidare finns ett behov av att införa styrande rutiner och processer för granskning och uppföljning inom i stort sett samtliga av de 12 undersökta områdena, både för kommunen i helhet och för Upplands-Brohus. Slutligen behöver Upplands-Brohus utföra en analys om ett eget dataskyddsombud behövs och dokumentera ett besluttagande. 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 2 december 2019

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

4. Bilaga 1: Förteckning över intervjuade funktioner

4.1. Upplands-Bro Kommun

- Informationssäkerhetsstrateg
- Dataskyddsombud/Kommunjurist
- IT-chef

4.2. Upplands-Brohus

- Ekonomichef
- IT-strateg

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. Bilaga 2: Dokumentförteckning

5.1. Upplands-Bro Kommun

- Riktlinjer för hantering av arkiv, 2018
- Protokollsutdrag från Kommunstyrelsens sammanträde den 5 december 2018, §34 Intern kontrollplan 2019 för Kommunstyrelsen
- Protokollsutdrag från Kommunstyrelsens sammanträde 25 september 2019, §101 Dataskyddsombudets årsrapport
- Intern kontrollplan 2019 för Kommunstyrelsen
- Intern kontrollplan 2019 för Kommunstyrelsen (tabell)
- Policy för informationssäkerheten i Upplands-Bro kommun, 2010
- Informationssäkerhetsinstruktion för medarbetare, 2016
- Informationssäkerhetsinstruktion för systemförvaltning, 2010
- Informationssäkerhetsinstruktion för kontinuitet och drift, 2010
- Handlingar till Kommunstyrelsens sammanträde 6 mars 2019
- Digitaliseringsstrategi, 2019
- Dataskyddsombudets årsrapport 2018
- Dataskyddsombudets årsrapport
- Delegationsordning för kommunstyrelsen, 2018
- Säkerhetsskydd, informationssäkerhet och dataskydd, 2019

5.2. Upplands-Brohus

- Policy för informationssäkerheten i Upplands-Bro kommun, 2010
- Att behandla personuppgifter enligt GDPR, 2018
- Övningsuppgifter till att behandla personuppgifter enligt GDPR, 2018
- Svar till övningsfrågor till att behandla personuppgifter enligt GDPR, 2018
- Anmälan av personuppgiftsincident (blankett)
- Behandling av personuppgifter för lokalhyresgäster, 2018
- Behandling av personuppgifter vid bostadsuthyrning, 2018
- GDPR registerförteckning
- Dokumenthanteringsplan, 2015

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 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 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 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.

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.