Kommunstyrelsen
Jörgen Sandström
Epost: jorgen.sandstrom@vasteras.se

Kommunstyrelsen

Kopia till
Västerås stads revisorer, förskolenämnden, grundskolenämnden, utbildnings- och arbetsmarknadsnämnden, nämnden för personer med funktionsnedsättning, äldrenämnden, tekniska nämnden

Tjänsteutlåtande - Revisionsrapport 2020:5 - Granskning av efterlevnad av GDPR, dataskyddsförordningen - Västerås stad

Förslag till beslut

Förslag till kommunfullmäktige:

1. Förslag till yttrande daterat den 2021-10-21 antas och överlämnas till Västerås stads revisorer.
2. Revisionsrapporten läggs till handlingarna.

Ärendebeskrivning

Ernst & Young (EY) har på kommunrevisionens uppdrag genomfört en granskning av stadens hantering av personuppgifter och efterlevnad av GDPR. Granskningens syfte har varit att kunna bedöma staden övergripande status avseende dataskyddsarbetet. Därför har stadens Dataskyddsombud samt representanter från vård- och omsorgsförvaltningen, barn- och utbildningsförvaltningen och teknik- och fastighetsförvaltningen intervjuats, och respektive förvaltnings och dataskyddsombudens dokumentation har granskats.

EY:s bedömning är att stadens generella mognadsgrad avseende dataskyddsarbetet är något högre jämfört med andra kommuner. Dock anser man att arbetet främst kopplat till kontroll och utbildning behöver förstärkas.

Stadsledningskontoret tar till sig revisionens slutsatser och rekommendationer i det fortsatta arbetet och bedömer att dataskyddsarbetet i Västerås stad utvecklas på ett betryggande sätt.

Stadsledningskontoret har till kommunstyrelsen lämnat följande förslag till beslut:

Förslag till kommunfullmäktige:

1. Förslag till yttrande daterat den 2021-10-21 antas och överlämnas till Västerås stads revisorer.
2. Revisionsrapporten läggs till handlingarna.

Beslutsmotivering

EY konstaterar i sin granskningsrapport att Västerås stad har en något högre mognadsgrad än övriga kommuner de granskat. Man konstaterar att staden har ett väl utvecklat arbete med informationssäkerhet där riskhantering sker genom en väl utarbetad process för systemsäkerhetsanalyser och förvaltningarna får ett gediget stöd från stadsledningskontorets funktioner. Avseende dataskyddsorganisationen anser man att kunskapsnivån är hög och att arbetssättet är strukturerat. Man bedömer att arbetet är väl utvecklat och utifrån en tydlig organisation.

Förbättringspotentialen anser EY ligger i att utveckla arbetet med kontroll och utbildning. Man rekommenderar fler granskningar av de personuppgiftsansvarigas regelefterlevnad, samt fler utbildningsinsatser.

Västerås stad instämmer i ovanstående av EY:s slutsatser och rekommendationer. Man redogör också i rapporten för de rekommendationer som redan är genomförda, och de som är planerade.

I Västerås stad är varje nämnd och styrelse ansvarig för sina respektive personuppgiftsbehandlingar. I det avseendet finns ingen hierarki eller liknande. Om en nämnd brister i sitt dataskyddsarbete är det inte kommunstyrelsens sak att granska detta eller komma med förslag på åtgärder, utan granskning och tillsyn sker via Dataskyddsombud, tillsynsmyndighet och domstolar.

För att hantera detta i praktiken så samordnas det operativa arbetet genom dataskyddsombuden som säkerställer att man drar nytta av varandras kompetenser och resurser, men är noga att hålla på de formella gränserna så att det inte uppstår otydligheter kring ansvaret.

Genom att arbeta med ett resultatfokus där det skett stegvisa förbättringar har de goda resultaten nåtts hittills. Arbetet har utgått från ett ”bottom-up”-perspektiv där Dataskyddsombuden utbildat, skapat kunskapsflöden, utvecklat mallar, processer och byggt relationer med de personer som de facto har mest inflytande på stadens dataskyddsarbete och personuppgiftsbehandlingar.

I rapporten påpekas att Västerås stad har ett antal äldre system som inte är helt anpassad för GDPR. Dataskyddsarbete är ett ständigt pågående utvecklingsarbete och vi har valt att prioritera långsiktighet. Bedömningen är att ändra mer än nödvändigt i befintliga system och leverantörsavtal kostar väldigt mycket resurser, och utfallet är normalt sett ganska magert. Därför prioriterar vi arbete med nya system/nya inköp av system. Därmed kommer vi, med en rimlig resursåtgång, att succesivt förbättra både systemens funktionalitet, tekniska uppbyggnad och avtalsvillkoren.

Sammantaget är bedömningen att dataskyddsarbetet i Västerås stad utvecklas på ett betryggande sätt. Det är ett utvecklingsarbete där vi ser det som naturligt att alla delar inte är klara på en gång. Det är också ett arbete där förutsättningarna kontinuerligt förändras, och därför kommer arbetet aldrig att bli färdigt i strikt mening. Utifrån dataskyddsombudens resonemang i deras yttrande är det dock tydligt att fortsatt utveckling i linje med de flesta

av rekommendationerna i EY:s rapport dels redan är genomförd, dels är planerad.

Juridisk bedömning

Kommunstyrelsen är behörig att fatta beslut i ärendet.

Ekonomisk bedömning

Förslaget beslut har inga ekonomiska konsekvenser.

Hållbar utveckling

Perspektivet är ej relevant med anledning av ärendets karaktär och innehåll.

Helene Öhrling	Jörgen Sandström
Stadsdirektör	Digitaliseringsdirektör

Granskning av efterlevnad av
Dataskyddsförordningen GDPR
På uppdrag av de förtroendevalda revisorerna
Västerås stad

Dokumentnummer 2020:5

Dnr 2020/00967

Västerås stad

Granskning av efterlevnad Dataskyddsförordningen GDPR

Oktober 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 Västerås stads förtroendevalda revisorer genomfört en granskning av kommunens hantering av personuppgifter och efterlevnad av dataskyddsförordningen (The General Data Protection Regulation, GDPR).

Granskningens syfte har varit att ge en övergripande förståelse av huruvida kommunen, d.v.s. kommunstyrelsen och övriga nämnder, bedriver ett ändamålsenligt arbete med dataskyddsförordningen och hur väl man uppfyller de åtgärder som förordningen stipulerar. Analysen har baserats på intervjuer med identifierade nyckelpersoner i verksamhetens personuppgiftssäkerhetsarbete samt genomgång av insamlad styrdokumentation. Intervjuer har skett med stadens dataskyddsombud (DSO) och informationssäkerhetsstrateg samt med de tre utvalda förvaltningarna Vård- och omsorgsförvaltningen (VOF), Barn- och utbildningsförvaltningen (BUF) samt Teknik- och fastighetsförvaltningen (TFF). Förvaltningarna valdes för att få ett representativt urval av kommunens verksamheter, med fokus på både de mest kritiska förvaltningarna (VOF och BUF) samt en mindre kritisk (TFF) vad gäller personuppgiftshantering. Analys och iakttagelser har faktagranskats av de identifierade nyckelpersonerna.

En översiktlig granskning av 12 olika områden med utgång i EY:s ramverk för personuppgiftshantering gentemot dataskyddsförordningen för kommunala verksamheter har genomförts under juni till september 2020. Enligt metoden bedöms verksamhetens 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 Västerås stad ha den genomsnittliga mognadsgraden 3,1 av 5,0. 3,1 är en något lägre mognadsgrad än vad EY rekommenderar för en kommun, givet den stora mängd personuppgifter och känsliga personuppgifter som hanteras inom förvaltningarna, men något högre än vad EY generellt observerar för kommuner.

Kommunen har lagt mycket resurser på arbetet med informationssäkerhet vilket avspeglas i ett en väl utvecklad organisation och rutiner. Kunskapsnivån inom dataskyddsorganisationen är hög och de ansvariga arbetar överlag strukturerat med dataskyddsfrågor. Således bedöms mognadsgraden vara högst inom organisation och ansvar, samt de två rutintunga områdena behandling av personuppgifter och riskhantering.

Rapportens huvudsakliga iakttagelse berör området kontroll. Kommunens granskning och rapportering inte har utvecklats i samma takt som övrigt arbete och i dagsläget saknas granskning av förvaltningarnas arbete med personuppgiftssäkerhet i stort sett helt. Det finns varken internkontroller inom förvaltningarna som tydligt täcker in de olika aspekterna av dataskyddsarbetet, eller granskningar från centralt håll. Detta bidrar till att den faktiska efterlevnaden av rutiner för personuppgiftshantering är oklar. Viktigt att notera är att EY i och med denna rapport har granskat utformningen av organisationen, ramverk och rutiner, men inte tagit stickprov på hur väl denna struktur efterlevs i praktiken. Verksamheten bör införa kontrollrutiner, där granskningar för personuppgiftshantering genomförs regelbundet och

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

rapportering sker mellan förvaltningarna, dess nämnder, DSO och kommunledningen. Genom att införa mer strukturerade analyser och åtgärdsplaner kommer även arbetet inom övriga områden förbättras ytterligare.

Den samlade bilden är således att kommunen initialt valt att prioritera införande av fungerande processer genom verksamheten, vilket EY bedömer har fungerat väl, men att det nu är hög tid att införa strukturerade granskningar och rapportering i relation till arbetet. EY rekommenderar vidare att kommunen inför regelbundna utbildningsinsatser inom GDPR samt att de mest kritiska verksamheterna tydliggör sin strategi för utbildningsinsatser och medvetenhet hos sina medarbetare och inför åtgärder därefter.

EY har även genomfört en separat granskning av kommunens bolagskoncern. Anmärkningsvärt är att Västerås stad trots helägarskap i flera av bolagen inte i en betydande grad har samordnat arbetet med personuppgiftssäkerhet med bolagen. Iakttagelserna kring detta återfinns i den separata granskningsrapporten.

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

Sammanfattning **1**

1. Inledning **3**

1.1. Bakgrund 3
1.2. Syfte 3
1.3. Avgränsning 4
1.4. Metod 4
1.5. Definitioner 6

2. Analys **7**

2.1. Nuläge och iakttagelser 10
2.2. Övergripande rekommendationer 22

3. Revisionsfrågor **24**

4. Slutsatser **26**

5. Bilaga 1: Förteckning över intervjuade funktioner **27**

5.1. Centrala dataskyddsorganisationen 27
5.2. Barn- och utbildningsförvaltningen 27
5.3. Vård- och omsorgsförvaltningen 27
5.4. Teknik- och fastighetsförvaltningen 27

6. Bilaga 2: Dokumentförteckning **28**

6.1. Centrala dataskyddsorganisationen 28
6.2. Barn- och utbildningsförvaltningen 28
6.3. Vård- och omsorgsförvaltningen 29
6.4. Teknik- och fastighetsförvaltningen 30

7. Bilaga 3: Definitioner **31**

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 Västerås stad med dess verksamheter hanterar stora mängder personuppgifter, har de förtroendevalda revisorerna beslutat att genomföra en granskning av efterlevnaden av dataskyddsförordningen för kommunen som helhet.

1.2. Syfte

Syftet med granskningen är att ge en övergripande förståelse av huruvida Västerås stad bedriver ett ändamålsenligt arbete med dataskyddsförordningen och hur man uppfyller de åtgärder som förordningen stipulerar.

Granskningen ska svara på följande tre revisionsfrågor:

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

- Uppfyller Västerås stad de krav och regleringar för personuppgiftshantering som har införts i och med dataskyddsförordningen (GDPR)?
- Är Västerås stads policyer och riktlinjer ändamålsenliga för att uppnå regelefterlevnad med avseende på dataskyddsförordningen (GDPR)?
- Har Västerås stad ändamålsenlig kontroll och uppföljning av arbetet med dataskyddsförordningen (GDPR)?

1.3. Avgränsning

De iakttagelser och rekommendationer som presenteras i denna rapport baseras enbart på den information som inhämtats under intervjuer och genom granskning av erhållna dokument, såsom riktlinjer, rutiner och policys. Granskningen utgår från arbetet som kommunen bedriver på central nivå men inkluderar även arbetet som bedrivs inom följande utvalda nämnder: Förskolenämnden, Grundskolenämnden, Utbildnings- och arbetsmarknadsnämnden, Nämnden för personer med funktionsnedsättning, Äldrenämnden, Tekniska nämnden och Fastighetsnämnden. Dessa granskades genom intervjuer med deras förvaltningar Barn- och utbildningsförvaltningen (BUF), Vård- och omsorgsförvaltningen (VOF) och Teknik- och fastighetsförvaltningen (TFF). 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 centrala dataskyddsorganisationen och de utvalda nämnderna samt genomgång av relevant styrdokumentation (se 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 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:

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. Styrande dokument/styrning
2. Riskhantering
3. Kontroll
4. Organisation och ansvar
5. Behandling av personuppgifter
6. Val av skyddsåtgärder
7. Inbyggt dataskydd
8. Hantering av leverantörsrelationer
9. Hantering av incidenter
10. Information till registrerade
11. Begäran från registrerade
12. Profilering

Mognadsgrad beskrivs på en standardiserad skala enligt nedan:

1. Begynnande – Det finns ingen dokumentation eller uppföljning, händelser hanteras ad hoc.
2. Upprepbar – Viss grundläggande dokumentation finns, men denna kan variera mellan olika enheter och vara bristfällig i sin omfattning och tillämpning.
3. Definierad – Det finns dokumenterade processer och dessa tillämpas i stor mån genom hela organisationen.
4. Förvaltad – Förutom väl dokumenterade processer som tillämpas i hela organisationen, finns det dessutom ett system för uppföljning.
5. Optimerad – Baserat på uppföljningen finns också rutiner för kontinuerlig förbättring och uppdatering av processer och ramverk.

Ett områdes färgkod visar en genomsnittlig mognadsgrad som beräknas över alla krav som ingår i området. Respektive krav har inte viktats. Mognadsgraden per område indikerar vilka områden som har störst förbättringsbehov, men på grund av genomsnittsberäkningen kan 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 EY:s GDPR-specialister ett arbetsmöte med nyckelpersoner inom respektive granskad verksamhets informationssäkerhetsarbete (se Bilaga 1: *Förteckning över intervjuade funktioner*). Under arbetsmötena avhandlades samtliga 12 områden. Efter att EY analyserat resultatet av arbetsmötena sammanställdes ett rapportutkast som faktagranskades av de intervjuade. EY genomförde sedan justeringar och uppdateringar av rapporten som även kvalitetssäkrades av EY:s verksamhetsrevisorer, varefter de förtroendevalde revisorerna på kommunen erhöll en slutlig rapport med övergripande rekommendationer för fortsatt arbete.

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

Tidsplanen för arbetet såg ut enligt följande:

- Maj 2020 – Förberedelser, planering och insamling av dokumentation.
- Juni-Augusti 2020 – Dokumentanalys, utförande av arbetsmöten (2020-06-12, 2020-06-22, 2020-08-17 och 2020-08-24), granskning av kompletterande dokumentation och uppföljningsfrågor, färdigställande av rapport, samt faktagranskning av intervjuade nyckelpersoner.
- September 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. Analys

Baserat på utförd granskning konstateras att Västerås stad har en förhållandevis god mognadsgrad inom personuppgiftshantering jämfört med vad EY generellt observerar i offentlig verksamhet av motsvarande storlek och karaktär, även om det återstår arbete inom flera områden.

Från centralt håll har ett i flera hänseenden ambitiöst arbete skett. Det finns en övergripande strategi och styrdokumentation som avseglar sig genomgående i kommunens arbete. Den centrala dataskyddsorganisationen har utifrån de övergripande strategiska målen och GDPR-lagstiftningen utformat gedigna planer för införande av rutiner. Organisationens utformning och ansvarsfördelning mellan de olika delarna av kommunen är välavvägd och bedöms vara resurseffektiv. Det främsta förbättringsområdet är att kommunen inte följer upp arbetet med dataskydd specifikt genom granskning och rapportering, vilket bidrar till att verksamheternas följsamhet till rutinerna i många delar är svårbedömd och att arbetet riskerar att inte bedrivas med den kvalitet kommunen och dess invånare förväntar sig. Från centralt håll kan detta härledas till att prioritet lagts på att införa rutiner och komma i fas med analyser. Dessutom är informationssäkerhetspolicyn inte uppdaterad sedan 2011 och det finns ingen centralt beslutad policy eller motsvarande som innefattar en särskild del tillägnad personuppgifter. En riktlinje är dock för närvarande på delegation för beslut i kommunstyrelsen. En avsaknad av en särskild policy kan bidra till att kommunledningen inte prioriterar dataskydd, missar att inhämta rapportering och att arbetets strategiska inriktning blir alltför personberoende. Ytterligare en iakttagelse av det större slaget är att ca 50 % av kommunens medarbetare inte har genomgått någon utbildning rörande GDPR specifikt, vilket innebär att medarbetare löper högre risk att begå misstag och missa att rapportera incidenter. Varken kommunen från centralt håll eller förvaltningarna har därtill inte heller en utbildningsplan för kontinuerligt uppdaterad medvetenhet och kunskap hos de anställda.

De granskade förvaltningarna, d.v.s. Vård- och omsorgsförvaltningen (VOF), Barn- och utbildningsförvaltningen (BUF) och Teknik- och fastighetsförvaltningen (TFF), täcker in totalt sju nämnder. Nämnderna är enligt direktiv personuppgiftsansvariga, förvaltningarna utför det operativa arbetet, och DSO arbetar stödjande samt har utformat mycket av grunden för dataskyddsarbetet sett till rutiner, mallar och målsättningar. Förvaltningarna har dragit nytta av den centrala styrningen och initiativen. VOF och BUF har dessutom tagit mycket eget initiativ till att följa GDPR och annan lagstiftning som berör personuppgifter, vilket resulterar i en högre mognadsgrad än för TFF. De tre förvaltningarnas arbete kan överlag anses vara ändamålsenligt sett till förvaltningarnas storlek och den mängd personuppgifter varje förvaltning hanterar. De största förbättringspunkterna är, liksom noterades ovan, granskning och utbildning. Förvaltningarnas internkontrollplaner täcker inte in GDPR specifikt och det saknas arbetsrutiner för att följa upp och förbättra verksamheten genom till exempel årsplaneringar med åtgärdsplaner. Särskilt för VOF och BUF är det viktigt att säkerställa att all relevant personal har informerats om GDPR eftersom deras medarbetare i det dagliga arbetet ofta kommer i kontakt med en stor mängd personuppgifter och känsliga personuppgifter. Det noteras även att det återstår att genomföra riskanalyser och informationsklassningar för flera system och behandlingar, men risken förknippat med detta bedöms som lägre då verksamheterna uppger att alla kritiska system är genomgångna.

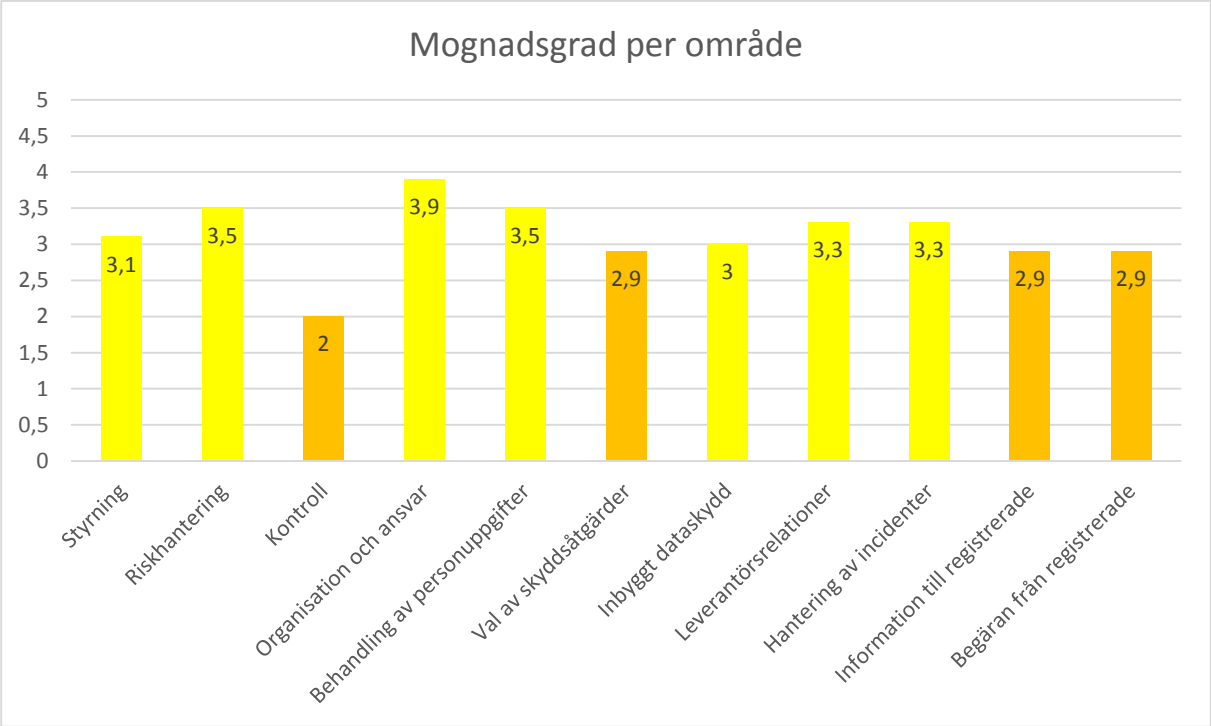
Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

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

Slutligen är det värt att notera att arbetet i begränsad utsträckning har samordnats med de kommunala bolagen, som istället har sökt stöd från annat håll. Bristande följsamhet i de kommunala bolagen riskerar att slå tillbaka på kommunen som helhet. Mer information kring detta återfinns i separat granskningsrapport.

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

Figur 1: Mognadsgrad per område

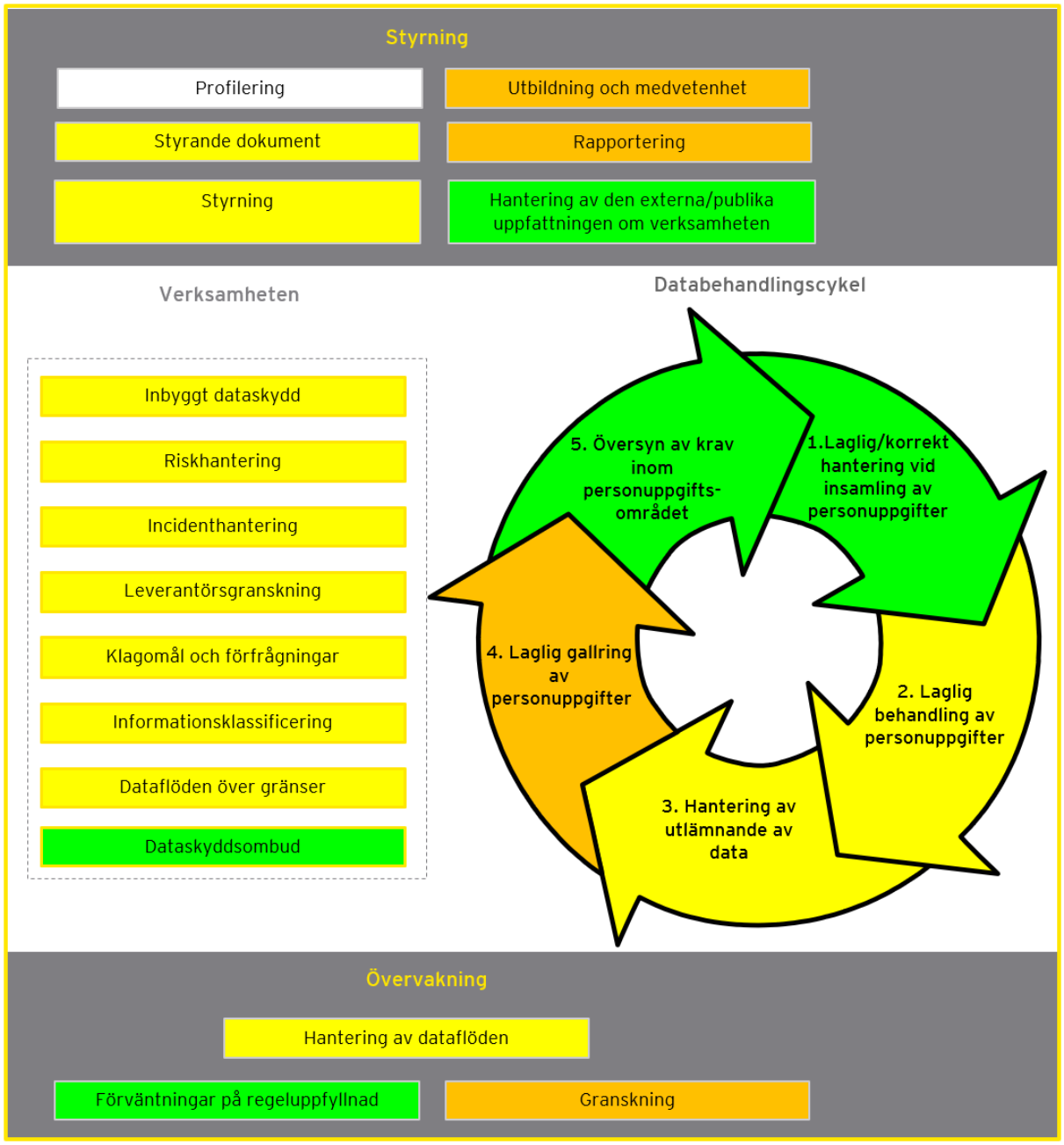


Nivå 5 representerar hög mognadsgrad medan nivå 1 representerar låg mognadsgrad.

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	Västerås stad har en informationssäkerhetspolicy antagen 2011. Den täcker in flera relevanta delar som kan kopplas till arbetet med dataskydd, men nämner inte personuppgifter explicit. En omfattande riktlinje för arbetet med informationssäkerhet antogs 2019. Det finns däremot ingen riktlinje eller annan övergripande styrdokumentation som specifikt behandlar relevanta områden kopplat till personuppgiftssäkerhet och Dataskyddsförordningen och som exempelvis ställer krav på att rutiner inom relevanta områden ska finnas, utöver det som redan täcks in i det generella informationssäkerhetsarbetet. Kommunens DSO och digitaliseringsdirektör har tillsammans utformat och fastställt dokumentet ”Ramverk för dataskyddsarbetet” och i övrigt är beslut om riktlinjer inom området delegerat till digitaliseringsdirektör. Det specificerar ansvar, uppdrag, strategi och principer för utförandet samt instruerar mer detaljerat vad detta innebär, exempelvis genom att tydliggöra dataskyddsombudens arbetsuppgifter. DSO:s arbete styrs övergripande utifrån ett antal strategiska mål, där digitalisering och strategiska avvägningar i metodiken kopplat till dataskydd är i fokus. DSO har utifrån dessa styrande mål och strategier, samt de formella krav som Dataskydds-förordningen anger, själva utformat en årlig verksamhetsplan för sitt arbete inkluderat förbättringsområden och prioriteringar. Kommunledningen har på så sätt fokuserat på en mer långsiktig strategisk styrning som till stor del förlitar sig på DSO:s kompetens för att utforma	Informationssäkerhetspolicyn är inte uppdaterad sedan 2011 och det finns ingen centralt beslutad policy som hanterar personuppgifter eller dataskydd. Det finns inga av kommunledningen fastslagna kommunövergripande riktlinjer för dataskydd. Utformningen av flertalet processer inom dataskydd är till stor del beroende av DSO. För att undvika intressekonflikter vore det optimalt om detta ägs och drivs av någon annan.	3,1

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

	en tydligare styrning för arbetet med personuppgiftssäkerhet specifikt. I praktiken är det värt att notera att denna styrning hittills har genererat betydande resultat avseende processer, dokumenterade rutiner och instruktioner samt övrigt stöd mot förvaltningarna och det praktiska arbetet. Däremot kan det inte uteslutas att DSO:s höga involvering i utformningen av processer och dokumentation skapar en intressekonflikt, eftersom det kan vara svårt att granska processer man själv har designat. De granskade förvaltningarna har ingen ytterligare formell dokumentation av den övergripande styrningen än vad som finns från centralt håll. VOF och BUF har däremot tagit fram specifika instruktioner eller uppdragsbeskrivningar för det operativa arbetet där så har ansetts nödvändigt, vilket är lämpligt då de behandlar en mycket stor mängd personuppgifter och dessutom berörs av fler lagkrav än GDPR. TFF har i större utsträckning enbart förlitat sig på de instruktioner och krav som kommunicerats från centralt håll. Dataskyddsarbetet har i begränsad utsträckning samordnats med bolagen och ingen styrning eller rapportering kopplat till dessa sker i dagsläget. Varje nämnd är personuppgiftsansvarig och ansvarar för sina egna insamlade personuppgifter. Det finns inga fastställda rutiner som beskriver hur behandlingen av personuppgifter går till i praktiken när en nämnd behandlar personuppgifter för vilka en annan nämnd är ansvarig. Dataskyddsombuden har dock diskuterat detta och har tankar kring att formalisera riktlinjer för hur sådan behandling ska ske.	Arbetet med dataskydd har i begränsad utsträckning samordnats med bolagen, som istället har sökt stöd från andra håll. Ingen uppföljning har gjorts av hur behandling av personuppgifter går till i praktiken när en nämnd behandlar personuppgifter för vilka en annan nämnd är ansvarig.	

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	Riskhantering sker enligt en tydligt utformad instruktion för systemsäkerhetsanalys. Denna instruktion täcker in hela processen inklusive informationsklassning, systemsäkerhetsanalys, konsekvensbedömning, hot- och riskanalys, kontinuitetsplanering och uppföljning samt specificerar även ansvarsfördelning inom ramen för arbetet. Instruktionen hänvisar även till mer detaljerade instruktioner och mallar för de olika stegen i processen. Dataskyddsombuden har formella instruktioner att bistå i systemsäkerhetsanalysen vid frågor som berör personuppgiftshantering, exempelvis vid konsekvensbedömningar. Kommunens centrala informationssäkerhetsfunktion med ansvariga medarbetare har som mål att vara involverade i så många systemsäkerhetsanalyser som möjligt, men på grund av det stora antalet system i staden har detta inte varit praktiskt genomförbart. Kommunen har som ambition att riskanalyser ska genomföras för samtliga befintliga system, dock noteras både från centralt håll samt inom BUF att det återstår att utföra flertalet riskanalyser för mindre kritiska system och personuppgiftsbehandlingar. Prioritering har i dessa fall givits av respektive förvaltnings systemförvaltningsansvariga. Kommunen genomför dock alltid systemsäkerhetsanalys för nya system vid upphandlingar och förnyar dessa analyser efter en viss tid där det anses nödvändigt. Det finns en lista över de mest kritiska systemen där den centrala informationssäkerhetsorganisationen stöttar objektsägarna i genomförande av årlig informationsklassning och riskanalys.	Det återstår riskanalyser för flera system och behandlingar.	3,5

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 två DSO är utsedda kontaktpersoner gentemot Datainspektionen för att svara på eventuella förfrågningar och för att rapportera personuppgiftsincidenter. Förvaltningarnas ansvariga har frekvent kontakt med DSO för rådgivning och vägledning. I årets verksamhetsplan för DSO har framtagande av granskningsrapporter kring dataskyddsorganisationens uppbyggnad och incidenter inkluderats som en aktivitet inför hösten. Ingen dokumenterad rapportering har hittills skett, varken till förvaltningar eller till ledning, men är planerade till hösten 2020. Det finns inte heller dokumenterade rapporteringskrav från förvaltningarna eller den centrala organisationen till ledningen. Förvaltningarna själva genomför i nuläget begränsad eller ingen intern granskning av dataskyddsarbetet. BUF och VOF har internrevisioner där de följer upp identifierade risker men personuppgiftsfrågor har inte specifikt behandlats inom ramen för dessa.	Det har hittills inte utförts några oberoende granskningar eller internkontroller med fokus på att dataskyddsarbetet genomförs i enlighet med dataskyddsförordningens krav. Rapporteringskrav är vid tidpunkt för granskningen inte heller definierade.	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	För kommunens övergripande organisation av dataskyddsarbetet finns tydlig dokumentation, både vad gäller ansvarsfördelning och ansvariga roller i dataskyddsorganisationen. Kommunen har två DSO varav den ena är jurist och med ett fokus på digitalisering i arbetet. DSO har stöd av en central informationssäkerhetsstrateg och en rad andra ansvariga ute i verksamheterna, som har tydliga roller i informationssäkerhetsarbetet. Dataskyddsorganisationen har utformats över tid och strukturen ser olika ut i respektive förvaltning. Det råder ännu inte full tydlighet i kommunens verksamheter kring hur rapportering och förfrågningar till och från DSO och övriga intressenter ska ske i samtliga fall. DSO har identifierat och presenterat olika dataskyddsroller som varje förvaltning bör ha. Det råder dock inte full tydlighet kring dessa roller hos samtliga nyckelfunktioner i förvaltningarna och förvaltningarna har ännu inte anpassat organisationen och formaliserat föreslagna dataskyddsroller. Kunskapsnivån i den centrala dataskyddsorganisationen upplevs vara mycket god. Ansvariga i de granskade förvaltningarna har varierande men överlag ändamålsenliga kunskaper, där VOF och BUF utmärker sig med goda personalresurser och medvetenhet kring arbetet med dataskydd. Resurstilldelningen bedöms överlag vara god då de granskade förvaltningarna har genomfört arbete inom de kritiska områdena och har personal tilldelad med avsatt tid till de olika arbetsuppgifterna.	Det har inte implementerats ett konsekvent tänk genom hela kommunen för ansvar och kommunikation mellan olika delar av organisationen, framför allt till och från DSO.	3,9

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	Varje förvaltning ansvarar själva för att upprätta registerförteckning, vilket har gjorts i form av Excelfiler baserat på inventeringsmall från DSO. Dessa filer är omfattande och som stöd till förvaltningarna finns även en detaljerad instruktion och omfattningsbeskrivning med förklaringar till de frågor som måste besvaras i. Informationen i registerförteckningen styr sedan hur personuppgifterna ska behandlas. Förvaltningarna har i nuläget ingen kontrollmekanism för att säkerställa att registerförteckningarna är korrekta och uppdaterade. I framtiden planeras förteckningarna överföras till ett kommungemensamt digitalt verktyg.	Det saknas rutiner för att säkerställa registerförteckningens fullständighet och riktighet över tid.	3,5
	Grunden för gallring ligger i kommunens generella informationshanteringsplan samt beslutad redovisningsplan per nämnd. Det måste finnas ett gallringsbeslut kopplat till planen, unikt för varje system och varje dokumenttyp. För krav i upphandlingar och i PUB-avtal är detta alltid centralt. Systemförvaltare för respektive system ansvarar för gallringen. Det finns dock inga formella kontroller för att detta sker korrekt och det saknas rutiner för att säkerställa att personuppgifter endast behandlas för de ändamål de samlades in för. Dataflöden mellan system dokumenteras i systemsäkerhetsanalysen.	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.	

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	Informationsklassificering sker enligt instruktioner i systemsäkerhetsanalysen. Liksom för arbetet med att genomföra riskanalys har informationsklassning skett för de befintliga system vilka identifierats som kritiska, och ytterligare arbete kvarstår för att täcka in samtliga relevanta system.	Samtlig strukturerad information har inte klassificerats.	2,9
	Det finns kommunövergripande instruktioner för hur man ska klassa ostrukturerad information men det återstår arbete med att säkerställa att respektive förvaltning genomför klassning enligt dessa. Förvaltningarna har till viss del arbetat med att inventera och strukturera ostrukturerad information.	Samtlig relevant ostrukturerad information har inte klassificerats.	
	DSO har vid årsskiftet 2019/2020 genomfört två större målgruppsanpassade utbildningar i dataskydd med ansvariga inom verksamheterna såsom registratorer, nämndsekreterare och upphandlare. Samma utbildning är nu genomförd med objektledare, objektspecialister, tjänsteansvariga och liknande funktioner. Tanken är att dessa utbildningar ska fortsätta och att fler personalgrupper ska beröras.		
	Från centralt håll har alla medarbetare utöver detta fått ta del av en nano-utbildning inom informationssäkerhet online, denna har dock inte inkluderat frågor eller varit obligatorisk att genomföra. Det återstår även ännu att genomföra en utbildning som berör incidenthantering specifikt. Slutligen finns från centralt håll även en mikroutbildning med fokus på GDPR som alla medarbetare har kunnat ta del av. I övrigt är ansvar för utbildning av medarbetare till stor del fördelat ut till nämnderna.	Det finns ingen formell utbildningsplan med obligatoriska utbildningar för alla relevanta medarbetare, exempelvis en årlig kort utbildning med kontrollfrågor att besvara.	
	Förvaltningarna genomför i nuläget begränsat med utbildningsinsatser inom området personuppgiftssäkerhet. BUF har en funktionsbrevlåda dit mycket frågor inkommer, och det anordnas träffar för ansvariga i de olika verksamheterna för uppföljning av relevanta frågeställningar. VOF inkluderar information kring	Förvaltningarna med flest personuppgifter och störst organisationer, har inte infört utbildningsinsatser för alla relevanta medarbetare som skulle kunna behövas för att öka kunskapen i alla verksamheter till välfungerande nivåer.	

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

	personuppgiftssäkerhet i introduktion för nyanställda, dock ej specifikt rörande krav kopplat till GDPR, och anordnar informationsmöten med personalen där de informerar om regler och skyldigheter.		
Inbyggt dataskydd	Möjligheterna till inbyggt dataskydd beaktas framför allt i upphandlingsprocessen, där rutiner finns för att se till att nya system exempelvis inte innehåller onödiga fritextfält för registrerade. DSO har tillsett att inbyggt dataskydd inkluderas i utbildning till systemförvaltare, vilka är ansvariga för att respektive system uppfyller gällande krav. För äldre system vidtas åtgärder för inbyggt dataskydd i viss mån, men det har inte säkerställts att alla system är ändamålsenliga. Från centralt håll prioriteras stöd vid nya upphandlingar men man har även inventerat de mest kritiska systemen för att säkerställa att dessa uppfyller kraven på funktionalitet som krävs för att uppfylla Dataskyddsförordningen. Periodiska genomgångar av behörigheter ska genomföras åtminstone årligen för system klassade som kritiska enligt Västerås riktlinje för informationssäkerhet. För dessa system ska det även finnas behörighetsstrukturer med ett begränsat antal höga behörigheter. VOF har upprättat särskilt gedigen dokumentation inom detta område, vilket är lämpligt med tanke på verksamheten som bedrivs och den mängd personuppgifter som hanteras.	I äldre system är inte åtgärder för inbyggt dataskydd fullt ut implementerade**.**	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

Hantering av leverantörs-relationer	Det finns nyligen uppdaterade och utförliga kommunövergripande instruktioner och mall för PUB-avtal, baserat på SKR:s mall. Inventering för att säkerställa att PUB-avtal tecknats med samtliga relevanta leverantörer har ingått i åtgärdsplanen för GDPR, men det finns inte någon centralt dokumenterad rutin för inventering eller lista som visar att alla nödvändiga PUB-avtal är på plats. Arbetet med att upprätta PUB-avtal skiljer sig för nya och gamla system. För nya system finns det en gedigen upphandlingsprocess där dataskydd och PUB-avtal inkluderas som obligatoriska moment. För äldre system har uppdatering av existerande avtal skett i flera fall, men det återstår arbete för ett antal viktiga system. Förvaltningarna, med objektsägare och avtalsansvariga, ansvarar för kontakten med leverantörer och eskalerar till DSO vid svårigheter. BUF har följt upp säkerhetsarbetet med vissa leverantörer genom att skicka frågor kring processerna för dataskydd hos leverantören. VOF samarbetar aktivt med leverantörerna då de upptäcker brister. I övrigt har det inte noterats att någon dokumenterad uppföljning av leverantörernas dataskyddsarbete sker i kommunen, efter projektet vid införandet av Dataskyddsförordningen 2018, då en genomgång gjordes av samtliga leverantörsavtal. Lagring utanför EU/EES ingår som kontrollmoment vid upphandlingar. Det har blivit aktuellt vid enstaka tillfällen och regleras då i avtalen från fall till fall.	Kommunen saknar PUB-avtal med vissa leverantörer. Det saknas en dokumenterad rutin för att säkerställa att personuppgiftsbiträden långsiktigt agerar i linje med dataskyddsförordningen.	3,3

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

Hantering av incidenter	Det finns centrala väldokumenterade rutiner som beskriver vad en personuppgiftsincident är, roller och ansvar i rapporteringsprocessen samt hur man ska gå tillväga för att rapportera. Det finns tillhörande checklistor och mallar för att dokumentera och vidarerapportera incidenter. DSO har en ledande roll för att bedöma om incidenten ska anmälas till Datainspektionen. Varje förvaltning har en ansvarig med insyn i exempelvis IT-systemen för koordinering gentemot DSO. Det finns en centralt tillsatt incident manager som kopplas in för att se till att incidenten hanteras och inte sker igen. Från centralt håll är man medvetna om att kommunens organisation är komplex och att det kan vara svårt för en enskild anställd att veta vad som faktiskt utgör en incident och hur man ska rapportera. DSO har därför utformat en utbildning som planeras skickas ut till alla anställda och man jobbar även aktivt med att skapa medvetenhet angående kontaktvägar. Ansvaret för incidenthanteringsprocessen ligger på personuppgiftsansvarig, d.v.s. respektive nämnd. Nämndernas förvaltningar har dock inte utformat några ytterligare rutiner eller åtgärder för incidenthantering utöver de som tillhandahållits från centralt håll. Utbildning av medarbetarna har inte skett regelbundet eller dokumenterats, och medvetenheten i verksamheterna kan variera. Det finns inga etablerade rutiner på plats för att kontrollera att de interna instruktionerna eller rutinerna gällande personuppgiftsincidenter efterlevs.	En rutin för att granska efterlevnaden av rutinerna gällande personuppgiftsincidenter saknas. Detta är särskilt aktuellt för identifiering av misstänkta incidenter, vilket ska ske av medarbetarna ute i verksamheterna.	3,3

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

Information till registrerade	Vid insamling av personuppgifter lämnas utförlig information till den registrerade om hur personuppgifterna kommer användas. Information till registrerade lämnas framför allt via kommunens hemsida, till vilken även blanketter och annat material som riktar sig till registrerade hänvisar för mer information. BUF och VOF, vilka i stor utsträckning använder sig av blanketter för insamling av information, har ett pågående arbete med att inventera och uppdatera samtliga blanketter. Texter som uppdateras granskas av DSO. TFF har en separat rutin som hänvisar till deras kundcenter. När samtycke används för insamling av personuppgifter används blanketter vars utformning säkerställer att individernas samtycke bygger på en aktiv handling och är distinkt, tydligt och inte ihopblandat med andra samtycken. Kommunen har överlåtit ansvaret till nämnderna att utforma rutiner för lagring av samtycken och för att möjliggöra för registrerade att dra tillbaka samtycken. Ingen av förvaltningarna har dock kompletta rutiner för detta. Processen för var samtycken lagras och hur de kan dras tillbaka är inte klarlagd.	Kommunen har inte säkerställt att det i efterhand går att visa att samtycke har samlats in från de registrerade. Processen för var samtycken lagras och hur de kan dras tillbaka är inte klarlagd.	2,9

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 central kontaktväg hanterad av DSO där registrerade kan framföra förfrågningar och klagomål via mail och telefon. Kring detta finns utförlig information till registrerade på kommunens hemsida. Via hemsidan finns en blankett som den registrerade kan fylla i för att begära registerutdrag. Begäran skickas sedan till berörd förvaltning, och en mall finns som stöd för verksamheterna att använda för att fylla i den information som efterfrågas. Processen för att samla in samtliga uppgifter är i dagsläget sårbar då den i stor utsträckning är personberoende. Endast systemansvarig har tillgång till eller vet hur utdrag ska gå till för specifika system eftersom det saknas detaljerade rutiner för hur utdragen ska gå till i praktiken. Det systemstöd som planeras införas för att möjliggöra en kommunövergripande registerförteckning skulle även kunna underlätta processen för registerutdrag, vilket förvaltningarna har noterat vore välkommet. Det saknas dokumenterade rutiner för hantering av förfrågningar gällande felaktiga, inte längre behövda, eller radering av personuppgifter.	Det saknas detaljerade rutiner för registerutdrag ur de olika systemen och det har inte skett kvalitetskontroller av registerutdragen. Det finns ingen rutin för att följa dataskyddsförordningens krav om en giltig begäran om ”rätt att bli bortglömd” inkommer.	2,9
Profilering	De granskade förvaltningarna 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

2.2. Övergripande rekommendationer

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

Kontroll

Västerås stad har kommit långt i implementationen av rutiner för säker personuppgiftshantering. Nästa steg för att förbättra arbetet med dataskydd är att utöka kontrollen av verksamheternas efterlevnad. Det bör för varje nämnd finnas dokumenterade rutiner för granskning av efterlevnad av dataskyddsförordningen med tillhörande åtgärdsplaner, som uppdateras på regelbunden basis. Detta kan framförallt ske genom centralt förankrade granskningar med tillhörande åtgärdsplaner godkända av ledningen. Exempelvis skulle DSO kunna införa en rutin för årlig granskning av samtliga förvaltningars dataskyddsarbete, och det bör säkerställas att denna, med tillhörande åtgärdsplaner, medför tillräckligt eftertryck och precision för att säkerställa att förvaltningar som visar sig ligga efter med dataskyddsarbetet åtgärdar problemen inom rimlig tid. Dessutom kan stickprovstestning utökas och ske oftare för att lättare identifiera brister. Stickprovskontroller skulle med fördel kunna utföras för registerförteckning, registerutdrag, gallring, systemsäkerhetsanalys och PUB-avtal. Granskningsresultat bör även kommuniceras till ledningen på regelbunden basis, exempelvis årligen.

Utbildning

Västerås stad genomför för närvarande inte utbildningar regelbundet eller vid nyanställning för alla medarbetare där det vore relevant. Instruktioner, såsom stadens incidenthanteringsdokument, riskerar att bli verkningslösa om inte personalen är medveten om vad som utgör en incident eller att instruktionerna existerar. Dessa instruktioner och rutiner bör kommuniceras regelbundet. Kommunen bör se till att nyanställda genomför en utbildning inom alla relevanta aspekter av personuppgiftshantering och att alla medarbetare genomför utbildningar regelbundet, exempelvis en gång per år. Särskilt för VOF och BUF är det viktigt att säkerställa att all relevant personal har informerats om och förstår rutinerna för dataskydd eftersom deras medarbetare i det dagliga arbetet ofta kommer i kontakt med en stor mängd personuppgifter och känsliga personuppgifter. En närhet till verksamheterna samt exempelvis en obligatorisk nano-utbildning för varje verksamhet med en kritisk mängd personuppgifter skulle minska risken för fel och öka förmågan hos de anställda att skilja på vilka initiativ som kan genomföras och inte med avseende personuppgiftssäkerhet.

Styrande dokument

Västerås stad bör säkerställa att samtliga styrande dokument, både på kommunövergripande nivå samt inom respektive förvaltning, där så är lämpligt, är uppdaterade enligt kraven i dataskyddsförordningen. Kommunen rekommenderas även att se över att styrande dokument och lokala riktlinjer tillsammans bildar en logisk kedja där beslut, ansvarsfördelning

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

och instruktioner är tydliga och som alla medarbetare förstår. Detta för att säkerställa att processerna och det dagliga arbetet med personuppgiftshantering i verksamheterna otvetydigt kan utföras i enlighet med kommunens övergripande strategi och målsättning för dataskyddsarbetet.

Registerförteckning

Varje förvaltning ansvarar för att själva upprätta registerförteckning för samtliga personuppgiftsbehandlingar, vilket i dagsläget sker i Excelfiler baserade på en centralt utformad mall. Processen för att hålla registerförteckningarna kompletta och uppdaterade samt för att hantera begäran om registerutdrag från registrerade har noterats vara sårbar. EY rekommenderar att Västerås stad undersöker möjligheten att implementera ett centralt system för registerförteckning, där en större del av arbetet är automatiserat och där innehållet blir mer överskådligt och lättillgängligt. Vid tidpunkten för granskningen noteras att ett projekt pågår där DSO arbetar för att införa ett sådant system.

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. Revisionsfrågor

Revisionsfrågorna besvaras utifrån granskningen som helhet, det vill säga stadens kommunala verksamheter i en sammanvägd bedömning.

Färgkod	Förklaring
	Revisionsfråga uppfylls ej
	Revisionsfråga uppfylls delvis
	Revisionsfråga uppfylls

Revisionsfråga	Svar	
Uppfyller Västerås stad de krav och regleringar för personuppgiftshantering som har införts i och med dataskyddsförordningen (GDPR)?	Västerås stad, exklusive de helägda bolagen, bedöms delvis uppfylla de krav och regleringar som införts i och med dataskyddsförordningen (GDPR). Det återstår visst arbete med riskanalyser och dokumentation, men staden och dess förvaltningar har utfört ett ambitiöst arbete och är på god väg att helt uppfylla de krav och regleringar som införts.	
Är Västerås stads policyer och riktlinjer ändamålsenliga för att uppnå regelefterlevnad med avseende på dataskyddsförordningen (GDPR)?	Västerås stads policyer, riktlinjer och instruktioner inom personuppgiftsområdet bedöms som delvis ändamålsenliga med avseende på dataskyddsförordningen (GDPR). Den informationssäkerhetspolicy som är antagen är inte uppdaterad sedan 2011 och det finns knapphändig dokumenterad styrning rörande GDPR från högsta nivå. Detta medför att verksamheterna själva har fått utforma ramverk att stödja sitt personuppgiftsarbete på. Ramverk och verksamhetsplaner för dataskyddsarbetet är utformade och förvaltningarna har implementerat processer enligt instruktioner från DSO samt enligt egna initiativ. Avsaknaden av tydlig styrning från ledningsnivå innebär också att rapportering till kommunledningen inte har skett ändamålsenligt.	

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

Har Västerås stad ändamålsenlig kontroll och uppföljning av arbetet med dataskyddsförordningen (GDPR)?	Västerås stad bedöms inte ha ändamålsenlig kontroll och uppföljning med avseende på dataskyddsförordningen (GDPR). Västerås Stad genomför vid tidpunkten för granskningen ingen kontroll och uppföljning på kommunövergripande nivå och det saknas även en strukturerad granskningsplan. Ej heller finns dokumenterade rutiner för uppföljning på verksamhetsnivå och således sker ingen rapportering kring uppföljning och efterlevnad av verksamheternas faktiska dataskyddsarbete. Den samlade bilden är att kommunen initialt valt att prioritera införande av fungerande processer genom verksamheten. Detta bör nu kompletteras med rutiner för att följa upp efterlevnaden och införa mer strukturerade analyser och åtgärdsplaner för att säkerställa att arbetet fortsätter att förbättras.	

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. Slutsatser

Syftet med granskningen har varit att genomföra en övergripande kartläggning av huruvida arbetet kring personuppgiftshantering i Västerås stad sker i enlighet med dataskyddsförordningen. Kommunen har bedömts i relation till andra offentliga organisationer av liknande storlek vad gäller antal anställda, övergripande verksamhet samt karaktär och mängd personuppgiftshantering.

Västerås stad uppnår mognadsgraden 3,1 av 5,0. Detta är en något högre nivå än vad EY generellt observerar för kommuner. Samtidigt rekommenderar EY att vissa åtgärder tas för att höja mognadsgraden ytterligare, givet den stora mängd personuppgifter och känsliga personuppgifter som hanteras.

Kommunen har lagt mycket resurser på arbetet med informationssäkerhet vilket avspeglas i ett en väl utvecklad organisation och rutiner. Kunskapsnivån inom dataskyddsorganisationen är hög och de ansvariga arbetar överlag strukturerat med dataskyddsfrågor.

Således bedöms mognadsgraden vara högst inom organisation och ansvar, samt de två rutintunga områdena behandling av personuppgifter och riskhantering. Västerås Stad har två DSO på heltid samt en utvecklad och tydlig organisation kring dataskyddsfrågor. De granskade förvaltningarna arbetar medvetet med behandling av personuppgifter, har genomfört arbete inom de kritiska områdena och har personal tilldelad med avsatt tid till de olika arbetsuppgifterna. Riskhantering sker genom en väl utarbetad process för systemsäkerhetsanalyser och förvaltningarna får gediget stöd från centralt håll.

Rapportens huvudsakliga iakttagelse berör området kontroll. Kommunens granskning och rapportering inte har utvecklats i samma takt som övrigt arbete och i dagsläget saknas granskning av förvaltningarnas arbete med personuppgiftssäkerhet i stort sett helt. Det finns varken internkontroller inom förvaltningarna som tydligt täcker in de olika aspekterna av dataskyddsarbetet, eller granskningar från centralt håll. Detta bidrar till att den faktiska efterlevnaden av rutiner för personuppgiftshantering är oklar. Verksamheten bör införa kontrollrutiner, där granskningar för personuppgiftshantering genomförs regelbundet och rapportering sker mellan förvaltningarna, dess nämnder, DSO och kommunledningen. Genom att införa mer strukturerade analyser och åtgärdsplaner kommer även arbetet inom övriga områden förbättras ytterligare. EY rekommenderar vidare att kommunen inför regelbundna utbildningsinsatser inom GDPR samt att de mest kritiska verksamheterna tydliggör sin strategi för utbildningsinsatser och medvetenhet hos sina medarbetare och inför åtgärder därefter.

Stockholm den 7 oktober 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

5. Bilaga 1: Förteckning över intervjuade funktioner

5.1. Centrala dataskyddsorganisationen

- Båda dataskyddsombuden
- Informationssäkerhetsstrateg

5.2. Barn- och utbildningsförvaltningen

- Direktör
- Utvecklingsledare
- Sekreterare
- Enhetschef
- Samordnare

5.3. Vård- och omsorgsförvaltningen

- Direktör
- Digitaliseringsstrateg
- Systemförvaltare
- Strateg
- Samordnare

5.4. Teknik- och fastighetsförvaltningen

- Direktör
- Enhetschef
- 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

6. Bilaga 2: Dokumentförteckning

6.1. Centrala dataskyddsorganisationen

- Bifogat bekräftelsebrev Registerutdrag
- Bilaga 1, checklista vid utredning av personuppgiftsincident
- Bilaga 2, Dataskyddsombudets omedelbara bedömning
- Bilaga 3, Mall för beslut om anmälan till Datainspektionen
- Bildspel grundläggande dataskydd, steg 1, 2019-11-29
- Bildspel Grundläggande dataskydd, steg 2, 2020-01-17
- Checklista inför upphandling av IT
- Dataskydd och PUB-avtal för UIC, 2019-10-10
- Diverse länkar
- DPIA, mall
- Handledning och rutiner
- Informationssäkerhetspolicy_Västerås_stad_KFM_111201
- Instruktion – Systemsäkerhetsanalys för Västerås Stad_v5
- Instruktion för inventeringsmall – med åtgärder
- Inventeringsmall exempel
- Kompletterande instruktion till PUB, version 3
- Kravbibliotek – Icke-funktionella, informationssakerhets och tekniska_200603
- ORDFÖRANDEBESLUT-radering
- Protokoll 2018-04-11
- PUB-avtal, KS eller enskild nämnd som PUA , leverantör som PUB, version 2.0, slutversion mall
- PUB-avtal, KS eller enskild nämnd som PUA , leverantör som PUB, version 2.0, som ersätter tidigare PUB-avtal
- Registerutdrag
- Riktlinje för informationssäjerhet_2019_v1.0
- Rutin för personuppgiftsincidenter i Västerås stad
- Stöd och mall – Samtycke vid behandling av personuppgifter
- Stöd och mall för information
- Styrmodell och organisation av dataskyddsarbetet i Västerås stad
- Verksamhetsplan dataskyddsombud 2020
- Verksamhetsplan dataskyddsombud höst 2019

6.2. Barn- och utbildningsförvaltningen

- DSF BUF Uppdragsbeskrivning från ht 20
- Handbok för hantering av personuppgifter inom barn- och utbildningsförvaltningen
- IST-Extens Integrationer
- Matriser för lagring av digital information 191018
- Prorenata - s405 -aktföringsmodulen - Handlingsplan - 2019-11-04
- Redovisningsplan för förskolenämnden - 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

- Redovisningsplan för grundskolenämnden - 2020
- Redovisningsplan för utbildnings- och arbetsmarknadsnämnden – 2020
- Registerförteckning
- Stödmaterial - Begäran om utlämnande av handling
- Svar_Prorenata_Västerås stad - frågor till leverantör

6.3. Vård- och omsorgsförvaltningen

- 160309 Instruktion Skyddade personuppgifter v 1_0 Dnr 2016_169_KS_009
- Ansvar och behörighetstilldelning chef
- Behörighetsbevis HSL
- Bilaga 4 Matris för innehåll i grundbehörigheter Cosmic
- Brister avvikelser åtgärdsplan revision
- DPIA- Resfria möten Mindspace ver 1.0
- Förvaltningsplan Vård och omsorg 2020
- Mail angående:
    - Hantering av dataflöden
    - Klagomål och förfrågningar
    - Kontroll
    - Laglig behandling av personuppgifter
    - Laglig gallring av personuppgifter
    - Översyn av krav inom personuppgiftsområdet
    - Riskhantering
    - Utbildning och medvetenhet
- Information om HSA till personal med skyddade personuppgifter
- Instruktion loggning i Pulsen Combine
- Internrevisionsrapport SITHS , HSA 181204
- Internrevisionsrapport SITHS , HSA 191212
- Introduktion av nya medarbetare
- Inventering sociala nämndernas förvaltning 2018-08-22
- Kopia av enkät Klagomål och synpunkter_ÄN
- Kravspecifikation arbetsmaterial190930
- Loggkontroll Rutin 150326
- Loggkontrollprotokoll
- Offert 2-faktorsinloggning i MO - Västerås Stad
- Organisationsscheman VOF 200325
- Process klagomålshantering
- PUB-avtal Mind Space ver 1.0
- Redovisning av allmänna handlingar (redovisningsplan) för äldrenämnden
- Redovisning av allmänna handlingar (redovisningsplan) för nämnder för personer med funktionsnedsättning
- Registratorsrutin Synpunkt-Klagomålsärende
- Rutin behandling och lagring av personuppgifter
- Rutin klagomålshantering

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

- Rutiner Skyddad identitet upphör
- Rutiner Skyddad identitet
- Sithskort rutin vård och omsorg
- Skyddad identitet- blankett godkännande SOSFS_20119
- SSA Objekt VoO
- Tjänstutlåtande - Projekt - Inventering av personuppgiftsbehandlingar inom Sociala nämndernas förvaltning NF
- Tjänstutlåtande - Projekt - Inventering av personuppgiftsbehandlingar inom Sociala nämndernas förvaltning
- Upphandlingskrav - 2019-10-02_Mindspace

6.4. Teknik- och fastighetsförvaltningen

- Rutin för personuppgiftincidenter i Västerås stad.docx
- Bilaga 1, checklista vid utredning av personuppgiftsincident.docx
- Rutin för hur TFF säkerställer att information ges om hur personuppgifter behandlas.docx
- Rutin vid inkommen förfrågan om registerutdrag.docx
- Rutin vid personuppgiftsincidenter.docx
- Stöd och mall för information.docx
- Teknik o fastighetsförvaltning introduktion.docx

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 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.

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

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.

Tredje part: Med tredje part avses en fysisk eller juridisk person, offentlig myndighet, institution eller organ som inte är den registrerade, den personuppgiftsansvarige,

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

personuppgiftsbiträdet eller de personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar är behöriga att behandla personuppgifterna.