Ds 2018:6

Granskning av Transportstyrelsens upphandling av it-drift

REGERINGSKANSLIET

Näringsdepartementet

SOU och Ds kan köpas från Norstedts Juridiks kundservice.
Beställningsadress: Norstedts Juridik, Kundservice, 106 47 Stockholm
Ordertelefon: 08-598 191 90
E-post: kundservice@nj.se
Webbadress: www.nj.se/offentligapublikationer

För remissutsändningar av SOU och Ds svarar Norstedts Juridik AB
på uppdrag av Regeringskansliets förvaltningsavdelning.
Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02).
En kort handledning för dem som ska svara på remiss.
Häftet är gratis och kan laddas ner som pdf från eller beställas på regeringen.se/remisser

Omslag: Regeringskansliets standard
Tryck: Elanders Sverige AB, Stockholm 2018

ISBN 978-91-38-24768-6
ISSN 0284-6012

Förord

Regeringen gav den 17 augusti 2017 justitierådet Thomas Bull i uppdrag att granska den upphandling rörande förändrad it-drift hos Transportstyrelsen som har medfört att säkerhetskänslig och av andra skäl sekretessbelagd information har hanterats på ett sätt som strider mot svensk lag (N2017/04991/SUBT). I september anställdes som utredningssekreterare kammarrättsrådet Hanna Kristiansson, enhetschefen Tina J Nilsson och avdelningsdirektören Martin Waern.

Denna promemoria är resultatet av ett gemensamt arbete av mig och sekreterarna. Den är därför skriven i vi-form. Jag är dock ensam ansvarig för slutsatserna. Genom denna promemoria, Granskning av Transportstyrelsens upphandling av it-drift, är uppdraget slutfört.

Stockholm i februari 2018

Thomas Bull

/Hanna Kristiansson
Tina J Nilsson
Martin Waern

Sammanfattning

Regeringen beslutade den 3 augusti 2017 att en utredare ska granska den upphandling av it-drift som gjordes av Transportstyrelsen under 2014 och 2015. Denna rapport utgör resultatet av granskningen.

Granskningen har funnit brister i Transportstyrelsens hantering av hemliga uppgifter och andra skyddsvärda uppgifter, bl.a. känsliga personuppgifter. Vi drar slutsatsen att den helt grundläggande orsaken till varför Transportstyrelsens upphandling och outsourcing kom att dras med dessa brister var att man i allt för hög grad saknade relevant kunskap om vilken information myndigheten hade och saknade kännedom om hur denna information ska hanteras. Skälen till detta är flera.

Ett första är att arbetet med informationssäkerhet vid myndigheten var eftersatt under lång tid, ett andra att säkerhetsfunktionerna vid myndigheten var utspridda och saknade tillräcklig samordning och ett tredje att de som haft kännedom och kunskap om säkerhetsfrågorna av säkerhetsskäl inte velat tala om dem. Till sist har man saknat tillräckliga kunskaper om relevanta regler och hur de ska tillämpas.

Den andra huvudsakliga orsaken till att upphandlingen av it-driften ledde till olyckliga konsekvenser var en orealistisk tidplan. Även detta hade flera olika skäl.

För det första inledde Transportstyrelsen inte mindre än tre upphandlingar samtidigt. En andra faktor var den snäva tidsgränsen för IBM:s övertagande av it-driften och slutpunkten för Trafikverkets leverans. En tredje faktor var att dokumentation och analys av befintlig information i it-systemen var bristfällig, vilket drog resurser och orsakade förseningar.

Den tredje grundläggande orsak som vi kunnat identifiera gäller bristen på kommunikation, såväl inom myndigheten som med andra berörda aktörer. Även denna brist har flera olika ursprung.

Organisationen kring upphandlingen var komplex och därför ett hinder för effektiv kommunikation inom myndigheten. Kontakterna med Trafikverket kunde också ha varit mer omfattande och på högre nivå. Styrelsen verkar endast ha fått översiktlig information om händelseförloppet och regeringen har inte involverats för att hantera de uppkomna svårigheterna.

När det gäller ansvarsfrågan härleds alla dessa tre huvudsakliga brister främst till myndighetens ledning. Utredningen menar bl.a. att det innebär att styrelsen och de tidigare generaldirektörerna har haft ett ansvar för hur myndigheten varit organiserad, prioriterat sina resurser och agerat i praktiken. Även andra bär dock ett ansvar, såsom ansvariga avdelningschefer, projektledare och säkerhetsfunktioner som alla brustit i olika hänseenden när det gäller de tre ovan angivna bristerna.

Innehåll

1 Utredningens uppdrag, arbete och allmänna utgångspunkter

1.1 Bakgrund

Transportstyrelsen genomförde under 2014 och 2015 en upphandling om förändrad it-drift. Resultatet av upphandlingen blev att IBM Svenska AB (IBM) tilldelades kontraktet för Transportstyrelsens it-drift och ett avtal tecknades i april 2015. IBM skulle enligt avtalet ansvara för att maskinvara, nätverk och program fungerar. Detta omfattar också driften av de register som Transportstyrelsen har ansvar för såsom vägtrafikregistret. IBM övertog ansvaret för driften den 1 november 2015. Under övergången av it-driften till IBM beslutades om en rad avsteg från svensk lagstiftning vilket i sin tur medförde att säkerhetskänslig och av andra skäl sekretessbelagd information hanterats på ett sätt som strider mot svensk lag. Med anledning av dessa beslut har Säkerhetspolisen genomfört en förundersökning avseende vårdslöshet med hemlig uppgift. Transportstyrelsens tidigare generaldirektör Maria Ågren har enligt ett av henne godkänt strafföreläggande gjort sig skyldig till vårdslöshet med hemlig uppgift.

Regeringen beslutade den 3 augusti 2017 att en utredare ska granska den aktuella upphandlingen utifrån att det på grund av de uppgifter som framkommit finns starka skäl att kartlägga och analysera vad som medfört att myndighetens ledning har fattat beslut som strider mot svensk lag.[1]

[1] Uppdrag att granska Transportstyrelsens upphandling av it-drift, N2017/0499/SUBT.

1.2 Uppdraget

Enligt uppdraget ska granskningen omfatta följande frågeställningar:

- Undersöka hur och varför Transportstyrelsen initierade processen att upphandla myndighetens it-drift samt vilken analys och vilka överväganden som låg till grund för myndighetens agerande. I detta ingår att klargöra beslutsordningen inför beslut att inleda upphandling, val av upphandlingsförfarande och val av potentiella leverantörer.
- Kartlägga processen från det att Transportstyrelsen beslutade att påbörja arbetet med en förändrad it-drift och it-organisation fram till i dag. Därvid ska viktiga tidpunkter, gjorda vägval, beslut som fattats på olika nivåer inom myndigheten och information som lämnats till Regeringskansliet redovisas.
- Redovisa vilka alternativ som utreddes och vilka analyser och bedömningar av konsekvenser och risker som gjordes vid olika tidpunkter under processen samt vilka typer av interna och eventuellt externa kontakter och specialistroller som bidrog till dessa.
- Undersöka säkerhetskulturen inom Transportstyrelsen med avseende på risker med relevans för den aktuella upphandlingsprocessen. I det ligger att undersöka relevanta interna rutiner och riktlinjer samt organisationens gemensamma förhållningssätt, prioriteringar och agerande.
- Bedöma vilka åtgärder som hade kunnat vidtas för att undvika att skyddsvärd information kunde komma att hanteras felaktigt samt vilka roller och kompetenser som deltog eller saknades vid viktiga analyser och beslut.
- Redovisa vilka eventuella åtgärder som Transportstyrelsen har vidtagit för att säkerställa att myndigheten har nödvändig kompetens kring it-säkerhet, informationssäkerhet, säkerhetsskydd och offentlig upphandling.
- Utifrån granskningen redogöra för vilka lärdomar som kan dras av den aktuella upphandlingen.

1.3 Avgränsningen av uppdraget

Utredningen ska enligt direktiven granska den upphandling och outsourcing av it-drift hos Transportstyrelsen som har medfört att säkerhetskänslig och av andra skäl sekretessbelagd information har hanterats på ett sätt som strider mot svensk lag. Det är således Transportstyrelsens agerande som är föremål för utredningens granskning. Andra myndigheters agerande faller därmed i huvudsak utanför granskningen. Granskningen omfattar dock att utvärdera hur Transportstyrelsen har samverkat med andra statliga myndigheter inom ramen för den aktuella upphandlingen. Andra myndigheters ageranden kan i det sammanhanget komma att omfattas av granskningen.

Den aktuella upphandlingen genomfördes under 2014 och 2015. I utredningens uppdrag ingår dock att undersöka hur och varför Transportstyrelsen initierade processen att upphandla myndighetens it-drift samt att kartlägga processen från det att Transportstyrelsen beslutade att påbörja arbetet med en förändrad it-drift och it-organisation fram till i dag. Detta innebär att tidsperioden omfattar tiden redan från 2009 när Transportstyrelsen bildades och fram till hösten 2017.

Vad gäller uppgiften att redogöra för vilka lärdomar som kan dras av den aktuella upphandlingen har utredningen valt att tolka direktiven på så sätt att denna uppgift omfattar dels att konkret redogöra för de lärdomar som Transportstyrelsen som enskild myndighet kan göra, dels redogöra för de lärdomar som kan dras på ett mer generellt plan. I sistnämnda avseende är det viktigt att anlägga ett förhållandevis brett perspektiv. Utredningen kommer i detta avseende att föra mera allmängiltiga resonemang om myndigheters ledningsformer, organisation och interna kultur för att diskutera hur sådana faktorer påverkar statliga myndigheter.

I direktiven nämns inte uppgiften att analysera vem eller vilka som bär ansvar men enligt utredningens mening faller det sig naturligt att en granskning av detta slag också utmynnar i ställningstaganden avseende ansvar.

Det är viktigt att i detta sammanhang komma ihåg att en granskning av en myndighets handlande i en specifik situation där beslut ibland fattas under osäkerhet och tidspress måste ske med respekt för att man vid tidpunkten för granskningen sitter med mycket av

facit i hand. Utredningen redogör i avsnitt 1.6 för sina överväganden kring ansvarsbegreppet.

1.4 Utredningens arbete

Utredaren och utredningssekreterarna har träffats regelbundet under granskningen för att planera, diskutera och gå igenom texter. Utredningen har gått igenom regleringsbrev, arbetsordningar, riktlinjer och andra styrande dokument vid Transportstyrelsen som varit gällande vid olika tidpunkter under den tidsperiod som har granskats. Även dokumentation och underlag kring upphandlingen och övergången av it-driften till IBM har inhämtats.

Utredningen har inhämtat dokumentation och underlag från i första hand Transportstyrelsen, men även från andra myndigheter som Trafikverket, Säkerhetspolisen och Kammarkollegiet. Utredningen har samrått med Datainspektionen, Myndigheten för samhällsskydd och beredskap, Säkerhetspolisen och Upphandlingsmyndigheten. Utredningen har även haft kontakt med Konstitutionsutskottet samt träffat Försvarsmakten vid ett tillfälle.

Utredningen har arbetat helt självständigt gentemot Regeringskansliet. Material har inhämtats från Regeringskansliet när det varit nödvändigt men utredningen har inte samrått med departementet om innehållet i eller omfattningen av granskningen.

Utredningen har genomfört ett trettiotal intervjuer med personer som varit involverade i den aktuella upphandlingen på olika sätt. De flesta av de intervjuade personerna är eller har varit anställda på Transportstyrelsen under hela eller delar av den aktuella tidsperioden. Minnesanteckningar har förts över samtalen och de intervjuade har beretts tillfälle att lämna synpunkter på dessa. En lista över de intervjuade personerna återfinns i bilaga 2.

I sammanhanget bör framhållas att det mesta som utredningens granskning gäller avser förhållanden som ligger flera år eller ännu längre tillbaka i tiden. Detta har inneburit särskilda utmaningar i form av att minnesbilder hos de inblandade bleknat, att skriftlig dokumentation inte längre finns kvar eller är förhållandevis intetsägande och att inblandade personer inte längre har de roller de då hade, samt att i dag verksamma personer inte var involverade i det nu granskade händelseförloppet. Det har således funnits vissa

svårigheter att ge en helt fullständig och entydig bild både av det som skett, de ställningstaganden som gjorts och de skäl som legat bakom dessa.

Generellt kan sägas att den skriftliga dokumentation av händelseförloppet under upphandlingen och dess efterföljande faser som utredningen fått ta del av inte är komplett, det är t.ex. svårt att tydligt utröna vilka personer och funktioner som ingått i olika arbets- och projektgrupper samt styrgrupper vid olika tillfällen och vilka personer som deltagit på vissa möten. De underlag som finns till möten är mestadels i form av power point-presentationer vilket gör att mycket information inte finns i skriftlig form att ta del av i efterhand. Det är därför svårt att följa det arbete som görs under upphandlingen och outsourcingen i detalj. För säkerhetsarbetet har utredningen inte fått någon skriftlig dokumentation. Mycket av de fakta som utredningen lagt till grund för sin granskning kommer därför från de intervjuer som utredningen har genomfört med anställda vid Transportstyrelsen.

1.5 Rapportens struktur

I nästföljande avsnitt (1.6) redogör utredningen för sin syn på uppgiften att granska, utvärdera och göra en ansvarsanalys. I avsnitt 1.7 återfinns en redogörelse för vissa allmänna utgångspunkter för utredningens arbete och i avsnitt 1.8 redovisas några grundläggande begrepp av betydelse.

I kapitel 2 görs en kortare genomgång av gällande bestämmelser avseende de aktuella frågorna.

Kapitel 3 beskriver myndigheten Transportstyrelsen och dess historik, uppgifter och organisation.

Kapitel 4 beskriver Transportstyrelsens organisation, styrning och hantering av säkerhetsskydd, informationssäkerhet och it-säkerhet.

Kapitel 5–8 syftar till att ge beskrivningar av vad som skett samt redogöra för de iakttagelser som utredningen kunnat göra utifrån händelseförloppen.

Kapitel 5 återger händelseförloppet under upphandlingen av it-drift från det att Transportstyrelsen påbörjade arbetet med att överväga en förändrad it-drift till det att avtal tecknas med IBM.

Kapitel 6 återger händelseförloppet under övergången av it-driften till IBM samt de beslut om avsteg som fattades i samband med detta.

Kapitel 7 innehåller en redogörelse för Säkerhetspolisens tillsyn, från det att Säkerhetspolisen kontaktar Transportstyrelsen avseende säkerhetsskyddet till dess att tillsynsrapporten är klar.

Kapitel 8 innehåller en beskrivning av händelseförloppet under tiden efter det att IBM tagit över it-driften till det att ett nytt reviderat avtal med IBM fanns på plats.

Kapitel 9 innehåller utredningens slutsatser och en redogörelse för de lärdomar som enligt utredningens mening kan dras av den aktuella upphandlingen.

1.6 Ansvarsbegreppet

1.6.1 Utredningens uppdrag avseende ansvar

Det har under modern tid funnits flera kommittéer och utredningar som haft i uppdrag att granska specifika händelser eller företeelser.[2] 2005 års katastrofkommission har i sitt betänkande en längre redogörelse och diskussion av ansvarsbegreppen. Kommissionen skriver bl.a. följande.[3]

Kommissionens uppdrag har som framgått två huvudkomponenter, en granskande (bakåtblickande) och en förslagsinriktad (framåtblickande). Dessa hänger intimt samman via ansvarsbegreppet. För att granska och utvärdera olika befattningshavares eller myndigheters agerande är det nödvändigt att noggrant beskriva hur ansvaret för olika uppgifter har varit fördelat. (…) Kommissionen menar därför att en granskning förutsätter en konkret behandling av frågor om ansvaret och dess fördelning. Kommissionen väljer att arbeta med ett ansvarsbegrepp som inrymmer att kritik av varierande styrka ska kunna riktas mot dem som visat sig inte motsvara de krav som framgår av gällande bestämmelser eller som annars rimligen bör kunna ställas. Om en sådan analys inte görs, försvåras möjligheterna

[2] Bl.a. Osmo Vallo-utredningen, SOU 2002:37 och 2005 års katastrofkommission om hanteringen av tsunamikatastrofen, SOU 2005:104. Även granskningen av Karolinska Institutet och Macchiarini-ärendet från 2016 kan nämnas.
[3] SOU 2005:104 s. 51.

att lära av misstagen och medborgarnas förtroende för myndigheterna urholkas. Att göra en analys av ansvarsfrågorna är en sak. Däremot är det inte, det ska betonas, en uppgift för kommissionen att utkräva ansvar.

Denna utrednings uppdrag inrymmer precis som katastrofkommissionens både en bakåtblickande granskning och en framåtblickande del. Utredningen kommer därför inom ramen för sitt uppdrag att kunna rikta viss kritik mot dels enskilda roller, dels organisationslösningar. Det är dock inte denna utrednings uppdrag att utkräva ansvar.

1.6.2 Ansvar som företeelse

Katastrofkommissionen använde sig av ett klassiskt, individuellt ansvarsbegrepp som anpassades till den organisatoriska miljö där analysen tillämpas. Utgångspunkten för ett sådant begrepp är att chefen har ansvaret för verksamheten men att ansvar kan delegeras nedåt i organisationen genom skrivna instruktioner, råd och anvisningar. Delegeringen förutsätter att ledningen vidtar tillräckliga åtgärder för att de som får delegerat ansvar ska kunna utföra sina uppgifter väl. Det är också ledningens ansvar att genom uppföljningar säkerställa att organisationen har uppfattat vilka ansvarsförhållanden som gäller. Om en tydlig delegation görs kommer ansvarsbedömningen inte att handla om ett delat ansvar för det hela utan om delegerat ansvar och vad detta omfattar. Vid osäkerhet om ansvarsfördelningen gäller att den högre nivån har ansvaret.[4]

Denna utredning kommer också att använda sig av detta ansvarsbegrepp. Utredningen har därför studerat hur ansvaret var fördelat inom Transportstyrelsen under den aktuella tidsperioden genom att analysera myndighetsinstruktion, arbetsordningar och andra interna styrdokument av betydelse.

En annan aspekt av ansvarsfrågan är den om en person kan vara lite ansvarig för något som hänt, om det också är andra personer som är ansvariga. Även här delar utredningen katastrofkommissionens mening att en person visserligen kan dela ansvaret med andra men

[4] SOU 2005:104 s. 67 f.

att detta endast innebär att alla de som ska anses ansvariga är fullt ut ansvariga; ”Att ansvaret delas gör det inte mindre för var och en”.[5]

I detta sammanhang kan nämnas Statens ansvarsnämnds generella uttalande avseende ansvarsfrågan för myndighetschefer i sitt beslut att avskeda Maria Ågren.[6] Ansvarsnämnden uttalade bl.a. följande (s. 17): ”Den svenska förvaltningsmodellen bygger på att myndigheter är självständiga under regeringen. Transportstyrelsen är en styrelsemyndighet. Generaldirektören ansvarar inför styrelsen och ska hålla den informerad samt sköta den löpande förvaltningen i enlighet med styrelsens riktlinjer. Som en utgångspunkt gäller dock att en myndighetschef inte kan avhända sig sitt eget ansvar för sina myndighetsåtgärder genom att informera om beslut eller förankra dem hos styrelsen eller regeringen”.

1.7 Allmänna utgångspunkter

1.7.1 Det statliga förvaltningssystemet

Myndigheternas roll i det statliga förvaltningssystemet regleras i viss utsträckning i regeringsformen (RF). Enligt 1 kap. 6 § RF är det regeringen som styr riket och enligt 12 kap. 1 § RF lyder de statliga förvaltningsmyndigheterna under regeringen. Dessa förvaltningsmyndigheters uppgift är att bl.a. verkställa den politik som lagts fast. Regeringen har i det sammanhanget till uppgift att styra myndigheterna i den omfattning den finner lämpligt. Det är regeringen som kollektiv som utövar denna bestämmanderätt över myndigheterna, 7 kap. 3 § RF, och man brukar därför säga att Sverige saknar s.k. ministerstyre. Myndigheterna har befogenheter att självständigt och utan regeringens och riksdagens ingripande hantera det dagliga arbetet. I 12 kap. 2 § RF finns ett förbud för bl.a. regering och riksdag att bestämma hur en myndighet ska besluta i ett ärende som rör myndighetsutövning mot enskild eller tillämpning av lag.

[5] SOU 2005:104 s. 491 f. Även granskningen av Karolinska Institutet och Macchiarini-affären anslöt sig till detta synsätt, se s. 31 i deras rapport.
[6] Statens ansvarsnämnds beslut 2017-09-28, Ä 12/2017.

1.7.2 Allmänt om myndighetsstyrning

Statsförvaltningen med dess myndigheter är som framgått regeringens viktigaste instrument för att styra riket. Det är därmed också regeringens uppgift att ange mål för den statliga verksamheten och på olika sätt och med olika medel styra sin förvaltning. Uttryckliga regler om hur denna styrning ska gå till saknas i RF. De styrmedel som regeringen har att tillgå kan i de flesta fall dock härledas från grundlagsreglerna om normgivningsmakt (8 kap. RF), finansmakt (9 kap. RF), utnämningsmakt (12 kap. RF) och kontrollmakt (13 kap. RF).

Myndigheternas verksamhet styrs i första hand genom generell normgivning, dvs. genom lagar beslutade av riksdagen och förordningar beslutade av regeringen vari myndigheterna ges vissa konkreta uppgifter och befogenheter. Regeringen använder också sin normgivningsmakt till att styra myndigheterna såväl generellt som mer direkt. Det förra sker framför allt genom myndighetsförordningen (2007:515) och det senare genom de enskilda myndigheternas instruktioner, vilka också ges genom förordning. Några gemensamma och grundläggande krav som regeringen ställer framgår av myndighetsförordningens 3 § och innefattar att verksamheten ska bedrivas effektivt och i enlighet med gällande rätt. Inom myndigheterna kompletteras sedan dessa styrande dokument genom antagande av interna arbetsordningar och handläggningsordningar.

Riksdagen anger genom beslut om budgetpropositionen de ekonomiska ramarna för myndigheternas olika verksamhetsområden. Utifrån detta beslutar regeringen om varje enskild myndighets ekonomiska villkor för det kommande verksamhetsåret genom ett särskilt beslut, ett s.k. regleringsbrev. I regleringsbrevet för en myndighet anges myndighetens verksamhet och mål, hur verksamheten ska finansieras och vilka krav på bl.a. återrapportering som regeringen ställer. Utifrån regleringsbrevet upprättar myndigheterna sedan egna verksamhetsplaner för sin verksamhet och hur den ska följas upp.

Enligt 3 § förordningen (2000:605) om årsredovisning och budgetunderlag ska myndigheten årligen upprätta och till regeringen lämna årsredovisning och budgetunderlag. Handlingarna ska kortfattat ge underlag för regeringens uppföljning, prövning eller budgetering av myndighetens verksamhet.

Av 8 § förordningen om årsredovisning och budgetunderlag framgår att årsredovisningen ska skrivas under av myndighetens ledning. Underskriften innebär att ledningen intygar att årsredovisningen ger en rättvisande bild av verksamhetens resultat och av kostnader, intäkter och myndighetens ekonomiska ställning. Ledningen vid de förvaltningsmyndigheter under regeringen som omfattas av förordningen (2007:603) om intern styrning och kontroll ska i anslutning till underskriften i årsredovisningen lämna en bedömning av huruvida den interna styrningen och kontrollen är betryggande.

Det är regeringen som förordnar myndighetschefer och utser ledamöter i myndigheters styrelser. Denna utnämningsmakt är också ett styrinstrument för regeringen. Regeringens styrning genom kontroll sker på flera sätt. Ett väsentligt inslag är regleringsbrevens återrapporteringskrav, som redan nämnts ovan. Även regeringens mål- och resultatdialog är en form av kontroll som innefattar styrning. Reglerna i internrevisionsförordningen (2006:1228) och förordningen om intern styrning och kontroll innebär också en styrning från regeringens sida vad gäller myndigheternas verksamhet. En från regeringen fristående kontroll av myndigheterna sker genom Riksrevisionens årliga revision och effektivitetsrevision. Ytterligare former av styrning genom kontroll är förvaltningsdomstolarnas överprövning av myndigheternas beslut efter överklagande och Justitieombudsmannens och Justitiekanslerns granskande verksamheter.

1.7.3 Olika ledningsformer[7]

I myndighetsförordningen (2007:515) regleras tre ledningsformer. En myndighet leds enligt förordningen antingen av

- en myndighetschef (enrådighetsmyndighet),
- en styrelse (styrelsemyndighet) eller
- en nämnd (nämndmyndighet).

Enligt den förvaltningspolitiska proposition som regeringen lämnade till riksdagen i mars 2010 väljer regeringen den ledningsform

[7] Texten i detta avsnitt kommer delvis från Statskontorets rapport *Myndigheternas ledningsformer – en kartläggning och analys*, Statskontoret 2014:4 s. 16 f.

som bäst gagnar verksamheten. Utgångspunkter för valet av ledningsform är

- verksamhetens art,
- politiska prioriteringar, samt
- regeringens behov av att styra på ett visst sätt.[8]

Enrådighetsmyndigheter

Enrådighetsmyndigheter leds av en myndighetschef som sköter den löpande verksamheten och som också ansvarar för verksamheten inför regeringen. I enrådighetssmyndigheter kan regeringen föreskriva att det vid sidan av myndighetschefen ska finnas ett s.k. insynsråd. Insynsråden har inga beslutsbefogenheter utan deras uppgift är att utöva insyn och ge myndighetschefen råd.

Styrelsemyndigheter

I styrelsemyndigheter är det styrelsen som har ansvaret för myndighetens verksamhet inför regeringen. Myndighetschefen ska svara för den löpande verksamheten enligt styrelsens direktiv och riktlinjer. Myndighetschefen har också att hålla styrelsen informerad om verksamheten, förse styrelsen med underlag för beslut och verkställa dessa. Styrelsen ska besluta om en arbetsordning där bl.a. arbetsfördelningen mellan styrelse och myndighetschef fastställs.[9]

Nämndmyndighet

I nämndmyndigheter är det nämnden som kollektiv som utgör myndighetens ledning och ansvarar för verksamheten inför regeringen. En nämndmyndighets beslut fattas i regel av nämnden i dess helhet. Ärendena bereds av ett kansli som i huvudsak ansvarar för handläggning av ärenden och för administration. Vid större nämnder finns det ofta en kanslichef.

[8] Proposition 2009/10:175, *Offentlig förvaltning för demokrati, delaktighet och tillväxt*, s. 108 f.
[9] 4 och 13 §§ myndighetsförordningen.

1.7.4 En vidare kontext

I detta avsnitt presenteras den vidare kontext där upphandlingen och outsourcingen ingår. Det handlar om att kortfattat presentera några faktorer som påverkar statsförvaltningen generellt. I detta ingår effektivitetskrav, arbetet med informationssäkerhet vid svenska myndigheter generellt och vilken roll upphandling och outsourcing kommit att få för myndigheternas verksamhet samt vilka krav som bör ställas vid outsourcing.

Statsförvaltning under förändring

Transportstyrelsen är en myndighet i den statliga förvaltningen. Den svenska statsförvaltningen har varit under ett starkt förändringstryck sedan 1990-talet. Ambitionerna att skapa effektivare, mer demokratiskt förankrade och transparenta myndigheter går dock längre tillbaka än så.[10]

Ett flertal faktorer har bidragit till denna utveckling. Det handlar om generella effektiviseringskrav som ställs på den offentliga sektorn, om nya krav med hänsyn till ökad internationalisering och om teknisk utveckling som både möjliggör nya sätt att arbeta för förvaltningen men också skapar nya utmaningar. Digitalisering och framväxten av s.k. e-förvaltning med målet att myndigheter ska kunna nås av medborgarna på tider och sätt som är smidiga, effektiva och billiga är en del av denna utveckling. Man talar ibland om 24-timmars-myndigheten som ett mål i sig och detta ställer så klart höga krav på myndigheterna när det gäller teknisk utveckling och kompetens, tillgänglighet och säkerhet.

Informationssäkerhet

Den ökade användningen av modern informationsteknologi i statsförvaltningen har gjort att frågor om informationssäkerhet blivit viktigare än någonsin. Att brister i sådan säkerhet kan få dramatiska konsekvenser är känt.[11]

[10] Se redogörelsen i SOU 2007:75, *Att styra staten* s. 71–104 för en beskrivning av utvecklingstrender från 1960-talet och framåt.
[11] Se t.ex. redogörelsen i kapitel 2 av Riksrevisionens rapport RiR 2014:23 *Informationssäkerheten i den civila statsförvaltningen*.

Trots detta har det under en ganska lång tid stått klart att statsförvaltningen har haft svårt att leva upp till de ökade kraven på informationssäkerhet. Riksrevisionen har i ett flertal rapporter pekat på brister i hur statsförvaltningen hanterar informationssäkerheten och i hur regeringen styr myndigheterna i dessa avseenden. Utan att gå in på detaljer vill utredningen här lyfta fram några av Riksrevisionens iakttagelser och rekommendationer som mer direkt kan anses ha bäring på denna granskning.[12]

Redan 2007 identifieras informationssäkerheten som ett särskilt riskområde för staten och Riksrevisionen konstaterade brister i uppföljningen av ett antal myndigheters interna styrning och kontroll av informationssäkerheten. I en rapport från 2014 konstateras att de stöd- och tillsynsmyndigheter som finns på området endast delvis har vidtagit nödvändiga åtgärder för att informera sig och regeringen om vilka hot som finns mot den civila statsförvaltningen, i vilken omfattning de realiseras och vilka skyddsåtgärder som vidtas.[13] Bristerna från 2007 konstaterades vara kvar och Riksrevisionen ansåg att det regelverk som styr myndigheternas arbete med informationssäkerhet kan behöva anpassas till olika typer av statlig verksamhet. Bland de mer konkreta förslagen fanns att låta tillsynsmyndigheten utfärda sanktioner efter att en tillsyn visat brister och att säkerhetsläget återkommande rapporteras till Regeringskansliet.[14]

Av Myndigheten för samhällsskydd och beredskaps rapport från samma år kan utläsas att det finns brister avseende hur informationsklassning sköts i praktiken, hur engagerade myndigheters ledning är i säkerhetsfrågor och i hur riskanalyser används vid myndigheters planeringsarbete.[15]

I Riksrevisionens senaste granskning av området från 2016 konstateras att arbetet med informationssäkerhet ligger på en nivå som är märkbart under vad som är tillräckligt. En viktig förklaring är att förståelsen för vikten av en god informationssäkerhet överlag är alltför liten. Detta får till följd att arbetet med informationssäkerhet

[12] Rapporterna är RiR 2007:10, *Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen*, RiR 2014:23 (se ovan), och RiR 2016:8, *Informationssäkerhetsarbetet vid nio myndigheter*. Vi har även tagit del av Myndigheten för samhällsskydd och beredskaps rapport *En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter*.
[13] RiR 2014:23 s. 11.
[14] RiR 2014:23 s. 13.
[15] A. rapport s. 8.

inte blir tillräckligt högt prioriterat i förhållande till de risker som finns.[16]

Granskningen visar att myndigheternas ledningar har delegerat ansvaret för informationssäkerhet, utan att se till att de ansvariga har tillräckligt mandat och tillräckliga resurser. De funktioner som ansvarar för informationssäkerheten har svårt att hävda sig mot kärnverksamheten, vilket får till följd att verksamhetens krav på funktionalitet mestadels går före kraven på säkerhet. Trots att myndigheterna har tagit fram policyer, riktlinjer och handledningar i fråga om informationssäkerhet är kännedomen om dokumentens innehåll och syfte låg hos många medarbetare och chefer.[17]

Riksrevisionen rekommenderade regeringen att utreda behovet av en central funktion som skulle lämna ett operativt stöd till myndigheterna.

Outsourcing[18]

I den moderna statsförvaltningen är frågan om vad myndigheten själv ska utföra och vad som bättre och billigare görs av privata alternativ vanlig. Ibland är det t.o.m. så att kraven på teknisk spetskompetens och internationell förankring gör det närmast omöjligt med annat än privata leverantörer. Ett uppenbart exempel är ett så känsligt område som försvarsindustrin, där nästan ingen stat på egen hand kan leverera de varor och tjänster som försvarsmakten kräver, trots att detta innefattar säkerhetsrisker på flera nivåer.

Outsourcing kan definieras som att en myndighet (eller ett företag) låter en extern aktör ta hand om en verksamhet, funktion eller process som tidigare legat inom den egna organisationen. Myndigheter och andra organ inom den offentliga sektorn väljer i dag att i allt större utsträckning anlita externa parter för att utföra sådan verksamhet som inte utgör myndighetens kärnverksamhet. Outsourcing är således ett växande fenomen, både globalt och i Sverige, och är vad gäller it-verksamhet ännu vanligare i den svenska privata sektorn än i offentlig sektor.[19]

---

[16] RiR 2016:8 s. 6.
[17] A. rapport s. 7.
[18] På svenska kan begreppet utkontraktering användas. Denna utredning har valt att använda begreppet outsourcing då det får anses vara ett vedertaget begrepp även på svenska.
[19] IT inom statsförvaltningen, Riksrevisionens granskningsrapport RiR 2011:4., s. 13.

Myndigheterna står således inte inför valet att outsourca eller inte, utan snarare inför frågan om *vad* som kan outsourcas och *hur* detta i så fall ska skötas. E-delegationen uttalade 2009 bl.a. följande om vad en sourcingstrategi ska innehålla i sitt betänkande Strategi för myndigheternas arbete med e-förvaltning:

”En sourcingstrategi ska hantera den framtida kompetensförsörjningen, men också leda till ett effektivare utnyttjande av marknadens tjänster. En strategi ska alltid tas fram, även i de fall det inte är aktuellt att vända sig till marknaden. Det är viktigt att varje myndighets specifika situation vägs in i strategin och att övervägandena tydligt redovisas. Långsiktiga effektivitets-, kvalitets- och kompetenskonsekvenser ska belysas och eventuella risker beskrivas. Det slutliga valet mellan intern och extern leverans av IT-tjänster ska göras baserat på flera parametrar av vilka total kostnad, kvalitet och flexibilitet är några av de viktigaste.”[20]

Riksrevisionen kom i en rapport från 2011 också in på vilka krav som bör ställas på myndigheterna i dessa avseenden. Där framhålls att myndigheten bör ha genomfört en adekvat prövning om outsourcing av hela eller delar av it-verksamheten kan vara ett medel för att öka effektiviteten, minska riskerna och förbättra hushållningen av de resurser myndigheten fått till förfogande. Att ta fram en sourcingstrategi innebär att myndigheten tar ställning till hur verksamheten på bästa sätt ska försörjas med it-kapacitet.[21] Vidare påpekas att det krävs att myndigheten vet vilka system som är samhällskritiska, vilka krav som gäller för informationssäkerhet, vilka sekretesskrav som ställs och vilka krav som ställs på intern styrning och kontroll. Dessutom pekar Riksrevisionen på att det är viktigt att myndigheten vet vad den egna it-verksamheten faktiskt kostar.[22]

De möjliga fördelar som kan finnas med outsourcing är kostnadsbesparingar, fokus på kärnprocesser, innovation och förnyelse, tillgång till expertkompetens och flexibilitet/skalbarhet. Det finns dock även fallgropar som dolda kostnader, inlåsning, svårigheter att skriva kompletta avtal, avvikelser från avtal, kostnader för uppföljning, försämrad servicekvalitet och förlust av kompetens.[23]

[20] SOU 2009:86 s. 83.
[21] RiR 2011:4 s. 25.
[22] RiR 2014:4 s. 31 f.
[23] Riksrevisionens granskningsrapport RiR 2011:4., s. 79 f.

1.8 Grundläggande begrepp

Nedan redovisas ett antal grundläggande begrepp som förekommit frekvent under utredningens arbete. Då dessa begrepp inte kan sägas ha några allmängiltiga definitioner anser utredningen att det är viktigt att klargöra vad som avses med begreppen inom ramen för denna rapport.

Säkerhetskultur

Utredningen ska enligt direktiven undersöka säkerhetskulturen inom Transportstyrelsen med avseende på risker med relevans för den aktuella upphandlingsprocessen. Då begreppet säkerhetskultur inte kan anses vara ett vedertaget begrepp finns ett behov av att definiera begreppet.

Utredningen ser säkerhetskultur som de gemensamma attityder, värderingar och uppfattningar som chefer och anställda har om säkerhet. Säkerhetskulturen har alltså stor betydelse för hur man arbetar. Det som kännetecknar en god säkerhetskultur på en myndighet är att ledningen prioriterar och hanterar säkerhetsfrågor på alla nivåer i verksamheten och att de är en del av "kulturen".

Skyddsvärd information

Definitionen av begreppet skyddsvärd information beror på vilken verksamhet/organisation det handlar om. Vad som är skyddsvärd information bestäms alltså till stor del av verksamheten själv genom interna krav men också genom externa krav i form av lagar och föreskrifter. I dagens samhälle är tillgång till tillförlitlig information en kritisk resurs. Det är därför viktigt att myndigheterna genom informationsklassning tar ställning till vilken skyddsvärd information de hanterar.

En stor del av den information som skapas och lagras i samhället är viktig och samtidigt känslig. Personuppgifter kan innehålla integritetskänslig information, vilket därför omgärdas av särskild lagstiftning, t.ex. information i patientjournaler, brottsutredningar

eller underrättelseverksamhet. Andra exempel på känslig information rör tekniska produkter, affärsförhållanden och förhållanden som rör andra stater.[24]

En mer allmängiltig definition av begreppet skyddsvärd information skulle kunna vara: ”Skyddsvärd information är sådan information som myndigheten genom informationsklassning/säkerhetsanalys anser är värd att skydda med hänsyn taget till konsekvensen av vad skadan blir om informationen inte är tillgänglig, riktig eller har röjts för obehöriga”.

Säkerhetsskydd

Säkerhetsskydd syftar enligt 6 § säkerhetsskyddslagen (1996:627) till att förebygga spioneri, sabotage, terrorism och andra brott som kan hota rikets säkerhet samt att skydda uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) och som rör rikets säkerhet. Detta sker genom att samtliga myndigheter enligt 5 § säkerhetsskyddsförordningen (1996:633) bl.a. ska undersöka vilka uppgifter som ska hållas hemliga med hänsyn till rikets säkerhet (säkerhetsanalys).

Verksamhet som omfattas av säkerhetsskyddslagstiftningen ska ha det säkerhetsskydd som behövs med hänsyn till verksamhetens art, omfattning och övriga omständigheter. Det är säkerhetsanalysen som utgör grunden för säkerhetsskyddsarbetet på en myndighet. Analysen ska definiera vad som är skyddsvärt och varför det är skyddsvärt. En säkerhetsanalys ska således svara på frågorna *vad ska skyddas*, *mot vad* och *hur*. Baserat på säkerhetsanalysen behöver myndigheterna sedan t.ex. anpassa sin tillträdesbegränsning (behörighetshantering), informationssäkerhet och säkerhetsprövning av personal samt kontinuerligt utbilda sin personal.

Informationssäkerhet[25]

Informationssäkerhet innebär att skydda information utifrån krav på dess konfidentialitet, riktighet och tillgänglighet. Det gäller såväl

[24] *Informationssäkerheten i den civila statsförvaltningen*, Riksrevisionen, RIR 2014:23 s. 23.
[25] Källa: Myndigheten för samhällsskydd och beredskaps hemsida.

hos enskilda som hos organisationer, både i näringslivet och i offentlig verksamhet. Informationssäkerhet omfattar därför hela samhället, och är en angelägenhet för alla. I och med den ökande it-användningen i samhället är informationssäkerhet en förutsättning för att nya företeelser i samhället som till exempel e-förvaltning ska kunna fungera.

Informationssäkerhet omfattar de åtgärder som vidtas för att hindra att information läcker ut, förvanskas eller förstörs och för att informationen ska vara tillgänglig när den behövs. Informationen som ska skyddas kan vara tryckt på papper, vara lagrad elektroniskt, överföras med post eller med elektroniska hjälpmedel, visas på film eller yttras i en konversation.[26]

Brister i hantering av information leder till ett försämrat förtroende för tjänster och bakomliggande aktörer, och kan därför äventyra aktörens verksamhet och användningen av dess tjänster. Allvarliga och upprepade störningar kan leda till förtroendekriser, som också kan sprida sig till fler aktörer och tjänster och även till andra sektorer.

It-säkerhet

It-säkerhet handlar om att skydda en organisations tillgångar som information, maskinvara och programvara. It-säkerhet ingår som en beståndsdel i det totala säkerhetsramverket och ska utgöra skydd mot allehanda hot och faror mot organisationen och dess verksamhet, t.ex. olika katastrofer/olyckor, främmande makter och individer, medarbetare och dåligt utformad verksamhet. It-säkerhet koncentrerar sig på hot och skydd förenade med användning av informationsteknik. En viktig del i it-säkerhet är datasäkerheten som bland annat innebär att skydda sig mot hackare och datorvirus eller stöld av information på en dator eller i ett datornätverk samt att ha arbetssätt så att informationen inte oavsiktligt förstörs.

I detta sammanhang är en organisations behörighetshantering och logghantering mycket viktiga.

[26] Bestämmelser om informationssäkerhet finns i 9 § säkerhetsskyddslagen, 9–13 §§ säkerhetsskyddsförordningen samt i 2–4 kap. PMFS 2015:3.

2 Tillämpliga bestämmelser

2.1 Inledning

I detta kapitel redogörs för de bestämmelser som bedömts vara relevanta för utredningens arbete.

2.2 Offentlig upphandling

I första hand styrs upphandlingar enligt reglerna i lagen (2016:1145) om offentlig upphandling[27] men också lagen (2016:1146) om upphandling inom försörjningssektorerna, lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet, LUFS, och lagen (2016:1147) om upphandling av koncessioner kan vara aktuella.

Reglerna för offentlig upphandling bygger på EU-direktiv och är till stor del likadana inom hela EU. Grundprinciperna bygger på objektivitet och öppenhet. De upphandlande myndigheterna ska vara sakliga och välja leverantör utifrån det som köps. Valet av leverantör ska ske på affärsmässig grund och baseras på vilken leverantör som erbjuder den bästa varan eller tjänsten till de bästa villkoren.

För den aktuella upphandlingen gällde bestämmelserna i den numera upphävda lagen (2007:1091) om offentlig upphandling (LOU). Nedanstående redogörelse avser således denna lagstiftning.

Lagen (2007:1091) om offentlig upphandling

Lagen gäller enligt 1 kap. 1 § LOU för offentlig upphandling av byggentreprenader, varor och tjänster samt av byggkoncessioner. Av

[27] Denna lag trädde i kraft den 1 januari 2017 då lagen (2007:1091) upphävdes. Av punkt 3 i övergångsbestämmelserna framgår att den upphävda lagen gäller för sådan upphandling som påbörjats före ikraftträdandet.

1 kap. 9 § LOU framgår att upphandlande myndigheter ska behandla leverantörer på ett likvärdigt och icke-diskriminerande sätt samt genomföra upphandlingar på ett öppet sätt. Vid upphandlingar ska vidare principerna om ömsesidigt erkännande och proportionalitet iakttas.

En upphandling kan ske i olika former och i lagen definieras de upphandlingsformer som är godkända. De upphandlingsformer som finns är öppet förfarande, förhandlat förfarande, konkurrenspräglad dialog, selektivt förfarande, direktupphandling och förenklat förfarande. Av 4 kap. 1 § LOU framgår att huvudregeln är att öppet eller selektivt förfarande ska användas.

Med förhandlat förfarande avses enligt 2 kap. 9 § LOU ett förfarande där den upphandlande myndigheten inbjuder utvalda leverantörer och förhandlar om kontraktsvillkoren med en eller flera av dem. Förhandlat förfarande med eller utan föregående annonsering får användas under de förutsättningar och på det sätt som anges i 4 kap. 2–9 §§ LOU.

Förhandlat förfarande med föregående annonsering får enligt 4 kap. 2 § LOU användas bl.a. om det som ska upphandlas är av sådant slag eller förenat med sådana risker att det på grund av särskilda omständigheter inte går att ange något totalpris i förväg.

Av 4 kap. 3 § LOU framgår att vid förhandlat förfarande med föregående annonsering ska en upphandlande myndighet förhandla med anbudsgivarna om de anbud som de har lämnat, för att anpassa anbuden till de krav som myndigheten har angett i annonsen om upphandling och i förfrågningsunderlaget samt för att få fram det bästa anbudet.

Lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet

LUFS, som trädde i kraft den 1 november 2011, genomför Europaparlamentets och rådets direktiv 2009/81/EG av den 13 juli 2009 om samordning av förfarandena vid tilldelning av vissa kontrakt för byggentreprenader, varor och tjänster av upphandlande myndigheter och enheter på försvars- och säkerhetsområdet. LUFS ersatte det undantag för upphandling som rör rikets säkerhet som tidigare fanns i 15 kap. 22 § LOU. Syftet med direktivet inom försvars- och säkerhetsområdet är att skapa förutsättningar för upphandlingar av sådan

materiel och sådana tjänster som är av så känslig natur att de ordinarie upphandlingsreglerna inte lämpar sig för sådana inköp. De viktigaste skillnaderna mot den klassiska sektorn och försörjningssektorn är att direktivet innehåller bestämmelser om informationssäkerhet, försörjningstrygghet och underentreprenad.

Säkerhetsskyddad upphandling

När en myndighet (stat, kommun eller landsting) avser att begära in ett anbud eller träffa avtal om upphandling där det i förfrågningsunderlaget eller under uppdragets utförande förekommer hemliga uppgifter eller där leverantören kommer att delta i verksamhet med betydelse för rikets säkerhet, ska myndigheten enligt 8 § säkerhetsskyddslagen (1996:627) träffa ett skriftligt säkerhetsskyddsavtal med anbudsgivaren eller leverantören om det säkerhetsskydd som behövs i det särskilda fallet.

Innehåller förfrågningsunderlaget hemliga uppgifter ska ett säkerhetsskyddsavtal träffas redan innan underlaget lämnas ut till anbudsgivaren. I annat fall ska ett säkerhetsskyddsavtal träffas senast innan affärsavtalet träffas. Anledningen är att det ska finnas ett tillfredsställande säkerhetsskydd innan företaget får del av hemliga uppgifter.

Säkerhetsanalys

Enligt 5 § säkerhetsskyddsförordningen ska myndigheter och andra som förordningen gäller för undersöka vilka uppgifter i deras verksamhet som ska hållas hemliga med hänsyn till rikets säkerhet och vilka anläggningar som kräver ett säkerhetsskydd med hänsyn till rikets säkerhet eller skyddet mot terrorism. Detta ska dokumenteras i en säkerhetsanalys. I 1 kap. 5 § andra stycket i Säkerhetspolisens föreskrifter (PMFS 2015:3) anges att av säkerhetsanalysen bör framgå vilka it-system som behandlar uppgifter som är av betydelse för rikets säkerhet och vilka it-system som är i behov av skydd mot terrorism.

Säkerhetskyddsavtal

Syftet med säkerhetsskyddsavtalet är att de intressen som säkerhetsskyddslagstiftningen slår vakt om ska ha samma nivå på säkerhetsskyddet oavsett vart och hur verksamheten bedrivs. Myndigheten ska alltså ställa samma krav på nivå på säkerhetsskydd hos leverantörer som de ställer i sin egen verksamhet. Detta gäller både huvudleverantör och eventuella underleverantörer som tar del av hemliga uppgifter eller deltar i verksamhet med betydelse för rikets säkerhet. En huvudleverantör kan aldrig gentemot myndigheten ansvara för säkerhetsskyddet hos en underleverantör.

Säkerhetsskyddsavtalet bör i tillämpliga delar innehålla överenskommelse om säkerhetsskyddsorganisation, säkerhetsskyddsinstruktion, informationssäkerhet, behörighet, tillträdesbegränsning, säkerhetsprövning inklusive placering i säkerhetsklass och registerkontroll, utbildning och kontroll, tillsyn, fördelning av kostnaderna för säkerhetsskyddet, tystnadsplikt, äganderättsförhållanden och avtalsperiod.[28] Säkerhetsskyddsavtalet utgör också grunden för uppdragets placering i säkerhetsklass och beslut om registerkontroll. Ett säkerhetsskyddsavtal måste träffas innan registerkontroll får genomföras.

I affärsavtalet avseende de ekonomiska villkoren ska det göras en hänvisning till säkerhetsskyddsavtalet. En klausul ska alltid tas in i affärsavtalet som fastställer att säkerhetsskyddsavtalet gäller framför affärsavtalet om det förekommer motstridiga uppgifter i affärsavtalet. Hela förfarandet med den säkerhetsskyddade upphandlingen måste vara klart innan något arbete påbörjas eller hemliga uppgifter lämnas ut.

Myndigheten är skyldig att meddela Säkerhetspolisen när ett säkerhetsskyddsavtal har ingåtts eller upphört att gälla.[29]

Säkerhetsskyddsinstruktion

När ett säkerhetsskyddsavtal har ingåtts ska leverantören upprätta en säkerhetsskyddsinstruktion.[30] I instruktionen ska denne redovisa

[28] *Säkerhetsskyddad upphandling – en vägledning*, Säkerhetspolisen 2013, s. 12.
[29] 7 kap. 8 § Säkerhetspolisens föreskrifter och allmänna råd om säkerhetsskydd (PMFS 2015:3).
[30] 7 kap. 6 § PMFS 2015:3.

vilka säkerhetsskyddsåtgärder som kommer att vidtas för att uppfylla kraven i säkerhetsskyddsavtalet.

Säkerhetsskyddsinstruktionen ska godkännas av myndigheten. Av säkerhetsskyddsinstruktionen bör det exempelvis framgå hur myndighetens säkerhetsskyddsorganisation är utformad, en rutin för handläggning av säkerhetsprövning, regler och rutiner kring informationssäkerhet, tillträdesbegränsning, utbildningsplan för anställda, rutiner avseende internkontroll.[31] Om leverantören ska hantera och förvara hemliga uppgifter i sina egna lokaler ska myndigheten besöka företaget för att kontrollera att lokaler och övriga förhållanden är lämpliga från säkerhetsskyddssynpunkt.[32]

Krav på säkerhetsprövning

Alla som ska delta i uppdraget och som kan antas få del av hemliga uppgifter, eller delta i verksamhet av betydelse för rikets säkerhet ska säkerhetsprövas.[33] Om uppdraget är placerat i säkerhetsklass ska även en registerkontroll göras.[34] De som får del av hemliga uppgifter eller deltar i verksamheten ska upplysas om den tystnadsplikt som gäller. Ska företaget ansvara för säkerhetsprövningen av sina anställda och informationen om registerkontroll, ska formerna för detta regleras i säkerhetsskyddsavtalet. Framställan om registerkontroll görs hos Säkerhetspolisen.[35]

Det finns inga hinder i säkerhetsskyddslagen för att i ett uppdrag använda ett utländskt företag eller en utländsk medborgare, som därmed kan få del av hemliga uppgifter. Särskild hänsyn bör dock tas till svårigheten att genomföra en adekvat och trovärdig säkerhetsprövning. Normalt bör det här ställas högre krav på inhämtning av referenser än om säkerhetsprövningen gäller en svensk medborgare.[36]

[31] *Säkerhetsskyddad upphandling – en vägledning*, Säkerhetspolisen 2013, s. 13.
[32] 7 kap. 5 § PMFS 2015:3.
[33] 11 § säkerhetsskyddslagen.
[34] 12 § säkerhetsskyddslagen.
[35] 8 kap. 1 § PMFS 2015:3.
[36] *Säkerhetsskyddad upphandling – en vägledning*, Säkerhetspolisen 2013, s. 16.

2.3 Säkerhetsskyddslagstiftningen

Syftet med säkerhetsskyddslagen är bl.a. att ge säkerhetsskydd för statlig verksamhet som är av betydelse för rikets säkerhet eller som särskilt behöver skyddas mot terrorism. Till säkerhetsskyddslagen finns säkerhetsskyddsförordningen (1996:633) som bl.a. reglerar hur myndigheter på en mer detaljerad nivå ska arbeta med sitt säkerhetsskydd. Därutöver har tillämpningsföreskrifter och allmänna råd meddelats av Säkerhetspolisen och Försvarsmakten.[37] Föreskrifterna innehåller utförliga bestämmelser om hur uppgifter, som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400), OSL, och som rör rikets säkerhet, ska hanteras när det gäller t.ex. informationssäkerhet för it-system.

Säkerhetsskyddslagen är direkt tillämplig för såväl myndigheter, kommuner och landsting som verksamhet som bedrivs i olika företagsformer (1 § säkerhetsskyddslagen).

Säkerhetsskyddsåtgärder

Med säkerhetsskyddet avses bl.a. skydd mot spionerі, sabotage och andra brott som kan hota rikets säkerhet, skydd i andra fall av uppgifter som omfattas av sekretess enligt OSL och som rör rikets säkerhet, och skydd mot terrorism (6 § säkerhetsskyddslagen).

I 7 § säkerhetsskyddslagen anges närmare vad säkerhetsskyddet ska syfta till genom bestämmelser om de tre inriktningarna för säkerhetsskyddsåtgärder. En av säkerhetsskyddsåtgärderna i lagen är informationssäkerhet (7 § p. 1 säkerhetsskyddslagen).

Informationssäkerhet ska förebygga att uppgifterna obehörigen röjs, ändras eller förstörs. Vilka åtgärder en myndighet är skyldig att vidta i informationssäkerhetshänseende regleras såväl i säkerhetsskyddslagen som i säkerhetsskyddsförordningen och i Säkerhetspolisens föreskrifter.

De andra två säkerhetsskyddsåtgärderna är tillträdesbegränsning och säkerhetsprövning. Säkerhetsprövning är en säkerhetsskyddsåtgärd som vidtas i syfte att förhindra att personer som inte är pålitliga ur säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet (7 § p. 3 säkerhetsskyddslagen).

[37] PMFS 2015:3 samt Försvarsmaktens föreskrifter om säkerhetsskydd (FFS 2015:2).

Informationssäkerhet

Behovet av skydd vid automatisk informationsbehandling ska beaktas särskilt vid utformningen av informationssäkerheten (9 § säkerhetsskyddslagen). Av säkerhetsskyddsförordningen framgår bl.a. krav på att ett system som ska användas av flera personer för automatiserad behandling av hemliga uppgifter ska vara försett med funktioner för behörighetskontroll och registrering av händelser i systemen som är av betydelse för säkerheten (12 § säkerhetsskyddsförordningen). Ytterligare bestämmelser om informationssäkerhet för it-system finns i 4 kap. PMFS 2015:3.

Särskilt om säkerhetsprövning

Säkerhetsprövning är en säkerhetsskyddsåtgärd som ska vidtas i syfte att förhindra att personer som inte är pålitliga ur säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet (7 § p. 3 säkerhetsskyddslagen). Säkerhetsprövning ska göras innan en person genom anställning eller på annat sätt deltar i verksamhet som har betydelse för rikets säkerhet (11 § säkerhetsskyddslagen). Alla personer som ska delta i ett uppdrag och som kan antas få del av hemliga uppgifter, eller delta i verksamhet av betydelse för rikets säkerhet ska säkerhetsprövas. Om uppdraget är placerat i säkerhetsklass ska även en registerkontroll göras. De som får del av hemliga uppgifter eller deltar i verksamheten ska upplysas om den tystnadsplikt som gäller.

I 11 § säkerhetsskyddslagen anges att prövningen ska klarlägga om personen kan antas vara lojal mot de intressen som skyddas av säkerhetsskyddslagen och i övrigt pålitlig från säkerhetssynpunkt.

Av 27 § säkerhetsskyddslagen framgår att säkerhetsprövningen ska grundas på den kunskap som finns om den som prövas, de uppgifter som kommit fram vid registerkontroll och särskild personutredning, arten av den verksamhet för vilken prövningen görs samt omständigheterna i övrigt. Vidare framgår av 14 § säkerhetsskyddsförordningen att prövningen innebär kontroll av betyg, intyg och referenser och även en identitetskontroll.

Med registerkontroll avses enligt 12 § säkerhetsskyddslagen att uppgifter hämtas från ett register som omfattas av lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister eller

lagen (2010:362) om polisens allmänna spaningsregister samt att uppgifter som behandlas med stöd av polisdatalagen (2010:361) hämtas in. Det krävs att den som ska kontrolleras ger sitt samtycke innan någon registerkontroll genomförs (19 § säkerhetsskyddslagen).

Intern utbildning och kontroll

Myndigheter och andra som lagen gäller för ska se till att personalen får utbildning i frågor om säkerhetsskydd och att säkerhetsskyddet kontrolleras (30 § säkerhetsskyddslagen). Syftet med den interna kontrollen är att se till att bestämmelserna om säkerhetsskydd efterlevs vid den egna myndigheten och att skyddsnivån är jämn och hög.

Tillsyn, föreskrifter och anmälan till regeringen

Säkerhetspolisen och Försvarsmakten utför tillsyn av myndigheter enligt den fördelning av ansvaret som anges i 39 § säkerhetsskyddsförordningen.

Av 43 och 44 §§ framgår att Säkerhetspolisen får meddela närmare föreskrifter i fråga om förfarandet vid registerkontroll och att Säkerhetspolisen och Försvarsmakten i övrigt får meddela föreskrifter för sina respektive tillsynsområden.

Övriga myndigheters föreskriftsrätt regleras i 45 §, där det anges att myndigheterna ska meddela ytterligare föreskrifter om verkställigheten av säkerhetsskyddslagen i fråga om säkerhetsskyddet inom sina verksamhetsområden, om det inte är uppenbart obehövligt.

I 48 och 49 §§ säkerhetsskyddsförordningen finns bestämmelser om anmälan till regeringen. Sådan anmälan ska göras, bl.a. om det vid utövandet av tillsyn över säkerhetsskyddet konstateras brister som, trots påpekanden, inte rättas till.

2.4 Offentlighets- och sekretesslagen (2009:400)

Reglerna i offentlighets- och sekretesslagen gäller i första hand myndigheters verksamhet men de gäller även hos bl.a. kommunala bolag

och stiftelser samt hos vissa utpekade organ (2 kap. 1, 3 och 4 §§). Sekretess innebär ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnade av en allmän handling eller på något annat sätt (3 kap. 1 §). Det saknar således betydelse om uppgiften dokumenterats i en allmän handling, i en handling som inte är allmän eller om den inte alls har dokumenterats.

En myndighet som anlitar en utomstående aktör, t.ex. en driftleverantör, för att bearbeta, lagra eller på annat sätt hantera myndighetens information måste pröva om det är tillåtet att lämna ut informationen till leverantören i fråga och vilka eventuella konsekvenser ett utlämnande kan få. Utlämnandet måste vara förenligt med gällande sekretesslagstiftning för att vara lagligt. Om en leverantör anlitar underleverantörer måste myndigheten också ta ställning till om sekretess gäller mot dessa. Om en leverantör eller dess underleverantör kommer att lagra informationen utanför Sveriges gränser blir det ytterligare frågor att beakta.

Kopplingen mellan säkerhetsskyddslagen och offentlighets- och sekretesslagen

Som framgår av redovisningen av säkerhetsskyddslagen ovan är säkerhetsskyddslagen i hög grad uppbyggd kring behovet av åtgärder för att skydda hanteringen av hemliga uppgifter. Med hemlig uppgift avses en uppgift som omfattas av sekretess enligt OSL och som rör rikets säkerhet (4 § p. 1 säkerhetsskyddsförordningen). Bestämmelserna om informationssäkerhet tar sikte på hemliga uppgifter (7 § p. 1 säkerhetsskyddslagen). Också bestämmelser om placering i säkerhetsklass (17 § säkerhetsskyddslagen) utgår från att en anställd eller den som annars deltar i verksamheten får del av hemliga uppgifter.

I OSL är det främst den s.k. försvarssekretessen i 15 kap. 2 § som avser förhållanden av betydelse för rikets säkerhet. Det finns andra sekretessbestämmelser där det primära skyddsintresset är ett annat men som samtidigt kan avse förhållanden som i vissa fall kan vara av betydelse även för rikets säkerhet. Det gäller för utrikessekretessen i 15 kap. 1§ och förundersökningssekretessen i 18 kap. 1 §. Även övriga bestämmelser om sekretess i 18 kap. kan ge ledning om vilka slag av förhållanden som kan vara av betydelse för rikets säkerhet.

Utlämnande av sekretessbelagda uppgifter till en leverantör

Den som omfattas av tystnadsplikt som har författningsstöd t.ex. enligt OSL, och som felaktigt röjer en uppgift kan i vissa fall dömas för brott mot tystnadsplikten (20 kap. 3 § brottsbalken). När uppgifter lämnas ut till en privaträttslig aktör är det däremot ovanligt att personalen omfattas av en straffsanktionerad tystnadsplikt.

E-delegationen har i en förstudie framhållit att OSL kan tolkas på ett sätt som normalt sett ger tillräckligt stort utrymme för att utlämnanden till tjänsteleverantörer ska kunna ske, förutsatt att tjänsteavtalet tydligt anger leverantörens befogenheter och skyldigheter i fråga om tystnadsplikt, behandling av personuppgifter, rätten att ta del av information och egenkontroll av överträdelser.[38] Det är inte säkert att detta gäller när det är fråga om uppgifter av särskilt integritetskänsligt slag (som medicinska uppgifter)[39] eller uppgifter som t.ex. gäller rikets säkerhet. Myndigheten måste då ta ställning till om uppgifterna kommer att göras tillgängliga för leverantören på ett sådant sätt att de kan anses vara röjda i OSL:s mening. E-delegationen anser att det inte bör betraktas som ett röjande i OSL:s mening om en hemlig uppgift har gjorts tillgänglig för en utomstående på ett sådant sätt att det förefaller osannolikt att mottagaren faktiskt tar del av uppgifterna. Vid outsourcing av it-drift skulle det kunna säkerställas genom att tjänsteavtalet har försetts med ett tydligt förbud för leverantören och dennes personal att ta del av den information som hanteras i systemen, krav på kontrollmekanismer och kännbara civilrättsliga sanktioner vid överträdelser.[40]

E-delegationen har också granskat möjligheten för en myndighet att tillämpa den sekretessbrytande bestämmelsen i 10 kap. 2 § OSL för att kunna lämna ut sekretessbelagda uppgifter till exempelvis en driftsleverantör. Myndigheten måste i ett sådant fall överväga om det finns andra alternativ än att tillgängliggöra uppgifter. Något lägre kostnader eller något högre effektivitet är troligen inte tillräckligt

[38] E-delegationen poängterar dock att rättsläget måste bedömas som osäkert. *Sekretess vid outsourcing – en förstudie*, Fi 2009:01/2015/4, 2015-03-19, s. 8–9. E-delegationens bedömningar i dessa avseenden gäller enbart utlämnande av uppgifter till en tjänsteleverantör som är etablerad i Sverige och som hanterar informationen inom landets gränser. E-delegationen tog inte heller ställning till användandet av underleverantörer.
[39] Se JO:s beslut den 9 september 2014, dnr 3032–2011 avseende patientjournaler.
[40] E-delegationens förstudie s. 6–7.

för att outsourcingen ska anses nödvändig i den mening som avses i bestämmelsen.[41]

2.5 Lagen (2006:939) om kvalificerade skyddsidentiteter

Med en kvalificerad skyddsidentitet avses enligt 1 § lagen om kvalificerade skyddsidentiteter en särskilt beslutad skyddsidentitet som består av andra personuppgifter än de verkliga och som har förts in i statliga register eller i handlingar som har utfärdats av statliga myndigheter.

Ett beslut om kvalificerad skyddsidentitet får enligt 2 § endast avse vissa särskilt angivna personer och enligt 3 § får ett beslut om kvalificerad skyddsidentitet meddelas endast under vissa särskilda omständigheter.

Av 4 § framgår att i ett beslut om kvalificerad skyddsidentitet får det bl.a. förordnas att Transportstyrelsen ska utfärda körkort i den kvalificerade skyddsidentitetens namn. Ett förordnande att Transportstyrelsen ska utfärda körkort i den kvalificerade skyddsidentitetens namn får meddelas endast för den som innehar motsvarande körkort. I samband med förordnandet får det beslutas att Transportstyrelsen eller någon annan körkortsmyndighet ska föra in uppgifter om körkortet i vägtrafikregistret.

2.6 Personuppgiftslagen (1998:204)

Behandling av personuppgifter regleras i personuppgiftslagen (PuL). Personuppgiftslagen grundar sig på dataskyddsdirektivet[42] och har till syfte att skydda människor mot att deras personliga integritet kränks när personuppgifter behandlas (1 § PuL).

Av 2 § PuL följer att om det i lag eller förordning finns bestämmelser som avviker från lagen ska dessa bestämmelser gälla. Särregler i myndigheters registerförfattningar har således företräde. Lagen

[41] A. rapport s. 74.
[42] Den 25 maj 2018 ersätts personuppgiftslagen med dataskyddsförordningen (GDPR). Förordningen kommer att innebära en hel del förändringar för de som behandlar personuppgifter och stärkta rättigheter för den enskilde när det gäller personlig integritet.

(2001:558) om vägtrafikregister är en sådan registerförfattning, se nedan.

Med personuppgift avses all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet (3 § PuL). Begreppet "behandlas" är brett, det omfattar insamling, registrering, lagring, bearbetning, utlämnande, spridning, utplåning, med mera (3 § PuL). Lagen reglerar i princip all hantering av personuppgifter. Behandling av personuppgifter är tillåten endast i de fall och på de villkor som anges i personuppgiftslagen.

Enligt 13 § PuL är vissa personuppgifter att betrakta som känsliga i lagens mening. Det rör sig om personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt personuppgifter som rör hälsa eller sexualliv. Den som behandlar personuppgifter är skyldig att vidta lämpliga säkerhetsåtgärder för att skydda uppgifterna. När känsliga personuppgifter behandlas ställs högre krav på de åtgärder som vidtas.

Även uppgifter som inte klassificeras som känsliga enligt 13 § PuL kan vara särskilt integritetskänsliga och kräva samma höga skyddsnivå som känsliga personuppgifter. Vissa typer av personuppgifter räknas regelmässigt som integritetskänsliga såsom uppgifter om lagöverträdelser, ekonomisk hjälp eller vård inom socialtjänsten, uppgifter inom kreditupplysning eller inkassoverksamhet etc.

Personuppgiftsansvarig och personuppgiftsbiträde

Personuppgiftsansvarig är den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter (3 § PuL) I registerförfattningar finns ofta ett utpekat personuppgiftsansvar, t.ex. är Transportstyrelsen personuppgiftsansvarig enligt lagen om vägtrafikregister. Den personuppgiftsansvarige har ett skadeståndsrättsligt ansvar gentemot de registrerade (48 § PuL).

En aktör som behandlar personuppgifter för den personuppgiftsansvariges räkning kallas personuppgiftsbiträde (3 §). Ett personuppgiftsbiträde är en självständig part i förhållande till den personuppgiftsansvarige och får behandla personuppgifterna bara i enlighet

med de instruktioner som den personuppgiftsansvarige har utfärdat för uppdraget (30 § PuL).

Enligt 30 § andra stycket PuL ska det finnas ett skriftligt avtal om personuppgiftsbiträdets behandling av personuppgifter för den personuppgiftsansvariges räkning. Avtalet ska innehålla instruktioner till biträdet om att denne ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda uppgifterna som behandlas samt villkor som garanterar den personuppgiftsansvariges rätt till insyn och kontroll av biträdets behandling av personuppgifter.

När ett personuppgiftsbiträde anlitar egna underleverantörer ska den ansvarige se till att samtliga underleverantörer, som behandlar personuppgifterna, blir bundna av samma avtalsvillkor som personuppgiftsbiträdet. Detta kan göras antingen genom att den personuppgiftsansvarige tecknar personuppgiftsbiträdesavtal med samtliga underleverantörer eller i avtal samtycker till att leverantören anlitar underleverantörer under förutsättning att denne tecknar avtal med dessa vari framgår att de har samma skyldigheter som personuppgiftsbiträdet.

Säkerhetsåtgärder

Den personuppgiftsansvarige ska enligt 31 § PuL vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av de tekniska möjligheter som finns, vad det skulle kosta att genomföra åtgärderna, de särskilda risker som finns med behandlingen av personuppgifterna och hur pass känsliga de behandlade personuppgifterna är.

Med organisatoriska säkerhetsåtgärder avses bl.a. genomförande av en riskanalys, fungerande administrativa rutiner för behandlingen av personuppgifter, en fastställd säkerhetspolicy samt rutiner för rapportering och uppföljning av säkerhetsincidenter. Med tekniska säkerhetsåtgärder avses bl.a. kryptering, loggning, behörighetsstyrning, inloggningslösningar, säkerhetskopiering och skydd mot skadliga program.

Tillåten behandling

De grundläggande kraven för att behandla personuppgifter återfinns i 9 § PuL. En personuppgiftsansvarig ska bl.a. se till att personuppgifter behandlas bara om det är lagligt, korrekt och i enlighet med god sed, personuppgifter samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål, personuppgifterna är adekvata och relevanta i förhållande till ändamålen, att uppgifterna är riktiga och om nödvändigt aktuella och att personuppgifter inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Överföring av personuppgifter till tredje land

Dataskyddsdirektivet kräver att samtliga medlemsstater, och EES-stater har regler som ger ett likvärdigt skydd för personuppgifter och personlig integritet. Därför kan personuppgifter föras över fritt inom detta område utan begränsningar. Eftersom det inte finns några generella regler som ger motsvarande garantier utanför EU/EES har man ansett att överföring till sådana länder bör begränsas. Personuppgifter får därför 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 (13 § personuppgiftsförordningen [1998:1191] och 33 § PuL).

I 34 § PuL anges ett antal undantag från förbudet mot överföring av personuppgifter till tredje land. Dessa undantag är strikt avgränsade och rör främst fall där riskerna för den registrerade är förhållandevis små, där andra intressen har företräde framför den registrerades rätt till skydd för den personliga integriteten eller där den registrerade har lämnat sitt samtycke till överföringen.

Enligt 35 § PuL får regeringen meddela föreskrifter om undantag från förbudet i 33 § PuL för överföring av personuppgifter till vissa stater, bl.a. finns en möjlighet att använda EU-kommissionens standardavtalsklausuler som är av intresse för denna granskning. EU-kommissionen har fattat beslut om standardavtalsklausuler som kan användas vid överföring av personuppgifter till ett personuppgiftsbiträde i tredje land. Standardavtalsklausulerna är en uppsättning avtalsklausuler som innehåller skyldigheter för personuppgiftsansvariga som vill föra över uppgifter till tredje land

och för personuppgiftsbiträden som tar emot dessa uppgifter. Den personuppgiftsansvarige kan ge personuppgiftsbiträdet i uppdrag att ingå standardavtalsklausuler med ett biträde i tredje land för den ansvariges räkning.

Det bör poängteras att standardavtalsklausulerna ställer långtgående krav på skyddet för personuppgifter och att avtalsparterna måste följa samtliga avtalsvillkor för att personuppgifterna ska anses åtnjuta en adekvat skyddsnivå. En personuppgiftsansvarig bör inte per automatik kunna förlita sig på att användningen av standardavtalsklausulerna säkerställer en adekvat skyddsnivå för personuppgifterna som överförs. För att säkerställa ett adekvat skydd torde den personuppgiftsansvarige även behöva ta ställning till andra omständigheter som kan påverka skyddet för personuppgifterna, t.ex. mottagarlandets nationella lagstiftning och utländska myndigheters möjligheter att ta del av uppgifterna i fråga.[43]

2.7 Arkivlagstiftningen

De bestämmelser som styr statliga myndigheters registrering, arkivering, hantering m.m. av allmänna handlingar finns framför allt i tryckfrihetsförordningen (TF), OSL, arkivlagen (1990:782), arkivförordningen (1991:446) och i Riksarkivets föreskrifter och allmänna råd.

Arkivbestämmelserna omfattar allt material som är att anse som en allmän handling hos en myndighet. Definitionen av en allmän handling i TF är vid.

Av Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (RA-FS 2009:1) framgår bl.a. att en myndighet som upphandlar program eller tjänster för utveckling eller drift av ett system, ska komma överens med leverantören om tillgång till program och dokumentation i den utsträckning som krävs för tillämpningen av föreskrifterna.

I 6 kap. RA-FS 2009:1 ställs krav på informationssäkerhet. För att bedöma behovet av säkerhetsrutiner ska myndigheten t.ex. genomföra en riskanalys innan driftsättning eller innan uppdrag ges till annan myndighet eller enskild.

[43] Pensionsmyndighetens rapport *Molntjänster i staten – En ny generation av outsourcing*, Bilaga Juridisk analys, s. 34.

Riksarkivets föreskrifter ställer långtgående krav på myndighetens förebyggande och löpande hantering av allmänna handlingar i elektronisk form. Många av kraven är sådana att de måste beaktas i myndighetens förberedelser inför en upphandling, t.ex. vid genomförandet av en riskanalys.

2.8 Vägtrafikregistret

Svenska fordon har varit registrerade sedan början av 1900-talet. När den svenska bilregistreringen inleddes fanns 115 bilar registrerade.

Vägtrafikregistret skapades i början av 1970-talet under namnet bilregistret. Bilregistret reglerades i bilregisterkungörelsen (1972:599). Den 1 oktober 2001 trädde lagen (2001:558) om vägtrafikregister (LVTR) i kraft och bilregisterkungörelsen upphörde att gälla. Förordningen (2001:650) om vägtrafikregister (FVTR) trädde i kraft samtidigt.

Vägtrafikregistret innehåller personuppgifter. I vissa delar styrs verksamheten kring registret därför av PuL. Den huvudsakliga regleringen av vägtrafikregistret finns dock i LVTR och FVTR.

LVTR innehåller enligt 1 § i lagen bestämmelser om registrering av uppgifter om personer samt om motordrivna fordon och släpfordon i ett vägtrafikregister.

I fråga om personuppgifter ska vägtrafikregistret ha till ändamål att tillhandahålla uppgifter för bl.a. verksamhet för vilken staten eller en kommun ansvarar enligt lag eller annan författning i fråga om bl.a. fordonsägare, försäkringsgivning m.m.

Personuppgifter förs i vägtrafikregistret i samband med bl.a. registreringar om fordon, körkort, yrkestrafik, förarutbildning, förarprov, parkeringsanmärkningar, fordonsbesiktningar och förarkort för färdskrivare (6 § LVTR). Enligt 7 § LVTR är det Transportstyrelsen som för vägtrafikregistret med hjälp av automatiserad behandling och som är personuppgiftsansvarig för registret enligt PuL.

FVTR innehåller föreskrifter för verkställigheten av LVTR. Av 2 § FVTR framgår att Transportstyrelsen är registreringsmyndighet för vägtrafikregistret och ansvarar för det system- och programmeringsarbete som behövs.

Av 5 kap. 1 FVTR framgår att Polismyndigheten ska underrätta Transportstyrelsen om dom, beslut, strafföreläggande eller föreläggande av ordningsbot avseende ett stort antal brott. I bilagor till FVTR framgår vilka uppgifter som ska registreras avseende fordon, körkort, yrkestrafik, taxi, felparkering, trängselskatt m.m. Det är bl.a. fråga om uppgifter avseende hälsotillstånd och medicinska intyg.

2.9 Myndighetsförordningen (2007:515)

Myndighetsförordningen innehåller centrala och grundläggande bestämmelser om statliga myndigheters ledning, organisation och arbetssätt. Den kompletteras, för respektive myndighet, genom en instruktion där nödvändiga särbestämmelser ges för myndigheten. Myndighetsförordningen gäller enligt 1 § för förvaltningsmyndigheter under regeringen.

Enligt 2 § leds en myndighet av en myndighetschef eller en styrelse eller en nämnd. Av 3 § framgår att myndighetens ledning ansvarar inför regeringen för verksamheten och ska se till att den bedrivs effektivt och enligt gällande rätt och de förpliktelser som följer av Sveriges medlemskap i Europeiska unionen, att den redovisas på ett tillförlitligt och rättvisande sätt samt att myndigheten hushållar väl med statens medel.

Myndighetens ledning ska enligt 4 § besluta en arbetsordning och i denna besluta de närmare föreskrifter som behövs om myndighetens organisation, arbetsfördelningen mellan styrelse och myndighetschef, delegering av beslutsrätt inom myndigheten, handläggning av ärenden och formerna i övrigt för verksamheten. Ledningen ska också besluta en verksamhetsplan för myndigheten, säkerställa att det vid myndigheten finns en betryggande intern styrning och kontroll och avgöra andra ärenden som har principiell karaktär eller större betydelse eller som avser föreskrifter.

Av 6 § framgår myndighetens allmänna uppgifter. Dessa är att fortlöpande utveckla verksamheten och att verka för att genom samarbete med myndigheter och andra ta till vara de fördelar som kan vinnas för enskilda och för staten som helhet.

Särskilda bestämmelser för styrelsemyndigheter finns i 10–16 §§. Enligt 10 § består styrelsen av det antal ledamöter som regeringen

bestämmer. En av ledamöterna ska vara ordförande i styrelsen och en ska vara vice ordförande. Myndighetschefen ska ingå i styrelsen, men inte vara dess ordförande eller vice ordförande. Av 11 § framgår att styrelsen är beslutsför när ordföranden och minst hälften av de andra ledamöterna är närvarande. Myndighetschefen ansvarar enligt 13 § inför styrelsen och ska sköta den löpande verksamheten enligt de direktiv och riktlinjer som styrelsen beslutar. Myndighetschefen ska hålla styrelsen informerad om verksamheten, förse styrelsen med underlag för beslut och verkställa styrelsens beslut.

Att ärenden ska avgöras efter föredragning framgår av 20 §. I arbetsordningen eller i särskilda beslut får myndigheten bestämma att ärenden som avgörs av någon annan person än myndighetens chef inte behöver föredras. Myndighetschefen får fatta beslut utan föredragning i ärenden som inte kan skjutas upp.

För varje beslut i ett ärende ska det enligt 21 § upprättas en handling som visar 1. dagen för beslutet, 2. beslutets innehåll, 3. vem som har fattat beslutet, 4. vem som har varit föredragande, och 5. vem som har varit med vid den slutliga handläggningen utan att delta i avgörandet.

Det är enligt 22 § regeringen som utser ledamöter i styrelser, nämnder och insynsråd. Myndighetschefen anställs enligt 23 § av regeringen. Annan personal anställs av myndigheten.

2.10 Förordningen (2007:603) om intern styrning och kontroll

Förordningen om intern styrning och kontroll (FISK:en) gäller enligt 1 § för förvaltningsmyndigheter under regeringen som har skyldighet att följa internrevisionsförordningen (2006:1228).

Enligt 2 § avses med intern styrning och kontroll den process som syftar till att myndigheten med rimlig säkerhet fullgör de krav som framgår av 3 § myndighetsförordningen. Myndigheten ska enligt 3 § göra en riskanalys i syfte att identifiera omständigheter som utgör risk för att de krav som framgår av 3 § myndighetsförordningen inte fullgörs. Av 4 § framgår att med ledning av riskanalysen ska åtgärder vidtas som är nödvändiga för att de krav som framgår av 3 § myndighetsförordningen ska fullgöras med rimlig säkerhet.

Den interna styrningen och kontrollen ska enligt 5 § systematiskt och regelbundet följas upp och bedömas. Vid bedömningen ska iakttagelser som lämnas vid extern revision och internrevision beaktas. I 6 § anges att riskanalysen enligt 3 §, kontrollåtgärderna enligt 4 § samt uppföljningen och bedömningen enligt 5 § ska dokumenteras.

2.11 Internrevisionsförordningen (2006:1228)

Denna förordning gäller enligt 1 § för förvaltningsmyndigheter under regeringen i den omfattning som regeringen föreskriver i myndighetens instruktion eller i någon annan förordning eller beslutar särskilt.

Enligt 2 § ska det vid myndigheten finnas en internrevision som ska ledas av en chef som ska vara anställd i myndigheten. Av 3 § framgår att internrevisionen ska granska och lämna förslag till förbättringar av myndighetens process för intern styrning och kontroll.

Internrevisionen ska enligt 4 § utifrån en analys av verksamhetens risker självständigt granska om ledningens interna styrning och kontroll är utformad så att myndigheten med en rimlig säkerhet fullgör de krav som framgår av 3 § myndighetsförordningen

I 5 § anges att internrevisionen ska ge råd och stöd till styrelsen och chefen för myndigheten. Resultatet av internrevisionens granskning ska enligt 9 § redovisas i form av iakttagelser och rekommendationer och ska rapporteras till styrelsen. Enligt 10 § ska myndighetens styrelse besluta om riktlinjer för internrevisionen, revisionsplan för internrevisionen, och åtgärder med anledning av internrevisionens iakttagelser och rekommendationer.

Av 11 § framgår att styrelsen ska, i den utsträckning det inte möter hinder på grund av bestämmelse om sekretess, se till att internrevisionen får tillgång till de uppgifter och upplysningar som den behöver för att fullgöra sitt uppdrag.

2.12 Förordningen (2015:1052) om krisberedskap och bevakningsanvariga myndigheters åtgärder vid höjd beredskap[44]

Enligt 8 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap ska varje myndighet i syfte att stärka sin egen och samhällets krisberedskap analysera om det finns sådan sårbarhet eller sådana hot och risker inom myndighetens ansvarsområde som synnerligen allvarligt kan försämra förmågan till verksamhet inom området. Myndigheten ska minst vartannat år värdera och sammanställa resultatet av arbetet i en risk- och sårbarhetsanalys. De myndigheter som har ett särskilt ansvar för krisberedskapen enligt 10 § ska senast vid utgången av oktober månad varje jämnt årtal lämna en sammanfattande redovisning baserad på analysen till Regeringskansliet och Myndigheten för samhällsskydd och beredskap (MSB).

MSB har utifrån bemyndigande i 21 § p. 1 och 2 i förordningen meddelat föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1)[45] och föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser (MSBFS 2016:7)[46].

Av MSBFS 2016:1 framgår att en myndighet bl.a. ska upprätta en informationssäkerhetspolicy och andra styrande dokument som behövs för myndighetens informationssäkerhetsarbete, utse en person som leder och samordnar arbetet med informationssäkerhet och klassificera sin information med utgångspunkt i krav på konfidentialitet, riktighet och tillgänglighet.

[44] Förordningen trädde i kraft den 1 april 2016 och ersatte förordningen (2006:942) om krisberedskap och höjd beredskap.
[45] Föreskrifterna trädde i kraft den 4 april 2016 och ersatte MSBFS (2009:10) om statliga myndigheters informationssäkerhet.
[46] Föreskrifterna trädde i kraft den 1 augusti 2016 och ersatte MSBFS (2015:3) om statliga myndigheters risk- och sårbarhetsanalyser.

3 Transportstyrelsens uppgifter och organisation

3.1 Inledning

Detta kapitel beskriver Transportstyrelsens uppdrag och verksamhet. Kapitlet innehåller även en kortare bakgrund till inrättandet av Transportstyrelsen och vilka överväganden som då gjordes. Vidare innehåller kapitlet en redogörelse för Transportstyrelsens organisation, ansvarsfördelning och styrning.

3.2 Transportstyrelsens uppdrag och verksamhet

Transportstyrelsen har enligt 1 § i förordning (2008:1300) med instruktion för Transportstyrelsen till huvuduppgift att svara för regelgivning, tillståndsprövning och tillsyn inom transportområdet samt att bedriva marknadsövervakning. Transportstyrelsen ska verka för att de transportpolitiska målen uppnås. Verksamheten ska särskilt inriktas på att bidra till ett internationellt konkurrenskraftigt, miljöanpassat och säkert transportsystem. Transportstyrelsens uppgifter gäller samtliga de fyra trafikslagen; järnväg, luftfart, sjöfart och vägtrafik.

Transportstyrelsen har ansvar för ett antal register på transportområdet, bl.a. vägtrafikregistret. Transportstyrelsen driver också in och administrerar olika typer av skatter (t.ex. trängselskatt) och avgifter (t.ex. tillsynsavgifter). Transportstyrelsen har vidare ett myndighetsansvar för flygtrafiktjänst för civil och militär luftfart, vissa uppgifter enligt unionsrätten och internationella överenskommelser, fungerar som överklagandeinstans samt biträder regeringen med beredningen av ärenden i det internationella samarbetet på myndighetens område.

Transportstyrelsen finns på 14 orter i landet och har i dag cirka 1 870 medarbetare. Den största delen av verksamheten finns i Norrköping, Borlänge och Örebro och huvudkontoret är placerat i Norrköping.

3.3 Transportstyrelsen inrättas

Transportstyrelsen inrättades i januari 2009.[47] Myndigheten tog över hela Luftfartsstyrelsens och Järnvägsstyrelsens verksamheter, Sjöfartsverkets och Vägverkets inspektionsverksamhet, regelgivning, tillståndsprövning och tillsyn samt Vägverkets trafikregister. Samtidigt avvecklades Luftfartsstyrelsen och Järnvägsstyrelsen. Den 1 januari 2010 övertog Transportstyrelsen länsstyrelsernas uppgifter inom körkorts- och yrkestrafikområdet.[48]

Regeringen pekade på flera motiv för att inrätta den nya myndigheten. Ett grundläggande skäl var en önskan från regeringens sida om en trafikslagsövergripande myndighet i syfte att förbättra möjligheterna till helhetssyn och möjligheter till lärande mellan olika trafikslag. I detta låg också att renodla roller och funktioner bland myndigheterna inom transportområdet genom att skilja den myndighetsutövande rollen (t.ex. tillsyn) från förvaltarrollen (t.ex. förvaltning av statliga järnvägar).[49] Man ville på detta sätt garantera en effektiv och tillförlitlig tillsyn inom alla trafikslag.[50]

Regeringen pekade på att en förutsättning för en effektiv och tillförlitlig tillsyn är att det råder ett oberoende mellan det organ som utövar tillsynen och den verksamhet som tillsynen avser. Genom Transportstyrelsen skulle tillsyn och normgivning bedrivas skilt från infrastrukturförvaltare och transportansvariga inom hela transportområdet. Regeringen angav också att tillsynen var splittrad och svåröverskådlig inom många områden och att ett samlat tillsynsansvar över hela transportområdet skulle bidra till bl.a. rättssäkerhet och effektivitet.[51]

[47] Tilläggsdirektiv till Transportstyrelseutredningen (dir. 2008:45).
[48] Prop. 2009/10:20.
[49] Prop. 2008/09:31 *Transportstyrelsen och dess verksamhet* s. 47–48.
[50] Se också Transportstyrelseutredningens delbetänkande *En myndighet för all trafik* (SOU 2008:9).
[51] Prop. 2008/09 s. 47–48.

Möjligheten till likformighet och likabehandling mellan trafikslagen när det gäller tillsyn och normgivning lyftes också fram av regeringen som önskvärd. Man menade att förutsättningarna för detta ökade i en samlad verksamhet där det blir möjligt att göra jämförelser av erfarenheter. Regeringen framhöll också att en sammanslagen verksamhet skulle främja framväxten av ett trafikslagsövergripande synsätt vilket skulle medföra fördelar av olika slag. t.ex. att kunskap och erfarenhet från olika områden kan utbytas och samordnas på ett effektivt sätt.[52] I samband med inrättandet av den nya myndigheten kom också dess finansiering att övervägas och regeringens utgångspunkt var därvidlag att den huvudsakligen skulle finansieras genom avgifter från och med 2010.[53]

Ledningsform och organisation då Transportstyrelsen inrättades[54]

Vid inrättandet av Transportstyrelsen fanns det faktorer som talade för ledningsformen styrelse, bl.a. att myndigheten hade ett omfattande ekonomiskt ansvar. Det fanns också faktorer som talade för ledningsformen enrådighet, t.ex. att myndigheten skulle vara oberoende gentemot övriga aktörer inom området, ha en perspektivövergripande funktion och svara för en del myndighetsutövning. Regeringen valde ledningsformen enrådighetsmyndighet med ett insynsråd bestående av sju ledamöter där generaldirektören var ordförande. Det framgår inte klart i förarbetena varför denna ledningsform föredrogs.

Redan 2010 lyfte dock Transportstyrelsens insynsråd frågan om inte styrelseformen vore mer lämplig för myndigheten då insynsrådets roll och mandat uppfattades som otydligt. Dåvarande generaldirektör Staffan Widlert var enligt uppgift drivande bakom detta. Han hade erfarenhet från styrelsemyndighet sedan tidigare och ansåg att det var en bra styrform och att en styrelse har ett tydligare ansvar för verksamheten än ett insynsråd.

Regeringen var av samma mening och ledningsformen ändrades därför till styrelse från den 1 juli 2010. Antalet ledamöter i styrelsen angavs vara lägst fem och högst nio.

---

[52] A. prop. s. 57–58.
[53] Tilläggsdirektiv till Transportstyrelseutredningen (dir. 2008:45).
[54] Se även Statskontoret 2014:33 *Nya myndigheter på transportområdet – fördjupningsfrågor för uppföljning av Trafikverket och Transportstyrelsen*, s. 45 f.

3.4 Transportstyrelsens organisation och förändringar som gjorts

När Transportstyrelsen inrättades fick de verksamheter som förts över från andra myndigheter till en början fortsätta med en i stort sett oförändrad organisation. De tidigare verksamheterna utgjorde relativt självständiga och oberoende divisioner som inte påverkades särskilt mycket av att den nya myndigheten hade inrättats. Det fanns i delar av organisationen en önskan om att man skulle fortsätta arbeta på detta sätt. Ledningen bedömde dock att detta inte bidrog till målen om att arbeta trafikslagsövergripande och åstadkomma lärande mellan trafikslagen.

Dåvarande generaldirektör Staffan Widlert berättar i intervju med utredningen att det redan från början var uppenbart att det behövde göras mer för att myndigheten skulle bli en sammanhållen verksamhet där man tänkte över trafikslagen.

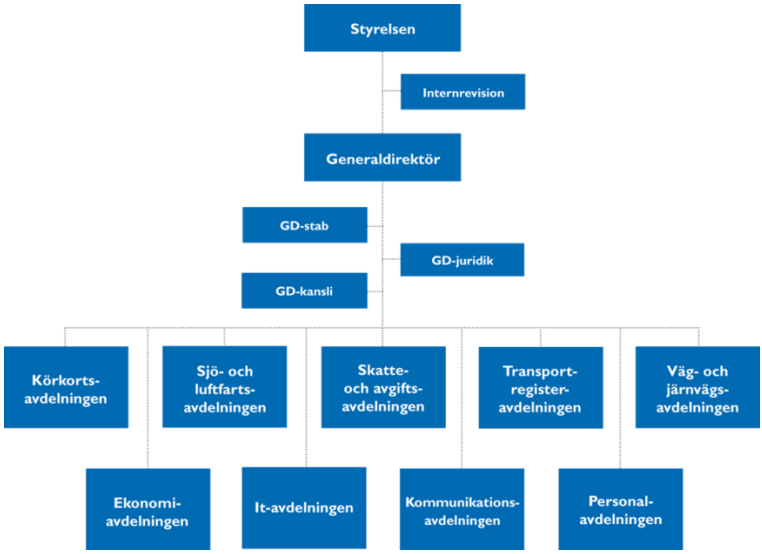
2011 lades vägtrafikavdelningen och järnvägsavdelningen samman till en gemensam avdelning. Under 2011 delades också det tidigare Trafikregistret i Örebro upp i fyra nya avdelningar. It-verksamheten vid Trafikregistret och it-avdelningen på huvudkontoret samlades i en it-avdelning som fick ansvar för all it-verksamhet inom myndigheten. Vid årsskiftet 2012/2013 lades luftfartsavdelningen och sjöfartsavdelningen samman till en gemensam avdelning. En översyn gjordes också av roller, bemanningskrav och kompetensprofiler och nya avdelningschefer rekryterades. Syftet var att förbättra effektiviteten inom myndigheten och förutsättningarna för samordning och skalfördelar framför allt inom de myndighetsövergripande funktionerna.[55]

2013 inleddes ett förändringsarbete där bland annat en översyn gjordes av huvudkontoret, vilket innebar att bemanningen minskade för ekonomi-, kommunikations- och personalavdelningarna.[56]

Transportstyrelsens organisation från 2014 fram till och med den 31 maj 2017 framgår av figur 1. Myndigheten bestod då av nio avdelningar samt tre enheter på ledningsnivå (GD-stab, GD-juridik och GD-kansli). Den nya organisationen som började gälla från den 1 juni 2017 beskrivs närmare i avsnitt 3.10.

[55] Transportstyrelsen Tertialrapport 2011-09-28.
[56] Transportstyrelsen, Årsredovisning 2013, TSG 2014–192.

Figur 1. Transportstyrelsens organisation 2014 – t.o.m. den 31 maj 2017



Källa: Transportstyrelsen.

Sammantaget kan konstateras att Transportstyrelsen sedan starten och fram till idag har genomgått flera mer eller mindre omfattande organisationsförändringar.

3.5 Ansvarsfördelning inom Transportstyrelsen enligt arbetsordningar

Transportstyrelsen har arbetsordningar på flera nivåer. På övergripande nivå finns ”Styrelsens beslut om arbetsordning för Transportstyrelsen”, som beskriver styrelsens ansvar och uppgifter i förhållande till generaldirektören. Den utgår från kraven i bl.a. myndighetsförordningen (2007:515). På myndighetsnivå finns ”Generaldirektörens beslut om arbetsordning för Transportstyrelsen”. Den beskriver organisation, beslutanderätt och delegering, handläggning av ärenden och former för verksamheten i övrigt. Under denna finns arbetsordningar för enskilda avdelningar. Arbetsordningarna för de olika nivåerna är utformade så att de sammantaget ska klargöra ansvarsförhållandena inom myndigheten.

Under perioden 2012–2017 har arbetsordningarna reviderats ett flertal gånger. Ofta är det förändringar i organisationen eller i grunduppdraget som är anledningen. I några fall handlar det om förändrat ansvar mellan styrelse och generaldirektör. Det gäller exempelvis beslut som avser Transportstyrelsens organisation (från styrelse till generaldirektör) och vissa beslut som rör internrevisionen (från generaldirektör till styrelse). I grunden är ansvarsfördelningen dock densamma inom organisationen under den aktuella perioden.

Styrelsen och dess uppgifter

Transportstyrelsen är, som tidigare beskrivits, sedan den 1 juli 2010 en styrelsemyndighet och styrelsen är myndighetens ledning. Av myndighetsförordningen framgår att styrelsen ansvarar inför regeringen för verksamheten och ska se till att den bedrivs effektivt och enligt gällande rätt och de förpliktelser som följer av Sveriges medlemskap i Europeiska unionen, att den redovisas på ett tillförlitligt och rättvisande sätt samt att myndigheten hushållar väl med statens medel. Regeringen är således uppdragsgivare och styrelseledamöterna uppdragstagare med ansvar för uppdraget inför regeringen.

En central rättslig förpliktelse som följer på ansvaret för myndigheten är att styrelsen ska besluta om och skriva under myndighetens årsredovisning. Transportstyrelsen är dessutom en myndighet med internrevision och ska därmed följa internrevisionsförordningen (2006:1228) och förordningen (2007:603) om intern styrning och kontroll (FISK). I anslutning till underskriften av årsredovisningen ska styrelsen lämna en bedömning av huruvida den interna styrningen och kontrollen är betryggande.[57]

Enligt myndighetsförordningen och arbetsordningen för styrelsen[58] ska styrelsen besluta om en arbetsordning. Av arbetsordningen ska framgå de närmare föreskrifter som behövs om myndighetens organisation, arbetsfördelningen mellan styrelse och myndighetschef, delegeringen av beslutanderätt inom myndigheten, handläggningen av ärenden och formerna i övrigt för verksamheten. Styrelsen ska också besluta om verksamhetsplan för myndigheten och säkerställa att det vid myndigheten finns en intern styrning och kontroll

[57] 2 kap. 8 § förordningen (2000:605) om årsredovisning och budgetunderlag.
[58] Transportstyrelsen, 2013-12-19, Arbetsordning Styrelsens beslut om arbetsordning för Transportstyrelsen, TSG 2011–318. Reviderad 2015-06-18 och 2017-02-17.

som fungerar på ett betryggande sätt. Därutöver ska styrelsen besluta om sådana dokument för Transportstyrelsen som är av synnerlig betydelse även utanför myndigheten, liksom för ärenden som styrelsen i övrigt förbehåller sig rätten att avgöra eller som generaldirektören hänskjuter till styrelsen. Styrelsen ska vidare avgöra andra ärenden som har principiell karaktär eller är av större betydelse. Styrelsens beslut och direktiv ska verkställas av generaldirektören.

Styrelsen ska också besluta om riktlinjer och revisionsplan för internrevisionen samt åtgärder med anledning av internrevisionens iakttagelser och rekommendationer.[59]

Internrevisionen

Transportstyrelsen är sedan starten 2009 en internrevisionsmyndighet med inrättad internrevision. Myndigheten ska därmed följa förordningen om intern styrning och kontroll vilket bl.a. innebär att den på ett systematiskt sätt ska hantera risker och dokumentera den interna styrningen och kontrollen. I förordningen anges ett antal obligatoriska moment som ska ingå i processen, nämligen riskanalys, kontrollåtgärder, uppföljning och dokumentation.

Internrevisionen är placerad direkt under styrelsen och dess uppdrag är att granska och lämna förslag till förbättringar av myndighetens process för intern styrning och kontroll. Internrevisionen ska utifrån en analys av verksamhetens risker självständigt granska om ledningens interna styrning och kontroll är utformad så att myndigheten med en rimlig säkerhet fullgör de krav som framgår av 3 § myndighetsförordningen. Som grund för internrevisionens riskanalys används myndighetsledningens analys av risker enligt förordningen om intern styrning och kontroll.

Resultatet av internrevisionens granskning ska redovisas i form av iakttagelser och rekommendationer. Dessa ska rapporteras till styrelsen. Internrevisionen ska också ge råd och stöd till styrelsen och chefen för myndigheten.[60]

[59] 10 § internrevisionsförordningen.
[60] 5 § internrevisionsförordningen.

Generaldirektören

Generaldirektören ansvarar enligt arbetsordningen inför styrelsen och ska sköta den löpande verksamheten enligt de direktiv och riktlinjer som styrelsen beslutar. Generaldirektören ska hålla styrelsen informerad om verksamheten, återrapportera sina kontakter med departementet och andra väsentliga händelser, förse styrelsen med underlag inför beslut och verkställa styrelsens beslut.[61]

Enligt arbetsordningen ska generaldirektören bl.a. besluta om arbetsordning och arbetsformer för Transportstyrelsen[62], verksamhetens mål, inriktning och finansiering enligt styrelsens riktlinjer, åtgärder med anledning av Transportstyrelsens årliga riskanalys och ekonomiska beslut av större betydelse eller som överstiger de belopp som fastställts i särskild delegations- och attestordning för ekonomiska beslut. Vidare ska generaldirektören besluta om styrande eller stödjande dokument av myndighetsövergripande karaktär och Transportstyrelsens föreskrifter, utom sådana som har särskild principiell betydelse eller annars är av större vikt[63].

Generaldirektören ska även besluta om framställningar, yttranden och skrivelser till riksdagen, regeringen och Regeringskansliet. I strategiska och policyskapande frågor ska generaldirektören besluta om framställningar, yttranden och skrivelser till andra statliga myndigheter och organisationer. Detsamma gäller för överenskommelser med andra myndigheter som innebär förpliktelser av viss omfattning för myndigheten.

Generaldirektören ska därutöver besluta om förslag till styrelsen, frågor som har principiell karaktär eller är av större betydelse men som inte behöver avgöras av styrelsen samt ärenden som generaldirektören i övrigt förbehåller sig rätten att avgöra.[64]

[61] Transportstyrelsen, Styrelsens beslut om arbetsordning för Transportstyrelsen, 2013-12-19, 2014-12-18, 2015-06-18, 2017-02-17.
[62] Här avses den reglering som behövs utöver den grundläggande arbetsordning som beslutats av Transportstyrelsens styrelse.
[63] Sådana föreskrifter beslutas av styrelsen enligt styrelseprotokoll 2010–3.
[64] Transportstyrelsen, Styrelsens beslut om arbetsordning för Transportstyrelsen, 2013-12-19, 2014-12-18, 2015-06-18, 2017-02-17. Transportstyrelsen, Generaldirektörens beslut om arbetsordning för Transportstyrelsen, 2013-12-20, 2015-02-25, 2015-06-18, 2017-03-29 och 2017-05-31.

Avdelningschefer

Närmast under generaldirektören har avdelningschefer enligt arbetsordning ansvar för verksamheten vid enskilda avdelningar. En chef för en avdelning ska inom sitt ansvarsområde bl.a. ansvara för ledning, styrning och uppföljning enligt arbetsordning, verksamhetsplan och fastställd budget. De ansvarar också för verksamhetsutveckling. Vidare ska avdelningscheferna se till att verksamheten bedrivs författningsenligt. De ska hålla generaldirektören underrättad om avdelningens kontakter med Regeringskansliet, i frågor av principiell karaktär eller av större betydelse. Avdelningscheferna ska också ta upp viktigare strategiska frågor i den centrala ledningsgruppen innan beslut och i övrigt informera ledningsgruppen om verksamhet som är av vikt för hela organisationen att känna till.

Motsvarande beskrivningar finns också för enhetschef och sektionschef.

En chef för en avdelning får inom sitt ansvarsområde delegera beslutanderätten där så är lämpligt. Avdelningschefen kan bestämma att enhetschefen får vidaredelegera sin beslutanderätt till sektionschef eller annan tjänsteman som har tillräcklig kunskap och erfarenhet för att kunna fullgöra uppgiften. Delegationsbeslut ska vara skriftliga om de inte framgår av en arbetsordning.

Centrala ledningsgruppen

Transportstyrelsens centrala ledningsgrupp leds av generaldirektören. I ledningsgruppen ingår ställföreträdande generaldirektör, samtliga avdelningschefer samt chefsjuristen.

Av Rutinbeskrivning för Transportstyrelsens ledningsgrupp[65] framgår att ledningsgruppen utgör forum för diskussion om strategiska frågor innan beslut fattas, tematiska diskussioner inom myndighetens verksamhetsområden samt ömsesidig information mellan generaldirektör och avdelningschefer.

De ärendetyper som normalt ska behandlas för diskussion eller beslut i ledningsgruppen är frågor om verksamhetens övergripande mål, inriktning och finansiering, strategiska och policyskapande

[65] Transportstyrelsen, Rutinbeskrivning för Transportstyrelsens ledningsgrupp, TSG 2013–185.

frågor som berör flera transportslag eller flera avdelningar samt frågor som kan komma att väcka större uppmärksamhet.

3.6 Ledningsorganisation och berörda avdelningar

Nedan redogörs för de delar av organisationen som är aktuella i utredningens granskning. Det innebär att avdelningar inom kärnverksamheten endast berörs indirekt.

GD-stab, GD-juridik och GD-kansli

Under perioden 2014–2017 (fram till den 31 maj 2017) fanns ledningsfunktionerna GD-stab, GD-juridik och GD-kansli placerade direkt under generaldirektören. De hade roller som stabsfunktion, som stödjande funktion till alla avdelningar och som controllerfunktion.

GD-stab ansvarade bl.a. för att biträda generaldirektören och Transportstyrelsens ledningsgrupp i strategiska frågor som t.ex. myndighetens utvecklingsarbete. GD-stab hade ansvaret för att driva, utveckla, samordna, följa upp och utvärdera det systematiska säkerhetsarbetet och säkerhetsskyddet enligt säkerhetsskyddslagen och säkerhetsskyddsförordningen. Här låg också ansvaret för myndighetens ledningssystem för informationssäkerhet (LIS). Inom GD-stab fanns GD-stabsenheten. En närmare beskrivning av organisationen för säkerhetsfrågor ges i kapitel 4.

GD-juridik ansvarade bl.a. för att biträda generaldirektören och Transportstyrelsens ledningsgrupp i strategiska juridiska frågor. De skulle också tillhandahålla löpande juridiskt stöd till generaldirektören och avdelningar och enheter inom Transportstyrelsen.

GD-kansli ansvarade bl.a. för sekretariaten för Transportstyrelsens styrelse och generaldirektörens ledningsgrupp.[66]

När det gäller it-driftupphandlingen har säkerhetsskyddsfrågor och informationssäkerhetsfrågor hanterats inom GD-stab. Därutöver har ställföreträdande generaldirektör och chefen för GD-stab varit involverade i olika frågor.

[66] Transportstyrelsen, Generaldirektörens beslut om arbetsordning för Transportstyrelsen, 2013-12-20, 2015-02-25, 2015-06-18, 2017-03-29.

It-avdelningen

Enligt arbetsordningen ansvarar It-avdelningen för att driva, utveckla, samordna, följa upp och utvärdera myndighetens it-verksamhet och it-säkerhet, inklusive metoder, modeller, standarder och avtal.[67]

Avdelningen är vidare myndighetens ingång för beställningar av it-verksamhet och ansvarar för att tillhandahålla leveranser och avtalsuppföljning av it-tjänster inklusive drift, it-förvaltningsledning, projektledning och systemutveckling. Det innebär att it-avdelningen har huvudansvaret för upphandlingar av it, medan inköpsenheten vid ekonomiavdelningen fungerar som stöd i upphandlingen. Ytterligare ett ansvarsområde för it-avdelningen är att biträda generaldirektören och Transportstyrelsens ledningsgrupp i strategiska it-frågor.

Inom It-avdelningen fanns fram till den 31 maj 2017 strategienheten som ansvarade för it-säkerhet, it-avtal och avrop. Enheten skulle också förse avdelningen med kompetens för att säkerställa ett rättssäkert agerande i all verksamhet. Drift- och infrastrukturenheten hade ansvaret för kontakter med Transportstyrelsens externa it-leverantörer. De ansvarade också för leverans av effektiva drift- och infrastrukturtjänster, dvs. en balans mellan driftsäkerhet och kostnader.[68]

It-avdelningen har haft huvudansvaret för it-driftupphandlingen och ett flertal personer från olika delar av it-avdelningen har varit drivande eller på andra sätt involverade i upphandlingen och det efterföljande arbetet med transition och transformation.

Ekonomiavdelningen

Ekonomiavdelningen ansvarar bl.a. för att driva, utveckla, samordna, följa upp och utvärdera myndighetens inköpsverksamhet. Inköpsenheten vid ekonomiavdelningen har det samlade ansvaret för myndighetens inköp och upphandlingar. Respektive avdelning ansvarar

[67] Transportstyrelsen, Generaldirektörens beslut om arbetsordning för Transportstyrelsen, 2013-12-20, 2015-02-25, 2015-06-18, 2017-03-29.
[68] Transportstyrelsen, Arbetsordning för It-avdelningen, 2011-12-19, 2012-02-13.

dock för de egna upphandlingarna, med stöd av inköpsenheten. Inköpsenheten har enligt uppgift förstärkts personalmässigt sedan myndigheten bildades.

Avdelningen ansvarar också för myndighetens riskhantering och riskanalys enligt kraven i förordningen (2007:603) om intern styrning och kontroll. Ytterligare ett ansvarsområde är att biträda generaldirektören och Transportstyrelsens ledningsgrupp i strategiska ekonomiska frågor.[69]

Inköpsenheten har haft en central roll i upphandlingen av it-drift. Ekonomidirektören fattade tilldelningsbeslutet innan avtalet skrevs på av generaldirektören.

Personalavdelningen

Personalavdelningen ansvarar bl.a. för myndighetens kompetensförsörjning. Avdelningen ska också biträda generaldirektören och Transportstyrelsens ledningsgrupp i strategiska personalfrågor.[70]

När det gäller it-driftupphandlingen har personalavdelningen hanterat frågor som rör behörigheter. De har också ansvarat för stöd till medarbetare med anledning av Säkerhetspolisens tillsyn.

It-rådet

It-rådet består av företrädare för kärnverksamheten och it-avdelningen och leds av it-direktören. It-rådet är ett beredande organ för strategiska frågor och prioriteringsfrågor mellan kärnverksamheten och it. I it-driftupphandlingen har it-rådet varit styrgrupp för de projekt som genomfört upphandlingen samt projekt för transition och transformation.

[69] Transportstyrelsen, Generaldirektörens beslut om arbetsordning för Transportstyrelsen, 2013-12-20, 2015-02-25, 2015-06-18, 2017-03-29.
[70] Transportstyrelsen, Generaldirektörens beslut om arbetsordning för Transportstyrelsen, 2013-12-20, 2015-02-25, 2015-06-18, 2017-03-29.

3.7 Styrande dokument

Transportstyrelsen har utöver arbetsordningar ett stort antal styrande dokument som reglerar verksamheten. För granskningen av it-driftupphandlingen är bl.a. följande dokument relevanta:

- Transportstyrelsens ledningssystem[71],
- dispositions- och delegationsordning för ekonomiska beslut[72],
- riktlinje för myndighetsövergripande uppföljning av verksamhet och ekonomi[73],
- riktlinje för mål och styrning inom it-området[74],
- riktlinje för it-försörjning[75],
- riktlinje för Transportstyrelsens informationssäkerhet[76],
- riktlinje för krav på informationssäkerhet[77],
- riktlinjer för åtkomst till it-lösningar och infrastrukturkomponenter[78],
- riktlinjer för behörighetsstyrning[79],
- riktlinje för arbetsformen projekt[80],
- rutinbeskrivningar för Transportstyrelsens inköp och upphandling[81],

[71] Transportstyrelsens ledningssystem, 2014-11-28.
[72] Dispositions- och delegationsordning för ekonomiska beslut, 2014-06-09, 2015-05-29, 2015-10-27, 2016-05-04, 2016-09-08, 2017-01-16, 2017-05-16.
[73] Riktlinje för myndighetsövergripande uppföljning av verksamhet och ekonomi, 2016-03-01.
[74] Riktlinje för mål och styrning inom it-området, 2013-02-22.
[75] Riktlinje för it-försörjning, It-försörjningsstrategi, 2012-09-06, TSG 2012–906.
[76] Riktlinje för Transportstyrelsens informationssäkerhet, 2012-03-27, 2014-12-02.
[77] Riktlinje för krav på informationssäkerhet, 2013-01-23.
[78] Riktlinjer för åtkomst till it-lösningar och infrastrukturkomponenter, 2011-05-18.
[79] Riktlinjer för behörighetsstyrning, 2011-05-18.
[80] Riktlinje för arbetsformen projekt, 2011-05-30.
[81] Rutinbeskrivning för Transportstyrelsens inköp, 2015-02-23. 2017-04-20. Rutinbeskrivning för beställning från ramavtal, 2015-02-23, 2017-04-20. Rutinbeskrivning för inköp enligt undantagsbestämmelse i lag om offentlig upphandling (LOU), Hantering av undantag från annonseringsplikt, 2015-02-23, 2017-04-20. Rutinbeskrivning för direktupphandling, 2015-02-23, 2016-10-03, 2017-04-20.

- rutinbeskrivning för informationssäkerhet, it-säkerhet och säkerhetsskydd vid inköp[82],
- rutinbeskrivning för genomförande av informationsklassning[83],
- rutinbeskrivning för hantering av projektdokumentation[84].

Det finns alltså ett flertal interna riktlinjer och rutinbeskrivningar för ledning, inköp, it-styrning, informationssäkerhet etc. Flera av dem har inte uppdaterats sedan de upprättades. Framför allt är det riktlinjer och rutinbeskrivningar inom it-området och för informationssäkerhet och behörigheter som inte uppdaterats.

Dispositions- och delegationsordning för ekonomiska beslut

Ett tilldelningsbeslut ska alltid föregås av ett inköpsbeslut. Enligt dispositions- och delegationsordningen fattas inköpsbeslut av avdelningschef för den egna verksamheten. Enligt medelsdisposition får avdelningschef göra inköp för upp till 10 miljoner kronor. För inköp därutöver ska generaldirektör fatta beslut om inköp.

Tilldelningsbeslut vid upphandling för obegränsat belopp fattas av ekonomidirektören.

Vid avtalstecknande gäller samma gränser som för medelsdispositioner. Avtal ska tecknas i samråd med inköpsenheten.

3.8 Riskanalyser och processen för intern styrning och kontroll

Flera förordningar ställer krav på riskanalys. Enligt förordningen om intern styrning och kontroll ska en riskanalys göras i syfte att identifiera omständigheter som utgör risk för att kraven i 3 § myndighetsförordningen inte kan fullgöras. Internrevisionen ska utifrån en egen riskanalys granska processen för intern styrning och kontroll i myndigheten. Enligt förordning (2015:1052) om krisberedskap och

[82] Rutinbeskrivning för informationssäkerhet, it-säkerhet och säkerhetsskydd vid inköp, 2016-02-22, 2017-04-20, TSG 2015–404.
[83] Rutinbeskrivning för genomförande av informationsklassning, 2013-06-17.
[84] Rutinbeskrivning för hantering av projektdokumentation, 2013-01-08.

bevakningsansvariga myndigheters åtgärder vid höjd beredskap ska Transportstyrelsen vartannat år[85] värdera och sammanställa resultatet av arbetet i en risk- och sårbarhetsanalys som ska redovisas till Regeringskansliet och Myndigheten för samhällsskydd och beredskap (MSB). Därutöver kan regeringen ge särskilda uppdrag om riskanalys, exempelvis har detta gjorts avseende informationssäkerhet. Det finns också andra krav på riskanalys som utredningen inte går in på närmare här.

Intern styrning och kontroll

Transportstyrelsen tog inte förrän 2017 fram en riktlinje för intern styrning och kontroll. Istället har riktlinjen för myndighetsövergripande uppföljning av verksamhet och ekonomi och ledningssystemet varit styrande dokument.

I riktlinjen för uppföljning anges när och hur planerade åtgärder ska rapporteras liksom en uppdaterad riskbedömning. Till detta finns anvisningar för vilket material som ska lämnas in för den riskanalys som ska göras inför verksamhetsplaneringen. I ledningssystemet från 2014 nämns bara att verksamhetsplanen ska innehålla identifierade risker. Enligt ekonomidirektören har det inte funnits någon egentlig styrning av vad som ska göras i processen.

Riskanalyser görs enligt uppgift på varje avdelning i samband med verksamhetsplaneringen på hösten. För att avgöra vilka risker som ska hanteras på myndighetsnivå analyserar Ekonomiavdelningen det samlade materialet. Uppföljning av risker har gjorts kvartalsvis.

Riksrevisionens årliga revision riktade 2016 i en revisionsrapport kritik mot Transportstyrelsens rutiner för intern styrning och kontroll. I revisionsrapporten[86] bedömer Riksrevisionen att den centrala styrningen och uppföljningen av processen för intern styrning och kontroll behöver stärkas. Verksamheten är i behov av tydligare vägledning vad gäller riskanalyser och hur risker ska värderas och hanteras. Stödet till avdelningarna behöver också stärkas och FISK[87]-samordnarna involveras i hela processen.

[85] Kravet fram till 2016 var att myndigheterna skulle ta fram en risk- och sårbarhetsanalys varje år.
[86] Riksrevisionen, Dnr 3.1.2-2016-0570, Revisionsrapport – Rutiner och intern styrning och kontroll 2016.
[87] Samordnar arbetet utifrån förordningen om intern styrning och kontroll (FISK).

Risk- och sårbarhetsanalyser

Risk- och sårbarhetsanalyser (RSA) redovisas vartannat år. Enligt ekonomidirektören har den centrala funktionen på GD-stab genomfört workshops om risk- och sårbarhetsanalyser på avdelningarna. Materialet har därefter sammanställts till en myndighetsövergripande RSA som Regeringskansliet och Myndigheten för samhällsskydd och beredskap sedan fått del av. Styrelsen har inte fått information om RSA.

Enligt uppgift från internrevisionschefen har risk- och sårbarhetsanalyserna inte tagits in i Transportstyrelsens riskanalys vilket ska göras enligt reglerna om intern styrning och kontroll. Internrevisionen har enligt uppgift påpekat att detta behöver ske.

3.9 Ledning och styrning i myndigheten

Utredningen har i sina intervjuer ställt frågor om Transportstyrelsens ledning och styrning. Dokumentgenomgångar har också gjorts som grund för de iakttagelser som redovisas nedan.

3.9.1 Styrelsen har haft en undanskymd roll i outsourcingen av it-drift

Enligt myndighetsförordningen och arbetsordningen ska styrelsen avgöra ärenden som har principiell karaktär eller är av större betydelse. Styrelsens beslut och direktiv ska verkställas av generaldirektören.

Av intervjuer med tidigare styrelseordföranden och generaldirektörer säger samtliga att det inte är självklart vilka ärenden som ska bedömas som strategiskt viktiga och av principiell karaktär i myndigheten. Vilka frågor som tagits upp i styrelsen har bestämts av vad myndigheten själv har velat ta upp och vad styrelsen varit intresserade av. Enskilda styrelseledamöters intressen har också påverkat.

Ansvaret i en styrelsemyndighet beskrivs också som knepigt. Styrelsen och dess ledamöter är ansvariga för verksamheten inför regeringen (förutom att utse och avskeda generaldirektören). Generaldirektören har ansvaret för den operativa verksamheten och har täta kontakter med departementet. Styrelsen och ordföranden träffar

företrädare för den politiska ledningen och departementet mer sällan. Informationen är då i regel redan känd och hanterad av generaldirektören. Detta faktum anses av tidigare styrelseordföranden göra det svårt för styrelsen att ta det fulla ansvaret för verksamheten.

Av intervjuer och styrelseprotokoll framgår att styrelsen fått information om it-driftupphandlingen vid några få tillfällen. Efter att Säkerhetspolisen inledde sin tillsyn har styrelsen varit mer involverad. Styrelsen har inte fattat några beslut om it-driftupphandlingen. I efterhand förklaras detta av dåvarande generaldirektör Staffan Widlert med att it-driftupphandlingen var viktig men inte en principiell fråga i sig. Den sågs som ett vanligt upphandlingsärende som hanterades enligt den ordinarie inköpsprocessen. Tidigare styrelseordförande Rolf Annerberg säger att styrelsen var mer intresserad av stordatormigreringen, eftersom den beskrevs som mer verksamhetskritisk och samhällspåverkande. Styrelsen ställde därmed inte heller några krav på att styrelsen skulle hantera frågan om it-driftupphandlingen.

3.9.2 Generaldirektörernas förhållningssätt har påverkat

Generaldirektören ansvarar enligt arbetsordningen inför styrelsen och ska sköta den löpande verksamheten enligt de direktiv och riktlinjer som styrelsen beslutar.

Staffan Widlert hade som organisationsutredare inför Transportstyrelsens bildande och som första generaldirektör många frågor att hantera. En av de viktigaste frågorna var att få ihop Transportstyrelsens olika verksamheter och kulturer till en. Staffan Widlert hade goda erfarenheter av styrelsemyndigheter sedan tidigare och var enligt uppgift angelägen om att diskutera frågor med styrelsen och få stöd av styrelsen. Detsamma gällde ledningsgruppen. Han hade också en ambition att effektivisera myndigheten och där var åtgärder inom it-avdelningen centrala för att hitta besparingar. Staffan Widlert uppfattades som mycket drivande och drog sig inte för att sätta igång många saker samtidigt. Stordatormigreringen var en fråga som man tidigare försökt åtgärda utan att lyckas. Att sätta igång migrering av stordatorn parallellt med outsourcing av it-drift och upphandling av nytt system för reskontra uppfattades av personal inom it-avdelningen och inköpsenheten som mindre lämpligt.

Maria Ågren tillträdde som generaldirektör den 1 mars 2015. Hon fick då ett kort möte med Staffan Widlert där de gick igenom sådant som var på gång i myndigheten. Hon fick beskrivningen att det var flera upphandlingar på gång inom it, att de var viktiga och att de inte fick gå i stå. Maria Ågren hade tidigare erfarenhet av myndigheter med insynsråd. Det var första gången hon hade en styrelse med fullt ansvar. Hon var ganska trevande i början för att se vilka frågor styrelsen ville ha på agendan.

Styrelsen verkar inte ha ställt några krav på Maria Ågren som ny generaldirektör. Av protokoll från styrelsemöte den 5–6 maj 2015[88] framgår att ”generaldirektören informerade om sina förväntningar och tankar inför styrelsearbetet. Det är angeläget att rätt frågor på rätt nivå och med rätt underlag lyfts till styrelsen. En diskussion i denna del kan därför komma att aktualiseras vid ett senare möte. Generaldirektören konstaterade också att ledningsformen innebär att ledamöterna har ett gemensamt ansvar för verksamheten gentemot regeringen, samt att ledamöterna i detta uppdrag företräder myndigheten, inte enskilda intressen.” Styrelsen lade därefter informationen till handlingarna. Det framgår inte av senare protokoll att frågan har tagits upp på nytt av styrelsen eller generaldirektören.

Av utredningens intervjuer med personal på Transportstyrelsen framkommer å ena sidan att Maria Ågren uppfattades ha tillit till myndighetens medarbetare och förlitade sig på deras kompetens och förmåga. Hon tyckte det var viktigt att vara ute i verksamheten och det fanns de som tyckte att hon gick förbi chefer i linjen. Å andra sidan beskrivs att hon slöt ledningsgruppen nära sig och stängde verksamheten utanför. Maria Ågren uppfattades dock som en erfaren och kompetent ledare som ställdes inför många beslut som hon inte själv hade varit med och tagit fram.

Utredningen konstaterar att generaldirektörerna har haft olika ledarstil gentemot organisationen och olika erfarenhet av styrelsemyndigheter. Båda har dock valt att inte involvera styrelsen i it-driftupphandlingen.

[88] Protokoll från sammanträde med Transportstyrelsens styrelse den 5–6 maj 2015, dnr 2015–02.

3.9.3 Myndighetsövergripande frågor har svårt att få genomslag i verksamheten

När Transportstyrelsen bildades var ett av syftena att få till stånd en mer trafikslagsövergripande verksamhet. Enligt dåvarande generaldirektör Staffan Widlert var det en stor utmaning att få de olika verksamhetsdelarna att samordna sig i en myndighet. I utredningens intervjuer framkommer att verksamheten fortfarande präglas av detta. Varje avdelning fokuserar i första hand på sin verksamhet och sina uppdrag.

Ledningsgruppen och It-rådet syftar båda till att få till ett verksamhetsövergripande förhållningssätt. Tanken är att ledningsgruppen ska stå bakom de beslut som fattas av generaldirektören. Tidigare generaldirektör Staffan Widlert kände enligt uppgift väl till transportområdet och kunde driva frågor gentemot ledningsgruppen. Maria Ågren hade däremot inte lika stor erfarenhet på transportområdet och var därför mån om att ha ledningsgruppen bakom sig. Enskilda avdelningsdirektörer har enligt uppgift kunnat stoppa frågor som inte passat deras verksamhet. Myndighetsövergripande frågor, som exempelvis säkerhetsskydd och informationssäkerhet, har haft svårt att få gehör i ledningsgruppen. Det vittnas om att en konsensuskultur gör att det händer för lite och att myndigheten inte kommer vidare i verksamhetsövergripande frågor.

It-rådet med företrädare för varje avdelning har varit styrgrupp i it-driftupphandlingen och i projekten för transition och transformation. Enligt den tidigare projektägaren för it-driftupphandlingen var det principiellt viktigt att få verksamheten att ta ansvar för bl.a. kravställning i it-driftupphandlingen. It-rådet hade därför en viktig roll för projektet. I praktiken har verksamheten haft svårt att ta ansvar för kravställningen eftersom de inte haft den organisatoriska mognaden och kunskapen. Istället har it-avdelningen fått ta på sig ansvaret och vara drivande. Verksamheten har sett det som att det är en fråga för it-avdelningen, medan it-avdelningen betonat att det är verksamhetens ansvar.

3.9.4 Avstegskultur

Transportstyrelsen har som beskrivits i avsnitt 3.7 tagit fram många riktlinjer och rutinbeskrivningar. Av intervjuer framgår uppfattningen att det finns för många styrdokument, att de har oklar status och att de inte är lätta att hitta. Efterlevnaden sägs bli därefter.

Utredningen har också fått höra att det funnits och finns en avstegskultur inom Transportstyrelsen, framför allt inom upphandlingsområdet. Under åren har det gjorts många avsteg i samband med verksamhetskritiska upphandlingar. Tidigare generaldirektör Staffan Widlert beskriver det som att de interna riktlinjerna har varit viktiga för att tala om vad som gäller i myndigheten samtidigt som beslut om avsteg varit vanliga.

3.9.5 Riskanalyser och granskningar har inte fått genomslag

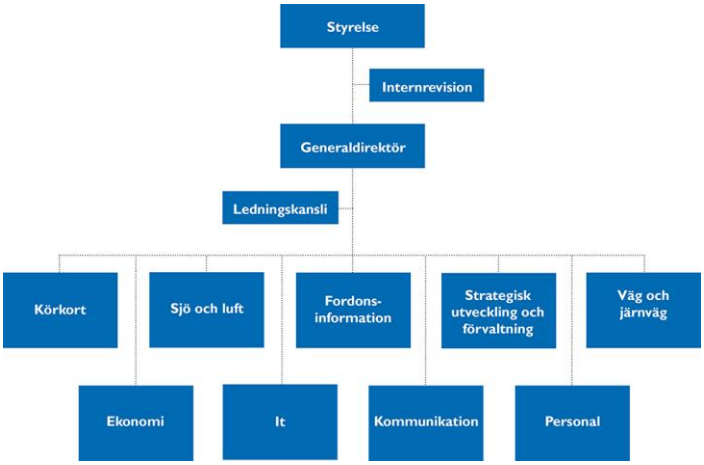
Internrevisionschefen har i intervju med utredningen framfört att internrevisionen tidvis har haft svårt att få gehör för internrevisionens riskanalyser och granskningar i styrelsen och i verksamheten. Internrevision har redovisat en rad iakttagelser och rekommendationer till styrelsen. Exempelvis granskade internrevisionen 2014 myndighetens it-styrning och informationssäkerhet och i riskanalyserna lyfts problem kring it-driftupphandlingen fram. Även i myndighetens riskanalyser och i risk- och sårbarhetsanalyserna har risker inom it-drift och it-styrning tagits upp.

Utredningen har noterat att samma punkter återkommer år efter år, exempelvis informationssäkerhet och behörighetshantering. Enligt uppgift har myndigheten tagit fram planer för att åtgärda problemen. I flera fall har dock frågorna prioriterats ned inom verksamheten och problemen har därmed inte lösts.

3.10 Transportstyrelsens organisation och ansvarsfördelning idag

Från och med den 1 juni 2017 gäller en delvis ny organisation för Transportstyrelsen och en ny arbetsordning.

Figur 2. Transportstyrelsens organisation från den 1 juni 2017.



Källa: Transportstyrelsen.

Direkt under generaldirektören har tidigare GD-stab, GD-juridik och GD-kansli samlats i ett ledningskansli. Inom ledningskansliet finns den ställföreträdande generaldirektören, chefsjuristen och säkerhetsskyddschefen som är direkt underställda generaldirektören. Ansvaret för myndighetens styrande och samordnande arbete med bl.a. säkerhetsskyddsfrågor ligger på ledningskansliet. *Den ställföreträdande generaldirektören* leder och fördelar arbetet inom generaldirektörens kansli för de personer som arbetar med säkerhetsskydds- och krisberedskapsfrågor samt frågor som rör totalförsvaret. *Chefsjuristen* ansvarar bl.a. för att kontrollera Transportstyrelsens efterlevnad av gällande rätt. *Säkerhetsskyddschefen* ansvarar för kontrollen över myndighetens säkerhetsskydd och ska följa upp och rapportera brister, risker och allvarliga missförhållanden inom säkerhetsområdet till generaldirektören.[89]

Även It-avdelningen har genomgått en omorganisation. De tidigare sex enheterna har ersatts med fyra enheter. Den tidigare drift- och infrastrukturenheten har avvecklats. Ansvaret för it-drift ligger numera på enheten för paketerade tjänster. Strategienheten finns

[89] Transportstyrelsen, Generaldirektörens beslut om arbetsordning för Transportstyrelsen, 2017-05-31.

fortfarande kvar, och här finns it-säkerhetsfunktionen som bl.a. ansvarar för strategisk kompetensförsörjning och utbildning liksom styr- och ledningsmodeller inom it-säkerhetsområdet.

De avtal myndigheten tecknar inom it-området ägs av it men förvaltningen av avtalen sker i samråd med inköpsenheten. För myndighetens större avtal inom it-området, som exempelvis it-drift, finns en utsedd avtalsansvarig på It-avdelningen. Det ska ske löpande avstämningar mellan inköpsenheten och avtalsansvariga. Förändringar av avtal sker via inköpsenheten som i vissa fall anlitar en extern resurs (it-jurist) för stöd med hanteringen.

Inom kärnverksamheten har den tidigare Skatte- och avgiftsavdelningen och Transportregisteravdelningen omorganiserats. Fordonsinformation och Strategisk utveckling och förvaltning är två nya avdelningar. Informationssäkerhetsansvarig finns idag på avdelningen Strategisk utveckling och förvaltning.

För övriga delar är organisationen densamma som tidigare.

Den nya arbetsordningen

Även i den av generaldirektören senast beslutade arbetsordningen[90] har ganska stora förändringar gjorts. Arbetsordningen har kortats ned och är inte lika detaljerad. Samtidigt lyfter den fram nya delar, som exempelvis medarbetarnas ansvar. För första gången finns också ett särskilt avsnitt om säkerhetsskyddschefens roll och ansvar. I grunden är ansvarsfördelningen mellan olika nivåer i myndigheten densamma.

Transportstyrelsens chefer ansvarar för att arbetet bedrivs enligt fastställda ramar och arbetssätt samt för att den interna styrningen och kontrollen är betryggande och förenlig med Transportstyrelsens övergripande interna styrning och kontroll. Verksamheten ska genomföras enligt instruktion och regleringsbrev och utifrån verksamhetskraven i myndighetsförordningen[91]. Cheferna ansvarar för att allt arbete utförs med en säkerhet som motsvarar verksamhetens risker och bedömda konsekvenser. De ansvarar också för att medarbetarna uppfyller ställda kompetenskrav.

[90] Transportstyrelsen, Generaldirektörens beslut om arbetsordning för Transportstyrelsen, 2017-05-31.
[91] 3 § myndighetsförordningen.

I ett avsnitt om befattningar, roller och ansvar står att medarbetarna ska följa gällande regler och förväntas rapportera om det finns brister och missförhållanden. Beroende på befattning och roll sträcker sig medarbetarnas ansvar olika långt.

Riktlinje för intern styrning och kontroll framtagen

Transportstyrelsen tog 2017 fram en riktlinje för intern styrning och kontroll[92]. Detta kan ses som ett svar på Riksrevisionens kritik från 2016. Först nu har Transportstyrelsen alltså en beslutad riktlinje för hur intern styrning och kontroll (FISK) ska hanteras i myndigheten.

Syftet med riktlinjen är att bidra till att säkerställa en god intern styrning och kontroll inom myndigheten genom verktyg för att hitta och motarbeta möjliga hinder för verksamheten och möjligheterna att leva upp till de krav som ställs. Riktlinjen beskriver ansvarsfördelning, aktiviteter och kriterier för detta. Styrelsen är ansvarig inför regeringen för att myndigheten lever upp till verksamhetskraven i myndighetsförordningen. Styrelsen behöver regelbundet ta del av riskanalys för myndigheten, status på kontrollåtgärder och ett underlag för bedömning av den interna styrningen och kontrollen inom myndigheten.

Generaldirektören ansvarar för den löpande verksamheten där momenten inom intern styrning och kontroll (riskanalys, kontrollåtgärder, uppföljning och dokumentation) ingår. Generaldirektören ansvarar också för att hålla styrelsen informerad om verksamheten, förse styrelsen med beslutsunderlag och verkställa styrelsens beslut. Avdelningscheferna ansvarar för att momenten inom intern styrning och kontroll genomförs på avdelningsnivå. Ekonomiavdelningen ansvarar för att samordna och bereda riskanalys, kontrollåtgärder, uppföljning och dokumentation för myndigheten. Ekonomi ska övervaka och säkerställa att avdelningarnas riskanalyser omfattar aktuella risker och att åtgärdsarbetet är effektivt.

Enligt ekonomidirektören gör avdelningarna idag riskanalyser under våren och de följs upp tertialvis istället för som tidigare kvartalsvis. Transportstyrelsen har också bildat ett internt nätverk för att skapa samsyn om riskhantering och riskvärdering i myndigheten.

[92] Transportstyrelsen, 2017-12-12, Riktlinje för intern styrning och kontroll, TSG 2017–3774.

3.11 Sammanfattande iakttagelser

Transportstyrelsen har sedan myndigheten bildades 2009 genomgått flera organisationsförändringar. De har omfattat både kärnverksamhet och stödverksamhet och har bl.a. syftat till att få ett mer trafikslagsövergripande och effektivare arbetssätt. 2010 fick myndigheten en styrelse istället för insynsråd.

Generaldirektörernas ledarstil och erfarenheter har påverkat hur frågor hanterats i myndigheten och hur verksamheten har involverats. Det har också påverkat hur enskilda händelser och beslut i it-driftupphandlingen har hanterats vid olika tidpunkter. Utredningen har noterat att styrelsen inte varit särskilt involverade i outsourcingen och upphandlingen av it-drift. Samtliga beslut inför, under och efter upphandlingen har fattats av generaldirektören. Styrelsen har fått information vid några få tillfällen och då efter att beslut fattats. Efter att Säkerhetspolisen inledde sin tillsyn har styrelsen mer löpande fått information om läget. Styrelsen har inte heller bett att frågan ska lyftas till styrelsen. Utredningen har fått uppfattningen att det är generaldirektören som har bestämt vilka frågor som styrelsen ska hantera.

Myndighetsövergripande frågor tycks ha svårt att få genomslag i verksamheten. Detsamma gäller riskanalyser och granskningar där samma brister återkommer år efter år. Utredningen ser det som ett tecken på att den här typen av frågor inte tas om hand och prioriteras i myndigheten.

Det finns ett stort antal riktlinjer och rutiner för Transportstyrelsens verksamhet. Enligt uppgift efterlevs inte alltid de fastlagda styrdokumenten. Utredningen har också fått beskrivet att det sedan tidigare finns en avstegskultur inom myndigheten. Det har framför allt gällt upphandlingar inom it-verksamheten.

Sammantaget konstaterar utredningen att Transportstyrelsen som myndighet fortfarande hanterar arvet av hopslagningen av trafikslagsspecifika verksamheter. Det innebär utmaningar i styrningen av myndigheten och i genomslaget för myndighetsövergripande frågor. Detta har i sig också påverkat förutsättningarna för it-driftupphandlingen och säkerhetsaspekterna i upphandlingen.

4 Hanteringen av säkerhetsfrågor inom Transportstyrelsen

4.1 Inledning

Utredningen ska enligt direktiven undersöka säkerhetskulturen inom Transportstyrelsen med avseende på risker med relevans för den aktuella upphandlingsprocessen. I det ligger att undersöka relevanta interna rutiner och riktlinjer samt organisationens gemensamma förhållningssätt och agerande avseende säkerhetsfrågor.

Detta kapitel innehåller en redogörelse för hur säkerheten har hanterats inom Transportstyrelsen. Redogörelsen omfattar bl.a. organisationen för säkerhetsarbetet i myndigheten, vem eller vilka funktioner som har varit ansvariga, vilka styrande dokument, relevanta interna rutiner och riktlinjer som har funnits samt hur säkerhetsarbetet har bedrivits i praktiken.

4.2 Transportstyrelsen hanterar en stor mängd information

Transportstyrelsen hanterar en stor mängd information i sin verksamhet. Det handlar exempelvis om uppgifter om fordon, körkort, yrkestrafik, trängselskatt och ansökningar om körkortstillstånd i vägtrafikregistret. Därutöver finns många andra uppgifter som ligger i andra system. Myndigheten själv säger att information är en av Transportstyrelsens viktigaste tillgångar och hanteringen av den är central i verksamheten.

Transportstyrelsen hanterar också en stor mängd personuppgifter, och är också en av de myndigheter som hanterar kvalificerade skyddsidentiteter.

Personuppgifter

Transportstyrelsen behandlar en stor mängd personuppgifter automatiserat med stöd av personuppgiftslagen (1998:204), PuL, och ett antal registerförfattningar, bl.a. lagen (2001:558) om vägtrafikregistret, lagen (1955:227) om inskrivning av rätt till luftfartyg, sjölagen (1994:1009) m.fl.

I vägtrafikregistret som innehåller information om alla fordon och förare i Sverige behandlas ett stort antal personuppgifter, varav vissa är att anse som känsliga enligt 13 § PuL, t.ex. uppgifter om hälsotillstånd och andra medicinska uppgifter av betydelse för körkort och körkortstillstånd. Även uppgifter som inte klassificeras som känsliga enligt 13 § PuL men som är särskilt integritetskänsliga, t.ex. uppgifter om lagöverträdelser behandlas i vägtrafikregistret.

Kvalificerade skyddsidentiteter

Transportstyrelsen hanterar även s.k. kvalificerade skyddsidentiteter (KSID), vilket framgår av lagen (2006:939) om kvalificerade skyddsidentiteter. I lagen beskrivs att en kvalificerad skyddsidentitet är en särskilt beslutad skyddsidentitet som består av andra personuppgifter än de verkliga och som har förts in i statliga register eller i handlingar som har utfärdats av statliga myndigheter. Kvalificerade skyddsidentiteter är av betydelse för rikets säkerhet och ska hanteras utifrån de krav som ställs i lagen (2009:400) om offentlighet och sekretess.

Informationen i Transportstyrelsens it-system

Transportstyrelsen beskriver i sin rapport[93] till regeringen den 23 januari 2018 avseende uppdraget att kartlägga hanteringen av vissa uppgifter (kartläggningsuppdraget) hur myndighetens it-miljö ser ut och hur den successivt har utvecklats sedan 1970-talet.

Av rapporten framgår att it-arkitekturen är utvecklad så att merparten av de olika systemen och deras innehåll är integrerade med

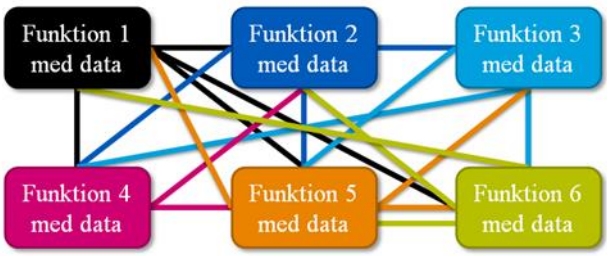
[93] Transportstyrelsens underlagsrapport *Kartlägga hanteringen av vissa uppgifter*, 2018-01-23, dnr TSG 2017–2515.

varandra och åtkomliga från flera håll. Fördelen med detta är att systemen kan återanvända införda uppgifter och samutnyttja resurser. Nackdelen är att om en del av informationen skulle avgränsas bort skulle de andra systemen inte längre fungera. Dessutom skulle det skapas ett tomrum i it-miljön som kan ge en indikation på att viss information i systemen hanteras på ett annat sätt än det normala.

Behörigheterna till systemen har utformats för att det ska vara enkelt att administrera it-miljön. De har därmed blivit väldigt omfattande. I praktiken innebär det att alla it-tekniker kan administrera alla system och data.

Transportstyrelsens it-miljö beskrivs i figur 3 nedan.

Figur 3. Transportstyrelsens integrerade it-miljö



Källa: Transportstyrelsen.

4.3 Säkerhetsskydd, informationssäkerhet och it-säkerhet inom Transportstyrelsen

Mängden information och karaktären på informationen ställer höga krav på Transportstyrelsens säkerhetsskydd, informationssäkerhet och it-säkerhet.

Säkerhetsskyddet omfattar i första hand skydd av rikets säkerhet, medan informationssäkerhet handlar om att skydda informationstillgångar utifrån krav på konfidentialitet, riktighet, tillgänglighet och spårbarhet. It-säkerhet omfattar mer teknisk säkerhet men kan även handla om t.ex. behörighetstilldelning. Säkerhetsskydd, informationssäkerhet och it-säkerhet hänger nära samman och kan ibland uppfattas överlappa varandra. I ett effektivt säkerhetsarbete är de nära integrerade och samarbetar med varandra.

4.3.1 Organisering och ansvarsfördelning enligt arbetsordningen

I utredningens intervjuer har det framkommit att det skett flera förändringar i organisationen för säkerhetsskydd. Fram till mitten av 2013 fanns en särskild enhet under ekonomiavdelningen som ansvarade för krisberedskap, säkerhet och skydd (KSS). Enheten lades därefter ned och säkerhetsskyddschefen placerades på GD-stab.

Enligt säkerhetsskyddsförordningen (1996:663) ska säkerhetsskyddschefen vara direkt underställd myndighetens chef och rapportera till generaldirektören.

I arbetsordningen som började gälla 2014[94] står att GD-stab ansvarar för att driva, utveckla samordna, följa upp och utvärdera myndighetens systematiska säkerhetsarbete och säkerhetsskydd (med begreppet säkerhetsskydd avses skydd mot rikets säkerhet enligt säkerhetsskyddslagen [1996:627] och säkerhetsskyddsförordningen). Befattningen säkerhetsskyddschef nämns inte. GD-stab ska också driva, samordna, följa upp och utvärdera arbetet med myndighetens ledningssystem för informationssäkerhet (LIS). I arbetsordningen under rubriken processer står att informationssäkerhet ingår som en del i myndighetens ledningssystem och en hänvisning görs till riktlinjer för informationssäkerhet. It-avdelningen har ansvaret för att driva, utveckla, samordna, följa upp och utvärdera myndighetens it-säkerhet inklusive metoder och modeller för detta.

Först i arbetsordningen som gäller från den 1 juni 2017[95] lyfts befattningen säkerhetsskyddschef fram. Där står att säkerhetsskyddschefen är direkt underställd generaldirektören och att säkerhetsskyddschefen ansvarar för kontrollen över myndighetens säkerhetsskydd och ska följa upp och rapportera brister, risker och allvarliga missförhållanden inom säkerhetsområdet till generaldirektören. Ansvaret för styrning och samordning av myndighetens övergripande informationssäkerhetsarbete har flyttats från It-avdelningen till den nya avdelningen Strategisk utveckling och förvaltning. Den it-säkerhetsansvarige är dock kvar på It-avdelningen.

[94] Transportstyrelsen, Arbetsordning Generaldirektörens beslut om arbetsordning för Transportstyrelsen, 2013-12-20, TSG 2011–294.
[95] Transportstyrelsen, Arbetsordning Generaldirektörens beslut om arbetsordning för Transportstyrelsen, 2017-05-31, TSG 2011–294.

Av intervju med säkerhetsskyddschefen framgår att han i det dagliga arbetet inte har rapporterat direkt till generaldirektören utom i enstaka ärenden. Istället har rapportering gjorts till enhetschefen och i viss utsträckning även ställföreträdande generaldirektör som båda också har haft ett arbetsledande ansvar för säkerhetsskyddschefen. Enligt uppgift rapporterar säkerhetsskyddschefen även idag till närmaste chef, som i dagsläget är chefsjuristen. Detta trots att det av den nya arbetsordningen framgår att säkerhetsskyddschefen är direkt underordnad generaldirektören.

Det finns inte någon säkerhetschef vid Transportstyrelsen som har ett övergripande ansvar för säkerheten, men rekrytering av en sådan pågår för närvarande.

4.3.2 Resurser för säkerhetsskydd, informationssäkerhet och it-säkerhet

Säkerhetsskyddschefen, informationssäkerhetsansvarig och it-säkerhetsansvarig har fram till den 1 juni 2017 varit placerade på olika avdelningar. Säkerhetsskyddschefen är placerad i Norrköping medan informationssäkerhetsansvarig och it-säkerhetsansvarig finns i Örebro.

Säkerhetsskydd

Säkerhetsskyddet inom Transportstyrelsen har i huvudsak hanterats av en person, dvs. säkerhetsskyddschefen. Det har inte funnits någon biträdande säkerhetsskyddschef, vilket är ett krav i säkerhetsskyddsförordningen, eller någon ersättare. I juni 2016 inrättades ytterligare en tjänst för säkerhetsskydd vid ledningskansliet, men denna person har varit sjukskriven under en längre period. De tre parallella upphandlingarna om it-drift, stordatormigrering och reskontra (DUBBing) har ställt stora krav på säkerhetsskyddsorganisationen.

Informationssäkerhet

Informationssäkerhetsansvarig har haft rollen sedan 2013 och har det myndighetsövergripande ansvaret för informationssäkerheten. Denne ska bl.a. samordna informationssäkerheten och kontrollera och följa upp efterlevnaden av informationssäkerhetskrav på myndigheten och rapportera avvikelser och lyfta frågor till berörd instans. Den informationssäkerhetsansvarige ska också ge stöd inom informationssäkerhetsområdet. Utöver informationssäkerhetsansvarig finns en medarbetare som har en mer stödjande roll.

Enligt riktlinjen för informationssäkerhet som beslutades 2012 och reviderades 2014 är informationssäkerhetsarbetet organiserat enligt följande. Informationsansvariga är respektive avdelningschef samt chefer för funktionerna direkt under generaldirektören. De informationsansvariga ska informationsklassa sina informationstillgångar och lämna över klassningsresultatet som krav till de stödfunktioner som ansvarar för verktyg och metoder för informationshanteringen. För alla it-system och it-komponenter ska kraven sedan överlämnas till chefen för it-avdelningen. De informationsansvariga ska också informera informationssäkerhetsansvarig och andra informationsansvariga när avsteg från informationssäkerhetskraven beslutas. På varje avdelning ska en eller flera lokala informationssäkerhetssamordnare utses bland medarbetarna. De ska bl.a. göra informationsklassningar och riskanalyser på uppdrag av den informationsansvarige och också ge råd till avdelningen.

I praktiken var de lokala informationssäkerhetsansvariga på plats först 2016. Den informationssäkerhetsansvarige menar att de fortfarande är underbemannade. Även om det idag finns lokala informationssäkerhetssamordnare så räcker det inte till.

It-säkerhet

It-säkerhetsansvarig har haft rollen sedan 2013 och det var också då som verksamheten inom it-säkerhet på It-avdelningen började byggas upp. Den it-säkerhetsansvarige ansvarar för it-säkerheten inom myndigheten. Rollen och ansvaret är i stort sett densamma som för informationssäkerhetsansvarig, fast på it-säkerhetsområdet. I dagsläget arbetar ett 15-tal personer med it-säkerhet. It-säkerhetsexperterna är fördelade över organisationen.

Samordning

Det framgår inte av arbetsordningen hur säkerhetsskydd, informationssäkerhet och it-säkerhet ska samarbeta eller förhålla sig till varandra. Den informationssäkerhetsansvariga och den it-säkerhetsansvariga är placerade på olika avdelningar, trots att ansvarsområdena har starka kopplingar. Vid intervjuerna framförs att det är en brist att säkerhetsskyddet, informationssäkerheten och it-säkerheten inte är samordnat i en funktion. När det gäller informationssäkerhet och it-säkerhet menar de ansvariga att det ändå fungerar bra, mycket p.g.a. att de fysiskt sitter i samma lokaler och kan samverka informellt.

4.4 Styrande dokument för säkerhetsskydd, informationssäkerhet och it-säkerhet

Utredningen har gått igenom styrdokumenten för säkerhetsskydd, informationssäkerhet och it-säkerhet.

4.4.1 Föreskrifter och styrdokument för säkerhetsskyddet saknas

Säkerhetsskyddsarbetet i Transportstyrelsen ska bygga på säkerhetsskyddslagstiftningen som är direkt tillämplig på myndigheten. Det innebär att Transportstyrelsen är skyldig att ge ett skydd för hemliga uppgifter och mot terrorism enligt kraven i säkerhetsskyddslagen med tillhörande tillämpningsföreskrifter.

Enligt säkerhetsskyddsförordningen ska en myndighet meddela ytterligare föreskrifter om verkställigheten av säkerhetsskyddslagen inom sitt verksamhetsområde om det inte är uppenbart obehövligt. Någon sådan föreskrift har inte beslutats av Transportstyrelsen. Det finns inte heller någon dokumentation som visar att myndigheten har kommit fram till att några föreskrifter inte behövs. Säkerhetsskyddschefen har enligt uppgift försökt att få till styrande dokument inom säkerhetsskyddet, men inte fått gehör för detta hos myndighetens ledning. Detsamma gäller enligt uppgift upprättande av rikt-

linjer för säkerhetsskyddet. Det finns inte några riktlinjer för säkerhetsskydd vid Transportstyrelsen. I intervjuer har framkommit att sådana riktlinjer borde finnas.

4.4.2 Flera styrdokument för informationssäkerhet och it-säkerhet

Det finns flera riktlinjer och rutiner för informations- och it-säkerhet. En av dessa riktlinjer klargör roller, ansvar och inriktning för arbetet med informationssäkerhet[96] på Transportstyrelsen och en annan riktlinje lägger fast krav på informationssäkerhet[97]. Vid Transportstyrelsen tillämpas ett ledningssystem för informationssäkerhet som bygger på LIS-standarden ISO 27000-serien. För myndighetens informationssäkerhetsarbete gäller bl.a. följande:

- Alla anställda och all kontrakterad personal ska ha grundläggande kunskap om myndighetens informationssäkerhetsarbete innan behörig åtkomst ges till informationstillgångar,
- Informationssäkerhetskraven ska beaktas i samtliga avtal,
- Myndighetens informationstillgångar ska vara definierade, ha utsedda ansvariga och vara klassade enligt myndighetens modell för informationsklassning, och
- Informationen ska skyddas med fysiska, tekniska och administrativa åtgärder på en balanserad nivå i relation till dess skyddsvärde.

I Rutinbeskrivning för genomförande av informationsklassning[98] beskrivs hur informationsklassning ska gå till och den riktar sig framförallt mot de lokala informationssäkerhetssamordnare som finns på avdelningarna sedan 2016. I rutinbeskrivningen anges att informationsklassningen bör genomföras i form av en workshop. Rutinen tar sikte på konfidentialitet, tillgänglighet och riktighet och innefattar även säkerhetsskydd. Till rutinen hör en bilaga som inne-

[96] Transportstyrelsen, 2012-03-27, Riktlinje för Transportstyrelsens informationssäkerhet, TSG 2011–938, reviderad version 2014-12-02. TSG 2013–1076.
[97] Transportstyrelsen, 2013-01-23, Riktlinje för krav på informationssäkerhet, TSG 2011–938.
[98] Transportstyrelsen, 2013-06-17, Rutinbeskrivning för genomförande av informationsklassning, TSG 2013–1075.

håller en kravkatalog på de krav som sammanhänger med informationens klassning. Rutinen refererar till Riktlinjen för krav på informationssäkerhet.

It-säkerheten styrs genom riktlinjer för it-säkerhet[99]. Riktlinjen är avgränsad till it-komponenter som t.ex. datorer, servrar och nätverk, men även mobiltelefoner. Riktlinjen ställer krav på ett formellt driftsgodkännande för it-komponenter. På it-säkerhetsområdet finns det även riktlinjer för it-riskhantering, åtkomst till it-lösningar och infrastrukturkomponenter och behörighetsstyrning. Dessa riktlinjer är till största del av teknisk karaktär. Riktlinjerna för behörighetsstyrning beskriver hur behörigheter ska tilldelas och har som grundprincip att behörigheten ska vara personlig och att användaren bekräftar sin identitet med lösenord eller motsvarande. Behörigheter ska dokumenteras av förvaltningsledare och revideras med maximalt tre års intervall.

Vid intervjuer har det framkommit att de styrande dokumenten i huvudsak utgör bra verktyg, men att de inte har använts i någon större utsträckning utom under den senaste tiden när fokus på informationssäkerhetsfrågor har ökat. Vissa dokument är också i behov av uppdatering.

4.5 Transportstyrelsens säkerhetskultur

Som framgår av avsnitt 1.8 definierar utredningen säkerhetskultur som de gemensamma attityder, värderingar och uppfattningar som chefer och anställda i myndigheten har om säkerhet. Säkerhetskulturen har stor betydelse för hur man arbetar med frågorna i myndigheten. Säkerhetskulturen i Transportstyrelsen beskrivs nedan.

Hanteringen av hemliga uppgifter har påverkat myndighetens förhållningssätt

Som beskrivits tidigare hanterar Transportstyrelsen en stor mängd uppgifter, där en delmängd är hemliga uppgifter.

[99] Transportstyrelsen, 2011-05-18, Riktlinjer för IT-säkerhet, TSG 2011–450.

Utredningen har utifrån intervjuer med olika företrädare för Transportstyrelsen fått en tydlig bild av hur myndigheten har förhållit sig till myndighetens information och de uppgifter som hanteras i systemen.

Tidigare generaldirektör Staffan Widlert berättar att han, när han var relativt ny som generaldirektör för myndigheten, blev kallad till ett möte med företrädare för Försvarsmakten och Säkerhetspolisen. Vid mötet deltog också avdelningsdirektören för körkortsavdelningen. Vid mötet gav Säkerhetspolisen och Försvarsmakten en översiktlig beskrivning av de hemliga delarna i registren. Staffan Widlert uppfattade att de fick rekommendationen att ju mindre de visste och ju mindre de pratade om förekomsten av hemliga uppgifter i systemen, desto bättre var det. Detta förhållningssätt tog Staffan Widlert med sig hem och tillämpade i myndigheten.

Det innebar att förekomsten av hemliga uppgifter inte diskuterades i myndigheten och inte i ledningsgruppen eller styrelsen. De enda som egentligen hade kännedom om detta var enligt Staffan Widlert säkerhetsskyddschefen, chefen för körkortsavdelningen och han själv. Sannolikt är detta en orsak till att styrelsen eller att inte hela ledningsgruppen säkerhetsprövats.

Ett annat råd som företrädare för Transportstyrelsen säger sig ha fått från Säkerhetspolisen och Försvarsmakten var att dölja de hemliga uppgifterna bland all övrig information som myndigheten hanterar i sina register, enligt principen ”nålen-i-höstacken”. Sannolikt påverkade detta också hanteringen av säkerhetsfrågor i stort i myndigheten liksom hanteringen av andra, icke-hemliga uppgifter.

Enligt uppgift har säkerhetsskyddschefen i sina kontakter med de personer som arbetade med upphandlingen av it-drift endast informerat om att det fanns information i systemen som ställde krav på säkerhetsskyddsåtgärder. Enligt uppgift har det inte varit tydligt vilken typ av information det handlat om och först i ett sent skede har det framkommit att det bl.a. omfattar hemliga uppgifter.

Detta förhållningssätt har fått konsekvensen att mycket få i Transportstyrelsens personal har känt till att myndigheten hanterar hemliga uppgifter och skyddsvärda uppgifter. Genom att inte ens alla avdelningschefer har känt till detta har säkerhetsfrågornas betydelse i organisationen prioriterats ned i verksamheten. Det gäller både informationssäkerhet och delar av it-säkerhet men framför allt för säkerhetsskyddet. Den personal på Transportstyrelsen som varit

involverade i upphandlingsprojektet har inte heller blivit upplysta om detta eller inte förstått den information de fått, vilket bidragit till bristerna i säkerhetsskyddet i it-driftupphandlingen.

Enligt uppgift finns fortfarande en avvaktande hållning i organisationen att prata om att det finns hemliga och skyddsvärda uppgifter. Detta upplevs påverka myndighetens förmåga att komma vidare i arbetet.

Myndighetens kompetens inom säkerhetsområdet

Transportstyrelsens förhållningssätt till säkerhetsfrågor verkar utifrån intervjuerna delvis utgå från rollen som tillsynsmyndighet. Fokus ligger då på andra aktörers förmåga att leva upp till säkerhetskrav. När det gäller myndighetens förhållningssätt till hanteringen av egna hemliga och skyddsvärda uppgifter framstår däremot mognaden och kunskapen om säkerhet vara låg.

Transportstyrelsen beskriver i rapporten avseende kartläggningsuppdraget kompetensen inom informationssäkerhets- och säkerhetsskyddsområdet i myndigheten. Mognaden inom informationssäkerhet mättes senast 2014 och uppdaterades i mars 2017. Av mätningen framgår att det finns en hög mognadsgrad om bl.a. riktlinjen för informationssäkerhet och av fysisk och miljörelaterad säkerhet. Mognadsgraden är låg för bl.a. efterlevnad och hantering av skydd och tillgångar, av incidenter och kontinuitetsplanering. Det tycks alltså finnas en större kännedom om de riktlinjer som finns, medan kunskapen om hur de ska efterlevas och hanteras i praktiken behöver höjas.

Den första grundläggande e-utbildningen i informationssäkerhet kom i augusti 2017. I dagsläget har 94 procent av personalen genomgått den. Den ska följas av mer riktade utbildningar. Då den generella kompetensen inom informationssäkerhet hos myndighetens medarbetare fortfarande bedöms vara låg, är behovet av vägledning och stöd inom informationssäkerhet stort. Transportstyrelsen skriver i rapporten att en ökad medvetande- och mognadsgrad inom organisationen förväntas leda till att informationssäkerhetsfrågorna omhändertas i större utsträckning än vad som tidigare varit fallet. I

samma rapport lyfter Transportstyrelsen fram att säkerhetsmedvetandet i organisationen behöver förbättras. Utbildning och information om säkerhetsskydd behövs för att höja medvetandet[100].

Bilden bekräftas i utredningens intervjuer. Där framkommer uppfattningen att kompetensen i säkerhetsfrågor generellt är för låg på Transportstyrelsen. Även om alla medarbetare inte behöver ha kunskap om allt, så finns det ändå delar som bedöms vara viktiga när man är anställd på Transportstyrelsen. Kunskap om informationssäkerhet är ett sådant exempel.

Vad gäller säkerhetsskydd har det inte genomförts någon utbildning i säkerhetsskydd för Transportstyrelsens personal, varken generellt eller specifikt för utpekade nyckelbefattningar. Detta trots att säkerhetsskyddslagen ställer krav på intern utbildning. Säkerhetsskyddet har uppfattats som något som primärt har varit säkerhetsskyddschefens ansvar och inte en del av verksamhetens ansvar. Tidigare generaldirektör Maria Ågren har till utredningen uppgett att hon i efterhand förstått att kompetensen i myndigheten på säkerhetsskyddsområdet inte varit tillräcklig.

4.6 Brister inom säkerhetsskydd, informationssäkerhet och it-säkerhet

Utredningen konstaterar att det funnits och finns ett antal brister i Transportstyrelsens arbete med säkerhetsskydd, informationssäkerhet och it-säkerhet. De beskrivs närmare nedan.

4.6.1 Transportstyrelsen saknade länge en säkerhetsanalys

Enligt 5 § säkerhetshetsskyddsförordningen ska myndigheter undersöka vilka uppgifter i deras verksamhet som ska hållas hemliga med hänsyn till rikets säkerhet. Detta ska dokumenteras i en säkerhetsanalys.

Transportstyrelsen tog först 2014 fram en säkerhetsanalys för myndigheten. Det gjordes efter att Säkerhetspolisen begärt in säkerhetsanalyser från Transportstyrelsen och 14 andra myndigheter. Tidplanen för att genomföra analysen var mycket kort och arbetet

[100] Transportstyrelsens underlagsrapport *Kartlägga hanteringen av vissa uppgifter*, 2018-01-23, dnr TSG 2017–2515 s. 14 f.

på Transportstyrelsen genomfördes under tidspress. I utredningens intervjuer framgår att det finns olika uppfattningar om kvaliteten på säkerhetsanalysen. Ställföreträdande generaldirektören anser att den var tillräckligt bra medan Säkerhetspolisen anger att den var bristfällig eftersom den bara behandlade sårbarheter och inte skyddsvärden.[101] Av intervjuerna framgår också att endast några få personer på Transportstyrelsen fick vetskap om analysen. Den kom därmed inte att användas i verksamheten och i upphandlingen av it-drift. En säkerhetsanalys ska normalt åtföljas av en säkerhetsplan för att omhänderta resultatet av säkerhetsanalysen. Någon sådan har dock vad utredningen vet inte utarbetats.

Myndigheten skulle revidera säkerhetsanalysen under 2015. Det gjordes dock först 2016. Säkerhetsskyddschefen ansvarade för detta arbete. Analysdelen blev klar under 2016 medan åtgärdsdelen inte blev klar förrän 2017. Säkerhetsanalysen fastställdes av generaldirektör Jonas Bjelfvenstam i maj 2017.[102]

Enligt uppgift valde tidigare generaldirektör Maria Ågren 2016 att inte distribuera analysdelen av säkerhetsanalysen till alla avdelningschefer eftersom vissa chefer inte var säkerhetsklassade. Avdelningscheferna uppges ha varit måna om att få säkerhetsanalysen som ett dokument, men mindre måna om att se till att den spreds och om att vidta lämpliga åtgärder med anledning av analysen. Utredningen har vidare uppfattat att säkerhetschefen fick arbeta mycket på egen hand med åtgärdsdelarna i säkerhetsanalysen tillsammans med ett antal personer som utsetts av avdelningscheferna. Problemet enligt uppgifter till utredningen är att åtgärdsförslagen aldrig fått en förankring hos avdelningscheferna vilket bidragit till att de inte heller drivit frågorna.

Av Transportstyrelsens rutinbeskrivning för informationssäkerhet, it-säkerhet och säkerhetsskydd vid inköp[103] som togs fram 2016 och som reviderades 2017 framgår att säkerhetsskyddsanalys genomförs årligen av informationsägarna (avdelningscheferna) med stöd av säkerhetsskyddschefen. Säkerhetsanalysen beslutas av generaldirektören.

[101] Skrivelse från Säkerhetspolisen 2014-10-13, Dnr 2014-5032-2
[102] Transportstyrelsens underlagsrapport *Kartlägga hanteringen av vissa uppgifter*, 2018-01-23, dnr TSR 2017–519 s. 8.
[103] Transportstyrelsen, 2016-02-22, Rutinbeskrivning för informationssäkerhet, it-säkerhet och säkerhetsskydd vid inköp, TSG 2015–404. Reviderad 2017-04-20.

Först sju år efter myndighetens bildande har myndigheten alltså lagt fast rutiner för genomförande av säkerhetsanalys.

4.6.2 Informationssäkerhetsarbetet har inte prioriterats i verksamheten

Det framkommer olika uppgifter och uppfattningar om hur stora delar av Transportstyrelsens information som har informationsklassats och när. I förstudien till it-driftupphandlingen från 2013 uppges att ett 10-tal it-lösningar av totalt 144 hade informationsklassats. I Transportstyrelsens rapport till regeringen 2018 om kartläggningsuppdraget står att myndigheten sedan 2014 aktivt arbetat med att klassa sin information.

Internrevisionen har sedan 2012 lyft fram bristerna inom informationssäkerhetsarbetet. 2014 gjorde internrevisionen också en särskild granskning[104] av informationssäkerhetsarbetet på Transportstyrelsen. Iakttagelser som lyftes fram var att myndighetens ledningssystem för informationssäkerhet inte hade implementerats på någon av avdelningarna. Internrevisionen noterade också att personalen inte utbildas om informationssäkerhetsrelaterade krav och att samordnarna för informationssäkerhet inte informerar den egna verksamheten om sådana krav. Revisionen skriver också att en systematisk kartläggning och klassificering av information, inklusive de system som hanterar information, endast har påbörjats och enbart i enstaka delar av myndigheten. Därmed saknas förutsättningar för att kunna fastställa skyddsbehovet för informationen och systemen.

Rekommendationen var att myndigheten skulle fastställa en plan för implementering av ledningssystemet för informationssäkerhet inom hela myndigheten liksom en plan för utbildning och information om informationssäkerhet. Arbetet med informationsklassificering skulle intensifieras för att säkerställa efterlevnaden av riktlinjen för informationssäkerhet.

GD-stab kommenterade i åtgärdsplanen för granskningen att avdelningarna internt behövde tydliggöra att informationsklassningar ska genomföras enligt vad som står i myndighetens riktlinje och till-

[104] Transportstyrelsen, Rapport, *Granskning av IT-styrning och informationssäkerhet med kommentarer från berörda verksamheter*, TSG 2014–114.

sätta resurser för detta. Enligt uppgift var de lokala informationssäkerhetsansvariga på plats först 2016 och har därefter fått kompetensutveckling för att kunna ge verksamheten stöd i arbetet.

Av utredningens intervjuer framgår samma bild, dvs. att arbetet med informationsklassning inte har varit prioriterat i myndigheten. Tidigare generaldirektör Staffan Widlert säger att informationsklassning är något väldigt arbetskrävande och att den inte uppfattades som den allra viktigaste säkerhetsfrågan i myndigheten. Avdelningscheferna, som enligt riktlinjen för informationssäkerhet är ansvariga för att informationsklassning genomförs, har inte heller prioriterat detta. Denna bild ger också den informationssäkerhetsansvarige.

Att Transportstyrelsen inte haft kunskap om sin information och hur den ska hanteras ur ett informationssäkerhetsperspektiv har direkt bidragit till de problem som senare uppstod i outsourcingen och upphandlingen av it-drift.

4.6.3 Brister i behörighetshanteringen

Såväl internrevisionen vid Transportstyrelsen och Riksrevisionen har framfört kritik avseende Transportstyrelsens bristfälliga hantering av behörigheter och spårbarhet (logghantering). Internrevisionen framförde redan 2012 att det fanns en hög risk för obehörig åtkomst till skyddsvärd information. Internrevisionen lämnade i sin granskning av it-styrning 2014 rekommendationer för att komma åt problemen. Myndigheten har också identifierat detta område som en risk i myndighetens riskanalys.

Internrevisionens granskning

Internrevisionen granskade 2014 it-styrningen på Transportstyrelsen[105]. I granskningen lyftes bl.a. bristfällig samverkan och samordning mellan avdelningarna fram, där respektive avdelning fokuserar på sitt verksamhetsområde. Ett flertal åtgärder pågick parallellt för att förbättra styrningen av it och det fanns en risk att åtgärderna

[105] Transportstyrelsen, Rapport, *Granskning av it-styrning och informationssäkerhet med kommentarer från berörda verksamheter*, TSG 2014–114.

inte samordnades. Granskningen lyfte också brister inom behörighetsstyrning och behörighetskontroll och risken bedömdes som hög. När det gällde verktyg för logganalys noterades att risker avseende avsaknad av logganalysverktyg identifierades vid myndighetens FISK-analys år 2012 och dessförinnan av Trafikregisteravdelningen år 2010 men att planerade åtgärder i s.k. logghanteringsprojektet fortfarande inte genomförts. Internrevisionens rekommendation var att myndigheten skulle inrätta en rutin för regelbunden uppföljning av att faktisk åtkomst till känslig information överensstämmer med beslut om tilldelning av behörigheter. Tilldelade behörigheter ska regelbundet verifieras av respektive chef.

Riksrevisionens granskning

Riksrevisionens årliga revision genomförde under 2015 en granskning av Transportstyrelsens avgiftsfinansierade verksamhet och processen för hantering av fordonsskatter. Riksrevisionen redovisade sin granskning i april 2015, strax efter att Transportstyrelsen slutit avtal med IBM och innan transitionen inleddes. I revisionsrapporten[106] identifierades ett antal brister i Transportstyrelsens behörighetshantering. Granskningen omfattade bara vissa system, men eftersom granskningen gällde generella it-kontroller menade Riksrevisionen att bristerna kunde vara aktuella även för andra system inom myndigheten.

Ett antal iakttagelser gjordes i granskningen. Det handlade om bristande dokumentation över godkända behörigheter, att anställda tilldelats högre behörigheter än nödvändigt, att det saknades regelbunden uppföljning och validering av tilldelade behörigheter samt att det inte fanns någon kontroll för att säkerställa att tidigare anställda inte låg kvar med behörighet till system.

Riksrevisionen påpekade att de konstaterat liknande brister vid tidigare granskningar och att det var viktigt att Transportstyrelsen omgående vidtog åtgärder. Riksrevisionens rekommendation var att Transportstyrelsen skulle se över rutinen för tilldelning och uppföljning av behörigheter till verksamhetskritiska system.

[106] Riksrevisionen, *Granskning av avgiftsfinansierad verksamhet och processen för hantering av fordonsskatter*, 2015-04-14, dnr 32-2014-0744.

Transportstyrelsens åtgärder

Transportstyrelsen har tagit fram olika planer för att åtgärda bristerna i behörighetshanteringen.

I beslut om åtgärdsplan med anledning av internrevisionens rekommendationer 2014 kommenterade generaldirektören, It-avdelningen och Personalavdelningen att åtgärder pågick. Ett underlag skulle tas fram inför generaldirektörens beslut att utse vem som är ansvarig för behörighetsstyrningen inom myndigheten. En process och kravställning skulle också tas fram. It-avdelningen uttryckte att det råder en otydlighet kring vem som är mottagare av logganalysverktyget, dvs. vem som ska använda verktyget. För behörighetshanteringen svarade Personalavdelningen att de behövde samarbeta med It-avdelningen. Utifrån kravställningen skulle tekniska förutsättningar inom ramen för GIB-projektet[107] tas fram liksom nödvändiga verktyg för att cheferna ska kunna hantera medarbetarnas behörigheter på ett effektivt sätt. Åtgärderna skulle vara klara senast den 30 juni 2015.

Vid ledningsgruppsmöte den 16 juni 2015[108] följdes frågan upp. Dåvarande personaldirektören föredrog ärendet. Av protokollet framgår att GIB-projektets syfte var att utveckla it-system som skulle säkerställa att alla medarbetare och externa parter har rätt behörighet vid rätt tillfälle men avslutades utan att problemet var löst. I stället fick personaldirektören i uppdrag att åstadkomma en struktur för behörighetsstyrning utan användning av nya it-stöd. Mot denna bakgrund redovisades ett förslag till riktlinje för behörighetshantering. I den efterföljande diskussionen konstaterades att en del frågor återstod att lösa. Ledningsgruppen ställde sig bakom innehållet i den föreslagna riktlinjen som generaldirektören därefter skulle besluta om.

Personaldirektören gav en lägesrapport vid ledningsgruppsmöte den 22 september 2015[109]. Med anledning av återkommande synpunkter från Riksrevisionen och internrevisionen behöver myndigheten visa på ett systematiskt förbättringsarbete. Annars kommer

[107] Gemensam Identitets-och Behörighetsstyrning.
[108] Protokoll från sammanträde med Transportstyrelsens ledningsgrupp den 16 maj 2015, dnr 2015–04.
[109] Protokoll från sammanträde med Transportstyrelsens ledningsgrupp den 22 september 2015, dnr 2015–08.

allvaret i anmärkningarna att trappas upp ytterligare. Ledningsgruppen konstaterade att även om det resursmässigt är ett ansträngt läge på it-området, bör det gå att finna enkla lösningar för att gallra bland behörigheterna. En åtgärd är att uppmana chefer/ägare av förvaltningsobjekt att i närtid redovisa tidplaner för genomförande av de analyser som krävs inför förestående gallring i respektive objekt.

Problemen kvarstår

Trots de planer och åtgärder som beskrivs ovan kvarstår fortfarande problemen i behörighetshanteringen. Enligt uppgift fanns i juni 2016 cirka 13 000 behörigheter i stordatorn som inte använts på 18 månader. Det fanns vid samma tidpunkt cirka 22 000 behörigheter i stordatorn.

Företrädare för Transportstyrelsen har uppgett till utredningen att det är svårt att förstå att myndigheten inte kunnat komma längre med behörighets- och logghanteringen sedan 2012. Även arbetet med informationsklassning, som ju har ett tydligt samband med behörighetshantering, har varit eftersatt. Enligt ekonomidirektören förekom det att medarbetare på Transportstyrelsen i vissa fall hade för höga behörigheter för att ”det var bra att ha”. Detta innebar att myndigheten behövde göra en total genomgång av alla it-system för att se till att rätt personer hade rätt tillgång till systemen.

4.6.4 Rutiner för säkerhetsskyddad upphandling saknades

Transportstyrelsen hade inte genomfört några säkerhetsskyddade upphandlingar innan upphandlingen av stordatormigreringen och it-driften gjordes 2014–2015. Enligt uppgift från säkerhetsskyddschefen var frågan uppe till diskussion i en upphandling av den s.k. utskriftstjänsten under 2012. I slutändan tecknades dock inte något säkerhetsskyddsavtal. Erfarenheten av säkerhetsskyddad upphandling och de moment som ingår i detta kan därmed sägas ha varit liten både hos myndigheten, inköpsenheten och säkerhetsskyddschefen när it-driftupphandlingen genomfördes.

Rutinbeskrivning för Transportstyrelsens inköp

Transportstyrelsen tog 2015 fram en rutinbeskrivning för myndighetens inköp.[110] Den är upprättad av inköpsenheten vid ekonomiavdelningen och beslutad av generaldirektör Staffan Widlert den 23 februari 2015, dvs. samtidigt som förhandlingen med IBM pågick. Vad utredningen kunnat se fanns ingen rutinbeskrivning innan denna.

Det finns ett särskilt avsnitt om säkerhet och säkerhetsskyddad upphandling med säkerhetsskyddsavtal. Där framgår att behovsägaren ansvarar för att hänsyn tas till den totala säkerhetsbilden i samband med inköp. Vilka som har rollen som behovsägare framgår inte, men utredningen tolkar det som att det är den som avser att göra ett inköp. Vidare står att de frågor som vanligen berörs vid upphandling är informationssäkerhet, it-säkerhet och säkerhetsskydd. Om det förekommer hemliga uppgifter i it-miljö som inköpet avser säkras hanteringen med hjälp av bilaga till säkerhetsskyddsavtal.

Under avsnitt om säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA) står när säkerhetsskyddsavtal ska träffas. Det är:

1. När myndigheten avser att begära in ett anbud eller träffa avtal om upphandling där det i förfrågningsunderlaget eller under uppdragets utförande förekommer hemliga uppgifter eller där leverantören kommer att delta i verksamhet med betydelse för rikets säkerhet.

2. Om verksamheten som upphandlas omfattas av säkerhetsskydd måste myndigheten träffa ett skriftligt säkerhetsskyddsavtal innan affärsavtalet träffas. Vid behov av underleverantörer tecknas säkerhetsskyddsavtalet även mellan myndigheten och underleverantören.

Det står också att ”De åtaganden leverantören förbinder sig till i och med tecknandet av ett säkerhetsskyddsavtal specificeras för aktuell avtalsnivå framtagen av säkerhetsskyddschefen på Transportstyrelsen.” Exempel på åtgärder vid tecknande av säkerhetsskyddsavtal ges också; delar av företagets ledning och berörd personal säkerhetsprövas, säkerhetsinstruktion upprättas av leverantören och

[110] Transportstyrelsen, 2015-02-23, Rutinbeskrivning för Transportstyrelsens inköp, TSG 2014–1898, reviderad 2017-04-20.

registerkontroll av berörd personal (om uppdraget är placerat i säkerhetsklass).

I rutinbeskrivningen saknas en beskrivning av vem som fattar beslut om att upphandlingen ska genomföras som en säkerhetsskyddad upphandling och vem som är ansvarig för de åtgärder som ingår i processen. Klart är dock att det är behovsägaren, vilket utredningen tolkar som den som tar initiativ till och ansvarar för upphandlingen, som ska bedöma säkerhetsbilden. Problemet är att detta utgår från att det är känt i myndigheten vilka uppgifter som är skyddsvärda eller hemliga.

Rutinbeskrivning för informationssäkerhet, it-säkerhet och säkerhetsskydd vid inköp

I februari 2016 beslutade dåvarande generaldirektör Maria Ågren om en särskild rutinbeskrivning för informationssäkerhet, it-säkerhet och säkerhetsskydd vid inköp[111]. Även den är upprättad av inköpsenheten vid ekonomiavdelningen.

Rutinbeskrivningen ska tillämpas på samtliga inköp som berörs av informationssäkerhet, it-säkerhet och säkerhetsskydd. Behovsägare och samtliga personer som genomför inköp ska tillämpa rutinen. Under inköpsregler redogörs kort för när lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet kan användas. Det står också att det är viktigt att identifiera om säkerhetskraven behöver vara uppfyllda under inköpsskedet eller under avtalstiden. Detta påverkar om säkerhetsskyddsavtal behöver tecknas innan anbudsgivare får ta del av hemliga uppgifter eller om det kan ske i samband med att affärsavtal tecknas.

Inköpsprocessen beskrivs i tre faser. Under planeringsfasen ska informationsklassning av data och uppgifter som berörs av inköpet genomföras. Genomförandefasen startar med val av inköpsmetod och då ska som huvudregel alla krav vara fastställda, även säkerhetskrav. Under uppföljningsfasen måste efterlevnaden av säkerhetskrav följas upp. Vid affärsavtalets upphörande måste också säkerställas att säkerhetsskyddsavtal avslutas på ett korrekt sätt.

Under säkerhetsbedömning vid inköp står att när en leverantör får tillgång till Transportstyrelsens information kan det vara aktuellt

[111] Transportstyrelsen, 2016-02-22, Rutinbeskrivning för informationssäkerhet, it-säkerhet och säkerhetsskydd vid inköp, TSG 2015–404. Reviderad 2017-04-20.

att ställa särskilda krav på leverantören för att se till att informationen inte används på ett felaktigt sätt. Här står bl.a. att informationsägaren måste beakta att informationen ska vara informationsklassad och att ett säkerhetsskyddsavtal ska tecknas om leverantören kommer i kontakt med hemliga uppgifter (vilket informationsklassningen ger svar på).

Av ansvarsfördelningen framgår att informationsägaren har ansvaret för merparten av aktiviteterna. Säkerhetsskyddschefen ansvarar för att bedöma om inköpet ska omfattas av säkerhetsskyddsavtal samt vilken säkerhetsnivå som ska gälla. Denne ansvarar också för att ta fram säkerhetsskyddsavtal och att genomföra säkerhetsprövning.

Ansvarsfördelningen för säkerhetsskyddad upphandling har därmed tydliggjorts från 2016 och framåt, dvs. först efter att it-driftupphandlingen gjordes.

Säkerhetsskyddsavtal

Eftersom Transportstyrelsen inte tidigare genomfört någon säkerhetsskyddad upphandling fanns inte någon mall för säkerhetsskyddsavtal framtagen. Säkerhetsskyddschefen var under hösten 2014 i kontakt med Säkerhetspolisen om detta och hänvisades då till den mall för säkerhetsskyddsavtal som Säkerhetspolisen tagit fram. Säkerhetsskyddschefen frågade även GD-juridik om de kunde hjälpa till, men fick enligt uppgift beskedet att de inte hade kompetens på området och därmed inte kunde bidra.

Säkerhetsskyddsavtal slöts med IBM Svenska AB enligt framtagen mall. Det fanns ingen process på plats för hantering av säkerhetsskyddsavtal med utländska underleverantörer. När det blev klart att IBM:s leverans även omfattade utländska underleverantörer översattes säkerhetsskyddsavtalet rakt av till engelska. Inköpsenheten förmedlade säkerhetsskyddsavtalen till underleverantörerna.

Säkerhetsprövning

Av rutinen för inköp som togs fram i början av 2015 står att registerkontroll av berörd personal ska göras om uppdraget är placerat i

säkerhetsklass. Utredningen har dock inte fått klarhet i om det fanns en rutin för hantering av registerkontroller och vem som ansvarade för detta gentemot Säkerhetspolisen. Eftersom personal vid Trafikverket som arbetade med Transportstyrelsens it-drift tidigare säkerhetsprövats så bör en sådan rutin ändå ha varit på plats. I rutinbeskrivningen för informationssäkerhet, it-säkerhet och säkerhetsskydd vid inköp som beslutades i februari 2016 klargörs att säkerhetsskyddschefen ansvarar för att genomföra säkerhetsprövning. Registerkontrollen utgör dock endast en liten del av säkerhetsprövningen. Utredningen har inte fått klarhet i hur övriga delar i säkerhetsprövningen var tänkt att genomföras, t.ex. vad gäller intervjuer.

När säkerhetsprövningen kom att omfatta anställda vid IBM:s utländska underleverantörer visar utredningen att säkerhetsskyddschefen inte visste hur detta skulle hanteras.

Godkännande av underleverantörer

Utredningen har tagit del av Transportstyrelsens rutin för hantering av ny underleverantör it-drift[112]. Rutinen togs fram först 2017 med slutversion i juli 2017. Transportstyrelsen säger dock till utredningen att de arbetat på detta sätt i it-driftupphandlingen.

Enligt rutinen ska leverantören anmäla ny underleverantör till taktiskt kommersiellt forum vars ordförande (Transportstyrelsens avtalsansvarige) ska meddela inköpsenheten grundläggande information om underleverantören. För att säkerhetsskyddshandläggaren på generaldirektörens ledningskansli ska kunna göra en bedömning av om säkerhetsskyddsavtal krävs och nivå på avtal och krav på skydd, ska ytterligare information framgå. Det handlar om vilka arbetsuppgifter som underleverantören ska utföra, varifrån arbetsuppgifterna ska utföras och om underleverantören ska spara någon information hos sig och i sådana fall vilken information och hur den förvaras.

Inköpsenheten ansvarar för att göra en kommersiell kontroll av underleverantören. Säkerhetsskyddshandläggaren gör bedömningen om säkerhetsskyddsavtal ska skrivas. Om säkerhetsskyddsavtal ska skrivas skapar inköpsenheten ett utkast till säkerhetsskyddsavtal och skickar det till funktionsbrevlåda. Säkerhetsskyddshandläggaren

[112] Rutin för hantering av ny underleverantör It-drift, daterad 2017-07-11, version 1.2.

skickar säkerhetsskyddsavtalet till utsedd kontaktperson hos leverantören eller direkt till underleverantören. Leverantören eller underleverantören återsänder undertecknat säkerhetsskyddsavtal till säkerhetsskyddshandläggaren som säkerställer att generaldirektören skriver under säkerhetsskyddsavtalet. Säkerhetsskyddshandläggaren meddelar avtalsansvarige att avtalet är färdighanterat samt diarieför avtalet. Avtalsansvarig lägger därefter till underleverantören i IT-driftsavtalets bilaga över godkända underleverantörer och skickar en uppdaterad bilaga till inköpsenheten för registrering i avtalsregistret.

Rutinen innehåller ingen skrivning om personuppgiftsbiträdesavtal med underleverantörer. Om en underleverantör ska hantera personuppgifter måste det enligt Transportstyrelens personuppgiftsbiträdesavtal med IBM tecknas skriftliga personuppgiftsbiträdesavtal (underbiträdesavtal). Det är oklart hur detta hanteras.

Utländska underleverantörer

Utmaningen för Transportstyrelsen och för säkerhetsskyddschefen kom när det blev klart att IBM:s leverans omfattade utländska underleverantörer. Myndigheten och säkerhetsskyddschefen hade inte erfarenhet av detta och flera frågor uppstod.

En fråga handlade om hur säkerhetsprövning av en person i ett annat land ska gå till. Vad utredningen förstått skickade säkerhetsskyddschefen i oktober/november 2015 in underlag för registerkontroll av utländsk personal till Säkerhetspolisen. Huruvida intervjuer gjordes med utländsk personal och i så fall av vem är oklart. I mars 2016 hålls ett informationsmöte hos Säkerhetspolisen där de informerar säkerhetsskyddschefen om hur registerkontrollen går till. Budskapet är att registerkontroll av utländska medborgare bosatta utomlands i stort sett är meningslös mot bakgrund av att registerkontrollen enbart görs mot svenska register.

Den andra frågan handlade om vilka länder som Sverige tecknat ett generellt bi- eller multilateralt säkerhetsskyddsavtal med. Fanns inte något sådant säkerhetsskyddsavtal tecknat krävs att myndigheten får ett bemyndigande av regeringen att teckna ett projektspecifikt säkerhetsskyddsavtal med en utländsk myndighet. Säkerhetsskyddschefen var i kontakt med Utrikesdepartementet och fick

en lista på de länder som Sverige tecknat säkerhetsskyddsöverenskommelser med. Han uppfattade detta som att underleverantörer i de länder som fanns på listan var godkända att använda i säkerhetsskyddade upphandlingar. Listan avser dock, som utredningen uppfattat det, endast de länder där man efter att ha iakttagit en viss procedur kan få de nationella myndigheternas hjälp med bl.a. registerkontroll. Den utgör inte ett generellt godkännande för säkerhetsskyddade upphandlingar. Även här kan utredningen konstatera att det funnits brister i kunskapsnivån.

4.7 Samarbetet mellan säkerhet och övriga organisationen

Av utredningens intervjuer med olika företrädare för Transportstyrelsen framträder två bilder av samarbetet mellan säkerhet och övriga organisationen. Å ena sidan den som säkerhetsskyddschefen, informationssäkerhetsansvarige och it-säkerhetsansvarige ger. Å andra sidan den bild som ges av företrädare för Ledningskansliet, It-avdelningen och de som varit involverade i upphandlingen av it-drift. Utredningen gör bedömningen att båda bilderna innehåller värdefulla iakttagelser och redovisar dem därför nedan.

Säkerhetsfunktionens syn

Säkerhetsskyddschefen menar att det varit svårt att få genomslag för säkerhetsskyddsfrågorna, både på ledningsnivå och i verksamheten. Det är enligt honom anledningen till att det inte tagits fram föreskrifter och riktlinjer för säkerhetsskyddet och att det inte gjordes någon säkerhetsanalys förrän 2014. Säkerhetsskyddschefen säger också att säkerhetsfrågorna kommit in alldeles för sent i upphandlingarna av it-drift och stordatormigreringen. I båda fallen ombads säkerhetsskyddschefen, informationssäkerhetsansvarig och it-säkerhetsansvarig ge synpunkter på säkerhetskraven i upphandlingarna kort innan annonsering skulle ske. De fick känslan att projektgruppen uppfattade säkerhetskraven som hinder för upphandlingen och outsourcingen. Enligt säkerhetsskyddschefen har det inte heller funnits stöd i organisationen för att genomföra en säkerhetsskyddad

upphandling där säkerhetsskyddsavtal slutits i samband med själva upphandlingen.

Informationssäkerhetsansvarig framhåller också att det är svårt att få genomslag för frågorna i organisationen. Informationssäkerhetsarbetet bygger på att organisationen tar ansvar och gör jobbet. Det har varit trögt. I beslut efter beslut saknas informationssäkerhetsaspekterna. På senare tid har dock medarbetare och sektionschefer börjat se säkerhetsfunktionen som ett stöd, vilket är en klar attitydförändring. Det gäller dock inte ledningsnivån.

It-säkerhetsansvarig uttrycker att det är ett problem att informationen i myndigheten ska vara öppen samtidigt som det finns en hel del skyddsvärda uppgifter. Verksamheten har för lite kunskap om vad som är skyddsvärt och därmed har man inte sett behovet och tagit frågorna på allvar. Säkerhetsfrågorna och säkerhetskompetens behöver komma in även på ledningsnivå.

Organisationens syn

Företrädare för Ledningskansliet på Transportstyrelsen säger att säkerhetsfrågorna och de som arbetat med detta har haft svårt att få gehör i organisationen. En bidragande orsak har varit att det funnits för lite kunskap i organisationen om vilken information myndigheten sitter på och därmed har man inte sett säkerhetsbehovet. Säkerhetsfrågorna har också uppfattats vara abstrakta och svåra att ta till sig. Ansvariga inom säkerhetsområdet har inte heller kunnat tydliggöra kraven.

De personer inom It-avdelningen och i andra delar av organisationen som arbetat med it-driftupphandlingen menar att samarbetet med säkerhetsfunktionen har varit svårt och inte fungerat på ett bra sätt. Det finns flera skäl till detta menar de. Ett problem har varit att säkerhetsfunktionen har ställt säkerhetskrav utifrån regelverket, utan att kunna konkretisera kraven och anpassa dem till Transportstyrelsens verksamhet. Det blev särskilt tydligt i kravställningen i upphandlingen. Ett genomgående problem upplevs också ha varit att säkerhetsskyddschefen inte berättat att det finns skyddsvärda och hemliga uppgifter i systemen. Det framkom först efter att avtalet med IBM var undertecknat. Uppfattningen är också att säkerhetsfunktionen varit otillgängliga och vid flera tillfällen inte

deltagit vid viktiga möten där säkerhetsfrågorna diskuterats. De har inte heller velat formulera säkerhetskraven skriftligt. Sammantaget har de uppfattats vara mer kravställande än stödjande och lösningsinriktade. Det framkommer också en uppfattning att säkerhetsskyddschefen inte haft tillräcklig kompetens att kunna ge stöd, ställa krav och i praktiken hantera de säkerhetsskyddsåtgärder som krävts i samband med it-driftupphandlingen.

4.8 Sammanfattande iakttagelser

Transportstyrelsen hanterar en stor mängd information och uppgifter, bl.a. personuppgifter och annan skyddsvärd information. Transportstyrelsen är också en av de myndigheter som hanterar kvalificerade skyddsidentiteter. Detta ställer krav på myndighetens säkerhetsskydd, informationssäkerhet och it-säkerhet. Förhållningssättet i myndigheten har dock varit att så få personer som möjligt ska ha kännedom om vilka typer av uppgifter myndigheten hanterar. Detta har fått negativa konsekvenser för säkerhetskulturen och säkerhetsmognaden i myndigheten. Fortfarande verkar det finnas en syn att detta inte berör verksamheten som helhet utan enbart vissa funktioner i myndigheten.

Vid myndigheten finns en säkerhetsskyddschef, en informationssäkerhetsansvarig och en it-säkerhetsansvarig. Enligt säkerhetsskyddsförordningen ska säkerhetsskyddschefen vara placerad direkt under generaldirektören och rapportera till denne, vilket kom på plats först den 1 juni 2017. De tre ansvariga är inte samordnade i en säkerhetsfunktion eller motsvarande, vilket försvårar samarbetet och samordningen av säkerhetsfrågorna vid Transportsstyrelsen. Utifrån de krav som ställs på myndighetens säkerhetsarbete tycks resurserna för säkerhet vara alltför knappa. Av ledningssystemet för informationssäkerhet (LIS) framgår att verksamheten ska äga och driva informationssäkerhetsarbetet, men så har det inte fungerat i praktiken.

Transportstyrelsen har tagit fram flera riktlinjer och rutiner för informationssäkerhet och it-säkerhet. Något motsvarande finns inte på säkerhetsskyddsområdet, trots att det där ställs krav på föreskrifter. Det ställs också krav på en säkerhetsanalys, vilket Transportstyrelsen tog fram först 2014. Även om det finns styrande

dokument för informationssäkerhet och it-säkerhet har internrevisionen återkommande pekat på brister i efterlevnaden av dessa. Även Riksrevisionen har pekat på brister. Det har handlat om att informationsklassning inte genomförts i verksamheten och att hanteringen av behörigheter har stora brister. Orsaken till dessa brister anges vara att ledningen inte prioriterat säkerhetsarbetet och att det inte funnits gehör för säkerhetsfrågorna i verksamheten.

Riktlinjer för säkerhetsskyddad upphandling togs fram först efter att it-driftupphandlingen var genomförd. Detta medförde att det varken fanns erfarenhet av eller rutiner för hur Transportstyrelsen skulle hantera det praktiska arbetet med säkerhetsskydd utifrån säkerhetsskyddsavtalet. När det blev klart att leveransen från IBM även omfattade utländska underleverantörer blev utmaningen för Transportstyrelsen än större.

Sammantaget bedömer utredningen att de brister som funnits och som delvis fortfarande finns i Transportstyrelsens säkerhetsarbete allvarligt har bidragit till de problem som uppstod i it-driftupphandlingen.

5 Upphandlingen av it-drift

5.1 Inledning

Utredningen ska enligt direktiven undersöka hur och varför Transportstyrelsen initierade processen att upphandla myndighetens it-drift samt vilken analys och vilka överväganden som låg till grund för myndighetens agerande. I detta ingår att klargöra beslutsordningen inför beslut att inleda upphandling, val av upphandlingsförfarande och val av potentiella leverantörer. Vidare ska utredningen enligt direktiven kartlägga processen från det att Transportstyrelsen beslutade att påbörja arbetet med en förändrad it-drift och it-organisation fram till i dag. Därvid ska viktiga tidpunkter, gjorda vägval, beslut som fattats på olika nivåer inom myndigheten och information som lämnats till regeringskansliet redovisas.

Detta kapitel återger händelseförloppet i upphandlingen av förändrad it-drift från det att Transportstyrelsen initierade processen att upphandla myndighetens it-drift till det att avtal träffas med IBM.

5.2 It-driften genom Trafikverket

Trafikverket (tidigare Vägverket) har ansvarat för Transportstyrelsens it-drift sedan Transportstyrelsen bildades 2009. Historiken går dock längre tillbaka än så.

I samband med sammanslagningen av Vägverket och Trafiksäkerhetsverket 1992 fick Vägverket ansvaret för den samlade it-driften. It-driftverksamheten ingick därefter i en myndighetssamverkan mellan Vägverket och Banverket där ansvaret för it-driften låg hos Banverket. Banverket byggde då upp den s.k. ICT-verksamheten (Information and Communication Technology) som kom att

ansvara för it-driften. Ambitionen var att ICT skulle övergå till att bli ett statligt bolag.

När Transportstyrelsen bildades 2009 genom sammanslagning av delar av Vägverket, Järnvägsstyrelsen, Luftfartsstyrelsen och Sjöfartsverket tog myndigheten över ett flertal register. Det mest omfattande registret som övertogs var vägtrafikregistret från Vägverket. Ansvaret för it-driften gick över till Transportstyrelsen men resurser i form av personal och maskiner låg kvar på Vägverket för att kort därefter föras över till Banverket ICT som utförare. Det gjordes alltså en bodelning mellan myndigheterna, men inte för it-driften. Istället hade man en myndighetssamverkan med ett beställar-utförarupplägg där Banverket ICT som utförare levererade till beställaren Transportstyrelsen. 2010 slogs Vägverket och Banverket samman till den nya myndigheten Trafikverket och Trafikverket blev leverantör av it-drift till Transportstyrelsen. Trafikverket ICT var den enhet som utförde åtagandena och som var förhandlande part gentemot Transportstyrelsen.

Avtalet mellan Transportstyrelsen och Trafikverket

När Transportstyrelsen bildades den 1 januari 2009 reglerades myndighetens preliminära behov av it-leveranser i ett föravtal mellan Transportstyrelsen och Vägverket. Från den 1 juni 2009 slöts ett ramavtal mellan Transportstyrelsen och Vägverket avseende leverans av it-tjänster. Avtalet gällde fram till den 31 januari 2011 och kunde förlängas med ett år i taget. I avtalet preciserades leveranser av olika tjänster genom underavtal. Som bilagor till avtalet fanns bl.a. tjänstekataloger, servicenivåer (SLA) och pris.

Vad gäller säkerhetskrav skulle Vägverket, enligt punkt 8.1 och 8.2 parternas åtagande i avtalet, tillhandahålla tjänster i enlighet med Transportstyrelsens krav avseende it-säkerhet. Av punkt 17.1 i avtalet framgår att åtagandena avseende it-säkerhetsskydd regleras i separat säkerhetsskyddsavtal mellan parterna.

För körkortstillverkningen fanns tydliga säkerhetskrav i form av riktlinjer för informationssäkerhet liksom informationssäkerhetsinstruktioner. Det ställdes också krav på registerkontroll av den personal som arbetade med it-drift kopplat till körkortstillverkningen. För övriga områden fanns inga specifika säkerhetskrav.

I samband med att Trafikverket tog över ramavtalet med Transportstyrelsen preciserades åtagandet mellan parterna genom ett tilläggsavtal till ramavtalet[113]. I tilläggsavtalet gjordes förändringar i bl.a. tjänstekatalog, servicenivåer och pris. Det gjordes inte några förändringar i säkerhetskrav eller liknande. Avtalet gällde under 2011 och förlängdes för avtalsperioden 2012.

I februari 2012 bekräftar Trafikverket ICT i ett mail till Transportstyrelsen att de accepterar förlängning av ramavtal gällande it-tjänster för perioden 2013, 2014 och 2015. Slutdatum för avtalet är den 31 december 2015.

Transportstyrelsen har på utredningens begäran tagit fram en ungefärlig kostnad för it-driften genom Trafikverket. Uppgifter finns för 2014 och 2015. För 2014 låg kostnaden på knappt 200 miljoner kronor. Till detta tillkom interna kostnader på Transportstyrelsen om drygt 20 miljoner kronor. Kostnaden för 2015 var ungefär densamma.

Trafikverkets beslut att avveckla externa åtaganden

När Trafikverket bildades 2010 fanns fortfarande en ambition att bolagisera ICT-verksamheten. Trafikverket såg över frågan 2012 och kom då fram till att det inte var lämpligt att avskilja en så pass tekniskt komplex och för transportsystemet kritisk verksamhet. Eftersom Trafikverket ICT var nära knuten till järnvägstransportsystemet och därmed också järnvägsunderhållet ansåg man att det var bättre att säkra verksamheten och kompetensen i Trafikverket.

Den 18 juni 2012 beslutade dåvarande generaldirektör Gunnar Malm med stöd av Trafikverkets styrelse att successivt konkurrensutsätta, konsolidera och centralisera it-verksamheten i Trafikverket. Den tidigare utspridda trafikslagsnära it-verksamheten samlades i en it-organisation och i denna ingick också ICT. Den nya it-organisationen i Trafikverket var på plats den 1 maj 2013.

En direkt konsekvens av beslutet 2012 var att alla åtaganden som var kopplade till ICT och som inte handlade om att sälja accesser på fibernätet successivt skulle avvecklas. Detta omfattade åtagandet till Transportstyrelsen på drift av stordator och av Transportstyrelsens

[113] Tilläggsavtal till Ramavtal avseende leverans av IT-tjänster mellan Transportstyrelsen och Trafikverket ICT, 2010-06-23.

it-system. Detta besked kom parallellt med att Transportstyrelsen började se över försörjningsstrategi och försörjningsmodell för it-driften.

Trafikverkets leverans till Transportstyrelsen

Av intervjuer med företrädare för Transportstyrelsen och Trafikverket framgår att det fanns ett missnöje med leveransen av it-drift från Trafikverket, särskilt under 2012 och 2013. Leveransformerna ansågs fyrkantiga och den tekniska utvecklingspotentialen var ganska begränsad. Leveransmodellen sägs vara mer ett resultat av en organisatorisk förändring i samband med Transportstyrelsens bildande, än en modell som utgick från myndighetens behov. Lösningen med Trafikverket ansågs vara dyr och inte ge tillräcklig kapacitet och förmåga att stödja Transportstyrelsen i myndighetens utvecklingsbehov.

Problemet var också att det inte fanns en tydlig specifikation från Transportstyrelsen på vad man ville ha och det framgick inte heller vad man fick från Trafikverket. Även om det fanns servicenivåer (kvalitetskrav) i avtalet, bl.a. för tillgänglighet och leveranstid så var tjänsterna inte säkrade hela vägen ner i infrastrukturen. De ekonomiska beräkningarna kopplade till detta var också bristfälliga. Ett exempel som ges är dokumentationen av it-driften. Enligt avtalet skulle Trafikverket säkerställa underhåll av överenskommen dokumentation. Mycket lite har dock dokumenterats avseende it-driften på Transportstyrelsen. Av intervjuer framgår att bristerna inte i första hand berodde på Trafikverket. Merparten av det som dokumenterats, exempelvis vad gäller applikationsdriften, upprättades på initiativ av Trafikverket. Enligt uppgift saknades en motpart på Transportstyrelsen att föra dialog med om behov och krav.

Ny leveransorganisation från 2014

Från februari 2014 ändrade Trafikverket sin leveransorganisation mot Transportstyrelsen[114]. En särskild enhet (Itae) bildades som enbart levererade till Transportstyrelsen. Enheten bestod då av 54 anställda och 32 konsulter. I samband med detta styrdes

[114] Trafikverket, PM, 2016-10-25, Trafikverkets IT-leverans till Transportstyrelsen.

leveransen upp, även vad gäller riktlinjer för säkerhet. Det fanns två säkerhetsnivåer i leveransen. Personer med tillgång till den generella it-miljön krävde inte säkerhetsklassning, medan de som hade tillgång till körkortstillverkningen (KTV) och Swedish Government Secure Intranet (SGSI) skulle vara säkerhetsklassade. Kort efter att den nya organisationen etablerades meddelade Transportstyrelsen att man skulle upphandla it-driften externt. Leveransen från Trafikverket kom från oktober 2014 därför att inriktas på att planera för kommande transition till ny driftleverantör. Företrädare för både Transportstyrelsen och Trafikverket säger att leveransen från Trafikverket fungerade väl under 2014–2015. I efterhand säger man från Transportstyrelsen att man fick en del gratis genom Trafikverket. Exempelvis fanns kompetens som jobbade med leveranser mot andra kunder som också hjälpte Transportstyrelsen vid behov.

Diskussion om verksamhetsövergång för Trafikverkets personal

Enligt uppgifter från Trafikverkets it-direktör fanns 54 anställda och 32 konsulter som arbetade med leveransen till Transportstyrelsen i februari 2014. Ju närmare i tid man kom till att avsluta leveransen till Transportstyrelsen minskade Trafikverkets personal i antal och konsulternas antal ökade. Enligt uppgifter från bl.a. tidigare chefen för drift- och infrastrukturenheten på Transportstyrelsen gjordes en verksamhetsövergång för 12 personer för driften av stordatormiljön.

Transportstyrelsen övervägde också övergång för fler personer än de som arbetade med stordatorn. Frågan var uppe i Transportstyrelsens ledningsgrupp och hos respektive chef på It-avdelningen som fick i uppdrag att undersöka behovet av specifik kompetens som fanns i Trafikverket. Tidigare chefen för drift- och infrastrukturenheten säger att han hade i uppdrag av både it-direktören och generaldirektören att vara restriktiv med att ta över personer från Trafikverket för att inte riskera övertalighet i ett senare skede. Under detta arbete konstaterades att kompetensen hos huvuddelen av Trafikverkets personal inte var unik kompetensmässigt. Några personer från Trafikverket sökte arbete på Transportstyrelsen när myndigheten rekryterade.

Denna bild bekräftas av uppgifter från Trafikverkets tidigare generaldirektör Gunnar Malm. Enligt honom diskuterades inledningsvis frågan om verksamhetsövergång för den personal som skötte it-driften avseende Transportstyrelsen. Från Trafikverkets sida sågs detta som ett naturligt sätt för Transportstyrelsen att behålla kompetensen. Enligt Gunnar Malm fanns det också ett intresse för Trafikverket att hantera de medarbetare som berördes på ett bra sätt. Hans bild är att Transportstyrelsen inte var intresserade av en verksamhetsövergång utan ville ha ”rent bord”. Det var i slutändan ett fåtal personer som skötte stordatordriften som kom att omfattas av verksamhetsövergång till Transportstyrelsen. Gunnar Malm menar att om Transportstyrelsen hade valt verksamhetsövergång hade myndigheten varit i en helt annan situation. Verksamhetsövergång hade enligt Gunnar Malm varit en billig lösning för att få den tid man behöver för ett driftövertagande.

Enligt den tidigare it-direktören valde Transportstyrelsen att inte göra en verksamhetsövergång eftersom man valt att upphandla en extern leverantör och då var det inte aktuellt att ta över personal.

5.3 Transportstyrelsens underlag och beslut inför upphandlingen

I juni 2011 tog generaldirektör Staffan Widlert initiativ till det s.k. Effektiviseringsuppdraget med syfte att identifiera och värdera åtgärder inom myndigheten som kunde ge kostnadsbesparingar. Uppdraget redovisades i en rapport[115] i december 2011 och innehöll både kortsiktiga och långsiktiga åtgärder med tonvikt på it-verksamheten. I rapporten står att uppdraget har sin bakgrund i det faktum att myndigheten framöver kan väntas få fler tillkommande uppgifter, samtidigt som regeringen förväntar sig att myndigheten ska kunna finansiera dem i huvudsak inom befintlig resursram. För Transportstyrelsen var det inte längre ett alternativ att höja avgifterna i takt med att kostnaderna ökar. Syftet var därför att identifiera områden i verksamheten som kan bedrivas mer kostnadseffektivt.

[115] Transportstyrelsen, PM 2011-12-07, Effektiviseringspotentialer inom TS – Förslag till åtgärder och effektbedömningar. Redovisning av GD-uppdrag.

Den identifierade effektiviseringspotentialen uppgick för perioden 2012–2014/15 till totalt 525 miljoner kronor för myndigheten. För It-avdelningen beräknades potentialen till 200 miljoner kronor. 70 miljoner kronor av dessa bedömdes kunna sparas på nya lösningar för it-driften. Kostnaden för driften beräknades då uppgå till 375 miljoner kronor årligen på en budget på totalt 800 miljoner kronor för it-verksamheten. Flera skäl anges till de höga kostnaderna för it-driften. Ett skäl var att korta kontraktstider (1-åriga) inte ger förutsättningar för en driftleverantör att minska driftskostnaderna. Ett annat var att leverantörsavtalen inte är upphandlade i konkurrens och förmodligen inte marknadsmässiga, dvs de är högre än marknadspriset. En åtgärd som anges är konkurrensutsättning av driftavtal för längre avtalsperiod, vilket bedöms kunna sänka driftkostnaderna väsentligt.

Av intervjuer framgår att målsättningen var att Transportstyrelsen, utifrån effektiviseringsuppdraget, skulle spara 250 miljoner kronor under perioden 2012–2014/15. Genom s.k. GD-uppdrag fick varje avdelningschef ett sparbeting. På It-avdelningen fick it-direktören uppdraget att spara 150 miljoner kronor i it-verksamheten under perioden. Bland åtgärderna ingick att se över områden för outsourcing, däribland it-driften.

Den 1 januari 2012 var också den nya it-avdelningen på plats. It-direktören påbörjade ett arbete som handlade om att ta kontroll, modernisera och arbeta med effekthemtagning i it-verksamheten. I den första fasen ville man få kontroll på vad som fanns i Transportstyrelsens it-miljöer. Man såg även över kostnader och åtgärder för effektivisering.

5.3.1 It-försörjningsstrategi

Under 2012 tog Transportstyrelsen fram en it-försörjningsstrategi[116] som beslutades av generaldirektören den 6 september 2012. Syftet med strategin var att säkerställa att it-försörjningen skulle ske på ett optimalt sätt genom att tydliggöra vilka principer som ska gälla vid val av it-försörjningsalternativ.

[116] Transportstyrelsen, 2012-09-06, Riktlinje för it-försörjning, it-försörjningsstrategi, TSG 2012–906.

Strategin lägger fast mål och principer för it-försörjningen, den går igenom olika it-försörjningsalternativ och presenterar en modell för utvärdering och val avseende it-försörjning. Den redovisar också vilka förändringar som kan ge anledning till att omvärdera it-försörjningen. Några exempel på förändringar är markanta kvalitetsbrister, att nya krav tillkommer, att avtalsförutsättningar förändras eller att en leverantörs leveransförmåga förändras markant.

Enligt strategin finns tre huvudalternativ för it-försörjning: intern försörjning, externt samarbete och extern försörjning.

Intern försörjning innebär att den levereras i Transportstyrelsen regi, eventuellt med stöd av externa aktörer.

Externt samarbete kan antingen ske genom samverkan/partnerskap med annan offentlig verksamhet eller genom partnerskap med leverantör.

Extern försörjning innebär att ansvaret för en tjänst (t.ex. drift av infrastruktur och applikationsdrift) utkontrakteras till en extern leverantör. Transportstyrelsen skiljer på *ekonomisk utkontraktering* med syfte att skapa kostnadseffektivitet och/eller flexibilitet i leveransen och *strategisk utkontraktering* med syfte att åstadkomma strategiska fördelar (t.ex. kompetens).

I strategin lyfter Transportstyrelsen också fram vilka upphandlingsformer som ska övervägas. I första hand gäller avrop från eget befintligt avtal, därefter avrop från centrala ramavtal och sist egen upphandling.

It-försörjningsstrategin hanterar inte frågan om vilken typ av verksamhet som lämpar sig för intern respektive extern försörjning. Det finns inte heller några resonemang om hur säkerhetsskydd, informationssäkerhet eller samhällsviktig verksamhet ska beaktas vid prövning av försörjningsform.

5.3.2 Upphandling av konsult som ska genomföra förstudie inför upphandling av it-drift

Med utgångspunkt i it-försörjningsstrategin beslutade generaldirektör Staffan Widlert den 1 september 2013 om start för projekt ”Nytt it-driftavtal”. Syftet var att förbereda, analysera och planera upphandling av applikations- och infrastrukturdrift (it-drift). Pro-

jektet skulle ta fram ett beslutsunderlag samt planera för en upphandling som skulle leda till att avtal för driftstjänster tecknas med vald leverantör.

Innan dess, i mars-april 2013, upphandlade Transportstyrelsen en extern konsult som skulle ta ett huvudansvar för kravinsamling, teknisk infrastruktur och arkitektur för att säkerställa ett nytt it-driftavtal[117]. Uppdraget delades upp i fyra delar, där delleverans 1 avsåg ett faktaunderlag med bl.a. mål, problem, dokumentation av tekniska systemsamband och beroenden samt riskanalys. Delleverans 2 omfattade att ta fram projektplan och projektorganisation, en GAP-analys[118] av kompetens samt underlag för beslut om inköpsmetod. Delleverans 3 avsåg själva upphandlingen inklusive kravställning och delleverans 4 var genomförande av transition. Delleverans 3 och 4 utgjorde optioner. Det framgår inte några specifika beskrivningar eller krav i uppdraget som rör säkerhetsfrågor.

Upphandlingen genomfördes som ett öppet förfarande. Av de tre anbud som kom in bedömdes Kontract IS Services AB vara den ekonomiskt mest fördelaktiga leverantören. Tilldelningsbeslut fattades av it-direktören den 3 maj 2013 och avtal tecknades mellan Transportstyrelsen och Kontract den 17 maj 2013. Avtalet förlängdes av chefen för drift- och infrastrukturenheten i november 2014 och Kontract medverkade i projektet även under själva upphandlingen.

5.3.3 Förstudie inför upphandlingen av it-drift

Projektorganisationen för förstudien i projekt Nytt It-driftavtal bestod av it-direktören som projektbeställare och chefen för drifts- och infrastrukturenheten som projektägare. Projektledaren liksom övriga i projektgruppen var konsulter från Kontract. I styrgruppen ingick till en början enbart chefer från it-avdelningen, men redan efter första mötet kompletterades styrgruppen med chefer från verksamheten.

[117] Transportstyrelsen, Förfrågningsunderlag 2013-03-13, Uppdragskonsulttjänster inför projekt ”Nytt it-driftsavtal” TSG 2013–202.
[118] GAP-analys innebär analys av nuvarande läge jämfört med potentiellt eller önskat läge och gapet däremellan.

Även företrädare för ledningsstaben bjöds in, men de deltog inte på några möten.

Relevanta delar i förstudien redovisas nedan.

Nulägesanalys

I nulägesanalysen redovisas nuläge, utmaningar och problem för ett antal områden, exempelvis applikationsregister, policys och lagkrav, organisation och Service Level Agreements (SLA).

Nulägesanalysen för applikationsregister omfattar en genomlysning av Transportstyrelsens applikationer. Som utmaningar och problem lyfts bl.a. att en verklig bild av verksamheternas krav inte är framtagen, vilket kan vara en risk som gör att utformningen av it-lösningar kan bli felaktiga.

Nuläget för policys och lagkrav beskrivs som att det finns en bra organisatorisk lösning för framtagande av policys. It-säkerhet, metoder, ansvar och roller bedöms vara beskrivna på ett mycket bra sätt. Här framgår också att ytterligare policys ska tas fram inom närtid. Informationssäkerhetsklassning är implementerad på ett 10-tal it-lösningar av totalt 144. De problem och utmaningar som lyfts fram är att efterlevnaden av policys är bristfällig och inte helt förankrad. Det saknas också en komplett process för att följa upp efterlevnaden av policys. Här framgår också att dateringarna av dokumenten skiftar och att det finns äldre dokument som skulle behöva ses över och eventuellt uppdateras.

Utmaningar och problem bedöms finnas för körkortstillverkningen, där extra säkerhetskrav kan bli betydande. Ingen fjärråtkomst får ske till dessa system.

Leverantörskriterier

Som leverantörskriterier lyfts strategisk passform, leveransförmåga och geografisk täckning. När det gäller geografisk täckning uttrycks att ”Leverantören bör ha en geografisk täckning som möjliggör att tjänster kan levereras i enlighet med Transportstyrelsens behov och legala krav.”[119] Vad man närmare lägger i detta är oklart.

[119] Transportstyrelsen, Beslutsunderlag Projekt nytt it-driftavtal, bilaga 6 leverantörskriterier och exempel på leverantörer.

Utifrån leverantörskriterierna ges också exempel på identifierade leverantörer. IBM är en av sex leverantörer som lyfts fram.

Omvärldsanalys

I projektets omvärldsanalys har man analyserat vad leverantörer på marknaden kan erbjuda. En utvärdering redovisas för IBM och för Tieto.

I analysen görs också en utvärdering av Trafikverkets leverans. Bland annat lyfts att Trafikverkets långsiktiga strategi är att inte ha externa leveranser samt att Trafikverkets tjänstepaketering inte kan jämföras med marknadens erbjudanden. Slutsatsen är att Trafikverket inte är en aktuell leverantör på lång sikt eftersom effektmålen för it-driften inte kan nås. På kort sikt kan Trafikverket vara aktuella för att leverera inom vissa områden. Vilka dessa områden är framgår dock inte.

Utvärdering av scenarier

Projektet har också gått igenom alternativen för it-försörjning enligt it-försörjningsstrategin.

Alternativ 1 är insourcing, dvs. att bygga upp en egen it-drift inom Transportstyrelsen. Alternativ 2 är att behålla leveransen via Trafikverket och Steria medan alternativ 3 är att omförhandla avtalen med befintliga leverantörer. Inget av dessa alternativ förordas, bl.a. utifrån argumenten att det skulle bli kostsamt ekonomiskt, att Transportstyrelsen själva skulle få leda utvecklingen av it-driften samt att it-leveransen riskerar att ligga kvar på en reaktiv nivå och tillföra låg nytta i verksamheten. Här lyfts återigen att Trafikverket på lång sikt inte kommer att tillhandahålla drift för externa kunder.

Alternativ 4 avser upphandling av flera externa leverantörer genom exkludering av stordatorplattformen medan alternativ 5 avser upphandling av en extern leverantör som även inkluderar stordatorplattformen. Bedömningen för alternativ 4 är att det är ett dåligt ekonomiskt alternativ att behålla stordatorn och att det inte finns bra ekonomiska förutsättningar att stanna kvar i stordatormiljön. Inte heller detta alternativ förordas.

Det alternativ som kvarstår och föreslås utredas vidare är alternativ 5, dvs att upphandla en extern aktör som också inkluderar stordatorplattformen. Ett av huvudargumenten är att kostnadseffektiviteten bedöms öka på lång sikt (4–8 år).

Den 31 oktober 2013 beslutade projektets styrgrupp att arbeta vidare utifrån scenariot ”upphandling med inriktning mot en leverantör”.

Prioriterade processer

Projektet lyfter fram ett antal prioriterade processer som måste implementeras för att myndigheten ska bli redo för en ny extern it-driftleverantör. Två processer som rör säkerhet lyfts fram.

Den ena processen är Information Security Management (dvs. ledningssystem för informationssäkerhet, LIS) vars syfte är att säkerställa konfidentialitet, integritet och tillgänglighet av en organisations information, data och it-tjänster. Eftersom data utgör den största tillgången i leveransen måste den skyddas enligt förutbestämda regler. Den andra processen är Access Management som syftar till att ge behöriga användare rätt att använda en tjänst, samtidigt som man förhindrar tillgång till icke-auktoriserade användare. Det måste etableras en behörighetsstruktur för data för att kunna bibehålla kontroll och skydda mot obehörig åtkomst.

Det är alltså samma processer som lyfts fram i internrevisionens riskanalyser.

Utvärdering av upphandlingsformer

Projektgruppen har också utvärderat olika upphandlingsformer för upphandlingen av it-drift. Det är avrop från Kammarkollegiets ramavtal, öppet förfarande, selektivt förfarande, förhandlat förfarande samt konkurrenspräglad dialog. Som underlag för analysen av formen konkurrenspräglad dialog har projektgruppen använt Kammarkollegiets vägledning 2010:1.

En rankning görs av de fem upphandlingsformerna. Förhandlat förfarande och konkurrenspräglad dialog bedöms ha starkast passform. Öppet förfarande och selektivt förfarande rankas som de två sämsta alternativen. Skälen som anges är bl.a. att det kräver att

Transportstyrelsen kravställer korrekt och att det inte ger möjlighet till förhandling. Avrop från Kammarkollegiets ramavtal bedöms som det tredje bästa alternativet. Fördelarna sägs vara att risken för överprövning är minst och att det är mindre resurskrävande. Nackdelarna är korrekt kravställande och att förhandling inte får ske samt risken att ramavtalet inte fullt ut är anpassat efter Transportstyrelsens behov.

Projektgruppen förordar formen konkurrenspräglad dialog. Det skulle ge större möjlighet för Transportstyrelsen och anbudsgivare att förstå behov och föreslå bra lösningar. Ett annat argument var att det initialt inte krävdes lika specificerade krav i upphandlingen. Upphandlingsformen bedömdes också ge möjlighet till ett avtal som motsvarade myndighetens behov av kvalitet och funktionalitet. Projektet tar inte upp eventuellt behov av att göra en säkerhetsskyddad upphandling.

5.4 Beslut om upphandling av it-drift

Resultatet av förstudien i projekt Ny it-drift föredrogs för Transportstyrelsens ledningsgrupp den 10 februari 2014 av chefen för drifts- och infrastrukturenheten inom It-avdelningen. Ledningsgruppen hade innan dess fått information om detta vid ledningsgruppsmötet den 17 december 2013[120].

Av protokollet från ledningsgruppsmötet[121] framgår att ledningsgruppen i diskussionen betonade vikten av att upphandlingen sker i samarbete med verksamheten och att riskerna analyseras och omhändertas. Ledningsgruppen ställde sig därefter bakom förslaget och generaldirektören Staffan Widlert beslutade att:

- En upphandling av applikations- och infrastrukturdrift som tjänst ska ske genom konkurrensutsättning enligt uppgjord plan inom ramen för projektet Nytt it-driftavtal med ett planerat driftsleveransövertagande senast 2015-06-15,
- Uppdra till it-avdelningen att tillsammans med övriga avdelningar inom Transportstyrelsen värdera och prioritera vilka uppdrag och

[120] Protokoll från sammanträde med Transportstyrelsens ledningsgrupp den 17 december 2013, dnr 2013-08.
[121] Protokoll från sammanträde med Transportstyrelsens ledningsgrupp den 10 februari 2014, dnr 2014–02, p. 13.

aktiviteter som är nödvändiga att genomföra parallellt med upphandlingen av applikations- och infrastrukturdrift, samt att

- Uppdra till it-avdelningen att detaljplanera, styra och genomföra de prioriterade kringliggande aktiviteter som projekt Nytt it-driftavtal är beroende av och som är kostnadsdrivare i ett framtida avtal samt tillsammans med berörda genomföra de prioriterade aktiviteter som kräver medverkan av andra avdelningar.

Utredningen kan utifrån styrelseprotokoll inte se att Transportstyrelsens styrelse informerades om beslutet.

Trafikverket fick informationen den 12 februari 2014. Enligt uppgift från Trafikverket framförde Transportstyrelsen i samband med detta att man ville att Trafikverket skulle delta i den kommande upphandlingen och konkurrera med andra externa aktörer. Trafikverket bedömde att ett sådant upplägg inte var juridiskt korrekt och att det inte var förenligt med Trafikverkets uppdrag. Trafikverket meddelade därför Transportstyrelsen att man inte kunde delta i upphandlingen, men att man kunde fortsätta i en myndighetssamverkan. Eftersom Transportstyrelsen beslutat att gå ut i en extern upphandling var dock detta inte aktuellt. Vid ledningsgruppsmöte den 4 mars 2014[122] informerar it-direktören om att berörd personal på Trafikverket har informerats om att upphandlingen av applikations- och infrastrukturdrift ska ske genom konkurrensutsättning.

Tidplanen

Som framgår av beslutet ovan var planen att en ny driftleverantör skulle ta över senast den 15 juni 2015, alltså 16 månader efter att beslutet om att gå ut i en extern upphandling fattades. I underlagen till ledningsgruppen finns en något mer detaljerad tidplan. Enligt denna ska upphandlingen vara klar första kvartalet 2015. Parallellt med detta ska myndigheten göra en genomgång av driftsdokumentation liksom tjänstepaketering. En beställarorganisation och samverkansmodell ska också utvecklas och etableras. Därefter vidtar etableringsfasen där den nya driftleverantören ska etableras (transition),

[122] Protokoll från sammanträde med Transportstyrelsens ledningsgrupp den 4 mars 2014, dnr 2014–03.

vilket beräknas pågå fram till första kvartalet 2016. Efter det ska driften utvecklas i transformationsfasen.

Av de riskanalyser som tagits fram framgår inte att projektet bedömt tidplanen som en risk. Inte heller ledningsgruppen tycks ha haft några synpunkter på tidplanen.

Att it-driftupphandlingen genomfördes parallellt med stordatormigreringen och hantering av reskontra (DUBBing) innebar att det ställdes stora krav på inköpsenheten, på it-avdelningen, säkerhetsfunktionen men också på myndigheten som helhet. Utifrån detta kan sägas att tidplanen redan vid beslutet får bedömas som alltför optimistisk.

5.5 Upphandlingen

När upphandlingen i projekt Nytt IT-driftavtal inleddes var tanken att Kontract även fortsättningsvis skulle leda och driva projektet. Transportstyrelsen hade bedömt att de själva inte hade förmågan, kompetensen eller resurserna att göra detta. I samband med den planerade annonseringen i april 2014 bedömde dock företrädare för både it-avdelningen och inköpsenheten att Kontract inte hade tillräcklig kompetens eller erfarenhet att leda och ansvara för en så stor och viktig upphandling. Med anledning av det omprövades styrmodellen, Transportstyrelsen tog över ledningen av projektet medan Kontract fick en mer stödjande roll. Som stöd hade Transportstyrelsen också en konsult från företaget Colligio.

I samband med detta etablerades nya roller i projektet, bl.a. affärsansvarig och operativ projektägare under projektägaren. Det etablerades också ett s.k. core team som bestod av personer från it-avdelningen och inköpsenheten med utpekade ansvarsområden för själva upphandlingen och dess olika faser. Core team skulle ha all information och fatta beslut i projektet, med undantag för de beslut som låg på it-direktören, It-rådet som styrgrupp eller generaldirektören. Medlemmarna i core team arbetade mot övriga organisationen utifrån frågeställningar som uppkom, oftast genom möten men ibland via mail. Det fanns ingen företrädare från säkerhetsfunktionen med i core team, men en person i core team ansvarade för att stämma av olika frågor mot säkerhetsfunktionen.

5.5.1 Val av upphandlingsform

Av intervjuer med företrädare för Transportstyrelsen framkommer att valet av upphandlingsform för it-driftupphandlingen inte var självklart. Projektgruppen förordade upphandlingsformen konkurrenspräglad dialog. Inköpsenheten var tveksamma till detta.

I januari 2014 utredde inköpsenheten om det fanns stöd för att välja konkurrenspräglad dialog. Det framkom dock att vare sig projektet (genom Kontract) eller Transportstyrelsen hade erfarenhet av att tillämpa upphandlingsformen. I samband med detta förtydligade inköpschefen i ett dokument[123] att inköpsenheten förespråkade upphandlingsformen förhandlat förfarande. Konkurrenspräglad dialog bedömdes vara mer tidskrävande än förhandlat förfarande och också mer riskfyllt. Av dokumentet framgår också att upphandlingen sågs som tillräckligt utmanande för inköpsenheten bara genom sin omfattning. Senare genomförde projektet och inköpsenheten också en workshop där de kom fram till att de steg som arbetsgruppen ville genomföra var möjliga att genomföra enligt det förhandlade förfarandet, bl.a. genom informationsmöten med de anbudsgivare som kvalificerat sig för steg 2 i upphandlingen.

Utifrån detta beslutade inköpschefen att förhandlat förfarande skulle användas och att vissa kompletterande moment skulle ingå i upphandlingen. Det framgår inte någonstans om myndigheten diskuterade valet förhandlat förfarande med annonsering eller utan annonsering. I praktiken genomfördes ett förhandlat förfarande med annonsering.

Säkerhetsskyddet i upphandlingen

Av utredningens genomgång av dokument fram till annonseringen i maj 2014 framkommer inte något som visar att det förekommit diskussioner om säkerhetsfrågor eller behovet av en säkerhetsskyddad upphandling. Det nämns inte i förstudien, det diskuteras inte på styrgruppsmöten och ledningsgruppen tar inte upp det i samband med beslutet. Inte heller i projektdirektivet till fas 3 (upphandlingen) daterat den 12 februari 2014 nämns detta.

[123] Transportstyrelsen, 2014-01-27, Förtydligande angående PM undantag från huvudregel vid val av upphandlingsförfarande i projekt Nytt IT-driftavtal.

Av intervjuer med olika företrädare för Transportstyrelsen framgår att säkerhetsfrågor ändå har varit uppe vid ett antal tillfällen i projektet. Vid ett möte på it-avdelningen i april 2014 hade säkerhetsfunktionen bjudits in för att godkänna ställda säkerhetskrav i upphandlingen. Säkerhetsfunktionen pekade då på att det krävdes en säkerhetsskyddad upphandling eftersom det fanns skyddsvärda uppgifter i systemen. Projektet och inköpsenheten reagerade på detta eftersom deras bild var att endast en liten del (körkortstillverkningen) omfattades av säkerhetsskydd. De ansåg därför inte att det var motiverat att göra en säkerhetsskyddad upphandling. Säkerhetsskyddschefen var också i kontakt med chefsjuristen för att få stöd i frågan om säkerhetsskyddad upphandling. Enligt uppgift svarade chefsjuristen att de inte kunde frågan och därför inte kunde delta. It-direktören och chefen för drift- och infrastrukturenheten lyfte också frågan till generaldirektören. Därefter beslutades att ett säkerhetsskyddsavtal skulle tecknas i anslutning till det affärsmässiga avtalet med den slutliga leverantören. Om det framgick för alla som var inblandade i upphandlingen vad detta innebar är osäkert. Myndigheten hade inte tidigare tecknat säkerhetsskyddsavtal utöver det som myndigheten hade med Trafikverket, men detta gjordes nu både i it-driftupphandlingen och i upphandlingen för stordatormigreringen som genomfördes parallellt.

Av intervjuerna framgår också att det i efterhand finns olika uppfattningar om det i slutändan gjordes en säkerhetsskyddad upphandling eller inte. Företrädare för inköpsenheten menar att det gjordes, medan andra (säkerhetsskyddschef, projektägare, partneransvarig) menar att det inte gjorts. Det visar på den begreppsförvirring som finns. I ett svar till Konstitutionsutskottet[124] skriver Transportstyrelsen följande: ”Transportstyrelsen vill understryka att vi har genomfört en säkerhetsskyddad upphandling, men vi tecknade inte ett säkerhetsskyddsavtal innan anbudsgivarna fick ta del av vårt förfrågningsunderlag. Bedömningen var att själva förfrågningsunderlaget inte innehöll hemlig information som krävde ett säkerhetsskyddsavtal. Däremot tecknades sekretessförbindelser med anbudsgivarna innan de fick ta del av underlaget. Transportstyrelsen har tecknat ett säkerhetskyddsavtal med den utpekade driftsleverantören.”

[124] Sveriges Riksdag, Dnr 2581–2016/17, 171 026, Granskningsärende 9 och 12 – Regeringens agerande i samband med Transportstyrelsens IT-upphandling.

Inköpschefen säger i intervju att de i efterhand funderat på om de skulle ha gjort en upphandling enligt lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet. Myndigheten hade dock inte erfarenhet av den typen av upphandling och om det hade varit möjligt.

Undantag från ramavtalsupphandling

Transportstyrelsen registrerade den 8 maj 2014 avsteg från det statliga ramavtalet IT-driftstjänster Helhetsdrift 2010. De skäl som angavs var att myndigheten avser att förhandla om både tjänstens genomförande och affärsmodell, vilket ramavtalet inte tillåter. Man skriver att myndigheten utifrån förstudier och behovsanalyser får svårt att nå i mål med en bra affär utan förhandling. Vidare skriver man att det troligen är omöjligt att i detalj specificera ett förfrågningsunderlag och lämna fasta priser utan förhandling.

Orsakerna anges vara en komplicerad infrastruktur och ansvarsfördelning. Det finns också behov av mycket stor flexibilitet i en ny lösning och avtal p.g.a. av att upphandlingen är beroende av upphandlingen av stordatormigrering som då inte var klar. Ytterligare en orsak är Transportstyrelsens öppenhet inför innovativa och nya lösningar i syfte att hitta den långsiktigt bästa leverantören och lösningen.

Därutöver anges ekonomisk omfattning på upphandling och avtalslängd som skäl liksom att det är en enstaka upphandling.

Kammarkollegiet skickar den 12 maj 2014 en bekräftelse på underrättelse om avsteg.

Transportstyrelsen frångår genom sin anmälan till Kammarkollegiet prioriteringsordningen på upphandlingsformer enligt itförsörjningsstrategin. Där anges egen upphandling som det sista alternativet efter avrop från eget befintligt avtal och avrop från centrala ramavtal.

5.5.2 Annonsering

Enligt tidplanen skulle inbjudan till upphandling och annonsering göras i april 2014. Enligt intervjuer framgår att den affärsansvarige, efter ett möte med upphandlingskonsulten, bedömde att inbjudan

för annonsering var undermålig och behövde arbetas om. Exempelvis framgick inte vad myndigheten ville upphandla och vad man ville åstadkomma med outsourcingen. Med stöd av it-direktören flyttades annonseringen fram så att man fick tid att arbeta igenom inbjudan.

Inbjudan

Inbjudan[125] annonserades den 8 maj 2014, en månad efter tidplan, till intresserade leverantörer att ansöka om att få delta i upphandling avseende it-drift och närliggande tjänster. Sista ansökningsdag var den 9 juni 2014.

Effektmålen som anges på kort sikt är driftstabilitet, standardisering, kapacitet att stötta verksamhetsförändring och kostnadseffektivitet. På lång sikt är rangordningen driftstabilitet, kostnadseffektivitet och kapacitet att stötta verksamhetsförändring.

I inbjudan redovisas under rubriken 1.4.4. Särskilda förutsättningar ett antal punkter som ska specificeras i förfrågningsunderlaget. I punkt 1 anges kopplingen till stordatormiljön. I punkt 4 anges att anbudsgivaren måste underteckna en Sekretess och säkerhetsförbindelse. Denna finns i bilaga och där anges att ”I de fall leverantören ges tillgång till enligt offentlighets- och sekretesslagen (OSL) sekretesskyddad information skall tillämpliga bestämmelser i nämnda lag beaktas”. I punkt 5 tas det fysiska skalskyddet för en mindre del av it-miljön upp. Endast personer med behov av åtkomst till utrustning och information som godkänts får beredas tillgång till dessa delar. I punkt 6 anges att Transportstyrelsens it-drift styrs och påverkas av lagar, reglering och krav inom säkerhet, säkerhetsskydd, IT-säkerhet och informationssäkerhet. Hanteringen av dessa kommer att förhandlas under anbudsgivningen för att nå en god balans i kravställningen av tjänsten. Det innebär t.ex. att ett säkerhetsskyddsavtal kommer att ingå i det slutliga avtalet.

Av rubriken 1.4.5. Befintlig miljö framgår ett antal servicenivåer (SLA) och här anges att drift av befintlig stordatormiljö inte ingår i upphandlingen.

Under 1.4.7. Avtalstid står att planerad avtalstid är 5 år, med möjlighet till förlängning i ytterligare maximalt 4 år.

[125] Transportstyrelsen, inbjudan upphandling, 2014-05-08, TSG 2014–379.

Enligt 1.5. Antal leverantörer avser Transportstyrelsen att sluta avtal med en (1) leverantör för hela uppdraget. Användande av underleverantörer är dock tillåtet och regleras av bestämmelser i förfrågan med bilagor.

Under punkt 3.5.8. Informationssäkerhetsarbete anges standarder som leverantören ska följa.

Punkt 3.5.10. SGSI anger kraven för hanteringen av SGSI (Swedish Government Secure Internet). Här står att när det gäller outsourcing av denna tjänst till tredje part så får SGSI utrustningen inte placeras utanför Sverige samt att minst en person hos leverantören ska ha behörighet i Försvarsmaktens kryptosystem.

När det gäller prövning och urval av anbud står i punkt 4.2.2. Urvalskriterium Referenser att Transportstyrelsen kommer bedöma referenser när det gäller bl.a. erfarenhet av leverans som omfattar samhällsviktig verksamhet och pågående leverans till kund med hantering av sekretesskyddad information enligt OSL eller motsvarande.

Leveransmodell

I inbjudan fanns inga uttalade krav på en specifik leveransmodell. Av intervjuer med olika företrädare för Transportstyrelsen framgår att strategin var att genom det förhandlade förfarandet hitta den bästa leveransmodellen genom förhandling med potentiella leverantörer.

Samtidigt framgår att frågan om leveransmodell hade varit uppe tidigare i olika sammanhang. Dåvarande generaldirektör Staffan Widlert berättar att han tidigt tog upp frågan om outsourcing med regeringen. Det handlade inte specifikt om it-drift utan om man kan outsourca systemutveckling till exempelvis Baltikum eller Indien. De signaler Staffan Widlert fick var att det inte var uteslutet i förväg, att Transportstyrelsen skulle tänka vidare på frågorna och återkomma om det skulle bli allvar av det. Även den tidigare it-direktören berättar att Transportstyrelsen adresserade frågan om leveransmodell till departementet tidigt i processen. Svaret från departementet var att det var OK med en europeisk leveransmodell.

En medarbetare på it-avdelningen minns att frågan också hade varit uppe på It-avdelningens konferens 2013. Under en av program-

punkterna fick medarbetare ställa frågor till dåvarande generaldirektör Staffan Widlert. En av frågorna var hur han såg på outsourcing och om det fanns skäl att behålla det inom Sveriges rikes gränser eller om Transportstyrelsen var mogna att gå mot internationell leverans. Fanns det några skäl som talade för eller emot den ena eller andra modellen? Enligt uppgift svarade Staffan Widlert att han inte kunde se något skäl till att behålla leveranser inom Sverige, varken av politiska skäl eller säkerhetsskäl.

Den tidigare partneransvarige för upphandlingen säger att de diskuterade krav på leverans inom EU utifrån EU-lagstiftning. Men de hade inga diskussioner om hinder för leverans från ett annat land inom EU, förutom för körkortstillverkningen där det krävdes en svensk leverans.

Flera av de vi intervjuat inom it-avdelningen framhåller att marknaden idag är internationell och att de flesta leverantörer erbjuder internationella leveransmodeller för att vara konkurrenskraftiga, både avseende pris och kompetens. Leveransmodellerna bedöms framförallt ur ett affärsmässigt perspektiv för att kunna göra den bästa affären.

Inkomna ansökningar

Öppning av inkomna ansökningar gjordes den 10 juni 2014. Åtta leverantörer hade då inkommit med ansökan om att få delta i upphandlingen. Av dessa bedömdes sex leverantörer kvalificera sig för vidare anbudsgivning. I svaret till IBM skriver Transportstyrelsen att IBM behöver säkerställa sin redovisning av samarbetsavtal för underleverantörer. Myndigheten kräver också en handling som stödjer samarbetet mellan olika IBM-bolag i IBM:s organisations- och leveransmodell.

Utredningen har tagit del av IBM:s anbud. Under punkt 3.2.3. Angivande av underleverantör finns en lista med IBM:s underleverantörer inklusive IBM-bolag utanför Sverige. Underleverantörerna är IBM-bolag i Indien, Polen, Irland, Finland, Danmark, Norge, Slovakien och Tjeckien. Därutöver finns tre underleverantörer som är bolag placerade i Sverige.

De sex leverantörerna får i samband med meddelande om kvalificering det sekretessavtal (förbindelse avseende säkerhet och sekretess) som ska skrivas på för att få tillgång till en stor del av informationen gällande upphandlingen. Alla bolag skriver på och skickar in förbindelserna.

Ledningsgruppen informeras

It-direktören informerar ledningsgruppen den 10 juni 2014[126] om att annonseringsperioden avseende upphandlingen av ny it-driftleverantör har löpt ut och att det är dags att analysera svaren. Vid samma möte sägs att målsättningen är att ha en ny driftleverantör på plats i mitten av 2015.

Styrelsen informeras

Vid Transportstyrelsens styrelsemöte den 19 juni 2014[127] informeras styrelsen, utifrån vad utredningen kunnat se, för första gången om läget i it-driftsupphandlingen. It-direktören gav då en statusrapport för stordatormigreringen och it-driftsupphandlingen (kommande arbete, tidplaner, ekonomi, måluppfyllelse och risker). Av protokollet framgår att projekten i huvudsak följer den ursprungliga planen både vad gäller tid och pengar och att de kommer att få en stor påverkan på leveranskapaciteten på it-området. Vidare sägs att driftupphandlingen redan idag påverkar möjligheten att genomföra förändringar. Successivt kommer allt fler resurser att vara upptagna i stordatormigreringen och under hösten 2016 kommer en frysperiod att påverka hela vägtrafikområdet.

Styrelsen underströk särskilt vikten av tydlig kommunikation om förutsättningarna för och konsekvenserna av arbetet, såväl externt som internt, samt av att ha handlingsberedskap avseende riskerna. Styrelsen önskade fortsatt rapportering av utvecklingen i projekten, närmast vid sitt sammanträde den 2 oktober 2014. Av protokoll framgår inte att upphandlingarna tas upp vid styrelsemötet i oktober 2014.

[126] Protokoll från sammanträde med Transportstyrelsens ledningsgrupp den 10 juni 2014, dnr 2014–06.
[127] Protokoll från sammanträde med Transportstyrelsens styrelse den 19 juni 2014, dnr 2014–03,

5.5.3 Kravställning

Genom det förhandlade förfarandet kunde kravställningen göras under själva upphandlingen. Kravarbetet hade påbörjats innan annonseringen men kom igång på allvar efter att annonsen gick ut.

En del i kravställningen omfattade ett internt arbete för att reda ut vilka krav som Transportstyrelsen hade. Enligt intervjuer med företrädare för it-avdelningen så fanns det en väl utvecklad projektorganisation som hanterade kravarbetet. Det drevs av it-avdelningen men förutsatte att verksamheten tog fram kraven. Här hade exempelvis it-rådet en viktig roll som styrgrupp. Verksamheten hade dock svårt att formulera konkreta krav, även på säkerhetsområdet.

En annan del i kravställningsarbetet gjordes gentemot leverantörerna. Det skedde i form av informationsmöten med syfte att fördjupa och klarlägga frågeställningar kring ett antal ämnesområden och lösningsalternativ. Detta kunde Transportstyrelsen sedan använda som grund för kravställning och utformning av anbudsunderlag. Områden som lyftes var transition och transformation, samverkan, tjänsteutveckling, flexibilitet, it-utveckling och dokumentation. Av den dokumentation utredningen fått del av framgår inte att säkerhetsområdet har lyfts vid informationsmöten med leverantörerna. Projektägaren menar dock i intervju att körkortstillverkningen och SGSI berördes eftersom det för denna del ställdes specifika krav på säkerhetsskydd och lokal leverans i Örebro med säkerhetsgodkänd personal.

Utredningen kan inte heller se att frågan om det är förenligt med offentlighets- och sekretesslagen (2009:400) att myndigheten lämnar ut sin information till en extern leverantör har diskuterats. I detta ingår också att ta ställning till om det är lämpligt att lämna ut informationen. Vidare noteras att det i systemen är fråga om behandling av personuppgifter vilket innebär att också de krav som ställs i personuppgiftslagen (1998:204), PuL, måste beaktas. Utredningen kan inte se att detta har tagits upp annat än att myndigheten sedermera tecknar ett personuppgiftsbiträdesavtal med den utvalda leverantören. En myndighet som Transportstyrelsen har även arkivlagstiftningen att ta hänsyn till.

I slutändan var kravställningen i stora delar densamma som den som fanns gentemot Trafikverket. Det gällde även kraven på säkerhetsområdet, vilket innebar att endast körkortstillverkningen och SGSI omfattades av särskilda säkerhetskrav.

Ledningsgruppen informeras

Vid ledningsgruppsmötet den 23 september 2014[128] informerar it-direktören om att driftsupphandlingen och stordatormigreringen löper på bra och följer tidplanen. Samma information ges vid ledningsgruppsmötet den 21–22 oktober 2014[129].

5.5.4 Förfrågningsunderlag

Utkast till förfrågningsunderlag skickades den 24 oktober 2014 på remiss till leverantörerna och även internt inom Transportstyrelsen. Av intervjuer med företrädare för projektet framkommer att det kom in ganska få synpunkter från anbudsgivarna. Däremot kom det fler synpunkter internt från bl.a. säkerhetsfunktionen och it-avdelningen. De interna synpunkterna handlade mer om lämpligheten med outsourcingen i sig än detaljsynpunkter på upphandlingen.

Den 7 november 2014 publicerades upphandlingsunderlaget[130] med bilagor (bl.a. nuläge, kravspecifikation, sekretess- och säkerhetsförbindelse och kommersiella villkor). Anbudstiden var fram till den 17 december 2014. I inledningen anges vad Transportstyrelsen vill uppnå genom upphandlingen. I korthet handlar det om att avsevärt sänka de totala it-kostnaderna, att få en stabilare drift, förändra leveranserna efter verksamhetens behov, skapa förändringskapacitet och att köpa tjänster och funktioner.

I förfrågningsunderlaget, punkt 2.1.1.1. Hantering av underleverantörer, framgår att om anbudsgivare anser att ytterligare leverantörer behövs så ska underleverantör och skälen till detta framgå tydligt i anbudet. De anbudsgivare som bjuds in till anbudsgivning ges

[128] Protokoll från sammanträde med Transportstyrelsens ledningsgrupp den 23 september 2014, dnr 2014–07.
[129] Protokoll från sammanträde med Transportstyrelsens ledningsgrupp den 21–22 oktober 2014, dnr 2014–08.
[130] Transportstyrelsen, Upphandlingsdokument, 2017-07-07 (utskrivet), TSG 2014–379.

möjlighet att komplettera med ytterligare leverantörer om det behövs för att uppfylla krav som tidigare inte framgått. Transportstyrelsen förbehåller sig rätten att diskvalificera anbudsgivare om denne bytt ut tidigare angiven underleverantör utan Transportstyrelsens skriftliga tillåtelse. Byte medges inte om det innebär att de krav som ställs inte kan uppfyllas.

Under 2.3 Utvärdering står att Transportstyrelsen kommer att anta det anbud som vid en sammantagen bedömning av pris och kvalitet är det ekonomiskt mest fördelaktiga.

I bilaga 11 kommersiella villkor it-drift står under punkt 10 att huvudregeln är att dokumentation och kommunikation rörande avtalet och leverantörens åtaganden ska ske på svenska. Transportstyrelsen kan dock godkänna kommunikation och dokumentation på engelska om det inte innebär en olägenhet för Transportstyrelsen. Under övrigt, punkt 27, står att Transportstyrelsen avser att under förhandling föra en diskussion om möjlighet till eventuellt personalövertagande av viss personal i samband med driftsövertagandet. Det gäller primärt ”driftnära” resurser där arbetsuppgifter kommer att ingå i leveransen och där det kan finnas ett mervärde i sådan överenskommelse för båda parter och berörd personal.

Säkerhetskraven i förfrågningsunderlaget

I bilaga 6 kravspecifikation it-drift, avsnitt 2.12 framgår kraven på säkerhet. Samtliga krav är ska-krav utom två (2.12.2 GAP-analys och 2.12.20 Logganalys).

I inledningen står att ”Syftet med säkerhetsarbetet är att förhindra, eller minska konsekvenserna av, oönskade händelser inom leveransen och att under alla omständigheter upprätthålla Transportstyrelsens förmåga att fullgöra sina åtaganden.” I detta ingår:

- Åtkomstbegränsning (Sekretess) – skydd mot obehörig åtkomst av information
- Riktighet – åtgärder för att åstadkomma rätt kvalitet på information
- Tillgänglighet – åtgärder för att säkra drift och funktionalitet
- Spårbarhet – möjligheten att fastställa vem som gjort vad eller att kunna verifiera orsaken till en händelse.

Under 2.12.2 står att anbudsgivaren tillsammans med Transportstyrelsen parallellt med transitions- och transformationsfaserna ska genomföra en *GAP-analys* med en jämförelse av säkerhetsriktlinjer och deras införande. Eventuella brister åtgärdas i samverkan som separat beställda tilläggstjänster och hanteras under transformationsfasen. Resultatet ska sedan ligga till grund för en säkerhetshandbok som ska styra säkerhetsarbetet under kontraktets livslängd. Säkerhetshandboken uppdateras under kontraktets gång i händelse av förändringar av riktlinjer och andra krav genom samverkan. Omfattningen av GAP-analysen sker i samråd och uppdraget beställs separat av Transportstyrelsen.

Under Hantering och skydd av tillgångar, 2.12.4, står att ”Eventuella avsteg från säkerhetskraven ska beslutas av Transportstyrelsen i samråd med Anbudsgivaren som en del av gapanalys och genom samverkansforum. Varje sådant avsteg ska vara dokumenterat där risker och konsekvenser med varje avsteg ska vara analyserade och bedömda genom formell riskanalys.”

Under Personalresurser och säkerhet, 2.12.5, står att ”Den personal hos anbudsgivaren som deltar i leveransen där säkerhetsskyddsavtal krävs ska ha genomgått godkänd bakgrundskontroll samt ha fått säkerhetsutbildning i enlighet med säkerhetsskyddslagen”. Vidare sägs i 2.12.6 att ”Personal hos Anbudsgivaren som deltar i leveransen ska ha genomgått godkänd utbildning enligt överenskommelse där bland annat lagstiftning runt hantering av personuppgifter ska ingå.”

Under 2.12.11 framgår de särskilda ska-krav som ställs på hanteringen av SGSI.

Under 2.12.23 står att ”Regelbunden uppföljning av tilldelade behörigheter samt borttagande av behörigheter som inte längre behövs ska utföras enligt överenskomna rutiner. Anbudsgivaren ska tillhandahålla rapporter för att styrka detta i enlighet med överenskomna samarbetsformer. ”

Under avsnitt 2.13 framgår kraven för Korttillverkningen. Under 2.13.4 står att ”Anbudsgivaren ska i samråd med Transportstyrelsen utsedd person upprätta en förteckning över godkänd behörig personal (…). Denna personal ska även vara säkerhetsprövad enligt gällande säkerhetsskyddsavtal.”

I bilaga 11 till förfrågningsunderlaget (Kommersiella villkor IT-drift) står att säkerhetsskyddsavtal i sin helhet tas fram av Transportstyrelsen. Säkerhetsskyddsavtalet måste undertecknas för att huvudavtalet ska vara giltigt. Under punkt 21 står att leverantörens anställda och underkonsulter ska följa samma sekretess som enligt OSL gäller för Transportstyrelsens anställda. Detta ska säkerställas genom särskild sekretessförbindelse mellan Transportstyrelsen och leverantören.

Frågor och svar

I samband med att förfrågningsunderlaget gick ut gavs anbudsgivarna möjlighet att ställa frågor i upphandlingen. Frågor och svar[131] sammanställdes av Transportstyrelsen och gick ut till anbudsgivarna den 9 december 2014.

I punkt 40 finns följande fråga: ”I vilka it-lösningar förekommer skyddsvärd information som omfattas av säkerhetsskyddsavtalet, och i vilken utsträckning ser ni att leverantörens personal kommer att ha tillgång till denna på ett sätt som kräver säkerhetsprövning/registerkontroll? Transportstyrelsens svar lyder ”Vi har än så länge inte genomfört detta för alla it-lösningar. I GAP-analys, bilaga 6 rubrik 2.12.2 kommer detta att utredas. Vi bedömer att detta gäller en mindre del av it-lösningarna.” Utredningen har inte fått klarhet i varifrån denna bedömning kommer.

I punkt 48 ställs frågan ”Vi kan inte se att anbudsunderlaget innehåller några restriktioner mot att data placeras eller på annat sätt hanteras utanför Sverige. Kan Transportstyrelsen bekräfta att det inte finns några sådana restriktioner (förutsatt att Personuppgiftslagens krav är uppfyllda) förutom vad som kan gälla för korttillverkningen. Om svaret inte är ja, kan Transportstyrelsen precisera vilka restriktioner som gäller inom detta område för a) placering av data, b) hantering av data (dvs tillgång från utlandet till Transportstyrelsens data för att leverera tjänsterna)? Punkt 75 rör samma fråga och lyder ”Hur ser Transportstyrelsen på möjligheten för anbudsgivarna att erbjuda Transportstyrelsen konsulter för driftstjänster från 1: EU, 2: från resten av världen?” Transportstyrelsens svar lyder

[131] Transportstyrelsen, Svar på frågor och informationsmeddelande gällande upphandling TSG 2014–379 IT-drift, 2014-12-09, TSG 2014–379.

”Placering/Lagring av data ska ske i Sverige. Hantering för drift och support kan ske utanför Sverige med förutsättning att övriga ställda krav och säkerhetsregler följs. Man hänvisar till samma svar för punkt 75 med tillägget att svaret även gäller konsulttjänster.

Ytterligare en intressant fråga finns under punkt 60 ”Har leverantören under avtalstiden möjlighet att lägga till eller ta bort underleverantörer om behov uppstår?”. Transportstyrelsen svarar ”Ja, men ändring av underleverantör som står för en icke oväsentlig del av leveransen ska godkännas av Transportstyrelsen. Ny underleverantör måste uppfylla de obligatoriska grundkrav som ställdes i upphandlingen, t.ex. gällande ekonomisk ställning, obligatoriska uteslutningsgrunder etc.” Krav på säkerhetsprövning nämns inte här.

Under punkt 14 efterfrågar anbudsgivare skisser på hur samtliga komponenter är sammankopplade. Transportstyrelsen svarar att de inte kan lämna ut information om detta innan ett säkerhetsskyddsavtal är påskrivet.

I punkt 70 görs förtydliganden om att det är ett obligatoriskt krav att vinnande anbudsgivare även undertecknar säkerhetsskyddsavtal samt sekretess- och säkerhetsförbindelse.

Av intervjuer framgår att det inte var självklart hur Transportstyrelsen skulle besvara frågorna 48 och 75 om leveransmodell (förutom för körkortstillverkningen). Frågan hanterades av säkerhetsfunktionen och inköpsenheten. Det är oklart om chefsjuristen tillfrågades. Enligt uppgift var det svårt att få någon att sätta ner foten och peka på vad som gällde. Uppgifterna skiljer sig också åt mellan olika intervjupersoner. Företrädare för it-avdelningen uttrycker att det framkom att det vid det tillfället inte fanns några hinder för en utländsk leverans om den uppfyllde de krav på säkerhet som ställts. Eftersom det enbart var körkortstillverkningen och SGSI som omfattades av särskilda säkerhetskrav enligt kravställningen så utgick man från att det räckte. Det framkommer också uppgifter om att Transportstyrelsen stämde av frågan med Säkerhetspolisen och att svaret var att det inte fanns något som pekade på att data och personal var tvungen att hållas inom Sverige. Detta förutsatt att Transportstyrelsen inte exporterade någon skyddsvärd information och så länge det skedde med säkerhetsgodkänd personal. Säkerhetsskyddschefen ger en annan bild. Klart är dock att frågan aktualiserades, att den var svår att besvara och att Transportstyrelsen i sitt svar öppnade för en utländsk leveransmodell.

Ledningsgruppen informeras

Vid ledningsgruppsmötet den 16 december 2014[132] informerar it-direktören om att tiden för att komma in med offerter i den pågående driftupphandlingen inom kort löper ut. Han säger vidare att samarbetet med inköpsenheten fungerar väldigt bra.

5.5.5 Anbud

Den 18 december 2014 var det dags för anbudsöppning[133]. Fyra leverantörer hade då inkommit med anbud. Dessa var CGI, Evry, IBM Svenska AB och Tieto. Anbuden från tre av leverantörerna byggde på i huvudsak utländska leveransmodeller (IBM, CGI och Tieto). Evry hade en svensk leveransmodell.

Utvärdering av anbud

I ett första steg gjorde Transportstyrelsen en genomgång för att säkerställa att anbuden uppfyllde samtliga obligatoriska krav. Därefter genomfördes anbudspresentation med samtliga anbudsgivare för att förstå och vid behov förtydliga anbuden. Efter det gjordes en bedömning av anbudens uppfyllnad av bör-krav och slutligen gjordes intervjuer med nyckelpersoner från anbudsgivarna. Efter anbudsgenomgång, anbudspresentation och intervjuer genomfördes en utvärdering för att avgöra vilken eller vilka parter som skulle kallas till förhandling. Utvärderingen utgick från en viktning på 75 procent kvalitet och 25 procent pris. Enligt uppgift berörde ca 4 procent av kvalitetskraven säkerhet. Företrädare för säkerhetsfunktionen deltog i utvärderingen.

Av den slutliga utvärderingen[134] framgår att IBM och Tieto i kvalitetsbedömningen båda hade högsta poäng. IBM:s anbudspris var lägst, därefter följde CGI, Tieto och Evry. När anbudspriset viktades mot kvalitet fick IBM det lägsta jämförelsepriset medan Tieto

[132] Protokoll från sammanträde med Transportstyrelsens ledningsgrupp den 16 december 2014, dnr 2014–09.
[133] Transportstyrelsen, Anbudsöppningsprotokoll, 2014-12-18, TSG 2014–379.
[134] Transportstyrelsen, Upphandlingsprotokoll, 2015-03-31, TSG 2014–379, Bilaga Resultatrapport.

hamnade tvåa. Övriga två leverantörer hade ett betydligt högre jämförelsepris.

Utifrån resultatet av utvärderingen beslutade Transportstyrelsen att endast bjuda in IBM till förhandling. Beslutet fattades av core team efter förankring med it-direktören och It-rådet (styrgruppen).

Styrelsen informeras

Vid styrelsemötet den 18 december 2014[135] orienterade it-direktören styrelsen om läget i stordatormigreringen och it-driftupphandlingen (viktiga händelser, kommande arbete, tidplaner, ekonomi, måluppfyllelse och risker). Projekten anges löpa på enligt plan och att de kommer att få stor verksamhetspåverkan och innebär att ändringar på väg-trafikområdet som rör vägtrafikregistret inte kan genomföras hösten 2016. Vidare konstaterades att myndigheten gjort en viss rensning av gamla system, men valt en 1–1-lösning för migreringen för att minimera riskerna, samt att Regeringskansliet är väl införstått med förändringarna och det kommande ändringsstoppet hösten 2016. Styrelsen förklarade att den önskar fortsatt återrapportering av utvecklingen i projekten, närmast vid sitt sammanträde den 18 juni 2015.

Ledningsgruppen informeras

It-direktören informerade vid ledningsgruppsmötet den 10 februari 2015[136] om läget i stordatormigreringen och it-driftupphandlingen. Han sa att myndigheten är inne i en period av minskad leveranskapacitet och att it-området under 2016 i princip kommer vara ”stängt på grund av underhåll”. Dåvarande generaldirektören Staffan Widlert konstaterade att det är viktigt att hålla i och genomföra arbetet. Förändringarna är nödvändiga, och effekterna på kapaciteten under tiden arbetet pågår var väl kända när beslutet togs.

[135] Protokoll från sammanträde med Transportstyrelsens styrelse den 18 december 2014, dnr 2014–06.
[136] Protokoll från sammanträde med Transportstyrelsens ledningsgrupp den 10 februari 2015, dnr 2015-01,

Nyckelordet är prioritering, både på kort och på lång sikt. Regeringskansliet har insikt om förhållandet. Det är fortsatt viktigt att kommunicera vad som sker, både internt och externt.

Utredningen förstår diskussionen som att den till största del handlade om stordatormigreringen.

5.5.6 Förhandling mellan Transportstyrelsen och IBM

Av intervju med projektägaren för Nytt IT-driftavtal framgår att Transportstyrelsens strategi i förhandlingen med IBM var att säkerställa att IBM:s anbud motsvarade Transportstyrelsens förfrågningsunderlag.

Utredningen har tagit del av två protokoll[137] från förhandlingar mellan Transportstyrelsen och IBM. Av protokollen framgår dock att åtminstone ytterligare 5–6 möten har hållits under februari 2015. Vid mötena deltog från Transportstyrelsen bl.a. it-direktören, projektägaren, en it-strateg och en upphandlare. Vid mötet den 30 mars 2015 deltog även en it-avtalsansvarig och en upphandlingsjurist från Transportstyrelsen. Från IBM deltog Sverigechefen för strategisk outsourcing, säljansvarig, kundansvarig, en jurist samt en kompetens inom teknisk lösning.

Av förhandlingsprotokollet den 17 februari 2015 (då 5–6 möten redan hållits) framkommer att parterna bl.a. kvalitetssäkrat pris/innehåll och övriga punkter. I förhandlingsprotokollet från den 30 mars 2015 framkommer att parterna diskuterat prisbilaga, huvudavtal och underavtal samt tidplan för avtalstecknande. Det framgår inte av protokollen att säkerhetsfrågor tagits upp. Enligt uppgift gjordes det inte och företrädare för säkerhetsfunktionen medverkade inte heller i förhandlingen.

Enligt uppgift togs frågan om eventuellt personalövertagande av driftnära resurser, som lyftes fram i bilagan kommersiella villkor punkt 27 i förfrågningsunderlaget, inte upp i förhandlingen med IBM då it-ledningen inte ville se över den möjligheten.

[137] Transportstyrelsen, Protokoll 2015-02-17, Förhandling i upphandling av IT-drift. Protokoll 2015-03-30, Förhandling nr 2 i upphandling av IT-drift.

Avtalsorganisation

Avtalet i sin helhet arbetades fram i dialog och förhandlingar mellan Transportstyrelsen och IBM.

Enligt uppgift från inköpschefen på Transportstyrelsen utgick Transportstyrelsen från IT & Telekomföretagens standardvillkor med Kammarkollegiets tillägg vid utformning av avtalet. Vissa avtalsvillkor var fastställda redan i förfrågningsunderlaget. Förfarande stämdes av med Konkurrensverket (som på den tiden hade upphandlingsstödet).

I avtalsorganisationen för Transportstyrelsen ingick projektägaren och projektledaren för it-driftupphandlingen, en upphandlare och en jurist från inköpsenheten, en it-avtalsansvarig, en upphandlingskonsult och en extern rådgivare samt företrädare för It-avdelningen. Även it-säkerhetsansvarig deltog i deltog i den interna dialogen om det kommersiella avtalet. Säkerhetsskyddsavtalet togs fram av säkerhetsskyddschefen separat från avtalsprocessen med affärsavtalet.

Transportstyrelsen hade enligt uppgift under hela avtalsprocessen, men främst inledningsvis, stöd av en advokatbyrå som beställdes via ramavtal för juridiska tjänster. Kvalitetssäkringen av avtalet gjordes av en annan advokatbyrå, som inte varit inblandad i processen med att ta fram avtalet. Kvalitetssäkringen var en begränsad granskning som främst hade fokus på att hitta oklarheter i avtalet.

5.5.7 Beslut om tilldelning

Den 31 mars 2015 fattar ekonomidirektören tilldelningsbeslut för upphandling av it-drift[138]. Av beslutet framgår att Transportstyrelsen efter genomförd slutlig utvärdering beslutat att anta IBM:s anbud som det ekonomiskt mest fördelaktiga anbudet. I den slutliga handläggningen av ärendet deltog it-direktören, projektägaren samt en upphandlare och en upphandlingsjurist.

Beslutet överklagades inte.

[138] Transportstyrelsen, Tilldelningsbeslut, 2015-03-31, TSG 2014–379.

5.5.8 Avtalet med IBM

Transportstyrelsen tecknar avtal[139] med IBM Svenska AB den 14 april 2015. Generaldirektör Maria Ågren och it-direktören undertecknar för Transportstyrelsen. Även säkerhetsskyddsavtalet undertecknas då. Det var meningen att Staffan Widlert skulle skriva på it-driftavtalet med den nya leverantören innan han gick i pension. Men eftersom upphandlingen var något försenad hann han inte göra det innan hans förordnande löpte ut. Istället fick Maria Ågren göra det kort efter att hon tagit över som generaldirektör på Transportstyrelsen. Maria Ågren säger i intervju med utredningen att undertecknandet av avtalet var en ceremoniell process. Hon hade stämt av med it-direktören innan om upphandlingen var korrekt gjord och om den överklagats.

Ledningsgruppen informeras

Tidigare samma dag hade ledningsgruppen fått information om driftsupphandlingen.[140] It-direktören informerade ledningsgruppen om att upphandlingen var genomförd, att tilldelningsbeslutet hade vunnit laga kraft och att närmast väntade avtalsskrivning med myndighetens nya driftleverantör. Ledningsgruppen erinrades även om syftet med och omfattningen av upphandlingen, samt informerades kortfattat om vad som skulle hända framöver.

Huvudavtalet

I huvudavtalet står att parterna enats om att samarbeta och verka för att tillgodose Transportstyrelsens behov och ambition att:

- Avsevärt sänka Transportstyrelsernas totala it-kostnader
- Höja kvaliteten i leveranserna och skapa en stabilare drift
- Skapa flexibilitet i att kunna förändra leveranserna utifrån verksamhetens behov

[139] Transportstyrelsen, Avtal om IT-drift, 2015-04-08, TSA 2015–54.
[140] Protokoll från sammanträde med Transportstyrelsens ledningsgrupp den 14 april 2015, dnr 2015-03.

- Skapa förändringskapacitet och i ett större sammanhang kunna använda de tjänster som marknaden och leverantörerna utvecklar
- Förflytta Transportstyrelsen i värdekedjan och köpa tjänster och funktioner.

På kort sikt innebär avtalet att leverantören genom *transition* övertar Transportstyrelsens infrastruktur och ansvaret för befintlig drift och genom *transformation* förflyttar Transportstyrelsens it-miljö till leverantörens standardtjänster. Genom detta skapas förutsättningarna att utveckla samarbetet och leveransen mot Transportstyrelsens långsiktiga mål.

Avtalstiden är 5 år med möjlighet till förlängning på två år och därefter ytterligare två år.

Under 2.9 Kopplade avtal i huvudavtalet framgår enligt 2.9.1 att ett separat tecknat säkerhetsskyddsavtal samt ett avtal om personuppgiftsbiträde är kopplat till huvudavtalet. Avtalets giltighet är beroende av att dessa två avtal tecknas mellan parterna. Av 2.9.2 framgår att ”Parterna genom ändringshanteringen i detta Avtal överenskomma om justering av ersättningen enligt Avtalet om Leverantörens kostnader väsentligen påverkas med anledning av förändrade åtaganden enligt Avtal om personuppgiftsbiträde eller Säkerhetsskyddsavtal.” Detta gäller bl.a. för ”c) ändringar i övrigt efter Avtalets tecknande av krav och instruktioner från Transportstyrelsen enligt Avtal om personuppgiftsbiträde eller Säkerhetsskyddsavtal.”

Under punkt 2.9.3 står att parterna under transition ska ta fram en detaljerad specifikation av omfattningen av respektive parts åtagande avseende säkerhetsskydd. Där står också att ”Leverantörens priser och villkor är baserade på den kravställning gällande säkerhetsskyddsavtal som har skett i upphandlingen. I den mån avvikelser från denna utgångspunkt identifieras när den detaljerade specifikationen tas fram eller identifieras senare hanteras de kommersiella konsekvenserna enligt vad som sägs ovan i punkt 2.9.2.” Enligt den tidigare projektägaren för it-driftupphandlingen innebar denna skrivning en möjlighet för Transportstyrelsen att under transitionen och inom avtalet utöka den del av leveransen som skulle omfattas av säkerhetsskydd. Detta skulle göras genom en GAP-analys. I frågor och svar i samband med att förfrågningsunderlaget låg ute, bedömde

Transportstyrelsen att det gällde en mindre del av it-lösningarna (se vidare avsnitt 5.5.4, Frågor och svar).

Under punkt 4 Leverantörens åtaganden står under punkt 4.1.3 att ”Leverantören ska tillhandahålla tjänster i enlighet med allmänna regelverk och i enlighet med Transportstyrelsens vid var tid gällande riktlinjer för IT-området, såsom IT-strategi, IT-arkitektur och krav avseende säkerhet.”

Under 4.2 Hantering av underleverantörer framgår av bilaga 6 godkända underleverantörer. Vidare står ”Byte eller tillägg av underleverantör måste skriftligen godkännas av Transportstyrelsen. I samband med begäran om godkännande av ny underleverantör kommer Transportstyrelsen att kontrollera denne med avseende på de krav, förutsättningar och villkor som ställts i upphandlingen. Byte eller tillägg av underleverantör ska inte förvägras utan sakliga skäl.”

Utredningen noterar att underleverantörer enligt bilaga 6 till huvudavtalet i stort är desamma som i anbudet. Kompletteringar har gjorts för några underleverantörer i Sverige samt en underleverantör i Rumänien.

Bilaga 3 Säkerhet

Av bilaga 3 framgår de säkerhetskrav som ställs på leveransen och leverantören. De är desamma som framgick av bilaga 6 kravspecifikation it-drift, avsnitt 2.12 (se avsnitt 5.5.4 ovan).

Säkerhetsskyddsavtalet

Säkerhetsskyddsavtalet för IT-drift[141] är upprättat av säkerhetsskyddschefen och undertecknat av generaldirektör Maria Ågren samt chefen för IBM Svenska AB den 14 april 2014. I avtalet benämns Transportstyrelsen för Myndigheten och IBM för Företaget. Avtalet avseende IT-drift kallas Uppdraget. Avtalet träder i kraft vid undertecknandet och gäller tills vidare eller tills det skriftligen sägs upp av endera parten. Som framgått i avsnitt 4.6.4 var säkerhetsskyddsavtalet framtaget från ett malldokument för säkerhetsskyddsavtal från Säkerhetspolisen. Mallen anpassades bara något för den aktuella upphandlingen.

[141] Transportstyrelsen, Säkerhetsskyddsavtal (nivå 1), 2015-04-14, TSA 2015-143.

Av avtalet framgår att säkerhetskyddsavtalet, tillsammans med företagets säkerhetsskyddsinstruktion, reglerar vilka säkerhetsskyddsåtgärder som företaget ska vidta i samband med uppdraget. Om det förekommer motstridiga uppgifter avseende säkerhetsområdet i affärsavtalet gäller säkerhetsskyddsavtalet framför affärsavtalet. Vidare framgår att företaget endast får använda underleverantörer som har tecknat säkerhetsskyddsavtal med myndigheten.

Av avtalets olika punkter framgår bl.a. att det vid företaget ska finnas en säkerhetsskyddsorganisation och att företaget ska ta fram en säkerhetsskyddsinstruktion när säkerhetsskyddsavtalet har undertecknats. Säkerhetsskyddsinstruktionen ska godkännas av myndigheten. Myndigheten ska reglera tilldelningen av behörigheter, fastställa nivå på tillträdesbegränsning och klargöra för företaget i vilken utsträckning handlingar som överlämnas till företaget innehåller hemliga uppgifter. Detaljerade regler om säkerhetsprövning anges och att myndigheten innan uppdraget påbörjas ska ge lämplig utbildning i säkerhetsskyddsfrågor till de personer på företaget som kan komma att få del av hemliga uppgifter. Myndigheten ges också rätt att kontrollera att regleringen följs. Vad gäller kostnader står att företaget ska bära eventuella kostnader som uppkommer med anledning av säkerhetsskyddsavtalet om inget annat avtalas i affärsavtalet.

Personuppgiftsbiträdesavtalet

Personuppgiftsbiträdesavtal mellan Transportstyrelsen och IBM Svenska AB om behandling av personuppgifter i system, register och databas som IBM driftar och förvaltar genom avtal IT-drift TSA 2015–54[142] är undertecknat av it-direktören och ansvarig för outsourcing på IBM Svenska AB den 14 april 2015. I avtalet benämns Transportstyrelsen som personuppgiftsansvarig och IBM som personuppgiftsbiträde.[143]

Av avtalet framgår bl.a. att personuppgiftsbiträdet får behandla personuppgifter endast i enlighet med avtalet och de ytterligare

[142] Transportsstyrelsen, Personuppgiftsbiträdesavtal, 2015-04-14, TSA 2015-142.
[143] En aktör som behandlar personuppgifter för den personuppgiftsansvariges räkning kallas personuppgiftsbiträde. Den personuppgiftsansvarige kan aldrig avsäga sig personuppgiftsansvaret.

skriftliga instruktioner som Transportstyrelsen lämnar. Personuppgiftsbiträdet är skyldigt att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas (30 och 31 §§ PuL). Om personuppgiftsbiträdet, med Transportstyrelsens godkännande, lägger över sina skyldigheter enligt avtalet på ett underbiträde, får detta endast ske genom ingående av skriftligt avtal med underbiträdet.

Avseende behandling av personuppgifter av underbiträde i tredje land har personuppgiftsbiträdet mandat att teckna personuppgiftsbiträdesavtal för Transportstyrelsens räkning med sådana underbiträden. I sådana fall ska Kommissionens beslut (2010/87/EU) om standardavtalsklausuler användas

I avtalet beskrivs de behandlingar som omfattas av avtalet; vilka som är de registrerade, vilken typ av personuppgifter som behandlas, vilka känsliga personuppgifter som behandlas, vilka integritetskänsliga personuppgifter som behandlas, hur personuppgifterna ska behandlas samt ändamålet med behandlingen.

Avtalet innehåller också instruktioner till personuppgiftsbiträdet rörande t.ex. utbildning, behörighetskontroll, spårbarhet och logg.

Avseende överföring av personuppgifter som är under behandling till tredje land anges att detta inte är tillåtet om inte landet har en adekvat skyddsnivå för skyddet av personuppgifterna. Om 13 § personuppgiftsförordningen (1998:1191) iakttas får personuppgifter trots detta överföras till tredje land.

Utredningen kan konstatera att det aktuella personuppgiftsbiträdesavtalet formellt ser ut att uppfylla de krav som kan ställas på ett sådant. I avtalet anges att IBM efter godkännande av myndigheten kan anlita underbiträden men endast genom skriftligt avtal. Enligt uppgift från Transportstyrelsen har IBM tecknat underbiträdesavtal med alla underleverantörer. Utredningen har dock inte tagit del av dessa underbiträdesavtal och vet därför inte hur de är utformade. Utredningen känner inte heller till när dessa underbiträdesavtal tecknades.

Skilda uppfattningar om vad säkerhetsskyddsavtalet omfattade

Utredningen har i intervjuer med företrädare för it-driftupphandlingen och medarbetare inom säkerhetsområdet fått bilden att det

funnits olika uppfattningar om vilka delar av leveransen som säkerhetsskyddsavtalet med IBM omfattade.

Företrädare för it-driftupphandlingen, bl.a. den dåvarande projektägaren, säger att det var väldigt tydligt att kraven på säkerhetsskydd omfattade körkortstillverkningen (KTV) och SGSI. För dessa krävdes säkerhetsprövad personal och en lokal leveransmodell. Utöver detta kunde enligt punkt 2.9.3 i huvudavtalet ytterligare delar tillkomma som omfattade krav på säkerhetsskydd. Detta skulle definieras i samband med GAP-analys under transitionen. Endast en mindre del av it-lösningarna bedömdes kunna komma att omfattas av krav på säkerhetsskydd. Varifrån denna bedömning kommer och vem som gjort den är dock oklart för utredningen.

En person som arbetar med it-säkerhet på It-avdelningen säger däremot i intervju med utredningen att KTV, dvs förkortningen för körkortstillverkningen, var ett kodord för samtliga särskilt skyddsvärda system inom Transportstyrelsen. Det avsåg alltså inte bara körkortstillverkningen i Örebro. Han menar att alla i it-driftupphandlingen var fullt införstådda med att KTV stod för något mer än körkortstillverkningen. För säkerhetsfunktionen var det därmed tydligt redan när avtal skrevs att fler delar än körkortstillverkningen och SGSI skulle komma att omfattas av säkerhetsskydd.

Utredningen har även varit i kontakt med IBM i frågan om vilka delar som omfattades av säkerhetsskyddsavtalet. IBM svarar enligt följande: Säkerhetsskyddsavtalet gäller hemliga uppgifter, och enligt punkt 5 i säkerhetsskyddsavtalet ska myndigheten klargöra för leverantören i vilken utsträckning "handlingar med mera som överlämnas" till leverantören innehåller sådana uppgifter. Förväntan vid avtalsskrivandet, baserat på upphandlingsunderlaget, var att de hemliga uppgifterna skulle kunna identifieras och begränsas till vissa definierade delar av leveransen. I takt med att arbetet i Transition avseende säkerhetskraven fortskred, från sommaren och under hösten 2015, framkom dock gradvis att Transportstyrelsen inte kunde göra någon sådan avgränsning. Därför blev slutsatsen att säkerhetsskyddsavtal behövde omfatta alla delar av leveransen som hanterade Transportstyrelsens data.

Utredningen kan konstatera att det redan vid avtalstecknandet alltså fanns skilda uppfattningar om vad säkerhetsskyddsavtalet omfattade men också vad det skulle kunna komma att omfatta efter GAP-analysen. Klart är att Transportstyrelsens integrerade it-miljö

försvårat möjligheten att avgränsa kraven på säkerhetsskydd. Det är också tydligt att it-driftprojektet och säkerhetsfunktionen har talat förbi varandra.

5.6 Läget inför transitionen

Var stod då Transportstyrelsen när affärsavtalet och säkerhetsskyddsavtalet med IBM var påskrivet och transitionen skulle starta?

Som framgår av säkerhetsskyddsavtalet skulle företaget, dvs. IBM, ha en säkerhetskyddsorganisation etablerad och företaget skulle upprätta en säkerhetsskyddsinstruktion som skulle godkännas av myndigheten. Transportstyrelsen skulle i sin tur klargöra i vilken utsträckning handlingar som överlämnas till företaget innehåller hemliga uppgifter, fastställa nivån på tillträdesbegränsning och göra säkerhetsprövningar av de personer som får del av hemliga uppgifter. Innan uppdraget påbörjades skulle lämplig utbildning i säkerhetsskyddsfrågor hållas för personer på IBM.

Som utredningen förstått det var inget av detta förberett eller genomfört på Transportstyrelsen när avtalet med IBM var påskrivet. Få eller inga rutiner fanns framtagna och någon utbildning för IBM hade inte hållits. Säkerhetsskyddschefen visste inte hur säkerhetsprövningar av personer i utlandet skulle göras. Hur mycket IBM hade på plats enligt avtalet har inte utredningen kännedom om. Med tanke på de problem som uppstod under transitionen och därefter så fanns sannolikt mycket lite på plats även hos IBM.

Utöver detta behövde Transportstyrelsen också göra ett omfattande arbete med bl.a. driftdokumentation gentemot den nya leverantören.

Transportstyrelsen hade dessutom en tight tidplan fastlagd gentemot Trafikverket som successivt började dra ner på resurserna i leveransorganisationen gentemot Transportstyrelsen.

Sammantaget ger detta bilden av att Transportstyrelsen hade en mycket stor utmaning framför sig.

5.7 Sammanfattande iakttagelser

Bakgrunden till att Transportstyrelsen beslutade att outsourca it-driften var att myndigheten identifierat it-driften som ett område

där myndigheten kunde kostnadseffektivisera. Myndigheten hade också tagit fram en it-försörjningsstrategi. Dessutom var Transportstyrelsen missnöjda med Trafikverkets leverans av it-drift. Parallellt med detta beslutade Trafikverket att avveckla sin leverans till externa kunder.

Transportstyrelsens it-försörjningsstrategi saknar resonemang om vilka verksamheter som är lämpliga att outsourca och hur säkerhetsskydd och informationssäkerhet ska beaktas vid val av försörjningsform. Säkerhetsfrågorna togs inte heller upp i förstudien inför beslutet att upphandla it-driften. Informationsklassning och behörigheter lyftes dock fram som två processer som måste finnas på plats innan myndigheten kan gå ut och outsourca it-driften. Dessa processer är fortfarande inte på plats i myndigheten.

Utredningen bedömer att det inte var fel att genomföra upphandlingen genom förhandlat förfarande. Upphandlingen tycks också ha genomförts på ett bra och genomarbetat sätt utifrån kraven i LOU. Utredningen bedömer dock att tidplanen för upphandlingen och för transition till ny leverantör redan från början var alltför optimistisk. Inte minst med tanke på att upphandlingen genomfördes parallellt med stordatormigreringen och reskontran (DUBBing).

Kravställningen i upphandlingen var bristfällig, framför allt vad gäller kraven på säkerhetsskydd. Om myndigheten hade genomfört informationsklassning och haft kännedom om vilka uppgifter myndigheten hanterar och var, hade kraven kunnat preciseras. Istället blev kravställningen densamma som den för Trafikverket, vilket innebar att endast körkortstillverkningen (KTV) och SGSI omfattades av krav på säkerhetsskydd.

Transportstyrelsen har haft svårt att besvara anbudsgivarnas frågor om eventuella restriktioner för leveransmodeller. Därmed har myndigheten också öppnat upp för leverans med utländska underleverantörer.

Utredningen bedömer att säkerhetsskyddsavtalet i sig hade kunnat ge ett gott säkerhetsskydd för outsourcingen av it-driften. Detta förutsatt att allt var på plats eller hade förberetts i samband med att avtalet med IBM undertecknades. Vad utredningen kunnat se fanns dock inga av åtgärderna på plats på Transportstyrelsen.

Säkerhetsfunktionen har hela tiden legat efter i upphandlingsprocessen, vilket kan bero på att de bjudits in i ett sent skede, att de inte fått gehör i organisationen men även på grund av att de inte haft

tillräcklig kompetens att ge stöd, ställa krav och vidta säkerhetsskyddsåtgärder.

Styrelsen har informerats bara vid några få tillfällen under upphandlingen. Ledningsgruppen har däremot fått mer löpande information.

Sammantaget bedömer utredningen att Transportstyrelsen inte förberett beslutet om outsourcing och upphandling av it-drift tillräckligt väl. Det gäller framför allt säkerhetsaspekter som informationsklassning och kravställning på leverantören. Upphandlingen i sig bedöms ha genomförts på ett bra sätt. Däremot var förberedelserna för säkerhetsskyddsåtgärder utifrån säkerhetsskyddsavtalet bristfälliga. Säkerhetsskyddsavtalet skulle också ha kunnat ge ett bra säkerhetsskydd om säkerhetsskyddsåtgärder hade förberetts och vidtagits i tid. Detta hade myndigheten inte gjort.

6 Övergången av it-driften till IBM

6.1 Inledning

Utredningen ska enligt direktiven kartlägga processen från det att Transportstyrelsen beslutade att påbörja arbetet med en förändrad it-drift och it-organisation fram till i dag. Därvid ska viktiga tidpunkter, gjorda vägval, beslut som fattats på olika nivåer inom myndigheten och information som lämnats till Regeringskansliet redovisas. Utredningen ska redovisa vilka alternativ som utreddes och vilka analyser och bedömningar av konsekvenser och risker som gjordes vid olika tidpunkter under processen samt vilka typer av interna och eventuellt externa kontakter och specialistroller som bidrog till dessa.

Detta kapitel återger händelseförloppet efter det att tilldelningsbeslut fattats och affärsavtal tecknats med IBM[144]. Redogörelsen omfattar övergången av it-driften (nedan kallad transitionen) till IBM samt de beslut om avsteg som fattades i samband med detta. Aktuell tidsperiod är från avtalets tecknande i april 2015 fram till transitionens avslut i november 2015.

6.2 Transition och transformation

Outsourcingen av it-driften är indelad i två delar; transition och transformation. Transitionen innefattar byte av driftsleverantör från Trafikverket till IBM vilket innebär att man byter de personer som utför leveransen men inte tekniken. Efter det att transitionen var genomförd skulle enligt avtalet transformationen starta.

[144] Även sekretessavtal, säkerhetskyddsavtal och personuppgiftbiträdesavtal tecknades.

Transformationen innebär en förändring av leveransen där man byter teknik och ersätter den med leverantörens (IBM:s) leveransmodell och tjänster. Transformationsfasen var planerad att påbörjas direkt efter avslutad transition och skulle enligt den ursprungliga tidplanen vara slutförd den 28 februari 2017. Transformationen är för närvarande uppskjuten på obestämd framtid. Transformationen beskrivs närmare i kapitel 8.

6.3 Vad innefattade transitionen?

Avtalet med IBM om it-drift undertecknades den 14 april 2015. I avtalsbilaga D-1 Transition anges att transitionfasen planeras att genomföras under perioden 1 maj 2015 – 31 augusti 2015. Stabiliseringsfasen för it är planerad för perioden 1 augusti 2015 – 31 augusti 2015 och ett driftövertagande av ny leverantör planeras ske den 1 september 2015.

Aktiviteterna i transitionsfasen syftar till att överta ansvaret för drift av Transportstyrelsens befintliga miljö och att fortsatt administrera och förvalta den i enlighet med nuläget (befintlig drift) beskrivet i avtalsbilagorna 5 Nuläge och 6 Kravspecifikation från upphandlingsfasen.[145]

De delprojekt som ingick i transitionen var kundmiljöanalys, projekt för samverkan, övertagande av tjänster, övertagande av leverantörskontrakt, övertagande av infrastruktur, nätverksuppkoppling, kunskapsöverföring och dokumentation, service desk/support.

Delprojekt Kundmiljöanalys omfattar enligt avtalsbilaga D-1 bl.a. att Transportstyrelsen ska tillhandahålla detaljerad information om it-miljön, bistå leverantören med behörighet till information, system samt till fysiska lokationer och verifiera att systemdokumentationen är uppdaterad. Leverantören ska ta emot, granska och analysera information om it-miljön och validera Transportstyrelsens tekniska dokumentation, data och verksamhetsprocesser.

Delprojekt Kunskapsöverföring och dokumentation omfattar enligt avtalsbilaga D-1 bl.a. att Transportstyrelsen ska överlämna befintlig dokumentation och arbetsinstruktioner och ta fram kompletterande dokumentation på förfrågan från Leverantören. Transportstyrelsens personal ska visa hur deras arbete går till samt lämna över

[145] Bilaga D-1 Transition, IT-drift TSA 2015–54, 2015-04-08.

dokumentation och arbetsbeskrivningar. Transportstyrelsen ansvarar för att Leverantörens personal utför vissa arbetsuppgifter i produktionsmiljö under överinseende och instruktion av Transportstyrelsen och dess nuvarande leverantörs personal.

Leverantören ska granska dokumentation som ska tas över, översätta dokumentationen till engelska och skapa struktur för lagring av dokumentationen. Leverantören ansvarar för parallellt utförande, dvs. Leverantörens personal utför huvudsakligen arbetsuppgifterna, men det övergripande ansvaret kvarstår hos Transportstyrelsen och dess nuvarande leverantör som bistår med support.

Delprojekt Övertagande av tjänster omfattar enligt avtalsbilaga D-1 bl.a. att Transportstyrelsen ska ge Leverantören tillgång till Transportstyrelsens personal samt underleverantörer som har kunskap om de tjänster som Leverantören ska ta över och sköta driften av, ge och godkänna användar-ID/behörigheter som behövs för tjänsteleveransen, validera och ge tillgång till relevant dokumentation, system och resurser för säkerhet och riskbedömning och identifiera en kontaktperson för områdena säkerhet och risk för tjänsteleveransen.

Leverantören ska analysera historisk information och data, granska infrastruktur och infrastrukturkapacitet, validera behörigheter samt identifiera ändringar eller undantag som ett resultat av säkerhetsanalysen och genomföra en GAP-analys[146] mellan CSD och Transportstyrelsens miljöer.

Utredningen har av företrädare för Transportstyrelsen fått information att någon GAP-analys avseende säkerhet aldrig genomfördes under transitionen. Att detta inte skedde torde ha försvårat arbetet med att uppfylla säkerhetskraven. Detta kan jämföras med det förberedelsearbete inför transitionen som Trafikverket genomförde för att skydda sin information. Detta arbete omfattade bl.a. att ta fram en säkerhetsanalys för transitionsprojektet och att ta fram en riktlinje för sekretess för den personal som deltog i projektet från Trafikverket.

[146] Analysen skulle identifiera om det fanns säkerhetsbrister i förhållande till planerad leverans. Det handlade inte bara om säkerhetsskydd utan även informationssäkerhet och it-säkerhet.

6.4 Arbetet med transitionen under maj

6.4.1 Inledande åtgärder

Transitionen startade den 4 maj 2015. It-rådet var ansvarigt för transitionen men det fanns olika styrgrupper inom It-rådet. För att genomföra transitionen fanns bl.a. en styrgrupp för delportfölj Framtidssäkring vars uppdrag var att hitta, definiera, äga och försöka lösa konflikter där behov i de ingående projekten (stordatormigreringen, it-driftavtal och reskontra (DUBBing)) står mot varandra och därför kan få stora konsekvenser.

I juni bildas projektet It-drift 2.0 för att samordna alla aktiviteter som behöver genomföras i processen för att byta leverantör av it-drift, inklusive transition, se nedan i avsnitt 6.5.1. Projektägare blir samma person som genomfört implementeringen av stordatormigreringen.

6.4.2 Transitionens uppstart

Enligt protokoll från It-rådsmöte den 5 maj 2015 fattades beslutet att prioritera projekt it-driftupphandlingen gällande säkerhetsskyddsavtal och de aktiviteter som behöver komma på plats till den 1 september 2015. Det antecknades att det fanns risk att beslutet skulle kunna påverka stordatormigreringen. I anteckningarna noterades också som en potentiell konflikt fysisk tillgång till it-infrastruktur i myndighetens datahallar.

Vidare framgår att projektet initialt innan anbudsgivarna kom in med sina offerter hade en budget som var lägre estimerad. En utökad budget med 8,5 miljoner kronor godkändes.

Det faktum att budgeten för transitionen direkt höjs med 8,5 miljoner kronor kan enligt utredningen ha samband med att förarbetet avseende denna fas och vad som skulle komma att krävas inte hade varit tillräckligt.

I underlaget för mötet anges att behov finns för insatser kring säkerhetsskyddsavtal och att det är en mycket trång resurs eftersom det endast är säkerhetsskyddschefen som kan genomföra insatserna. Enligt uppgift från personer vid Transportstyrelsen är det vid denna tidpunkt endast IBM Svenska AB som har undertecknat ett säkerhetsskyddsavtal. Detta bekräftas också av andra uppgifter.

Dokumentation

En viktig del av transitionen (och senare transformationen) var kunskapsöverföring och dokumentation, se ovan i avsnitt 6.3 om *Delprojekt Kunskapsöverföring och dokumentation*. Av företrädare för Transportstyrelsen har utredningen fått information att det fanns mycket lite dokumenterat gällande it-driften på Transportstyrelsen och att merparten av det som upprättats var på initiativ av Trafikverket. Vid transitionen till IBM från Trafikverket kunde man överlämna en mängd teknisk dokumentation, med vilka servrar som fanns, vad databaserna hette och liknande. Däremot fanns i princip ingen dokumentation om hur applikationerna fungerade, eller hur de skulle hanteras. Det fanns ett specifikt dokument kallat ”drifthandbok”, som användes för just det syftet – och av cirka 100 applikationer i portföljen hade enbart en handfull av dem detta dokument.

Att det saknades dokumentation i så hög utsträckning var problematiskt utifrån flera aspekter. Dels innebar det ett stort glapp i kunskap vid leverantörsbytet, dels innebar det att arbetet under transitionen behövde kompletteras med att ta fram och uppdatera applikationsdriftsdokumentationen. I den redan hårt pressade tidplanen för transitionen ställde detta till problem då det både krävde resurser och tog tid.

Personer på Transportstyrelsen har uppgett att en stor fråga i kunskapsöverföringen var språket då det var kravställt för att en svensk myndighet agerar på svenska med dokumentation och korrespondens på svenska. Viss dokumentation översattes via Google translate.

Säkerhetskrav och utländska underleverantörer

Säkerhetsskyddschefen har uppgett till utredningen att det vid samtal med IBM i maj 2015 blir tydligt att det rör sig om utländska underleverantörer och att säkerhetsskyddsavtal kanske krävs för ett stort antal länder. Han har vidare uppgett att kontroll om det var möjligt att teckna säkerhetsskyddsavtal med en utländsk leverantör gjordes med Utrikesdepartementet som gav grönt ljus samt att han under hösten 2015 fick en lista på de länder Sverige hade bilaterala avtal med vilket bl.a. var Ungern och Tjeckien.

Ekonomidirektören har uppgett att han fick veta att det var fråga om utländska leverantörer först efter att han skrivit på tilldelningsbeslutet den 31 mars 2015 men han såg det inte som ett problem då de hade ett säkerhetskyddsavtal. Informationssäkerhetsansvarig har uppgett att det var tydligt i projektet att det inte skulle ställas krav på svensk personal då detta skulle förstöra leveransmodellen och förhindra besparingar.

Projektägaren för upphandlingen av it-drift har uppgett till utredningen att det fanns en insikt om att det var fråga om utländska underleverantörer redan i november 2014 då myndigheten skickade ut kravspecifikationen. Det var dock endast körkortstillverkningen som vid denna tidpunkt hade krav på lokal leverans, säkerhetsskyddsavtal m.m. Det finns emellertid olika uppfattningar om vad som egentligen omfattades av dessa krav, se avsnitt 5.5.4.

Projektägaren för upphandlingen har uppgett att IBM reagerade med förvåning på de säkerhetskrav som kom fram i samband med att utländska underleverantörer presenterades. En överenskommelse togs fram med förtydligande av säkerhetskraven samt att IBM inte hade rätt till mer ersättning förutsatt att leveransmodellen med Tjeckien med flera länder kunde kvarstå. Enligt projektägaren för upphandlingen var det otydligt i det kommersiella avtalet om säkerhetsskyddsavtalet som skrivits under i april 2015 enbart avsåg körkortstillverkningen.

Enligt projektägaren för upphandlingen (under transitionen partneransvarig gentemot IBM) accepterade IBM dock att leverera utifrån att all deras personal skulle vara säkerhetsgodkänd och att alla underleverantörer skulle ha säkerhetsskyddsavtal utan någon ytterligare ersättning. Vidare har uppgetts att det varit svårt att internt få fram information om framstegen i själva säkerhetsprövningsprocessen, både kring godkännanden och avslag.

6.4.3 Styrelsen informeras

Styrelsen fick den 6 maj 2015 information och lägesrapport om stordatormigreringen och driftupphandlingen av it-direktören.[147]

[147] Protokoll från sammanträde med Transportstyrelsens styrelse den 5–6 maj 2015, dnr 2015–02, p. 9.

Styrelsen orienterades om och diskuterade viktiga händelser, kommande arbete, tidplaner, ekonomi, måluppfyllelse och risker i de båda pågående projekten stordatormigrering respektive driftupphandling. Sammanfattningsvis antecknades i protokollet att upphandlingarna är klara och att projekten löper enligt plan, men står inför en tuff period. Båda projekten uppgavs vara speciella, med stor inbördes påverkan, och krävde hög prioritet. Det angavs finnas starka motiv att hålla tidplanen, varje förseningsmånad bedömdes kosta ytterligare cirka 10 miljoner kronor.

Det framgår inte av protokollet vilka risker som styrelsen informerades om eller något närmare om hur tidplanen skulle kunna hållas. Det går inte att avgöra hur detaljerad information styrelsen har fått om de risker som identifierats i driftsupphandlingen eller vilken information styrelsen fått om tidplanen annat än att det fanns starka motiv att den skulle hållas. Det framgår inte om styrelsen vid detta tillfälle blivit informerad om de insatser som krävs för säkerhetsskydd och hur detta kan komma att påverka tidplanen. Värt att notera är att detta är Maria Ågrens första styrelsemöte som generaldirektör och under en tidigare punkt på mötet har hon gått igenom sina förväntningar på styrelsen och poängterat att styrelsen är gemensamt ansvarig för verksamheten inför regeringen.

Maria Ågren uppger i sin stämningsansökan till Arbetsdomstolen att hon i maj 2015 fick signaler från säkerhetsskyddschefen att säkerhetsprövningen av enskilda individer hos IBM tog längre tid än väntat p.g.a. långa svarstider hos Säkerhetspolisen. Denna information synes inte ha nått vare sig styrelse eller ledningsgrupp.

6.4.4 Ledningsgruppen informeras

Vid ledningsgruppsmöte den 6 maj 2015 gavs ingen information om it-driftsupphandlingen.[148] Först på ledningsgruppsmöte i november 2015 kommer frågan åter upp och då i form av att dåvarande ställföreträdande generaldirektör Jacob Gramenius informerar ledningsgruppen om att Säkerhetspolisen gör en tillsyn av myndighetens tillämpning av säkerhetsskyddslagstiftningen.[149]

[148] Protokoll från sammanträde med Transportstyrelsens ledningsgrupp den 6 maj 2015, dnr 2015–04.
[149] Protokoll från sammanträde med Transportstyrelsens ledningsgrupp den 3 november 2015, dnr 2015–10.

Utredningen kan inte utifrån de protokoll som finns från ledningsgruppens möten under 2015 bedöma om ledningsgruppen varit informerad om de risker som funnits eller de problem som uppstått med bl.a. tidplanen under transitionen. Det förefaller enligt utredningen som märkligt att ledningsgruppen inte informeras närmare om hur driftsövertagandet fortskrider, särskilt då det ganska tidigt uppstår problem med säkerhetsarbetet vilket i sin tur påverkar tidplanen.

Jacob Gramenius har till utredningen gjort reflektionen att den här typen av stora upphandlingar på ett tydligare sätt bör tas upp i ledningsgruppen.

6.4.5 Avsteg 1

Det första avsteget rubricerat *Beslut om avsteg från gällande lagstiftning och Transportstyrelsens riktlinjer för åtkomst till säkerhetsskyddad och sekretessbelagd information* är daterat den 8 maj 2015 och underskrivet av Maria Ågren den 20 maj 2015. Utredningen har fått uppgift om att avstegsbeslutet föredrogs av dåvarande it-direktören för generaldirektören. Ingen föredragande är angiven på beslutet och det saknar diarienr. Avsteget gäller till och med den 31 december 2015.

Av beslutet framgår bl.a. följande. Bakgrunden till avsteget är att en due diligence ska genomföras som en del i transitionsprojektet, dvs. en genomlysning av den it-infrastruktur som ska övertas av den nya driftleverantören IBM samt kunskapsöverföring och överlämnande av dokumentation. Enligt tidplanen för projektet ska det parallellt med due diligence och transitionsprojekt genomföras säkerhetsaktiviteter av administrativ karaktär som krävs för att Transportstyrelsen ska uppnå efterlevnad mot de regulativa och juridiska krav som ställs på verksamheten, primärt säkerhetsskyddslagen, personuppgiftslagen och offentlighets- och sekretesslagen. Dessa säkerhetsaktiviteter (inkl. säkerhetsskyddsavtal) av administrativ karaktär är normalt sett den första aktiviteten i en transitionsfas för att inte bryta mot regulativa och juridiska krav och innan kunskaps- och dokumentationsöverföring sker. Säkerhetsaktiviteterna anges innebära att Transportstyrelsen tecknar avtal inom dessa områden och genomför en del efterföljande aktiviteter tillsammans med IBM och dess underleverantörer.

Eftersom de säkerhetsaktiviteter som krävs inte är genomförda innebär det en risk att projektet bryter mot gällande lagstiftning. Två alternativ presenteras som möjliga.

Alternativ 1 innebär att projektet blir avsevärt försenat och består av bl.a. följande åtgärder. De uppstartade aktiviteterna gentemot tillsynsmyndigheten Säkerhetspolisen avseende säkerhetsskyddade uppgifter måste färdiggöras. Detta innebär säkerhetsprövningar av berörd personal med en ledtid som Transportstyrelsen inte kan påverka. Tidsuppskattning för detta är en till två månader. Utöver det ska även utbildningar genomföras av berörd personal. Sekretessbelagda uppgifter hanteras genom sekretessförbindelser och personuppgifter regleras genom personuppgiftsbiträdesavtal som tecknats med IBM. Det måste säkras att IBM har tecknat avtal med sina underleverantörer.

Alternativ 2 innebär att projektets begäran om avsteg godkänns och beskrivs enligt följande. Projektet vill begära ett beslut om avsteg från gällande lagstiftning (säkerhetsskyddslagen [1996:627], SSL, personuppgiftslagen [1998:204], PuL och offentlighets- och sekretesslagen [2009:400], OSL) och Transportstyrelsens riktlinje ”Riktlinje för krav på informationssäkerhet”. Konsekvensen av alternativ 2 är att förutom att röja skyddsvärd information som kan användas för vidare angrepp mot Transportstyrelsen och negativ publicitet, även riskerar brott mot ovan angiven lagstiftning.

Förslag på kompenserande åtgärder till alternativ 2 är att fortsätta ha sekretessförbindelser på individnivå samt att ha en instruktion och utbildning för hantering och överföring av kunskap och dokumentation. Denna måste tas fram innan man fortsätter med transitionen. Framtagning och genomförande beräknas från beslut till cirka 1–2 veckor.

Detta första avstegsbeslut är daterat endast två dagar efter att styrelsen informerats om driftupphandlingen och det tas fram mindre än en månad efter det att avtalet med IBM skrevs på. Det framkommer ingenstans att styrelsen har informerats om att läget var sådant att det skulle kunna bli nödvändigt att fatta ett sådant beslut om avsteg.

Utredningen noterar att enligt 20 och 21 §§ myndighetsförordningen (2007:515) ska ärenden avgöras efter föredragning och en handling ska upprättas som ska innehålla bl.a. vem som har varit föredragande. Enligt uppgift från dåvarande it-direktören var det

inte fråga om en formell föredragning och det var inte alltid som det var en föredragande på olika beslut inom Transportstyrelsen.

Det är oklart vad som egentligen händer som leder fram till att det första avstegsbeslutet tas fram redan ett par dagar in i transitionen. Utredningen har inte kunnat utröna om det är någon ny information som tillkommer eller om det är det faktum att säkerhetsskyddschefen anges som den enda resurs som kan genomföra arbetet med säkerhetsskyddsavtalen vilket innebär en tidspress som inte var möjlig att leverera mot och att det är först nu som alla berörda inser det.

Flera säkerhetspersoner på Transportstyrelsen har uppgett att avsteget togs fram för att visa att det inte går att göra avsteg från de säkerhetsaktiviteter som skulle genomföras. Tanken skulle alltså ha varit att avsteget skulle vara en ögonöppnare för generaldirektören och det var med förvåning dessa personer sedan såg att det skrevs på. Denna bild motsägs dock av andra som var involverade i avstegen. Maria Ågren har i sin stämningsansökan till Arbetsdomstolen uppgett att hon uppfattade avstegen som tillåtna tidsbegränsade dispenser i väntan på att en fullständig säkerhetsprövning skulle hinna ske med hjälp av Säkerhetspolisen. Båda synsätten kan enligt utredningens mening ifrågasättas.

Av bakgrunden till beslutet om avsteg framgår att Transportstyrelsen är väl medveten om att det krävs säkerhetsaktiviteter av administrativ karaktär men även att det krävs efterföljande aktiviteter av både myndigheten och leverantören samt att säkerhetsaktiviteterna av administrativ karaktär normalt är den första aktiviteten i en transitionsfas och ska ske innan kunskaps- och dokumentationsöverföring sker. Detta visar att kunskapen om vad som krävs finns men att man av olika skäl ändå väljer en annan väg. Det främsta skälet är enligt utredningen troligen att alternativ 1 innebär en avsevärd försening av projektet vilket gör att detta alternativ väljs bort.

Det är oklart för utredningen om de kompenserande åtgärder som tas upp i form av sekretessförbindelser på individnivå och framtagande av en instruktion och utbildning för hantering och överföring av kunskap och dokumentation har genomförts innan transitionen fortskrider. Säkerhetsskyddschefen har uppgett till utredningen att han inte vet vem som ansvarade för att sekretessförbindelser upprättades men att det kan ha varit it-säkerhet.

6.5 Arbetet med transitionen under juni

6.5.1 Projektdirektivet godkänns

Enligt minnesanteckningar från It-rådsmöte den 4 juni 2015 godkändes vid detta möte projektdirektivet för projekt It-drift 2.0 med ändringen att It-avdelningen ska finansiera projektet. Säkerhetsskyddsavtalen nämns återigen som en mycket trång resurs och att det endast är säkerhetsskyddschefen som kan genomföra insatserna. Det finns dock ingen analys eller beskrivning av vilka konsekvenser ett uteblivet resultat i denna del kan innebära.

I övrigt framkommer bl.a. följande avseende it-driftupphandlingen. Kritik finns kring kunskapsöverföringar till IBM. Det redovisas också en diskussion om vilket språk som ska användas vid dialog mellan Transportstyrelsen och IBM – svenska eller engelska.

Vidare konstateras att det finns en del frågetecken kring resurser från Trafikverket under juli månad. Projektet har identifierat en försening på cirka fem veckor p.g.a. osäkrade resurser och ett avvikelseunderlag finns framtaget. Projektet vill inte ändra tidplanen ännu utan först försöka säkra upp förseningen på andra sätt. Trots att projektet identifierar en försening på cirka fem veckor väljer man att inte ändra tidplanen. Det framgår inte vad projektet avser att göra för att säkra upp förseningen på andra sätt.

Utredningen ställer sig frågande till att frågan om resurser hos Trafikverket under sommaren 2015 inte säkerställdes innan transitionen påbörjas. Detta borde kanske till och med ha säkerställts redan då affärsavtalet undertecknades. Projektägaren för upphandlingen har uppgett till utredningen att kraven på säkerhetsprövning innebar att mer tid behövdes men att tidplanen var alltför optimistisk även utan dessa krav. Detta berodde främst på att Transportstyrelsen inte ville be Trafikverket att beordra sin personal att arbeta under semestern. Projektägaren för projektet It-drift 2.0 har uppgett till utredningen att hans bild direkt var att det inte kommer att fungera med den tidplan som var bestämd. Trots detta dröjer det ytterligare en månad till kontakt tas med Trafikverket och ny tidplan antas.

Kontakterna med Trafikverket om förlängning av driften

Projektägaren för It-drift 2.0 har uppgett till utredningen att han hade kontakter med Trafikverket i början av sommaren 2015 och då fick beskedet att Trafikverket som längst skulle kunna förlänga sin leverans till den 31 oktober 2015. Det står inte klart för utredningen om Transportstyrelsen vid denna tidpunkt bedömde att detta var ett tillfredsställande besked eller om man såg det som omöjligt att få Trafikverket att flytta fram detta datum ännu längre. En möjlighet hade varit att i ett sådant läge eskalera frågan för att säkerställa en längre tid med leverans av Trafikverket. Det framkommer dock en splittrad bild av om detta hade varit möjligt.

Tidigare generaldirektören Staffan Widlert har uppgett till utredningen att enligt hans mening hade Trafikverket varit tvungna att fortsätta driften om Transportstyrelsens generaldirektör hade tagit kontakt med Trafikverkets generaldirektör och begärt att Trafikverket skulle fortsätta driften trots att Trafikverket hade gjort sig av med de fast anställda och hade inhyrda konsulter. Enligt Staffan Widlert hade frågan kunnat eskaleras till departementet om Trafikverket hade vägrat.

Även den tidigare enhetschefen för drift- och infrastrukturenheten på Transportstyrelsen uppger till utredningen att det inte borde ha varit ett problem att kontakta Trafikverket och be om förlängning av driften.

Maria Ågren har uppgett att den bild som organisationen gav henne var att det inte var nödvändigt att fråga Trafikverket om de kunde förlänga driften under 2015 mer än vad som gjordes utan att det var först i februari 2016 som den riktiga krisen uppstod och då hade Trafikverket avvecklat sin verksamhet. Dock fanns det en rad indikationer på att projektet var drabbat av förseningar på grund av säkerhetsarbetet och avsteg 1 hade redan gjorts vilket borde ha varit en indikation på allvaret i situationen.

Trafikverkets it-direktör uppgav i förhör med Säkerhetspolisen att det fanns en rent teknisk och hypotetisk möjlighet för Trafikverket att fortsätta leveransen till Transportstyrelsen men att då skulle Transportstyrelsen ha fått ta de kostnader som i så fall uppstått. Leveransen hölls på slutet i huvudsak uppe med konsulter.

Enligt program- och projektledaren för avskiljningen av ICT på Trafikverket skulle Trafikverket dock ha behövt veta om att de

skulle fortsätta utföra driften ytterligare en tid redan under februari 2014. Om Transportstyrelsen då hade meddelat Trafikverket att de ville bygga in en option om fortsatt drift i ytterligare 6–12 månader så hade Trafikverket planerat för detta.

6.5.2 Tidplanen för säkerhetsskyddsavtal kommer inte att hålla

Enligt minnesanteckningar från extra It-rådsmöte den 25 juni 2015 presenterade projektägaren organisationen för projektet It-drift 2.0 och hur projektet ska gå från ett transitionsprojekt till ett transformationsprojekt. Vidare framgår att driftdokumentation inte är överlämnad och att kunskapsöverföring inte har startat. Förseningen kring kunskapsöverföring och överlämning av driftsdokumentation anges bero på att säkerhetsskyddet för IBM inte är klart ännu.

Det faktum att det saknades dokumentation avseende systemen (se ovan i avsnitt 6.4.2) innebar att tid och resurser behövde läggas på detta under transitionen som redan var tidspressad.

IBM antecknas efterfråga access in i Transportstyrelsens system för att kunna arbeta parallellt med Trafikverket för kunskapsöverföring. Det anges att IBM inte kan få detta förrän säkerhetsskyddsavtalet är klart.

I minnesanteckningarna anges att säkerhetsskyddschefen har fått i uppdrag av generaldirektören att säkra att alla säkerhetsskyddsavtal fullbordas med sluttidpunkt januari 2016. Det konstateras i anteckningarna att eftersom Trafikverket avslutar sitt åtagande helt senast den 31 december 2015 så kommer tidplanen för säkerhetsskyddsavtal inte att fungera.

It-rådet ger projekt It-drift 2.0 i uppdrag att ta fram ett förslag/beslutsunderlag för avsteg från säkerhetsskyddsavtalet under perioden fram till dess att säkerhetskyddsavtal är tecknat med alla parter.

Av underlaget till mötet framgår att övergång till parallellt utförande inom kunskapsöverföringen då IBM skulle tilldelas access in till systemen var planerad till den 1 juli 2015. Vidare anges att projektet bedömer att det är hög sannolikhet att kunskapsöverföringen inte kan fortskrida enligt plan med anledning av att aktiviteterna inom säkerhetsskydd inte har progress.

Det bör alltså vid denna tidpunkt stå klart för Transportstyrelsen att tidplanen för undertecknande av säkerhetsskyddsavtal inte kommer att hålla. Myndigheten väljer då att ta fram underlag för ytterligare ett avsteg från säkerhetsskyddsavtalet och det finns inga anteckningar om att myndigheten övervägt andra alternativ. Det finns såvitt utredningen kan se inga resonemang kring möjligheten att kontakta Trafikverket för att se om det går att förlänga deras leverans. Se ovan i avsnitt 6.5.1 om eventuella möjligheter till det.

Företrädare för Transportstyrelsen har uppgett till utredningen att det var för ont om tid och att myndigheten borde ha skaffat sig större rådrum. Vissa företrädare talar om att de borde ha sett till att de haft åtminstone ett år till med Trafikverket som leverantör för att kunna genomföra upphandling och transition.

6.6 Arbetet med transitionen under juli och augusti

6.6.1 Avsteg 2

Projekt It-drift 2.0 fick, som angetts ovan, den 25 juni 2015 i uppdrag att ta fram beslutsunderlag/förslag på avsteg från säkerhetsskyddsavtalet.

Beslut om avsteg 2 rubricerat *Beslut om avsteg från gällande lagstiftning och Transportstyrelsens riktlinjer för åtkomst till säkerhetsskyddad och sekretessbelagd information* är daterat den 29 juni 2016 och datum för beslut är den 3 juli 2015. Enligt uppgifter från företrädare för Transportstyrelsen föredras beslutet för Maria Ågren av it-direktören på telefon, då hon är på semester. Projektet agerar utifrån att beslutet fattas den 3 juli 2015. Det skriftliga beslutet skickas till Maria Ågrens hemadress och skrivs under av henne den 8 juli 2015. Ingen föredragande är angiven på beslutet och det saknar diarienummer.[150]

Av beslutet framgår bl.a. följande. I detta projekt har arbetet med säkerhetsaktiviteterna behövt löpa parallellt med övrigt arbete eftersom tidplanen hela tiden varit mycket tight. En tydlig ambitionshöjning har setts inom säkerhetsskyddet i och med bytet av it-driftleverantör. Detta motiveras delvis med att vi går från en leverans från en annan myndighet till en kommersiell aktör, men även

[150] Se ovan i avsnitt 6.4.5 vad som gäller enligt myndighetsförordningen.

med att arbetet tidigare varit eftersatt. Både avtalstecknande (säkerhetsskyddsavtal) med underleverantörer och de efterföljande åtgärderna är av olika skäl försenade i det pågående övertagandeprojektet.

Kunskapsöverföringen pågår nu utan att alla nämnda säkerhetsaktiviteter är genomförda vilket innebär en risk att projektet för driftövertagande bryter mot gällande lagstiftning.

Om inget avsteg beslutas måste den pågående kunskapsöverföringen pausas tillsvidare och de uppstartade aktiviteterna avseende säkerhetsskyddade uppgifter gentemot Säkerhetspolisen färdigställas. Konsekvensen utan detta avsteg blir att projektet blir ytterligare avsevärt försenat och därmed att även avtalad startdag måste senareläggas. Eftersom den nuvarande leveransen från Trafikverket upphör helt vid årsskiftet och stegvis avvecklas under hösten innebär detta en konkret risk för upprätthållandet av den dagliga driften av Transportstyrelsens it-system. Det innebär även omfattande merkostnader för Transportstyrelsen.

Avsteget anges innebära följande. Personal hos IBM och dess underleverantörer kan fortsätta att bygga upp sin kompetens kring de miljöer och it-system avtalet med IBM omfattar, att de kan tilldelas relevanta behörigheter samt att de kan ingå i IBM:s leveransorganisation parallellt med att arbetet med säkerhetsaktiviteterna pågår.

Avsteget gäller som längst till den 31 december 2015 och då senast ska de aktuella säkerhetsaktiviteterna vara genomförda.

Konsekvensen av avsteget är en förhöjd risk för röjande av skyddsvärd information som kan användas för vidare angrepp mot Transportstyrelsen, negativ publicitet och även risk för brott mot SSL, PuL och OSL.

Förslag på kompenserande åtgärder till avsteget är att fortsätta med sekretessförbindelser på individnivå. En handlingsplan har tagits fram som bl.a. innebär att begäran om registerkontroller för IBM Svenska AB ska vara inskickade till Transportstyrelsen senast den 11 augusti 2015 och att säkerhetsskyddsavtal för övriga IBM-länder och underleverantörer är inskickat till Transportstyrelsen senast den 11 augusti 2015 (inkluderar beskrivningar av säkerhetsorganisation och att säkerhetsskyddsinstruktion är bifogade).

I detta avsteg nämns således att IBM ska presentera en säkerhetsorganisation och säkerhetsskyddsinstruktion för Transportstyrelsen. Det normala i en säkerhetsskyddad upphandling är, som utredningen förstått det, att detta finns på plats direkt efter att affärsavtal och säkerhetsskyddsavtal undertecknats och innan tillgång till system och dokumentation som innehåller skyddsvärda och hemliga uppgifter medges.

I säkerhetsskyddsavtalet mellan Transportstyrelsen och IBM Svenska AB anges vad säkerhetsprövningen ska omfatta. IBM ansvarade för säkerhetsprövningen av sin egen personal men Transportstyrelsen skulle godkänna på redovisat underlag. Utredningen har inte tagit del av någon dokumentation kring detta.

Myndigheten nämner i avsteget att det finns en tydlig ambitionshöjning inom säkerhetsskyddsarbetet. Tyvärr har man inte gett projektet en tidplan som medger en sådan ambitionshöjning. Utredningen kan inte heller se att denna ambition funnits i myndigheten med tanke på hur t.ex. arbetet med behörighetshanteringen och informationsklassning hanterats.

6.6.2 Reviderad tidsplan presenteras och antas

På styrgruppsmöte (Transportstyrelsen, Trafikverket och IBM:s gemensamma styrgrupp) den 3 juli 2015 presenterades en reviderad tidplan med hänsyn tagen till de förseningar som då kunde konstateras inom transitionen. Styrgruppen beslutade att fastställa den reviderade planen och skjuta på start av tjänsteleveransen till den 1 november 2015. Detta innebar att Trafikverket skulle garantera leveransen till och med den 31 oktober 2015 och att IBM skulle ta över från den 1 november 2015.

Enligt minnesanteckningar från extra It-rådsmöte den 29 juli 2015 informerar projekt It-drift 2.0 att säkerhetsskyddsarbetet inte fortlöper enligt plan och att IBM:s övertagande måste skjutas till den 1 november 2015. It-rådet godkänner ändringarna av tidplanen enligt förslag. Det är en decimerad grupp som fattar det viktiga beslutet att skjuta på tjänsteleveransen, troligen p.g.a. att det är semestertider.

Av anteckningarna framgår vidare bl.a. följande. IBM har kommunicerat en reviderad tidplan till Transportstyrelsen. I denna

har många aktiviteter skjutits på. Utifrån tidigare tidplan finns det nu en försening på två månader. Bakgrunden till förseningen anges vara att konsekvenserna av semesterperioden blivit större än planerat. Trafikverket anges bl.a. inte ha kunnat möta upp med arbetskraft så att arbetet har kunnat fortgå under semesterperioden. Att det skulle kunna uppkomma förseningar p.g.a. semestrar diskuterades dock redan på It-rådet i början av juni och där angavs en försening på fem veckor.

Transportstyrelsen kontaktar i juli 2015 Trafikverket och förlänger deras leverans av it-drift med två månader. Även i detta läge fanns en möjlighet att överväga att förlänga Trafikverkets leverans ytterligare redan vid detta tillfälle då det också stod klart att säkerhetsarbetet inte haft nödvändig progress. Som redogörs för ovan i avsnitt 6.5.1 fanns dock olika uppfattningar huruvida detta hade varit möjligt.

I protokollet tas upp att seniora experter från Trafikverket behöver fångas upp som kan behövas fram till den 31 december 2015 och även en bit in under 2016. En tilltalande lösning anges vara att IBM säkrar de seniora experterna. Frågan om att säkra seniora experter skjuts dock upp till ett senare it-råd. Utredningen kan dock inte se att denna fråga har tagits upp igen under 2015.

Det faktum att frågan om att säkra seniora experter på Trafikverket tas upp är ytterligare en indikation på att Transportstyrelsen redan i detta läge borde ha försökt förlänga Trafikverkets leverans en längre period än som skedde då dessa seniora experter anges behöva vara tillgängliga fram till den 31 december 2015 och även under början av 2016.

Säkerhetsarbetet går inte enligt plan

Enligt minnesanteckningarna från extra It-rådsmöte den 29 juli 2015 hade inte säkerhetsarbetet vid den tidpunkten gjort nödvändiga framsteg. Av den anledningen har projektet nödgats ta fram en reservrutin till dess att säkerhetskyddsavtal är på plats. Underlaget till reservrutinen togs fram till veckan efter midsommar och beslut togs därefter om att använda den. Med reservrutinen utgår utredningen från att det som avses är det som anges i avsteg 2. Säkerhetsskyddsavtalen anges ska vara tecknade till den 11 augusti 2015.

I anteckningarna anges bl.a. följande avseende säkerhetsarbetet. Det har skett ett antal dialoger mellan Transportstyrelsen och IBM angående säkerhetsarbetet och nivå på säkerhetsskyddsavtal. Säkerhetsskyddsavtal måste slutas på individnivå. Transportstyrelsen anser att IBM måste lösa detta inom sin organisation då flera företag från flera länder är involverade. Säkerhetsskyddsavtalet innebär att den enskilde individen kan bakgrundskontrolleras. Vissa anställda på IBM har ställt sig avvaktande till en bakgrundskontroll och vissa har inte velat skriva ett säkerhetsskyddsavtal med Transportstyrelsen då deras åtagande är med IBM.

Vidare anges bl.a. att det i det ursprungliga affärsavtalet med IBM inte specificerades vilka delar som krävde bakgrundskontroll utan detta skulle tas fram under transitionen. Frågan om säkerhetsskyddsavtal kommer att tas upp på styrgruppsmöte med IBM som är planerat till den 30 juli 2015.

Det finns olika uppgifter om när det stod klart för Transportstyrelsen att det inte skulle gå att säkerhetspröva utländsk personal vilket i sin tur innebar att den tänkta leveransmodellen inte skulle fungera. Enligt uppgift från dåvarande it-direktören fick de veta detta i samband med att Säkerhetspolisen inledde sin tillsyn vilket var i september 2015. Projektägaren menar dock att det så sent som i slutet av oktober 2015 diskuterades hur många veckor det skulle ta innan personerna i fråga blev säkerhetsgodkända av Säkerhetspolisen.

Enligt andra företrädare för Transportstyrelsen var bilden att samtliga involverade trodde att de aktuella personerna från IBM skulle komma att godkännas vid säkerhetsprövningen. Bilden var att så snart säkerhetsskyddsavtalen var på plats och semesterperioden var över skulle personerna bli godkända. Diskussionen under semesterperioden 2015 var att det var fråga om resursbrist och hårt tryck på Säkerhetspolisen.

Utredningen kan konstatera att fokus i säkerhetsarbetet under den här perioden ligger på att se till att säkerhetsskyddsavtalen blir underskrivna på individnivå samt att registerkontroller ska genomföras. Det är dock viktigt att komma ihåg att ett påskrivet säkerhetsskyddsavtal och genomförd registerkontroll endast är en liten del av nödvändigt säkerhetsarbete. Enligt Säkerhetspolisen utgör t.ex. en

registerkontroll endast 10 procent medan myndighetens egen bedömning vid säkerhetsintervju, säkerhetsutbildning etc. utgör 90 procent.

Det finns således olika bilder av när Transportstyrelsen verkligen inser att det inte är möjligt att genomföra registerkontroller av utländska medborgare. Utredningen har inte kunnat fastställa exakt när detta skedde.

Säkerhetsskyddschefen har dock uppgett till utredningen att insändandet av registerkontrollunderlag till Säkerhetspolisen avseende svenska medborgare påbörjades i maj 2015 och avseende utländska medborgare i oktober/november 2015.

6.6.3 Styrelsen informeras

Vid styrelsemöte den 12 augusti 2015 informerar Maria Ågren styrelsen om att bytet av it-driftleverantör sannolikt kommer att försenas och skälen för detta samt om sina beslut om avsteg i anslutning till vissa inköpsbeslut under våren.[151] Styrelsen fick inte se avstegsbeslutet.

Bakgrunden till denna information är att internrevisionschefen har tillskrivit generaldirektören per e-post i juni 2015 och bl.a. frågat om styrelsen har informerats om avstegen och då fått uppfattningen att detta inte var planerat. Maria Ågren har å sin sida uppgett att hon troligen hade informerat styrelsen oavsett detta påpekande från internrevisionschefen och att hon i juni 2015 inte hade hunnit ta ställning till frågan.

Utredningen har i detta sammanhang också tagit del av minnesanteckningar från möte den 8 september 2015 mellan dåvarande styrelseordförande Rolf Annerberg, en styrelseledamot och internrevisionschefen. Av dessa minnesanteckningar framgår att internrevisionschefen frågar om Rolf Annerberg och styrelseledamoten som företrädare för styrelsen kan intyga att styrelsen informerats om att myndigheten gjort avsteg från PUL, OSL och SSL i maj-juni och eventuellt senare. Rolf Annerberg och styrelseledamoten svarar att styrelsen blivit väl informerad av generaldirektören vid styrelsemötet i augusti.

[151] Protokoll från sammanträde i Transportstyrelsens styrelse den 12 augusti 2015, dnr 2015–04.

Rolf Annerberg har till utredningen uppgett att han och de andra i styrelsen inte var särskilt angelägna om att dokumentera detta så väl. Rolf Annerbergs bild är att alla styrelseledamöter inte förstod vad Maria Ågren sa. Han har först efteråt förstått att någon jurist inte var inblandad och när han fick se avstegsbeslutet första gången vid förhöret hos Säkerhetspolisen såg han att det saknades föredragande vilket han tyckte var märkligt. Enligt Rolf Annerberg var styrelsens budskap till Maria Ågren att hon skulle ta upp detta med departementet. Han visste vid den tidpunkten också att avsteget redan var anmält till Säkerhetspolisen. Rolf Annerberg funderade över att själv kontakta departementet men bestämde sig för att det räckte att Maria Ågren gjorde det.

Maria Ågren har till utredningen uppgett att informationen till styrelsen inte dokumenterades då det var fråga om känslig information. Hennes bild var att styrelsen uttryckte oro över att avsteg hade gjorts men att styrelsen delade hennes bedömning av situationen. I stämningsansökan till Arbetsdomstolen har Maria Ågren uppgett att styrelseordförande uppgav vid styrelsemötet att han ansåg avstegen som allvarliga men att han hade svårt att finna något annat alternativ. Maria Ågren uppger att hon inte vid denna tidpunkt gav information om avstegen till departementet då hon inte förstod riktigt hur allvarligt avstegen var. Departementet informerades dock löpande under 2015 om projekten. Maria Ågrens bild var att departementets fokus var att Transportstyrelsen skulle kunna säkerställa att projekten genomfördes utan förseningar.

6.6.4 Utökad styrgrupp träffar IBM

Den 21 augusti 2015 träffar en utökad styrgrupp från It-rådet, extra inbjudna som It-rådet fått bjuda in och it-ledningsgruppen representanter från IBM. Det framgår inte av minnesanteckningarna vilka personer som deltog från It-rådet, vilka som var extra inbjudna eller vilka som deltog från It-ledningsgruppen eller IBM. Utredningen kan därför inte se om någon person från säkerhet deltog.

I punkt 6 i anteckningarna ställer projekt It-drift 2.0 frågan om vilka tankar som finns om det skulle tillstöta något så att leverans den 1 november blir svårt att klara. Svaret på detta är att myndigheten inte är i det läget utan får se andra vägar som att ta bort delar,

tilldela mer resurser och acceptera en lägre kvalitet. Alla i projektet ska veta att uppstår problem så ska det eskaleras direkt – inte dagen efter. Datumet måste hållas.[152]

I underlaget för mötet anges bl.a. följande utmaningar för projektet; kort tid för transition, inget övertagande av personal, språk, begrepp och organisation och dubbla leveransmodeller under lång tid. Underlaget innehåller också en redogörelse för de länder som är involverade i leveransmodellen. Ledning och styrning ska ske från IBM Svenska AB med underleverantörer i Tjeckien, Rumänien, Ungern och Irland. Utredningen noterar att det parallellt pågår en process med att omförhandla leveransmodellen för att godkänna nya underleverantörer. Denna process avslutas först i februari 2016, se avsnitt 8.2.

Avseende projektstatus framgår följande (projektets bedömningar). Transition har fattat ett styrgruppsbeslut att förlänga transitionen med två månader, t.o.m. oktober. Det innebär att avtalat startdatum är den 1 november 2015. Säkerhetsskyddsavtal är tecknat med IBM Svenska AB, men inte med underleverantörer i övriga länder. Generaldirektören har undertecknat ett i tid begränsat avsteg för de säkerhetsskyddsavtal som saknas. Kunskapsöverföringarna har kommit fram till de två sista faserna som totalt tar cirka sju veckor att genomföra.

Den övergripande projektstatusens utmaningar anges vara bl.a. säkerhetsskyddsarbetet och möjligheterna för IBM att använda sin globala organisation och sina underleverantörer, att kunskapsöverföringen inte har kommit igång med anledning av att arbetet inom säkerhetsskyddet inte fortskridit enligt plan och att accesstilldelningar försenats.

På frågan varför projektet är försenat anges två skäl; avsaknad av resurser hos Trafikverket under semesterperiod som föranledde att kunskapsöverföringen blev försenad samt att arbetet inom säkerhetsskydd inte färdigställts som föranledde att t.ex. dokumentation och accesser inte kunde lämnas över till IBM.

Sannolikheten att det ska bli ytterligare förseningar inom arbetet med säkerhetsskydd bedöms som hög. Handlingsplanen för denna risk är framtagning och godkännande av avsteg för att temporärt lösa

[152] Projektägaren för It-drift 2.0 meddelade också i augusti att den 1 november 2015 var en skarp deadline och att situationer som påverkade tidplanen negativt måste hanteras på andra sätt än genom att skjuta på tidplanen.

situationen, tät dialog och bevaka aktiviteterna med säkerhetsavdelningen, synkronisering av aktiviteter med projekt stordatormigreringen för att effektivisera arbetet då motsvarande arbete sker där och ytterligare resursförstärkning inom säkerhetsområdet.

Utredningen noterar att risken för ytterligare förseningar p.g.a. implementering av säkerhetsskyddsavtalen bedöms som hög. I handlingsplanen som tas fram finns dock inga resonemang kring möjligheten att återigen kontakta Trafikverket för att se om det går att förlänga deras leverans eller andra möjliga lösningar för att fortsätta driften under den tid som det kommer ta att genomföra alla nödvändiga säkerhetsåtgärder. Det som anges i minnesanteckningarna från It-rådet den 21 augusti 2015 avseende vad projekt It-drift 2.0 ska göra om något skulle tillstöta som försvårar leverans till den 1 november 2015 ger en tydlig bild att det inte är ett alternativ att flytta fram IBM:s leveransstart.

6.6.5 Avsteg 3

Genom avsteg 3 daterat den 13 augusti 2015 och rubricerat *Beslut om avsteg från gällande lagstiftning och Transportstyrelsens riktlinjer för åtkomst till säkerhetsskyddad och sekretessbelagd information* revideras avsteg 2 på så sätt att andra punkten under kompenserande åtgärder ändras till att lyda: ”att säkerhetsskyddsavtal (inkluderande beskrivning av säkerhetsorganisation och säkerhetsskyddsinstruktion) för övriga IBM-länder och underleverantörer där så krävs är inskickade till Transportstyrelsen senast den 21 september 2015”.

Enligt uppgift till utredningen föredrar it-direktören ärendet för generaldirektören per telefon och meddelar sedan projektägaren via e-post att projektet ska agera ”som att beslutet är påskrivet”. Projektägaren meddelar detta vidare till projekt It-drift 2.0 samt affärsansvarig för IBM, säkerhetsskyddschefen, enhetschefen för GD-stab och dåvarande enhetschefen för drift och infrastrukturenheten. Detta sker den 13 augusti 2015. Generaldirektören skriver under beslutet den 8 september 2015. Ingen föredragande är angiven på beslutet och det saknar diarienummer. [153]

[153] Se ovan i avsnitt 6.4.5 om vad som gäller enligt myndighetsförordningen.

Säkerhetsskyddschefen har uppgett till utredningen att han skickade in även avsteg 2 och 3 till Säkerhetspolisen i början av september 2015 och att detta ifrågasattes av dåvarande ställföreträdande generaldirektören Jacob Gramenius och Maria Ågren.

6.6.6 Tilldelning av behörigheter till den nya leverantören

Det står inte helt klart för utredningen när icke-säkerhetsklassad personal från IBM faktiskt fick tillgång till systemen första gången. Uppgifterna om detta går nämligen isär. Enligt uppgift från personer vid Transportstyrelsen var planeringen att IBM redan i februari 2015 skulle vara inne och lära sig systemen och då tilldelas behörigheter. Utredningen har inte kunnat utröna om så faktiskt var fallet, dvs. att icke-säkerhetsprövad personal från IBM var inne i systemen redan innan tilldelningsbeslutet fattades och innan avtal om it-driften slöts. Detta påstående innebär att man också måste ställa sig frågan om även icke-säkerhetsprövad personal från de andra i upphandlingen aktuella leverantörerna hade tillgång till systemen vid denna tidpunkt.

I minnesanteckningar från It-rådet som styrgrupp för portfölj Framtidssäkring den 25 juni 2015 antecknas IBM efterfråga access in i Transportstyrelsens system för att kunna arbeta parallellt med Trafikverket för kunskapsöverföring. Det anges att IBM inte kan få detta förrän säkerhetsskyddsavtalet är klart. Av underlaget till mötet framgår att övergång till parallellt utförande inom kunskapsöverföringen då IBM skulle tilldelas access in till systemen var planerad till den 1 juli 2015. Dessa uppgifter överensstämmer inte med uppgiften om att personal från IBM var inne i systemen redan i februari 2015 eller uppgifterna i Transportstyrelsens svar till Konstitutionsutskottet och Transportstyrelsens rapport[154] till regeringen den 23 januari 2018 avseende uppdraget att kartlägga hanteringen av vissa uppgifter (kartläggningsuppdraget).

Transportstyrelsen har i sitt svar till Konstitutionsutskottet den 16 oktober 2017 angett att från maj 2015 hade icke-säkerhetsklassad

[154] Transportstyrelsens underlagsrapport *Kartlägga hanteringen av vissa uppgifter*, dnr TSR 2017–519, 2018-01-23, s. 19.

personal vid leverantören och underleverantörerna tillgång till myndighetens system. Detsamma anges i Transportstyrelsens rapport avseende kartläggningsuppdraget enligt vilken personal från IBM haft åtkomst till systemen från maj 2015. [155]

I augusti 2015 gjordes beställningar av konton och behörigheter för egen åtkomst för IBM:s personal och underleverantörers personal. Företrädare för Transportstyrelsen uppger att det var i detta skede som det blev skarpt läge då det bl.a. handlade om behörigheter med priviligierad åtkomst. It-säkerhetsfunktionen ska vid denna tidpunkt ha bett om ett skriftligt beslut att dessa behörigheter kunde tilldelas. Enligt uppgift var det då avsteg 3 togs fram och beslutades.

Dåvarande enhetschefen för drift- och infrastrukturenheten uppger till utredningen att Trafikverket var ovilliga att släppa in annan personal i systemen när de fortfarande hade leveransansvar. Transportstyrelsen tog då fram en tillfällig rutin för behörighetstilldelning åt IBM:s personal.[156] Det behövdes ett flöde där någon attesterade behörigheter och enhetschefen var en av de personer som hade detta uppdrag. Hans bild var att de beslutade avstegen möjliggjorde detta och att det inte fanns något alternativ i detta läge.

Även enligt andra företrädare för Transportstyrelsen hörde Trafikverket av sig i detta skede då de inte ansåg att hanteringen var acceptabel. Det är oklart för utredningen på vilken nivå i organisationen dessa kontakter togs. Trafikverket hade redan tidigare ifrågasatt på operativ nivå att personal från IBM skulle vistas i deras lokaler under kunskapsöverföringen när de inte var säkerhetsprövade. Detta löstes enligt uppgift från personer på Transportstyrelsen genom att IBM:s personal fick sitta i ett konferensrum och se hur verksamheten bedrevs på en skärm där.

Interimshantering av behörighetsbeställningar

Utredningen har tagit del av den instruktion för interimshantering av behörighetsbeställningar som dåvarande enhetschefen för drift- och infrastrukturenheten nämner. Denna togs fram i juli 2015 med

[155] A. rapport s. 19.
[156] Instruktion för interimshantering av behörighetsbeställningar under kunskapsöverföringsmomentet i transitionsprojektet, slutversion daterad den 23 oktober 2015.

tillägg i oktober 2015 avseende utlämning av priviligierade behörigheter. I detta sammanhang kan noteras att säkerhetsskyddsavtalet med IBM Svenska AB och dess underleverantörer revideras den 19 oktober 2015, se nedan i avsnitt 6.8.2.

Av instruktionen framgår att innan behörighet godkänns ska säkerhetsfunktionen säkerställa att sekretessavtal är undertecknat. Beställningen ska därefter godkännas av säkerhetsfunktionen och driftchef. När det gäller administrativa användarbehörigheter (priviligierad åtkomst) anges tillägget att säkerhetsfunktionen hos Transportstyrelsen ska kontrollera att blanketten ”Framställan om registerkontroll” är undertecknad av person som behöver åtkomst.

It-säkerhetsansvarig och ämnesområdesansvarig för it-säkerhet på Transportstyrelsen har till utredningen uppgett att de motsatte sig denna hantering. Denna bild bekräftas också av andra personer på Transportstyrelsen samt av den notis angående it-säkerhet som upprättades av ämnesområdesansvarig för it-säkerhet den 14 augusti 2015 av vilken framgår bl.a. följande:

”Nedanstående beställningar 15 st. + 2 omkörningar av beställningar från transitionsprojektet är utan utförd registerkontroll och upprättat säkerhetsavtal med underleverantör. Samtliga beställningar skickades vidare för attest till Driftchef den 14 augusti 2015 enligt instruktion från projektägare. It-säkerhetsfunktionen är frånkopplad attestflöde för senare inkomna beställningar då kontrollparametrar inte kan uppfyllas. Detta enligt projektets önskemål då avsteg att följa säkerhetsskyddslag beordrats av projektägare, projektledare och arbetsledande chef.”

Efter detta var enligt uppgift till utredningen it-säkerhetsfunktionen inte längre ansvariga för att attestera behörigheterna. Det kan dock konstateras att instruktionen för interimshantering anger att säkerhetsfunktionen samt driftchefen ska godkänna beställningar av behörigheter innan dessa kan utföras. Utredningen har inte kunnat klarlägga vem eller vilka personer på säkerhetsfunktionen som haft denna roll.

Av de beställningar av behörigheter som utredningen tagit del framgår att det är dåvarande enhetschefen för drift- och infrastrukturenheten som auktoriserat dessa. Flera av de beställningar som görs i september och oktober 2015 avser personer som arbetar för en av IBM:s underleverantörer i Serbien. Vissa av beställningarna utförs redan i september 2015 och personerna tilldelas behörigheter på

olika nivåer i Transportstyrelsens system. Här bör också nämnas att underleverantören i Serbien vid denna tidpunkt inte är formellt godkänd som underleverantör och såvitt utredningen kunnat se fanns inte heller något säkerhetsskyddsavtal tecknat med den aktuella underleverantören vid denna tidpunkt.

Några beställningar avser personer från en underleverantör i Tjeckien och åtminstone två av dessa personer erhåller behörigheter redan i augusti 2015. Vid denna tidpunkt fanns såvitt utredningen kunnat se inte heller något underskrivet säkerhetsskyddsavtal med denna underleverantör. Att det inte fanns ett säkerhetsskyddsavtal med denna underleverantör i augusti 2015 bekräftas av protokoll från möte i It-rådet som styrgrupp för delportfölj Framtidssäkring den 10 september 2015.

Enligt dåvarande enhetschefen för drift- och infrastrukturenheten tilldelades ett 30-tal personer hos IBM och underleverantörer (administratörsbehörigheter) utan att vara säkerhetskontrollerade. Enligt flera personer på Transportstyrelsen fanns det bekymmer med hur behörigheterna var strukturerade. Detta bekräftas i Transportstyrelsens rapport avseende kartläggningsuppdraget i vilken framgår att när upphandlingen genomförts och IBM tog över itdriften var Transportstyrelsens it-miljö inte anpassad för det. Säkerhetsåtgärder i form av avgränsade behörigheter och övervakning av systemanvändning fanns inte på plats.[157]

Av samma rapport framgår att när IBM tog över driften gavs motsvarande omfattande behörigheter som Trafikverket tidigare hade använts sig av, till personal hos IBM. Det innebar att även dessa personer i praktiken fick åtkomst till Transportstyrelsens hela it-miljö och dess information. Vad gäller stordatorn och körkortstillverkningen så har behörigheter till dessa system endast tilldelats svensk säkerhetsprövad personal.[158] Se mer om Transportstyrelsens behörighetshantering i avsnitt 4.6.3.

[157] Transportstyrelsens underlagsrapport Kartlägga hanteringen av vissa uppgifter, 2018-01-23, dnr TSR 2017–519 s. 18.
[158] A. rapport s. 19.

6.7 Arbetet med transitionen under september

6.7.1 Budgeten utökas och säkerhetsarbetet fortsätter

Vid möte i It-rådet som styrgrupp för delportfölj Framtidssäkring den 10 september 2015 beslutas att utöka budgeten för driftsprojektet med 10 miljoner kronor relaterat till förseningen på två månader för Transportstyrelsens resurser inklusive konsulter och Trafikverket.

I underlaget för mötet framgår bl.a. följande. Projektet planerar inför övertagandet den 1 november 2015 med IBM, t.ex. gällande produktionssättningen. Säkerhetsskyddsavtal är tecknat med IBM Svenska AB, men inte med IBM:s underleverantörer. Generaldirektören har undertecknat ett i tid begränsat avsteg för de säkerhetsskyddsavtal som saknas.

Av protokollet framgår vidare följande avseende projektet It-drift 2.0. Arbetet med säkerhetsskydd löper både hos Transportstyrelsen och IBM. Avsteget hjälper projektet under tiden.

Vad gäller risker har ett arbete initierats med att ta en ögonblicksbild av status i kunskapsöverföringen. Bl.a. ger det nya språket, där engelska används i vissa lägen, viss komplikation.

Såvitt utredningen kan se diskuteras inte möjligheten att ytterligare förlänga tiden för Trafikverkets drift i detta skede trots att kunskapsöverföringarna ännu inte är klara och att man har identifierat att det nya språket ger viss komplikation. Vid denna tidpunkt hade Trafikverket kvar 10 anställda och 50 konsulter i sin leveransenhet för Transportstyrelsen.

6.7.2 Avsteg 4

Avsteg 4 med rubricering *Beslut om avsteg från gällande lagstiftning och Transportstyrelsens riktlinjer för åtkomst till säkerhetsskyddad och sekretessbelagd information* reviderar Avsteg 3 på så sätt att slutdatum sätts till den 31 oktober 2015 vilket är sista dagen innan IBM formellt tar över driftansvaret. Beslutet är daterat den 15 september 2015 och undertecknat av generaldirektören den 21 september 2015. Ingen föredragande är angiven på beslutet och det saknar diarienummer.

It-direktören meddelar projektägaren att generaldirektören har fattat beslutet. Projektägaren meddelar projekt It-drift 2.0, it-säkerhetsansvarig, informationssäkerhetsansvarig, säkerhetsskyddschefen och dåvarande enhetschefen för drift och infrastrukturenheten.

I beslutet anges att ändringarna görs som en konsekvens av 1) att datumet för avtalad startdag har ändrats från den 1 september till den 1 november eftersom detta beslutats av Transportstyrelsen tillsammans med IBM och 2) att det tidigare avsteget var formulerat att gälla året ut under förutsättning att säkerhetsskyddsavtal hade tecknats med underleverantörerna senast den 21 september 2015. I denna revidering gäller avsteget endast till den 31 oktober 2015, dagen före avtalad startdag. Då ska både relevanta säkerhetsskyddsavtal vara tecknade och övriga aktuella säkerhetsskyddsaktiviteter vara genomförda.

I avsteget anges att relevanta säkerhetsskyddsavtal ska vara tecknade och övriga aktuella säkerhetsskyddsaktiviteter vara genomförda senast den 31 oktober 2015. Samtidigt anges att säkerhetsskyddsavtalet inte ännu är underskrivet av alla underleverantörer. Det är svårt att förstå hur de säkerhetsskyddsaktiviteter som krävs ska kunna genomföras i tid. Säkerhetsskyddsavtalet är t.ex. en förutsättning för att registerkontroller ska kunna begäras, dessutom ska säkerhetsintervjuer genomföras och säkerhetsutbildning genomföras av aktuell personal.

I en fotnot anges att IBM kommit framåt i arbetet och den 17 september 2015 meddelat att IBM Tjeckien, IBM Danmark och IBM Rumänien nu skrivit under säkerhetsskyddsavtalet. Som anges nedan stämmer inte detta med de uppgifter som utredningen tagit del av.

Förslag på kompenserande åtgärder till avsteget är fortsätta med sekretessförbindelser på individnivå hos leverantören. Vidare anges att en handlingsplan tagits fram av projektet för att arbetet inom säkerhetsskydd ska fortskrida med en ökad progress den närmaste tiden och vara helt färdigställt innan avtalad startdag 1 november 2015. Handlingsplanen innebär bl.a. följande.

– Att arbeta fram och överenskomma med IBM om en ”baseline” för säkerhetsskyddsaktiviteterna. Av denna handling ska framgå exakt vilka säkerhetsskyddsaktiviteter som ska genomföras innan

1 november 2015 och för vilka dotterbolag och underleverantörer.

– Att Transportstyrelsen tillsammans med IBM ser över vilka formuleringar i säkerhetsskyddsavtalet som eventuellt kan justeras utan att tappa sin funktion men samtidigt underlätta för IBM och dess underleverantörer att teckna de aktuella avtalen.

Utredningen reagerar på formuleringen i avsteget att säkerhetsskyddsavtalet ska justeras för att underlätta för IBM. De justeringar som sedermera genomförs i säkerhetsskyddsavtalet redogörs för nedan i avsnitt 6.8.2.

6.8 Arbetet med transitionen under oktober

6.8.1 Dagen för övertagande närmar sig

Av protokoll från It-rådet som styrgrupp för delportfölj Framtidssäkring den 8 oktober 2015 framgår bl.a. följande. Genomgång av status med fokus på den stora utmaning som finns med att komma i mål med allt till den 1 november 2015. Ett antal riskområden finns och många parallella aktiviteter pågår för att eliminera riskerna. En positiv sak är att både Trafikverket och IBM känner att arbetet med produktionssättningen den 1 november 2015 går väldigt bra och inte känns som ett stort riskområde. Utbildningsdagen i veckan gick också bra och säkerhetsskyddsarbetet går stegvis framåt.[159]

Av underlaget till mötet framgår bl.a. följande. Säkerhetsskyddsavtal är tecknat med IBM Svenska AB och underleverantör i Danmark, säkerhetsskyddsavtalen med underleverantörer i Rumänien och Tjeckien är överskickade och ska tecknas. Återstår en handfull underleverantörer som ska tecknas. Skrivningen i säkerhetsskyddsavtalet är under revidering och utförs av IBM och Transportstyrelsen tillsammans. Generaldirektören har undertecknat ett avsteg t.o.m. den 31 oktober 2015 för de säkerhetsskyddsavtal som saknas.

[159] Enligt uppgift från säkerhetsskyddschefen var temat för denna utbildningsdag säkerhetsskydd. Han höll dock inte själv i denna utbildning.

Vidare framgår att budgeten för transitionen åter har utökats. Finansieringen av utökningen anges vara klar och sker med centrala medel.

Utredningen noterar att det som anges avseende vilka säkerhetsskyddsavtal som har undertecknats inte stämmer med vad IBM uppgett vid mötet den 17 september 2015.

6.8.2 Säkerhetsskyddsavtalet revideras

I Avsteg 4 och i protokoll från möte i It-rådet som styrgrupp för delportfölj Framtidssäkring den 8 oktober 2015 framgår som nämnts ovan att säkerhetsskyddsavtalet ska revideras i samarbete med IBM för att underlätta för IBM och dess underleverantörer att teckna de aktuella avtalen. Revideringarna ska göras av projekt It-drift 2.0, IBM och säkerhetsfunktionen.

Dessa revideringar genomförs den 19 oktober 2015 via tillägg till de säkerhetsskyddsavtal som Transportstyrelsen tecknat med IBM Svenska AB och dess underleverantörer.[160]

Bl.a. görs ett tillägg som innebär att så snart en säkerhetsprövning initierats för en resurs så kan Transportstyrelsen godkänna att resursen startar arbetet inom leveransen. Tillägg görs också avseende tillgång till resurser vid akuta problem så att dessa kan användas utan säkerhetsprövning.

Att möjliggöra att personer som inte genomgått säkerhetsprövning kan godkännas att starta arbetet och tas in som resurs vid akuta problem inom leveransen strider mot 11 § säkerhetsskyddslagen. I realiteten var skillnaden dock inte så stor mot hur man redan arbetade då Transportstyrelsen redan vid denna tidpunkt hade tilldelat icke säkerhetsprövad personal från IBM behörigheter, se ovan om tilldelning av behörigheter.

Säkerhetsskyddschefen har uppgett till utredningen att han inte deltog i detta arbete trots att det anges att revideringarna ska göras av projekt It-drift 2.0, IBM och säkerhetsfunktionen. Det förefaller också naturligt att säkerhetsskyddschefen skulle ha deltagit i detta arbete.

[160] Tillägg till Säkerhetsskyddsavtal TSA 2015–142 kopplat till Avtal om IT-drift, TSA 2015–54

6.8.3 Säkerhetsskyddsavtal uppges vara tecknat med samtliga underleverantörer

Enligt uppgift från projektägaren för projekt It-drift 2.0 meddelar IBM den 30 oktober 2015 att säkerhetsskyddsavtal är tecknat med samtliga underleverantörer. Frågan är vad detta innebär i realiteten och om denna uppgift stämmer med annan information som utredningen erhållit.

Av uppgifter som utredningen tagit del av framgår att säkerhetsskyddsavtal med t.ex. underleverantör i Tjeckien undertecknades av först senare under hösten 2015 och att en underleverantör i Ungern i maj 2016 fortfarande inte hade undertecknat säkerhetsskyddsavtal. Detsamma gäller för åtminstone två andra av IBM:s underleverantörer, varav en i Danmark och en i Serbien. Utifrån detta finns skäl att ifrågasätta det som IBM uppgett avseende att säkerhetsskyddsavtal var tecknat med samtliga underleverantörer vid denna tidpunkt. Projektet har dock inte ifrågasatt detta. Här kan noteras att avsteget endast gällde till t.o.m. den 31 oktober 2015 vilket skulle täcka upp för de säkerhetsskyddsavtal som saknades.

Den omständigheten att säkerhetsskyddsavtal är tecknat innebär inte heller att en leverantörs personal kan släppas in i systemen utan att personalen är säkerhetsprövad. Dessutom ska en rad andra åtgärder vidtas vilket också framgår av de säkerhetsskyddsavtal som faktiskt har tecknats. Exempelvis ska leverantören ta fram en säkerhetsskyddsinstruktion, säkerhetsintervjuer ska genomföras som en del av säkerhetsprövningarna, säkerhetsutbildningar ska genomföras samt registerkontroller. Vad gäller säkerhetsskyddsinstruktion så är den som utredningen tagit del av för IBM Svenska AB endast ett utkast och ofullständig.

Enligt uppgifter från personer på Transportstyrelsen har IBM genomfört säkerhetsintervjuer med personal i Tjeckien, Serbien och Sverige samt genomfört säkerhetsutbildningar med personal i bl.a. Rumänien. Utredningen har dock inte kunnat se att det finns något underlag avseende dessa genomförda insatser som IBM lämnat till Transportstyrelsen. Enligt säkerhetsskyddschefen har IBM genomfört säkerhetsbesök utomlands. Säkerhetsskyddschefen hade inte möjlighet att göra detta på grund av bristande resurser.

6.8.4 Styrelsen informeras

Vid styrelsesammanträde den 14 oktober 2015 informerar Maria Ågren styrelsen om de stora it-projekten. Det framgår inte närmare vilken information som ges till styrelsen så det är oklart om styrelsen informerades om tillsynen eller om problemen med säkerhetsprövningarna.[161]

6.9 Övergången genomförd och transitionen stängs

Övergången genomförd

Av protokoll från It-rådet som styrgrupp för delportfölj Framtidssäkring den 5 november 2015 framgår bl.a. följande. Det har gått bra med övergången till IBM. Trafikverkets resurser kommer att finnas kvar till den 18 december med full back-up under november för att sedan trappa ned.

Av underlaget till mötet framgår följande avseende säkerhetsarbetet. Alla IBM:s bolag och underleverantörer som ingår i leveransen har nu tecknat säkerhetsskyddsavtal. Arbete pågår med att genomföra de individuella säkerhetsavtalen med intervjuer och bakgrundskontroller.

Som utredningen konstaterat ovan i avsnitt 6.8.3 finns skäl att ifrågasätta om uppgifterna att alla IBM:s bolag och underleverantörer vid denna tidpunkt har tecknat säkerhetsskyddavtal verkligen stämmer.

Transitionen stängs

Vid möte i It-rådet som styrgrupp för delportfölj Framtidssäkring den 3 december 2015 konstateras att allt är överlämnat från restlistan för transition och att tidplanen som är avtalad med IBM avseende transformationen sannolikt kommer att förskjutas ordentligt. Transitionen avslutades formellt den 13 november 2015.

[161] Protokoll från sammanträde med Transportstyrelsens styrelse den 14 oktober 2015, dnr 2015–05.

Information till Regeringskansliet i december 2015

Utredningen ska enligt direktiven redovisa information som lämnats till Regeringskansliet om upphandlingen. Utredningen har inte kunnat se att Transportstyrelsen har gett Regeringskansliet någon detaljerad information om de risker och problem som uppstod i it-driftsprojektet och den bild som framkommit av intervjuer med företrädare för Transportstyrelsen är att informationen mestadels handlade om hur projekten drevs framåt och tekniken med mest fokus på stordatormigreringen. Enligt dåvarande generaldirektören Maria Ågren var det mest fokus på tidplanen vad gäller it-driften med utgångspunkt i ny lagstiftning som skulle genomföras.

Utredningen noterar i detta sammanhang att den rapport som Transportstyrelsen tog fram enligt det uppdrag som erhållits i regleringsbrevet för 2015 att beakta och analysera informationssäkerheten innehåller en hel del information om it-driftsprojektet. Rapporten redovisades som en bilaga till Transportstyrelsens risk- och sårbarbetsanalys för 2015[162] i december 2015 och var adresserad till Regeringskansliet (Näringsdepartementet) och Myndigheten för samhällsskydd och beredskap (MSB).

Utredningen noterar att Transportstyrelsen i denna rapport relativt tydligt redovisar att det finns klara brister i informationssäkerhetsarbetet vad gäller byte av driftsleverantör. Myndigheten tar upp projektens korta tidplaner som medfört att t.ex. riskanalyser inte genomförts fullt ut, att projekten vid projektstarten inte haft kunskap om sitt nuläge rörande verksamhetskrav och införda skyddsåtgärder och att projekten saknat kunskap om vilka krav som verksamheten ställer utifrån informationens skyddsvärde då informationsklassningar endast delvis gjorts av verksamheten. I rapporten anges också att leveransmodellen innebär underleverantörer i EU men även i tredje land. [163]

Enligt uppgift var det informationssäkerhetsansavarig på Transportstyrelsen som tog fram denna rapport. Han valde dock att inte stå som författare av rapporten då han inte kunde stå för dokumentet efter att det hade reviderats. Det som enligt uppgift togs bort från dokumentet var mer detaljer om outsourcingen och de risker som

[162] Risk- och sårbarhetsanalys för Transportstyrelsens verksamhet 2015, dnr TSG 2015–1384, november 2015.
[163] RSA – bedömning av Transportstyrelsens informationssäkerhet, TSG 2015–1384, daterad den 8 december 2015.

kunde konstateras. Enligt informationssäkerhetsansvarig har denna risk- och sårbarhetsanalys avseende informationssäkerhet inte följts upp internt. Enligt uppgift från företrädare för Transportstyrelsen har ingen återkoppling på denna rapport skett från Regeringskansliet eller MSB.

Utredningen har inte kunnat se att Regeringskansliet när rapporten kom in tog kontakt med Transportstyrelen för att få mer information utifrån denna rapport trots att det i rapporten enligt utredningens mening framkommer flera saker som borde väckt frågor och kanske även varit anledning till oro.

Av Näringsdepartementets svar till Konstitutionsutskottet den 16 oktober 2017 framgår att departementet bedömde att Transportstyrelsens redovisning av de viktigaste sårbarheterna och bristerna i myndighetens krisberedskap var rimlig samt att de redovisade sårbarheterna och bristerna borde åtgärdas/följas upp. Risk- och sårbarhetsanalysen för 2015, inklusive den aktuella rapporten togs upp på dialogmöte med Transportstyrelsen den 11 mars 2016 under punkten Information från Transportstyrelsen. Det framkommer inte vad som då diskuterades.[164]

6.10 Var stod Transportstyrelsen när transitionen hade stängts?

Transitionen stängdes som nämnts ovan formellt den 13 november 2015 då projektets slutrapport godkändes av styrgruppen den 13 november 2015.

Vid möte i It-rådet som styrgrupp för delportfölj Framtidssäkring har konstaterats att säkerhetsarbetet inte är helt färdigställt utan att arbete pågår med att genomföra de individuella säkerhetsprövningarna med intervjuer och bakgrundskontroller. Det framgår inte hur många säkerhetsprövningar som är färdigställda eller hur många som kvarstår. Denna brist på underlag och dokumentation över säkerhetsarbetet har som tidigare påpekats varit ett generellt problem för utredningen och medför att det är svårt att se vilka framsteg som har gjorts och hur mycket arbete som kvarstår. Sådan dokumentation hade varit en viktig indikation över huruvida IBM:s leverans nu kommer att fungera.

[164] Promemoria från Näringsdepartementet, 2017-10-16, dnr SB2017/01203/RCK.

Utredningen är inte heller övertygad om att det stämmer att alla IBM:s underleverantörer vid denna tidpunkt har skrivit på säkerhetsskyddsavtal. Som tidigare nämnts har dokumentationen av säkerhetsskyddsavtalen varit bristfällig vilket Säkerhetspolisen också senare påpekar i sin tillsynsrapport. Vissa säkerhetsskyddsavtal har rapporterats till Säkerhetspolisen enligt de regler som finns men inte alla. Utredningen har bl.a. av denna anledning inte kunnat bedöma om det stämmer att alla säkerhetsskyddsavtal är på plats.

En ytterligare fråga som uppkommer i detta skede är vilka underleverantörer och vilka länder som egentligen ingår i leveransmodellen. Parallellt med arbetet med transitionen pågår ett arbete med att godkänna ytterligare underleverantörer och länder som tillkommit i ett senare skede och som inte fanns med i den ursprungliga leveransmodellen. Dessa underleverantörer fanns inte heller med i den leveransmodell som presenterades av IBM på det utökade styrgruppsmötet för It-rådet som styrgrupp för delportfölj Framtidssäkring i augusti 2015.

Det fanns alltså en rad utestående frågor gällande IBM:s leverans när transitionen formellt var avslutad. Dessutom pågick parallellt med detta arbete Säkerhetspolisens tillsyn, se kapitel 7. Utredningen kommer i kapitel 8 att beskriva det händelseförlopp som nu inleddes med fortsatt säkerhetsarbete, förändrad leveransmodell och slutligen omförhandling av affärsavtalet.

6.11 Sammanfattande iakttagelser

Den planerade tidplanen för överlämnandet av it-driften till IBM var redan från början optimistisk. När transitionen startar i maj 2015 var det endast fyra månader till planerad driftsstart den 1 september 2015. Till detta kommer att transitionen skulle genomföras under sommarmånaderna då både Transportstyrelsen och Trafikverket på grund av semestrar hade begränsat med resurser. Utredningen anser att det var ett misstag av Transportstyrelsen att inte säkerställa att det fanns tillräckligt med resurser på Trafikverket redan innan avtal slöts med IBM om planerad driftsstart den 1 september 2015.

Utredningen noterar att det i hög utsträckning har saknats dokumentation av Transportstyrelsens it-system vilket innebar ett stort

glapp i kunskap vid leverantörsbytet, dels att dokumentation behövde kompletteras under transitionsfasen. Detta krävde både tid och resurser i den redan hårt pressade tidplanen.

Utredningen har fått en splittrad bild av om det hade varit möjligt att förlänga Trafikverkets leverans ytterligare. Det framstår dock tydligt att Transportstyrelsen redan innan myndigheten gick ut i upphandlingen borde ha övervägt möjligheten till antingen verksamhetsövergång eller en option för Trafikverket att fortsätta driften en tid för att ha en back-up plan vid eventuella förseningar (upphandlingen hade t.ex. kunnat bli föremål för överprövning). Transportstyrelsen borde också tidigare under transitionen ha övervägt möjligheten att förlänga Trafikverkets leverans och när frågan om förlängning togs upp borde Transportstyrelsen ha säkerställt en längre förlängning än två månader med tanke på hur framförallt säkerhetsarbetet fortskred.

Att Transportstyrelsen är så fast besluten att hålla tidplanen för transitionen innebär att man väljer andra åtgärder, t.ex. att skapa en tillfällig riktlinje för behörighetstilldelning som möjliggör att personer som inte genomgått säkerhetsprövning tilldelas behörigheter. Myndigheten justerar också säkerhetsskyddsavtalet för att underlätta för IBM att ta över driften i tid. Dessutom tas underleverantörer in i leveransmodellen utan att vara formellt godkända.

Utredningens bild är att varken styrelse eller ledningsgrupp har erhållit tillräckligt med information om de risker som fanns eller om hur arbetet med transitionen fortskred utifrån tidplanen. Det förefaller enligt utredningen som märkligt att styrelse och ledningsgrupp inte informeras närmare om detta, och i synnerhet om de problem med säkerhetsarbetet som tidigt uppstår.

Den sammanlagda bilden är att Transportstyrelsen inte har haft tillräcklig kunskap om förekomsten av skyddsvärd information i sina egna system, innebörden av säkerhetskyddsavtal, säkerhetsprövningar, registerkontroll m.m. Detta har bl.a. inneburit att personer som arbetat med upphandlingen upplevt att informationen om säkerhetskraven kommit som en blixt från en klar himmel i maj/juni 2015. Detta har i sin tur inneburit att tidplanen blev omöjlig att hålla.

7 Händelseförloppet kring Säkerhetspolisens tillsyn

7.1 Inledning

Utredningen ska enligt direktiven redovisa vilka analyser och bedömningar av konsekvenser och risker med outsourcingen som gjordes samt bl.a. vilka externa kompetenser som bidrog till dessa. Vidare ska utredningen bedöma vilka åtgärder som kunnat vidtas samt vilka kompetenser som deltog vid dessa analyser och beslut.

Utredningen har i kapitel 6 beskrivit händelseförloppet under transitionen och i kapitel 8 beskrivs händelseförloppet efter att transitionen är avslutad. Parallellt med dessa händelseförlopp pågick Säkerhetspolisens tillsyn av Transportstyrelsen.

Säkerhetspolisen är en sådan extern aktör vars bedömningar och åtgärder i övrigt påverkade händelseförloppet kring outsourcingen. En del av dessa förhållanden redovisas på annan plats i denna rapport. I detta kapitel ligger fokus på den tillsyn som Säkerhetspolisen gjorde av Transportstyrelsen och vilka åtgärder som denna ledde till från såväl Transportstyrelsens sida som från Säkerhetspolisens. Av naturliga skäl hålls redogörelsen relativt kortfattad vad gäller Säkerhetspolisens mer konkreta insatser, men en översiktlig redogörelse för dessa måste till för att ge en fullständig bild av varför Transportstyrelsen kom att agera som myndigheten gjorde.

7.2 Säkerhetspolisens tillsyn

Säkerhetspolisen är enligt säkerhetsskyddslagstiftningen tillsynsmyndighet för den regleringen.[165] Vid utredningens möte med Säkerhetspolisen har följande framkommit angående det generella

[165] 39 § säkerhetsskyddsförordningen (1996:633).

arbetet med säkerhetsskyddsfrågor. Myndigheten har 380 skyddsvärda myndigheter som de ska utöva tillsyn över och ge råd till. Arbetet med säkerhetsskyddsfrågor får därför prioriteras till myndigheter och funktioner av särskild betydelse. Utbildning av säkerhetsskyddschefer på prioriterade myndigheter och sektorsvis tillsyn har ingått i det arbetet. Transportstyrelsen var en prioriterad myndighet.

Säkerhetspolisen har sedan länge arbetat med personal vid Transportstyrelsen eller vid myndighetens föregångare. Sedan 2012 hålls återkommande möten med säkerhetsskyddschefen vid bl.a. Transportstyrelsen. Det är säkerhetsskyddschefen som är Säkerhetspolisens egentliga kontaktyta med myndigheterna som de arbetar mot. Säkerhetspolisens kontakter med ledningen vid Transportstyrelsen avseende säkerhetsskyddsarbetet har gått genom säkerhetsskyddschefen. Dock kan nämnas att i vissa fall har kontakterna skett med handläggarna på Transportstyrelsen direkt och inte via säkerhetsskyddschefen, vilket enligt Säkerhetspolisen inte sker på andra myndigheter. En utgångspunkt är att det är myndigheternas ansvar att kunna relevant lagstiftning och ha nödvändig information, men Säkerhetspolisen bistår med utbildningar och rådgivning i förekommande fall.

7.2.1 Säkerhetsskyddschefen kontaktar Säkerhetspolisen

Som redogjorts för i kapitel 6 startar transitionen i början av maj 2015. Redan då projektdirektivet för transitionen tas fram konstateras att insatser kring säkerhetsskyddavtal behövs och att det är en mycket trång resurs.[166] Säkerhetsskyddschefen har uppgett till utredningen att det vid samtal med IBM i maj 2015 blir tydligt att det rör sig om utländska underleverantörer och att säkerhetsskyddsavtal kanske krävs för ett stort antal länder. Det första avsteget undertecknas av Maria Ågren den 20 maj 2015 och innebär att Transportstyrelsen kan gå vidare med kunskapsöverföringen till IBM utan att säkerhetsskyddsavtal är undertecknade med alla underleverantörer och utan efterföljande säkerhetsaktiviteter som säkerhetsprövningar inklusive registerkontroll, utbildning m.m.

[166] Protokoll från möte i It-rådet den 5 maj 2015.

Säkerhetsskyddschefen meddelar i brev daterat den 15 juni 2015 Säkerhetspolisen, Säkerhetsskyddsenheten att generaldirektören på förfrågan från it-direktören har fattat två beslut om avsteg från rutiner angivna i säkerhetsskyddsavtal avseende dels automatiserad kod, dels it-drift samt bifogar de aktuella avstegen. Säkerhetsskyddschefen har också uppgett till utredningen att han kontaktade Säkerhetspolisen per telefon i samma veva samt att han bjöd ner två handläggare från Säkerhetspolisen till Norrköping den 29 juni 2015. Vad som framkommer vid detta möte är inte helt klart för utredningen annat än att säkerhetsskyddschefen uppger att Säkerhetspolisen bekräftat hans farhågor. Enligt uppgifter i media har även andra myndigheter framfört oro till Säkerhetspolisen avseende Transportstyrelsens outsourcing av it-drift.

Säkerhetsskyddschefen kontaktade även internrevisionschefen i juni 2015. Internrevisionschefen kontaktade i sin tur generaldirektören per e-post och frågade bl.a. om styrelsen hade informerats om avstegen (se avsnitt 6.6.3).

Av pm daterat den 17 juni 2015 framgår att säkerhetsskyddschefen har informerat generaldirektören om sin rapportering av besluten om avsteg till Säkerhetspolisen. Generaldirektören har undertecknat att hon mottagit denna information. Vidare framgår att säkerhetsskyddschefen har informerat generaldirektören om att avsteget rörande it-drift bedöms kunna medföra att Försvarsmakten, Säkerhetspolisen och Polisen inte längre kommer att kunna använda sig av de kvalificerade skyddsidentiteter som regleras i lag (2006:939) om kvalificerade skyddsidentiteter. Säkerhetsskyddschefen antecknar att han avrått från avsteg från ingångna säkerhetsskyddsavtal.

Av pm:et framgår vidare att it-drift genom avsteget avser att tilldela extern part i utlandet (underleverantörer i Rumänien och Tjeckien) administratörsrättigheter till Transportstyrelsens applikationsdrift utan att IBM Svenska AB som huvudleverantör uppfyllt säkerhetsskyddets krav enligt ingånget säkerhetsskyddsavtal. Säkerhetsskyddsavtal anges inte ha tecknats med någon annan part rörande projektet it-drift.

Generaldirektören informeras således i mitten av juni 2015 om möjliga konsekvenser för de kvalificerade skyddsidentiteterna. Hon vidtar såvitt utredningen kan se inga särskilda åtgärder med anled-

ning av detta. Hon kontaktar inte Säkerhetspolisen eller Regeringskansliet. Säkerhetspolisen kontaktar inte heller henne då de får information om avstegen av säkerhetsskyddschefen i samma veva.

Maria Ågren har uppgett till utredningen att hon uppfattat säkerhetsskyddschefens agerande som att han ville dokumentera avstegen och att han inte ville gå bakom hennes rygg.

Säkerhetspolisen inleder ett arbete med förstudie för en eventuell tillsyn. Kontakten med Säkerhetspolisen återupptas vid möte den 20 augusti 2015 mellan Säkerhetspolisen och Transportstyrelsens säkerhetsskyddschef och ytterligare någon eller några personer med funktioner inom säkerhet. Några anteckningar från mötet har utredningen inte kunnat ta del av. Vid samma tidpunkt informerar Maria Ågren styrelsen om avstegen (se avsnitt 6.6.3).

7.2.2 Säkerhetspolisens tillsyn inleds

Den 25 september 2015 fattar Säkerhetspolisen formellt beslut om att inleda en tillsyn av Transportstyrelsen.[167] Bakgrunden var den information Säkerhetspolisen fått under sommaren 2015 om att Transportstyrelsen 2015 påbörjat två större outsourcingprojekt, att dessa omfattade hemliga uppgifter, att tillräckliga säkerhetsskyddsåtgärder inte vidtagits samt att det fattats beslut om att göra avsteg från säkerhetsskyddslagen.

Som beskrivits ovan får Säkerhetspolisen redan i mitten av juni information om de avstegsbeslut som fattats av Transportstyrelsens säkerhetsskyddschef och träffar honom också i samband med detta. Därefter går säkerhetsskyddschefen vid Transportstyrelsen på semester och Säkerhetspolisens kontakter med myndigheten återupptas först genom det ovan nämnda mötet den 20 augusti 2015. Den 17 september 2015 informeras Regeringskansliet vid ett möte med Säkerhetspolisen om den planerade tillsynen men det är först den 25 september 2015 som det formella beslutet att inleda tillsyn fattas.

Anledningen till denna tidsutdräkt mellan det att oroande information nådde Säkerhetspolisen och att beslut om tillsyn fattas var enligt uppgifter till utredningen att det tog tid att samla information och kompetens samt att det inte redan i slutet av juni kunde göras en bedömning av om upphandlingen borde avbrytas.

[167] Tillsyn av säkerhetsskyddet på Transportstyrelsen, dnr 2015-14215-3.

Den 5 oktober 2015 kommer ytterligare en anmälan om avvikelse in till Säkerhetspolisen från Transportstyrelsen. Dagen därefter hålls ett möte där alla intressenter vad gäller kvalificerade skyddsidentiteter (dvs. även Försvarsmakten och Polisen) informeras om situationen och därmed sammanhängande risker.

Ett uppstartsmöte för tillsynen hålls den 16 oktober 2015. Något protokoll eller några minnesanteckningar från mötet har vi inte kunnat ta del av. Vi har tolkat mötet som det tillfälle där Säkerhetspolisen informerar om tillsynen för den berörda myndigheten, men det finns också uppgifter om att ett sådant möte hölls redan i september.

Enligt uppgift till utredningen informeras i vanliga fall generaldirektören vid detta tillfälle, men när det gällde tillsynen av Transportstyrelsen var det den biträdande generaldirektören som företrädde myndighetens högsta ledning p.g.a. förhinder för Maria Ågren. Av de uppgifter som lämnats till utredningen framgår att övriga närvarande var bl.a. säkerhetsskyddschefen, it-direktören och projektägaren för projekt It-drift 2.0.

Säkerhetspolisen uppger också till utredningen att man vid detta tillfälle var tydliga med orsaken till att tillsynen inleddes. Av utredningens intervjuer framgår dock att man på Transportstyrelsen hade varierande uppfattningar om varför tillsynen påbörjades, vissa verkar ha haft uppfattningen att det rörde sig om en sedvanlig och rutinartad tillsyn utan koppling till någon särskild hotbild eller risk, andra uppfattade att Säkerhetspolisens tillsyn är riskbaserad och att tillsynen därför borde ha att göra med identifierade risker. Vårt samlade intryck av intervjumaterialet och av hur tillsynen hanterades formellt på Transportstyrelsen är att de flesta inblandade på myndigheten inte verkar ha förstått vad som föranlett tillsynen och allvaret i den uppkomna situationen. En faktor som utredningen kunnat identifiera som en betydelsefull förklaring till att man på myndigheten inte såg allvaret var den tid som tillsynen tog, vilket ledde till uppfattningen att den inte gärna kunde avse något akut.

Efter uppstarten bedrevs tillsynen genom att information begärs in från Transportstyrelsen och att personal vid myndigheten intervjuas vid ett flertal möten. Någon kontakt med Datainspektionen eller andra myndigheter som har uppgifter när det gäller hanteringen av personuppgifter övervägdes såvitt framkommit inte.

Av uppgifter från intervjuer framkommer att det efter att Säkerhetspolisen inlett sin tillsyn blev ett större fokus på säkerhetsfrågor i rapporteringen till ledningsgrupp och styrelse. Innan dess var dessa frågor inte alls uppe på bordet. Det är dock svårt att bekräfta att ett sådant skifte i fokus skett utifrån den tillgängliga skriftliga dokumentationen, eftersom såväl styrelseprotokoll och mötesanteckningar från projektgrupper m.m. är knapphändigt utformade. De belägg för att frågor om säkerhet och Säkerhetspolisens tillsyn varit uppe i myndigheten kommer från kortfattade informationspunkter från ledningsgruppen i november 2015 och från It-rådets agenda (och därmed på de projekt som tillsynen gällde) i december 2015.[168] Från de två styrelsemöten som hölls hösten 2015 finns ingen dokumentation om att tillsynen diskuterades.

En slående iakttagelse är att även med beaktande av de krav på korrekt information och rätt kompetens som rimligen måste ställas på en tillsyn av detta slag – och med hänsyn taget till att det var fråga om sommarmånader – så tar det alltså tre månader innan Säkerhetspolisen fattar beslutet att inleda en tillsyn från det att man fått relativt klara indikationer på att allvarliga missförhållanden råder. Det tar ytterligare en månad innan tillsynen verkar komma igång i praktiken. Detta innebar att de hot mot rikets säkerhet som senare kom att identifieras och konstateras kunde fortgå under hela denna tid utan någon egentlig åtgärd.

En faktor som också måste lyftas fram är det förhållandet att Säkerhetspolisen inte lyckades förmedla det allvarliga i den uppkomna situationen fullt ut, trots att man anger att man varit mycket tydliga i detta avseende. Något har helt uppenbart brustit i kommunikationen mellan Transportstyrelsen och Säkerhetspolisen eftersom två oförenliga bilder av tillsynens karaktär kom att etablerats. Båda myndigheterna bär rimligen ansvaret för denna brist. Vi har dock fått flera belägg för att tidsutdräkten innebar att personalen på Transportstyrelsen upplevde att det inte kunde vara några akuta problem. Detta kan således ha varit en bidragande faktor till att Transportstyrelsen inte vidtar särskilt omfattande direkta åtgärder förrän i ett sent skede utan väljer att invänta Säkerhetspolisens rapport.

[168] Protokoll från sammanträde med Transportstyrelsens ledningsgrupp den 3 november 2015, dnr 2015-10 och protokoll från möte i It-rådet som styrgrupp för delportfölj Framtidssäkring den 3 december 2015.

7.2.3 Säkerhetspolisens rekommendation

Under arbetet med tillsynen så skickar Säkerhetspolisen en skrivelse till Transportstyrelsen adresserad till Generaldirektören.[169] Skrivelsen är daterad den 25 november 2015. I den gör Säkerhetspolisen en genomgång av det underlag som tillsynen dittills genererat, viss relevant lagstiftning och av Transportstyrelsen fattade beslut och vidtagna åtgärder. Skrivelsen avslutas med några rekommendationer om omedelbara säkerhetsskyddshöjande åtgärder. Bland annat rekommenderades Transportstyrelsen att säkerställa att hemliga uppgifter inte kom obehöriga till handa genom att t.ex. avbryta outsourcing av hela eller valda delar.

Enligt uppgift till utredningen var anledningen till att rekommendationen skickades att det kommit fram sådana uppgifter att Säkerhetspolisen gjorde bedömningen att det behövdes en sådan skrivelse. Någon uppföljning eller kontroll av rekommendationens effekter gjordes däremot inte. Regeringskansliet eller andra myndigheter informerades inte heller om rekommendationen såvitt utredningen kunnat se.

Maria Ågren har uppgett att hon när skrivelsen kom samlade säkerhetsskyddschefen, it-direktören och ställföreträdande generaldirektören för att diskutera. Hon har vidare uppgett att skrivelsen mottogs med viss undran eftersom en generaldirektör vanligen tillskrivs från en motsvarande befattningshavare om en annan myndighet har synpunkter riktade till denne. Skrivelsen kom dock inte från Säkerhetspolisens myndighetschef utan från Säkerhetspolisens operativa chef. Maria Ågren har uppgett till utredningen att de därför hade svårt att avgöra vad som var avsändarens avsikt och diskuterade detta en del innan man funderade på rekommendationerna i sak. Hon bad också säkerhetsskyddschefen att kontrollera med sina kontakter på Säkerhetspolisen vad som gällde. Maria hade tidigare fått information från säkerhetsskyddschefen att Transportstyrelsen hade en bra säkerhetsanalys och hon blev förvånad över att Säkerhetspolisen inte tyckte det. Hon gav säkerhetsskyddschefen i uppdrag att ta fram en ny säkerhetsanalys. Därefter konstaterades att it-driften redan överlämnats till IBM. Att avbryta outsourcingen skulle medföra ett totalt stopp för

[169] Skrivelsen har benämningen ”Rekommendationer om omedelbara säkerhetsskyddshöjande åtgärder”.

myndighetens it-system under en längre tid. Det ansågs därför inte vara möjligt att efterkomma rekommendationen i denna del.

Av den skriftliga dokumentation som utredningen haft tillgång till kan inte utläsas att någon direkt åtgärd vidtas med anledning av denna rekommendation eller att frågan ens diskuteras. För ledningsgruppsmötet i december 2015 finns inte frågan om Säkerhetspolisens rekommendation med i protokollet.[170] Inte heller tas den upp i styrelsen såvitt framgår av protokoll.

Enligt intervjuuppgifter till utredningen så framträder en lite splittrad bild. Å ena sidan menar vissa att myndigheten inte vidtar någon omedelbar åtgärd, men å andra sidan framförs att stora ansträngningar gjordes för att svara upp mot Säkerhetspolisens rekommendationer, bl.a. rekryterades en person för att ge bättre administrativt stöd för detta arbete. Man ville ha bättre ordning på säkerhetsskyddshanteringen och förbättra de administrativa rutinerna. Vissa akutåtgärder ska också ha vidtagits med anledning av rekommendationen, främst kopplade till körkortsregistret, uppger funktionen för it-säkerhet till utredningen.

Bilden är således inte entydig, men det står klart att Säkerhetspolisens skrivelse inte föranledde Transportstyrelsen att göra någon helt ny värdering av outsourcingen. Enligt uppgifter ansågs det inte i detta läge – november 2015 – vara realistiskt att avbryta outsourcingen (”fanns inte på kartan”).

Utredningens intryck är att detta sannolikt beror på att rekommendationens dels utformats så att den gett befattningshavarna på Transportstyrelsen intrycket att det finns ett utrymme för att väga de nackdelar som Säkerhetspolisen pekar på mot de som skulle uppstå om upphandlingen avbröts. Utformningen som en rekommendation kan sägas ha inbjudit till en sådan tolkning, särskilt med beaktande av att mottagaren inte var särskilt positivt inställd till rekommendationens sakliga innehåll. Dessutom påverkade det förhållandet att rekommendationen inte åtföljts av något om uppföljning eller avrapportering angående vad myndigheten vidtagit för åtgärder. Vårt intryck är att Transportstyrelsen därför uppfattade det som att rekommendationen kunde läggas till handlingarna efter det att man bedömt att det var ogörligt att avbryta outsourcingen och vissa övriga justeringar av säkerhetsarbetet gjorts.

[170] Protokoll från sammanträde med Transportstyrelsens ledningsgrupp den 15 december 2015, dnr 2015-12.

Vid möte i It-rådet som styrgrupp för delportfölj Framtidssäkring den 18 januari 2016 informerar projektägaren för It-drift 2.0 kort om Säkerhetspolisens pågående tillsyn och att Transportstyrelsen kan förvänta sig krav på åtgärder från Säkerhetspolisen.

Den 26 januari 2016 beslutar Säkerhetspolisen att inleda en förundersökning avseende vårdslöshet med hemlig uppgift (19 kap. 9 § brottsbalken). Från denna tidpunkt bedrivs således ett tillsynsärende och en förundersökning parallellt, något som ställer höga krav på den myndighet som har ansvaret att inte blanda ihop dessa roller. Säkerhetspolisen har uppgivit till utredningen att detta var en komplicerande faktor i tillsynsärendet och vi drar slutsatsen att det kan ha bidragit till att tillsynsrapportens färdigställande drog ut på tiden.

Det kan noteras att Säkerhetspolisen såg sig föranledd att kontakta Transportstyrelsen trots att tillsynen inte var avslutad och att denna kontakt kunde göras relativt snart efter påbörjad tillsyn. Man kan bara spekulera i vad som hade hänt om tillsynen kunnat starta i juli och rekommendationen därför kunnat komma redan i september eller oktober, dvs. före det att IBM tagit över driften av it-systemen.

Utformningen av rekommendationen beror delvis på att författningsregleringen inte vid den tidpunkten gav Säkerhetspolisen några särskilt skarpa instrument mot en myndighet som bröt mot regelverket. Någon annan möjlighet än att i skarpa ordalag rekommendera Transportstyrelsen att vidta åtgärder fanns inte. Inte desto mindre är det värt att lägga märke till att just ordvalet rekommendation, tillsammans med sättet som denna kommunicerades på och det förhållandet att inget krav på återkoppling eller uppföljning fanns bidrog till att Transportstyrelsen tvärtemot Säkerhetspolisens strävanden fortsatte med sitt agerande. Direkta personliga kontakter, kanske på högsta nivå, hade sannolikt varit ett bättre sätt för Säkerhetspolisen att försäkra sig om att allvaret i situationen gick fram. Nu förlitade man sig på Transportstyrelsens egen förmåga att prioritera säkerhetsfrågorna, trots att man visste att denna var förhållandevis svag. Att det i formell mening var Transportstyrelsens, och inte Säkerhetspolisens, ansvar förtar inte bilden av att myndigheterna hade kunnat kommunicera bättre med varandra.

7.2.4 Möte mellan Säkerhetspolisen och generaldirektören

Den 1 februari 2016 har Maria Ågren, efter eget initiativ, ett möte med Säkerhetspolisen, bl.a. representerat av den biträdande generaldirektören. Det finns inte något protokoll eller några minnesanteckningar från mötet. Enligt uppgift från Maria Ågren är det först vid detta möte som hon får klart för sig vilka säkerhetsrisker som outsourcingen medfört och vad myndighetens åtgärder med avsteg fått eller kan få för konsekvenser. Hon fick också information om vad som var mest allvarligt och behövde åtgärdas akut. Säkerhetspolisen klargjorde också vid detta möte att registerkontroll av utländsk personal inte kan genomföras.

I det ledningsgruppsmöte som hålls den 4 februari 2016 tycks dock inget om säkerhetsrisker eller problem i samband med outsourcingen ha behandlats.[171] Det finns visserligen en punkt om hanteringen av skyddade personuppgifter i protokollet, men den betecknas som en framtidsfråga och protokollet ger intryck av att det närmast var en mer allmän diskussionspunkt och inte en beslutspunkt gällande akuta åtgärder. Vid nästkommande ledningsgruppsmöte den 16 februari 2016 nämns inte heller säkerhetsrisker eller outsourcingen i protokollet.[172] Däremot informeras styrelsen vid det första styrelsemötet för 2016, som sker vid samma tidpunkt, om Säkerhetspolisens tillsyn i samband med myndighetens stora it-projekt.[173]

Muntliga uppgifter till utredningen anger att det efter mötet med Säkerhetspolisen kom en direkt order om att flytta vissa system och detta genomfördes så snabbt som på en vecka. Efter detta kommer också säkerhetsfrågorna i fokus på ett nytt sätt. I den tillgängliga dokumentationen får dessa minnesbilder också visst stöd. Ledningsgruppen har t.ex. uppe en punkt om ändringar i säkerhetskraven i mars 2016 och återkommer till frågan också i maj samma år.[174] I pro-

[171] Protokoll från sammanträde med Transportstyrelsens ledningsgrupp den 4 februari 2016, dnr2016-01.
[172] Protokoll från sammanträde med Transportstyrelsens ledningsgrupp den 16 februari 2016, dnr 2016-02.
[173] Protokoll från sammanträde med Transportstyrelsens styrelse den 19 februari 2016, dnr 2016-01.
[174] Protokoll från sammanträde med Transportstyrelsens ledningsgrupp den 8 mars 2016, dnr 2016-03 och den 17 maj 2016, dnr 2016-06.

tokoll från möte i It-rådet som styrgrupp för delportfölj Framtidssäkrings från april 2016 framkommer att säkerhetsfrågorna var centrala i projektet om outsourcing.[175]

7.2.5 Säkerhetspolisens rapport

Tillsynsrapporten kommer den 23 maj 2016. I denna konstaterar Säkerhetspolisen bl.a. följande. Transportstyrelsens säkerhetsanalys är otillräcklig, säkerhetsskyddsavtal saknas med vissa leverantörer, gällande lagstiftning har inte följts fullt ut och Transportstyrelsen har inte själv följt de krav som myndigheten ställt.

Transportstyrelsens generaldirektör och ställföreträdande generaldirektör gavs viss förhandsinformation om rapportens innehåll. Ledningsgruppens protokoll i juni 2016 innehåller en särskild punkt där det anges att aktuella säkerhetsfrågor och hanteringen av dem diskuteras.[176] Detta uppfattar utredningen som den punkt där myndighetens ledning tog ställning till rapporten även om detta inte klart anges och intervjuerna inte kunnat bekräfta detta. Generaldirektören var enligt uppgifter till utredningen mycket bekymrad vid denna tidpunkt. Vid det styrelsemöte som hölls i juni 2016 togs dock inte Säkerhetspolisens rapport upp som en särskild punkt och inte heller i övrigt går det att se om styrelsen informerades i det läget.[177] Istället kom styrelsen att få information först vid ett möte i augusti 2016 där det av protokollet framgår att generaldirektören informerat om säkerhetshöjande åtgärder avseende vissa it-system.[178]

Enligt vad som uppgivits till utredningen så uppfattade Transportstyrelsens ledning att man hamnat i en hopplös sits. Säkerhetspolisen rekommenderade att avbryta upphandlingen men ett sådant avbrytande ansågs helt enkelt inte vara möjligt utan att all väsentlig verksamhet vid myndigheten skulle avstanna. Det diskuterades om vidare kontakter borde tas med Säkerhetspolisen och departementet, men någon sådan kontakt togs inte. Angående varför man inte vände

[175] Protokoll från möte i It-rådet som styrgrupp för delportfölj Framtidssäkring den 28 april 2016.
[176] Protokoll från sammanträde med Transportstyrelsens ledningsgrupp den 21 juni 2016, dnr 2016-08, punkt 5.
[177] Protokoll från sammanträde med Transportstyrelsens styrelse den 17 juni 2016, dnr 2016-04.
[178] Protokoll från sammanträde med Transportstyrelsens styrelse den 11 augusti 2016, dnr 2016-05. Även vid nästa sammanträde i styrelsen den 13 oktober 2016 så var säkerhetsfrågor en informationspunkt (dnr 2016-05).

sig direkt till departementet i den uppkomna situationen så framgår av uppgifter till utredningen att myndighetsledningen uppfattat att regeringen inte vill ha mer information än vad som är absolut nödvändigt och förväntar sig att myndighetscheferna klarar av sina uppdrag utan sådana kontakter.

Säkerhetspolisens rapport innehöll krav på en åtgärdsplan. Denna arbetade man med inom Transportstyrelsen under sommaren 2016. Eftersom man ganska snabbt kom att bestämma sig för att det inte gick att avbryta den pågående outsourcingen av it-driften föreslogs vad man betecknade som kompensatoriska åtgärder. Generaldirektören skickade denna planering till Säkerhetspolisen den 6 september 2016. Enligt uppgift till utredningen hanns inte något mera omfattande och konkret arbete med dessa åtgärder med under hösten 2016.

Säkerhetspolisen har till utredningen uppgivit att man ansåg att åtgärdsplanen var svårbegriplig avseende vilka åtgärder som skulle vidtas och vad som faktiskt hade gjorts. Kontakt togs med säkerhetsskyddschefen för att få information om detta. Det tog dock lång tid att reda ut dessa oklarheter och i januari 2017 ställdes därför skriftliga frågor direkt till generaldirektören. Därmed kan man säga att Säkerhetspolisens tillsynsärende avslutades även i sin förlängda del. Angående vad som i övrigt skedde under 2016–2017 återkommer vi till i kapitel 8.

Vi noterar att inom Transportstyrelsen behandlades rapporten såsom mycket känslig och endast ett fåtal personer som var säkerhetsprövade fick insyn i den eller i de slutsatser som dras där. Det var därför inte lätt för personer i mellanchefställning att ta till sig vad som var problemet och hur man kunde lösa det, något som i sin tur minskade myndighetens förmåga att hantera de utmaningar den innebar. För få personer kände till den för att kunna förändra myndighetens pågående arbete.

Utredningen kan vidare konstatera att det verkar ha funnits en ovilja eller oförmåga att ta kontakter direkt mellan myndighetschefer och mellan myndighet och regering som i det här fallet sannolikt bidrog till att försvåra situationen. Vad det kan bero på diskuteras i vårt avslutande kapitel (kapitel 9), men redan här kan noteras att den svenska förvaltningsmodellen med självständiga och sektorsvis ansvariga myndigheter tycks ha en del inbyggda brister.

7.3 Sammanfattande iakttagelser

Utredningen noterar för det första att flera ledande personer inom Transportstyrelsens organisation framfört att man inte förstod allvaret i tillsynen, utan uppfattade den som en tämligen rutinartad åtgärd. Tillsynen medförde inte heller några omedelbara åtgärder eller beslut från myndighetens sida, inte ens när Säkerhetspolisen i november kom med en relativt klart utformad rekommendation om att avbryta upphandlingen eller delar av den.

För det andra tog tillsynen förhållandevis lång tid, vilket bidrog till att man på Transportstyrelsen kunde bibehålla intrycket av att inget akut fel förelåg fram till en bit in på 2016.

När tillsynsrapporten sedan kom sent på våren samma år så hölls den hemlig på Transportstyrelsen även avseende dess mer allmänna delar, vilket bidrog till att man fortfarande under sommaren 2016 inte hade helt klart för sig vari bristerna bestod och alltså hade svårigheter med att vidta adekvata åtgärder. Vårt underlag tyder på att konkreta och systematiska åtgärder inte kom igång förrän sent 2016 eller först 2017.

8 Tiden efter övergången

8.1 Inledning

Utredningen ska enligt direktiven kartlägga processen från det att Transportstyrelsen beslutade att påbörja arbetet med en förändrad it-drift och it-organisation fram till i dag. Därvid ska viktiga tidpunkter, gjorda vägval, beslut som fattats på olika nivåer inom myndigheten och information som lämnats till Regeringskansliet redovisas. Utredningen ska redovisa vilka alternativ som utreddes och vilka analyser och bedömningar av konsekvenser och risker som gjordes vid olika tidpunkter under processen samt vilka typer av interna och eventuellt externa kontakter och specialistroller som bidrog till dessa.

Detta kapitel återger händelseförloppet efter det att övergången (transitionen) avslutats och IBM har tagit över ansvaret för it-driften. Aktuell tidsperiod är från transitionens avslut i december 2015 fram till att det nya affärsavtalet med IBM är klart i juni 2017. Kapitlet avslutas med en kort redogörelse för det nya avtalet med IBM och för var Transportstyrelsen står idag med driftleveransen.

8.2 Godkännande av underleverantörer

Som angetts i avsnitt 6.10 är en fråga som uppkommer under hösten 2015 och som kvarstår när IBM har tagit över leveransen och transitionen avslutats vilka underleverantörer och vilka länder som egentligen ingår i IBM:s leveransmodell vid olika tidpunkter.

Parallellt med arbetet med transitionen pågår nämligen under hösten 2015 ett arbete med att godkänna ytterligare underleverantörer och länder som tillkommit i ett senare skede och som inte fanns med i den ursprungliga leveransmodellen. Detta arbete avslutas först i februari 2016. Utredningen noterar i detta sammanhang

att nya underleverantörer och länder har lagts till i leveransmodellen och tilldelats behörigheter redan innan denna process var avslutad.

Utredningen har tagit del av den rutin för hantering av ny underleverantör it-drift som Transportstyrelsen säger sig ha använt i detta arbete (se avsnitt 4.6.4). Rutinen nedtecknades dock först under 2017 med slutversion i juli 2017. [179]

Utifrån de uppgifter som utredningen tagit del av rörande underleverantörerna som ingått i IBM:s leveransmodell gör utredningen bedömningen att denna rutin inte har följts under arbetet med transitionen under 2015 och 2016. Ett antal av IBM:s underleverantörer fanns inte med i den ursprungliga leveransmodellen vid avtalstecknandet i april 2015. Vissa av dessa underleverantörer fanns inte heller med i den leveransmodell som presenterades av IBM på styrgruppsmötet för It-rådet som styrgrupp för delportfölj Framtidssäkring i augusti 2015. Som beskrivits i avsnitt 6.6.7 tilldelades personal från dessa underleverantörer behörigheter i systemen innan dessa underleverantörer godkänts eller tecknat säkerhetsskyddavtal.

Av underlag från möte med utökat It-råd den 21 augusti 2015 framgår att ledning och styrning ska ske från IBM Svenska AB med huvudsakliga leveranscenter via underleverantörer i Tjeckien, Rumänien, Ungern och Irland. Utredningen konstaterar att Ungern har lagts till som underleverantör i leveransmodellen jämfört med vid avtalstecknandet i april 2015. Enligt uppgifter från Transportstyrelsen godkändes underleverantören i Ungern dock formellt som underleverantör först den 4 februari 2016. Av uppgifter som utredningen tagit del av framgår att underleverantören i Ungern i maj 2016 fortfarande inte hade undertecknat säkerhetsskyddsavtal, se avsnitt 6.8.3.

En av IBM:s underleverantörer i Serbien godkänns också formellt som underleverantör den 4 februari 2016. Trots detta tilldelas behörigheter på olika nivåer i Transportstyrelsens system till personal hos denna underleverantör redan i september 2015. Enligt de uppgifter som utredningen tagit del av fanns det i maj 2016 fortfarande inget undertecknat säkerhetsskyddsavtal med den aktuella underleverantören.

I december 2016 godkänns ytterligare två underleverantörer, och under 2017 godkänns totalt ytterligare fem underleverantörer. Ut-

[179] Rutin för hantering av ny underleverantör It-drift, daterad 2017-07-11, version 1.2.

redningen har inte kunnat fastställa om personal hos dessa underleverantörer tilldelats behörigheter i Transportstyrelsens system innan de godkänts formellt som underleverantörer eller när de har tecknat säkerhetsskyddstavtal. I oktober 2017 görs en rensning av alla inaktuella underleverantörer, se nedan i avsnitt 8.5.

En brist som Säkerhetspolisen har påtalat gällande hanteringen av säkerhetsskyddsavtalen är att alla säkerhetsskyddsavtal som tecknats i den aktuella upphandlingen inte har skickats in till Säkerhetspolisen för registrering. Det har också varit oklarheter med datum och vilken upphandling som säkerhetsskyddsavtal som har skickats in faktiskt har avsett (it-driftsupphandlingen eller stordatormigreringen).

Den rutin som Transportstyrelsen har nedtecknat avseende godkännande av underleverantörer är en bra utgångspunkt för denna hantering. Rutinen har dock inte följts i alla steg.

Rutinen innehåller ingen skrivning om tecknande av personuppgiftsbiträdesavtal med underleverantörer. Utredningen har inte heller sett att det finns en annan rutin för tecknande av personuppgiftsbiträdesavtal Om en underleverantör ska hantera personuppgifter måste det enligt punkt 5.10 i Transportstyrelsens personuppgiftsbiträdesavtal med IBM tecknas skriftliga avtal med dessa (underbiträdesavtal). Enligt uppgift från Transportstyrelsen har sådana underbiträdesavtal tecknats med alla IBM:s underleverantörer. Utredningen har dock ingen uppgift om när detta har skett i processen.

Överföring av personuppgifter till tredje land

I detta sammanhang måste frågan om överföring av personuppgifter till tredje land beröras kort. Utredningen bedömer att överföring till tredje land har skett i och med att personal hos en underleverantör i Serbien har tilldelats behörigheter.

Personuppgifter får föras över till tredje land i någon av följande situationer; 1. om det finns en adekvat skyddsnivå i mottagarlandet (t.ex. efter beslut av EU-kommissionen), 2. när den registrerade ger sitt samtycke till överföringen, 3. om det i annat fall är tillåtet enligt föreskrifter eller särskilda beslut av regeringen eller Datainspektionen därför att det finns tillräckliga garantier för att de registrerades

rättigheter skyddas (genom standardavtalsklausuler godkända av EU-kommissionen eller bindande företagsinterna regler (BCR)).

Utredningen konstaterar att i punkt 5.11 i personuppgiftbiträdesavtal mellan Transportstyrelsen och IBM anges att personuppgiftsbiträdet ges mandat att teckna personuppgiftbiträdesavtal för Transportstyrelsens räkning med underbiträden i tredje land i enlighet med EU-kommissionens beslut om standardavtalsklausuler.

Serbien omfattas inte av något beslut om adekvat skyddsnivå från EU-kommissionen och det finns inte heller några indikationer på att den aktuella underleverantören har s.k. BCR. Utredningen har inte tagit del av det personuppgiftsbiträdesavtal som IBM ska ha tecknat med den aktuella underleverantören i Serbien och kan därför inte bedöma om detta avtal innehåller de angivna standardavtalsklausulerna. I detta sammanhang kan konstateras att EU-kommissionens standardavtalsklausuler ställer långtgående krav på skyddet för personuppgifter och en personuppgiftsansvarig bör inte per automatik kunna förlita sig på att användningen av standardavtalsklausulerna säkerställer en adekvat skyddsnivå för personuppgifterna som överförs (se avsnitt 2.6).[180]

8.3 Transformationsprojektet

Av protokoll från möte i It-rådet som styrgrupp för delportfölj Framtidssäkring den 18 januari 2016 framgår bl.a. följande. Beslutet enligt målbild Transformation, att gå vidare enligt plan, underlättar för projektet. Det innebär att det inte blir några stora avvikelser mot den plan man redan arbetar efter. Arkitekterna på Transportstyrelsen arbetar tillsammans med IBM kring design av lösningen. Tidplanen är nu utdragen och avslutas inte januari 2017 som avtalats. Innan sista maj 2016 kommer ingenting att flyttas.

Av underlaget för mötet framgår hur organisationen för projektet ska se ut fortsättningsvis, budget samt en risklista med topp 3. Där anges att resursbrist för Transportstyrelsen, Transportstyrelsens strategi enligt ”Målbild Transformation” och utökad kravbild med avsteg från 1–1 transformation försenar och fördyrar projektet och projektkonflikt med stordatormigreringen. Konsekvenserna av

[180] Pensionsmyndighetens rapport *Molntjänster i staten – En ny generation av outsourcing*, Bilaga Juridisk analys, s. 34.

dessa risker anges vara försening av tidplan, större kostnad samt vad gäller stordatormigreringen anges att Transportstyrelsen inte orkar med flera stora parallella projekt.

Det finns inget angivet om säkerhetsfrågorna eller behörighetshanteringen och hur dessa ska hanteras fortsättningsvis. I underlaget nämns dock att det ska vara en kick-off med riskanalys den 25 januari 2016.

8.3.1 Projektstatus i februari 2016

Av protokoll från möte i It-rådet som styrgrupp för delportfölj Framtidssäkring den 4 februari 2016 framgår att den kommersiella diskussionen med IBM är under uppstart eftersom förutsättningarna har förändrats. Det antecknas att det är olyckligt att kravbilden har farit iväg något men att det behöver hanteras. Vidare antecknas att projektdirektivet är färdigt och att arbete med projektspecifikationen pågår, se nedan i avsnitt 8.3.2 om projektdirektivet.

Det framgår inte av protokollet eller av underlaget till mötet vilka förutsättningar som har förändrats eller vad som avses med att kravbilden har farit iväg något. I underlaget till mötet nämns att man nu genomfört den ovan nämnda riskanalysen och att man identifierat 72 risker samt att åtgärdsplaner ska tas fram. Av dessa 72 risker identifieras 26 stycken ha hög sannolikhet och hög effekt på projektet. Som exempel på kritiska risker nämns t.ex. risk att förvaltningsobjekten inte har tillräckliga resurser för medverkan samt prioriterar andra projekt/annan verksamhet före transformationen och risk för motstånd från verksamhetssidan mot att vara tidig i flytten.

Det är värt att notera att säkerhetsarbetet inte tas upp som exempel på en kritisk risk i detta skede trots att Säkerhetspolisens tillsyn fortfarande pågår samt att man redan på möte i januari 2016 antecknade att Transportstyrelsen kan förvänta sig krav på åtgärder från Säkerhetspolisen.

Som beskrivits i kapitel 7 hade dåvarande generaldirektören Maria Ågren dessutom ett möte med Säkerhetspolisen den 1 februari 2016 där hon enligt egen uppgift fick allvaret i situationen klar för sig. Enligt uppgifter från personer på Transportstyrelsen tog man med anledning av detta hem två specifika system i mars 2016.

8.3.2 Projekt It-drift 2.0 får nytt projektdirektiv

I projektdirektivet för projekt It-drift 2.0 från den 12 februari 2016 (med justeringar den 26 februari 2016) anges bl.a. följande. Bytet av leverantören av Transportstyrelsens it-drift genomfördes under 2015. IBM ersatte Trafikverket och Steria som leverantörer av it-driften. Projektet It-drift 2.0 ansvarade för att genomföra leverantörsbytet. It-drift 2.0 bestod under 2015 av följande delprojekt:

- Transition: Byte av leverantör av it-driften till IBM enligt avtal.
- Driftstyrning: Etablera en samverkansmodell med en bemannad organisation från Transportstyrelsen och IBM med mötesforum och processer för beställningar, avvikelser, ändringar m.m.
- Ersätta Trafikverket IT:s leverans: Hantera de aktiviteter som Trafikverket ansvarat för och som inte är avtalade att IBM ska ta över.

Enligt uppgifter från personer på Transportstyrelsen gjordes en ny säkerhetsanalys under 2016. Säkerhetsskyddschefen ansvarade för den. Analysdelen blev klar under hösten 2016 medan åtgärdsdelen inte blev klar förrän 2017. Detta överensstämmer med det som anges i Transportstyrelsens rapport till regeringen från den 23 januari 2018 avseende uppdraget att kartlägga hanteringen av vissa uppgifter (kartläggningsuppdraget) där det anges att en reviderad version av dåvarande säkerhetsanalys fastställdes av generaldirektören i maj 2017. [181]

Utredningen har också fått uppgiften att Maria Ågren valde att inte distribuera analysdelen av säkerhetsanalysen till alla avdelningschefer eftersom vissa inte var säkerhetsklassade. Avdelningscheferna uppges ha varit måna om att få säkerhetsanalysen som ett dokument, men mindre måna om att se till att den spreds och att finna lämpliga åtgärder att vidta med anledning av den.

Utredningen har vidare uppfattat att säkerhetsskyddschefen fick arbeta mycket på egen hand med åtgärdsdelarna i säkerhetsanalysen tillsammans med ett antal personer som utsetts av avdelningscheferna. Problemet enligt personer på Transportstyrelsen är att åtgärdsförslagen aldrig fått en förankring hos avdelningscheferna

[181] Transportstyrelsens underlagsrapport Kartlägga hanteringen av vissa uppgifter, Dnr TSR 2017–519, 2018-01-23, s. 8.

vilket är en bidragande orsak till att säkerhetstänket inte blivit något som drivits av dessa.

8.3.3 Nya säkerhetskrav i februari 2016

I februari 2016 fastställs en bilaga till affärsavtalet med IBM: Bilaga 3.1 *Specifikation säkerhetsskydd*. I denna lämnas närmare detaljer om säkerhetsskyddad information inom Transportstyrelsen. I inledningen anges att eftersom upphandlingen inte genomfördes som säkerhetsskyddad upphandling kunde detaljer om säkerhetsskyddad information inom Transportstyrelsen inte lämnas till anbudsgivare. Dessa detaljer skulle i enlighet med avtalet specificeras som en del i transitionen efter att säkerhetsskyddsavtal tecknats.

Vidare anges att dokumentet syftar till att förtydliga omfattningen på kravställning gällande säkerhetsskydd. I detta dokument anges principer för åtkomst till säkerhetsskyddad information:

Utredningen konstaterar att det är oklart vad begreppet säkerhetsskyddad information innebär och omfattar. Transportstyrelsen inleder senare under året ett arbete med att ta fram en definition av begreppet skyddsvärd data som torde ha en större räckvidd (se nedan om Omtaget). I bilagan nämns en säkerhetsskyddsinstruktion som har upprättats. Enligt uppgift från IBM tog Transportstyrelsen och IBM gemensamt fram en säkerhetsskyddsinstruktion. Det är dock oklart när i tid detta skedde. Utredningen har endast sett ett utkast till en säkerhetsskyddsinstruktion.

8.3.4 Arbetet i projektet mars-september 2016

Projektstatus i mars 2016

Av underlag till möte med It-rådet som styrgrupp för delportfölj Framtidssäkring framgår bl.a. att arbetet med att sätta upp IBM:s datahallar inklusive nätverk är försenat cirka 6 veckor pga. ändrad hantering av IP-adresser. Arbetet med transformationsplanen antecknas gå enligt plan och leverans ska ske den 30 maj 2016. En kommersiell dialog pågår med IBM utifrån förändringarna mot den ursprungliga tidplanen.

I underlaget nämns att det pågår säkerhetsarbete hos Transportstyrelsen och IBM kring bemanningen av IBM:s resurser och att detta arbete riskerar att ge långa ledtider. Det framgår inte vad som avses med detta säkerhetsarbete. Kraven på säkerhetskontroller av IBM:s resurser med långa ledtider vid bemanning nämns nu som en kritisk risk. Konsekvensen av risken är försening av tidplan och större kostnad.

Enligt uppgifter från personer på Transportstyrelsen tog man hem två specifika system i mars 2016. Detta beordrades av Maria Ågren efter att hon träffat Säkerhetspolisen i februari 2016, se kapitel 7. IBM åtgärdade i ett första steg åtkomsten för dessa två system och klippte behörigheterna för direkt åtkomst för icke säkerhetsgodkänd utländsk personal. I ett andra steg åtgärdades indirekt åtkomst till miljöerna i dessa två system.

Enligt uppgift fortsatte Transportstyrelsen dock att parallellt med detta arbeta utifrån att utländsk personal skulle kunna säkerhetsgodkännas. Detta innebär i längden att det uppstod problem för IBM att garantera leveransen när det inte längre fanns några avstegsbeslut som möjliggjorde tilldelning av behörigheter till ny personal. Personalomsättning har inneburit att personal som fått behörigheter genom avstegen har slutat eller fått andra arbetsuppgifter. Detta ställs på sin spets i slutet av sommaren 2016, se nedan.

Projektstatus i april 2016

Av protokoll från möte i It-rådet som styrgrupp för delportfölj Framtidssäkring den 28 april 2016 framgår att den absolut största risken relaterad till beroendena mellan projekten (stordatormigreringen, DUBBing reskontra och it-drift) bedöms vara säkerhet. Resurserna behövs inom både It-drift 2.0 och stordatormigreringen och vissa säkerhetsfrågor har väldigt hög prioritet. Avseende It-drift 2.0 antecknas att de förtydligade säkerhetskraven får stor påverkan och prognosen för projektet har ungefär halverats på helåret 2016 eftersom ambitionen dragits ned kraftigt.

Av underlaget till mötet framgår bl.a. följande avseende driftleveransen. De nya säkerhetskraven påverkar transformationen. Leveransen ska utformas från de krav som säkerhetsanalysen kommer

fram till (detta uppdrag leds av säkerhetsskyddschefen och ska rapporteras under kvartal 2). Även Säkerhetspolisens rapport som kommer i april behöver beaktas. Transformationsprojektet ska planeras om utifrån de nya säkerhetskraven och ett kommersiellt omtag kommer att ske utifrån de nya förutsättningarna.

Omplaneringen redovisas med ett antal åtgärder som ska stoppas. Det är en relativt omfattande omplanering som görs och många delar av transformationen som ställs in på obestämd tid. Arbete med säkerhetsanalys pågår och ska rapporteras kvartal 2 vilket man redan är inne i. Samtidigt sköter, som utredningen har uppfattat det, fortfarande icke-säkerhetsgodkänd personal från IBM delar av leveransen vid denna tidpunkt.

Enligt uppgift från personer på Transportstyrelsen pausades Transformationen för att man skulle kunna bedriva ett arbete kopplat till kravfångst ur ett säkerhetsperspektiv, dvs. att identifiera informationssäkerhetskraven och hur dessa ska kunna tillämpas i en transformerad lösning.

Projektstatus i maj 2016

Av underlag till möte i It-rådet som styrgrupp för delportfölj Framtidssäkring den 26 maj 2016 framgår bl.a. följande. Avseende stordatormigreringen antecknas som en risk att Transportstyrelsen har för dålig koll på sin egen miljö och att de därför riskerar att upptäcka sådant som påverkar migreringen sent vilket påverkar tidplanen.

De förändrade säkerhetskraven innebär en kostnadsökning för driftövertagandet där tidigare prognos från IBM var 7,5 miljoner kronor och den nya offerten som accepterats av Transportstyrelsen är på 29,8 miljoner kronor. I projektet It-drift 2.0 förs in ett nytt delprojekt *Säkerhet* som ska hantera de säkerhetskrav som utmynnar från säkerhetsanalysen. Delprojekt *Säkerhet* innehåller två delar, en del för it-kraven och en annan del för att implementera kraven. Det antecknas också att kommersiell dialog pågår mellan Transportstyrelsen och IBM utifrån förändringarna mot den ursprungliga tidplanen. Som kritisk risk anges bl.a. risk att säkerhetsanalysen blir försenad.

Det är oklart för utredningen exakt vad de förändrade säkerhetskraven innebär. Det finns ingen skriftlig dokumentation om hur

arbetet med säkerhetsanalysen fortskrider. Utredningen har inte heller fått ta del av någon skriftlig dokumentation kring hur det fortsatta arbetet med säkerhetsprövningar, säkerhetsutbildning, registerkontroller m.m. fortskrider efter denna tidpunkt.

Projektstatus i juni 2016

I underlag till möte i It-rådet som styrgrupp för delportfölj Framtidssäkring den 16 juni 2016 anges bl.a. att delprojekt *Säkerhet* startade den 3 juni 2016 och är formerat med projektgrupp, två referensgrupper samt beslutsgrupp. Projektarbetet anges ha kommit igång ordentligt och både Transportstyrelsen och IBM arbetar med att dokumentera kraven. Som kritisk risk anges fortfarande bl.a. risk att säkerhetsanalysen blir försenad.

Projektstatus i augusti 2016

Av underlag till möte i It-rådet som styrgrupp för delportfölj Framtidssäkring den 26 augusti 2016 framgår bl.a. följande. Inriktningsbeslut är fattat av styrgruppen efter förankring hos generaldirektör. Inriktningsbeslutet är att datacentren sätts upp i IBM:s datahallar i Kista och Solna med svensk drift- och supportpersonal samt att transformationen ska utföras så att ny arkitektur utnyttjas.

Omförhandling av avtalet med IBM pågår och ett förhandlingsteam ska skapas på Transportstyrelsen. Delprojekt *Säkerhet* ska i Fas 1 hantera it-säkerhetskrav för stordatorn och har genomfört GAP-analys och tagit fram åtgärdsförslag och implementationsplan. Denna fas ska avslutas den 1 september 2016. I Fas 2 ska delprojektet hantera it-säkerhetskraven för övriga it och detta arbete är i planeringsstadiet.

Som kritiska risker anges bl.a. risk att omförhandlingen blir försenad och risk att flyttarna av it-lösningarna blir komplexa. Risken att säkerhetsanalysen blir försenad finns inte längre med som ett exempel på kritisk risk. Såvitt utredningen förstår är dock inte säkerhetsanalysen klar vid denna tidpunkt.

Av uppgifter i intervjuer framgår att det i slutet av sommaren 2016 blev kritiskt med IBM:s leverans. Säkerhetsskyddschefen meddelar enligt uppgift vid denna tidpunkt att det inte kommer att gå att

genomföra registerkontroller eller säkerhetsprövningar av utländsk personal. Detta var enligt partneransvarig gentemot IBM ny information både för honom och för IBM. Situationen med IBM blir komplicerad och myndigheten riskerar att hamna i en allvarlig situation där viktiga funktioner inte fungerar då IBM inte kan garantera leveransen p.g.a. att de inte har tillräckligt med säkerhetsgodkänd personal.

Projektstatus i september 2016

Av underlag till möte i It-rådet som styrgrupp för delportfölj Framtidssäkring den 29 september 2016 framgår bl.a. att skapandet av ett förhandlingsteam fortfarande pågår och att externa jurister arbetar med att tillföra kompetens inför omförhandlingen. Vad gäller delprojekt *Säkerhet* anges att frågan om att hantera it-säkerhetskraven för övriga it har uppstartsmöte den 29 september 2016.

Det nämns inget om status på säkerhetsanalysen som skulle ha rapporterats under kvartal 2.

Projektstatus i oktober 2016

Av protokoll från möte i It-rådet som styrgupp för delportfölj Framtidssäkring den 27 oktober 2016 framgår att transformationen är fortsatt stoppad till förmån för andra områden inom projektet. Vidare framgår att leveransen fram till dagens datum anses till viss del bristfällig men att det inte är tydligt hur behoven framöver egentligen kommer att se ut. Omförhandlingen med IBM anges som under initiering.

8.3.5 Delportfölj Framtidssäkring läggs ner

I protokoll från möte i It-rådet som styrgrupp för delportfölj Framtidssäkring den 15 december 2016 antecknas att delportföljen Framtidssäkring beslutas läggas ned då syftet är uppnått och det inte finns några pågående konflikter mellan projekten. Vidare antecknas att transformationen fortsatt ligger på is. Detta i avvaktan på omförhandling och säkerhetsarbetet.

Av underlaget till mötet framgår att avseende användarbehörigheter i stordatorn ska dessa flyttas 1:1 (dvs. att användarbehörigheterna flyttas över utan förändringar). Behörigheter för teknisk personal ska inte överföras 1:1 utan individ för individ. Behov av höga behörigheter ska motiveras och säkerhetsprövning ska initieras i förekommande fall samt påminnelse om sekretess.

Det framstår som att Transportstyrelsen har höjt medvetenheten kring behörighetshanteringen då man anger att behörigheter för teknisk personal inte ska överföras 1:1 och att höga behörigheter ska motiveras.

8.3.6 Risk- och sårbarhetsanalys 2016[182]

I risk- och sårbarhetsanalysen (RSA) för 2016 identifierar Transportstyrelsen it-störningar som myndighetens övergripande risk. Myndigheten anger bl.a. att större störningar kan uppkomma av olika anledningar.

Under avsnitt 4.1.1 Förutsättningar för ett fungerande vägtrafikregister anges bl.a. att myndigheten genom valet av ny driftsleverantör (IBM) vill uppnå förbättrad driftsstabilitet, kapacitet, ökad standardisering och effektivisering av kostnader samt att myndighetens bedömning är att valet av ny driftleverantör bör medföra att myndighetens förmåga att hantera de risker som identifierats i myndighetens RSA för 2016 stärks."

I analysen anges att arbetet med informationsklassning kvarstår och pågår i LIS-projektet. Dessutom anges att införande och implementering av loggverktyg pågår.

Det är förvånande att det i risk- och sårbarhetsanalysen för 2016 inte nämns något om de risker som uppstått i samband med upphandlingen och överlämnandet av it-driften till IBM. Inga åtgärdsförslag lämnas avseende detta, t.ex. att framtagandet av en säkerhetsanalys pågår. Inget nämns heller om åtkomstproblematiken eller behörigheterna som togs upp i 2015 års risk- och sårbarhetsanalys om informationssäkerhet.

[182] Risk- och sårbarhetsanalys för Transportstyrelsens verksamhet 2016, dnr TSG 2015–1151.

8.4 Omförhandling av avtalet med IBM inleds

Enligt uppgift från personer på Transportstyrelsen kom man redan under hösten 2016 fram till att det bästa var att omförhandla med IBM utifrån förändrade krav då myndigheten var i en situation med allvarliga säkerhetsbrister där tidsaspekten för att åtgärda dessa var viktig. Maria Ågren fattade beslutet att omförhandla och detta arbete startade i november 2016. Detta beslut var drivet av den situation myndigheten hamnade i när IBM inte kunde fortsätta leverera, se mer nedan i avsnitt 8.4.1.

Denna omförhandling ingick i det projekt som senare döptes till Omtaget och som formellt startade i januari 2017, se nedan i avsnitt 8.4.2. Enligt uppgifter från personer på Transportstyrelsen var knäckfrågorna i Omtaget säkerhetsprövad svensk personal och hanteringen av Transportstyrelsens information inom Sveriges gränser. Enligt säkerhetsfunktionen var detta endast en del av lösningen för att svara upp mot det som Säkerhetspolisen angett i sin tillsynsrapport. Enligt dåvarande ställföreträdande generaldirektören Jacob Gramenius handlade det om att se till att IBM enbart hade svenska konsulter och omfattade hela förhandlingen, vad som krävdes och hur det skulle lösas tekniskt och kommersiellt.

8.4.1 Bakgrund till omförhandlingen med IBM

IBM meddelade Transportstyrelsen den 6 september 2016 och den 3 november 2016 bl.a. att de inte längre kunde garantera drift enligt SLA (service level agreement). Som grund för detta angav IBM att processen för säkerhetsprövning är tidsödande, inte fungerar för utländsk personal och att IBM inte tillåts arbeta enligt avtalad modell.

Enligt uppgift från personer på Transportstyrelsen var både IBM och projekt It-drift 2.0 frustrerade över den situation de befann sig i med leveransproblem och säkerhetsarbetet som inte fortskred. Det fanns också en frustration över att denna situation inte eskalerades till generaldirektören. IBM:s meddelanden till Transportstyrelsen blev dock startskott för en eskalering.

Transportstyrelsen tar i samband med detta fram ett underlag för det vägval som myndigheten står inför. Detta underlag utarbetas av en arbetsgrupp bestående av bl.a. partneransvarig för IBM, chefen

för inköpsenheten, säkerhetsskyddschefen, it-säkerhetsansvarig, inköpsjurist och en extern jurist med kompetens avseende upphandlingsrätt och it-rätt.

Arbetsgruppen konstaterar att de två punkter som behöver åtgärdas är dels kapacitetsbrist hos IBM p.g.a. att leveransen inte kan ske med utländsk personal, dels utförande av åtgärder beträffande obehörig åtkomst i enlighet med återrapportering till tillsynsmyndigheten (Säkerhetspolisen).

De vägval som togs fram var 1. Kravställ på leverans från IBM:s svenska del och krav på svensk säkerhetsprövad personal, 2. Säga upp avtalet med IBM och genomföra en ny upphandling eller 3. Säga upp avtalet med IBM och ta hem leveransen.

De olika vägvalen hade olika plus och minus som kortfattat kan sammanfattas enligt följande. Vägval 1 att kräva leverans från IBM:s svenska del skulle lösa bristen på leveranskapacitet, innebära en implementation av utlovade åtgärder i enlighet med återrapportering till tillsynsmyndigheten och följa beslutad strategisk inriktning. Detta vägval skulle innebära en upphandlingsrättslig risk för upphandlingsavgift och ev. skadestånd p.g.a. otillåten ändring i avtalet, en kommersiell risk då lösningen har ett okänt pris och en risk att implementationen inte är synkad med tidplanen för återrapportering till tillsynsmyndigheten.

Vägval 2 att säga upp avtalet med IBM och genomföra en ny upphandling skulle vara upphandlingsrättsligt korrekt, vara en signal till tillsynsmyndigheten att Transportstyrelsen tar tillsynen på största allvar och följa beslutad strategisk inriktning. Detta vägval skulle inte lösa problemen på kort och medellång sikt (2–3 år), ge fortsatta säkerhetsrelaterade risker och brister i leveranskapacitet, innebära en exitkostnad för befintligt avtal, okända kommersiella risker för upphandling, risk att inga anbudsgivare inkommer med anbud p.g.a. höga krav, skulle vara ansträngande och resurskrävande för myndigheten och riskera en överprövning från IBM.

Vägval 3 att säga upp avtalet med IBM och ta hem leveransen skulle vara upphandlingsrättsligt korrekt och en signal till tillsynsmyndigheten att Transportstyrelsen tar tillsynen på största allvar. Detta vägval löser inte heller problemen på kort och medellång sikt (2–3 år) och det är dessutom okänt hur lång tid det tar att säkra resurser och kompetens för att bygga upp en stabil driftorganisation.

Vidare är det en okänd kostnad för realisering, exitkostnad för befintligt avtal och vägvalet följer inte beslutad strategisk inriktning. Detta vägval bedöms som det mest kostnadsdrivande.

Säkerhetsskyddschefen rekommenderade följande. Transportstyrelsen ska ha möjlighet att göra en fullgod säkerhetsprövning inklusive registerkontroll och teckna säkerhetsskyddsavtal med eventuella leverantörer. Verksamheten ska bedrivas inom landets gränser. Transportvägar för elektronisk kommunikation med data eller metadata ska inte gå utanför landets gränser.

Arbetsgruppen konstaterade att tillämpning av avtalade villkor med IBM innebar säkerhetsmässiga risker, ökade kostnader och upphandlinsmässiga risker och att förändrade krav innebar upphandlingsmässig risk och ökade kostnader. Arbetsgruppens rekommendation var att förändra kraven i avtalet, dvs. att omförhandla avtalet med IBM.

8.4.2 Omtaget startar formellt i januari 2017

Omtaget är Transportstyrelsens benämning på det projekt som myndigheten startar för att ytterligare tydliggöra säkerhetskraven gentemot IBM och säkerställa att dessa efterlevs snarast möjligt.

Enligt uppgift från personer på Transportstyrelsen fanns det i januari 2017 fortfarande utländsk personal som inte var säkerhetsgodkänd som hade behörigheter i systemen. Det ursprungliga antalet icke säkerhetsprövad utländsk personal med behörigheter var cirka 70 stycken som successivt ersatts med svensk säkerhetsprövad personal.

Av projektdirektivet som tas fram i januari 2017 (med justeringar i februari 2017) framgår att de två problem som identifierats är dels att det inte varit full följsamhet mot myndighetens säkerhetskrav då dessa har förändrats sedan tecknandet av avtalet och det finns behov av förtydliganden, dels att leveranskapaciteten begränsats i det korta perspektivet då förändrade säkerhetskrav försvårat delar av IBM:s leverans.

Uppdragets mål är reviderade, tydliga och väl förankrade säkerhetskrav som är kommunicerade med IBM. Kraven ska omfatta både dagens driftleverans samt driften efter den kommande transformationen. IBM:s lösningsförslag ska adressera säkerhetskraven fullt ut

samt vara godkänt av Transportstyrelsen och nödvändiga avtalsjuteringar ska vara genomförda.

Omtaget skulle genomföra en riskanalys kopplat till följande områden: säkerhetsskydd, it-säkerhet, informationssäkerhet, it-arkitektur, inköp och leverans/verksamhetsperspektiv. Lösningsförslaget ska remitteras inom följande funktioner: samverkansorganisationen med IBM, inköp, GD-juridik, it-arkitektur, it-säkerhet och säkerhetsskydd.

Planeringen var att Omtaget skulle vara avslutat den 1 april 2017 men uppdraget drog ut på tiden och avslutades först i juni 2017.

I core team för Omtaget ingick personer från It (förhandlingsledare, it-säkerhet, arkitektur, ekonomi (juridiskt stöd)) och GD-stab (säkerhetskyddschefen). Projektet rapporterade till dåvarande ställföreträdande generaldirektören Jacob Gramenius inom ramen för Säkerhetsprogrammet och hade en styrgrupp bestående av bl.a. it-direktören, enhetschefen för GD-stab, enhetschefen för inköpsenheten och enhetschefer på It-avdelningen. Resultaten skulle också rapporteras till generaldirektören som var beställare av uppdraget.

Utredningen konstaterar att både säkerhetsskyddschefen och it-säkerhetsansvarig är med i core team för Omtaget. Informationssäkerhetsansvarig deltar såvitt framgår inte i Omtaget, i vart fall inte i core team. Trots att säkerhetsskyddschefen och it-säkerhetsansvarig är med i core team kan utredningen inte se att de deltagit på något av de styrgruppsmöten som varit i Omtaget. Detta betyder dock inte att de inte deltagit i core teams arbete.

I januari 2017 entledigas Maria Ågren och den nye generaldirektören Jonas Bjelfvenstam tillträder den 19 januari 2017. Även dåvarande it-direktören slutar på Transportstyrelsen i samma veva.

Av uppgifter till utredningen framgår att i januari 2017 levereras serverdrift av personal i Sverige, Danmark, Tjeckien och Rumänien, applikationsdrift av personal i Sverige och Rumänien och nätverk av personal i Sverige. Monotorering utförs av personal i Serbien fram till den 31 januari 2017 och därefter av personal i Sverige. Den svenska personalen uppges vara säkerhetsprövad och registerkontrollerad. Den utländska personalen uppges vara säkerhetsprövad av IBM och personalen uppges delvis vara utbildad i säkerhetsskydd. Vad gäller behörighetshanteringen uppges denna

vara kvar i Tjeckien utom de allra högsta behörigheterna i Active Directory[183] som tagits tillbaka till Sverige.

8.4.3 Lösningsförslaget presenteras och behandlas i Omtaget

Tanken var att IBM snarast möjligt skulle presentera ett lösningsförslag och att detta skulle ske redan i januari 2017. Detta blev dock försenat och IBM presenterade ett lösningsförslag först den 17 februari 2017.

Vid styrgruppsmöte den 22 februari 2017 anges att det finns vissa frågetecken kring IBM:s lösningsförslag bl.a. avseende verktygen. Fem fokusområden anges i arbetet; säkerställa avtalade säkerhetskrav, säkerställa kravuppfyllnad i lösningsförslaget, säkerställa underhåll av befintlig infrastruktur, verifiera prisbilden och säkerställa avtalsjusteringarna. Tidplanen är att en sammanställning ska göras och återkopplas till IBM den 1 mars 2017. Avstämningstidpunkter med generaldirektören är inlagda i tidplanen. Vid denna tidpunkt är planeringen fortfarande att reviderat avtal ska tecknas med IBM den 1 april 2017.

Vid styrgruppsmöte den 1 mars 2017 konstateras att frågetecknen kring de globala verktygen ökar i IBM:s lösningsförslag, att priserna innehåller sådant som inte är relaterat till de förändrade kraven, att priserna innehåller oklarheter som IBM behöver förtydliga och att transformationsplanen ser orealistisk ut och sannolikt kommer att förskjutas ytterligare. Tidplanen är dock oförändrad med målsättning att reviderat avtal ska tecknas med IBM den 1 april 2017.

Vid styrgruppsmöte den 8 mars 2017 anges att IBM:s lösningsförslag i sin helhet ser ut att uppfylla de krav som Transportstyrelsen ställer men att säkerhetsfunktionen ser ett stort behov av att införa ytterligare skyddsmekanismer. Det framgår inte varför säkerhetsfunktionen ser detta behov eller vad det är för ytterligare skyddsmekanismer som behövs. Priserna bearbetas ur flera perspektiv utifrån vad som är motiverat relaterat dels till reviderade säkerhetskrav, dels i förhållande till andra kostnadsdrivare. IBM:s totala prislapp för

[183] Active Directory (AD) är en katalogtjänst från Microsoft som innehåller information om alla resurser i en domän (datornätverk) t.ex. datorer, skrivare och användare och används för att styra/kontrollera dessa.

återstående 43 månader är ca 260 miljoner kronor och en del är kostnaden för driftstjänster som köps av IBM och som ökar med 27 procent. Vid detta möte konstateras att den omständigheten att säkerhetsfunktionen ser ett stort behov av att införa ytterligare skyddsmekanismer kan påverka tidplanen och kostnaden för Omtaget. Tidplanen står dock kvar.

Uppgiften att säkerhetsfunktionen såg ett stort behov av att införa ytterligare skyddsmekanismer bekräftas av uppgifter från personer på Transportstyrelsen. Utredningen erfar att det varit problem att begränsa Omtaget till att justera det som behövs för tillfället och att det kom in många nya önskemål från säkerhetssidan.

Vid styrgruppsmöte den 15 mars 2017 anges att det pågår en dialog kring behovet projektet nu ser av att införa ytterligare skyddsmekanismer. Ett möte med Säkerhetspolisen anges ha ägt rum. Det konstateras att uppdraget inte kommer att kunna hålla tidplanen utan det är cirka två veckors förskjutning.

8.4.4 Riskanalys tas fram

Projektet presenterar den 22 mars 2017 en riskanalys. I denna bedömer projektet att det finns ett antal identifierade risker. Bl.a. tas upp risken att behov av och framförhållning med säkerhetsskyddavtal och säkerhetsprövningarna ska ge långa ledtider och påverka tidplanen. Denna risk bedöms dock endast ha ett risktal på 1 av 9. Detsamma gäller den identifierade risken att leveranskapaciteten inte ska möta myndighetens behov under transition/transformation.

Risken att Transportstyrelsen och leverantören brister i säkerhetsskyddskompetens bedöms ha ett risktal på 2 av 9 och risken att Transportstyrelsen brister i leverantörsstyrningen under genomförandet bedöms ha ett risktal på 4 av 9. Risken att ledningen får en felaktig bild av att detta löser hela säkerhetsproblemtiken bedöms ha ett risktal på 3 av 9.

De risker som får högst risktal, 6 av 9, är risken att scoopet är för begränsat och att nya omtag behövs i närtid, risken för otydligt mandat inom it-organisationen och därmed svårt att fatta beslut samt risken att Transportstyrelsen inte har kraft att ta en avtalsrelaterad tvist.

Risken för att säkerhetsskyddsavtal och säkerhetsprövningar ska ge långa ledtider bedöms således som liten. Detta beror troligen på att arbetet med dessa punkter fortskridit under hela tiden sedan affärsavtalet tecknades i april 2015, dvs. under nästan två års tid. För utredningens del är det dock fortfarande oklart vad som egentligen finns på plats i form av t.ex. säkerhetsskyddsinstruktion och om de nödvändiga säkerhetsprövningarna är genomförda. Det är något förvånande att risken att Tranportstyrelsen och leverantören brister i säkerhetsskyddskompetens endast får ett risktal på 2 av 9. Av det som framkommit framstår det för utredningen som att det finns allvarliga brister i säkerhetsskyddskompetensen, i vart fall hos Transportstyrelsen. Transportstyrelsens egen bedömning av myndighetens mognad i detta avseende i sin rapport till regeringen avseende kartläggningsuppdraget visar också på att detta risktal inte var rättvisande.[184]

Maria Ågren har till utredningen uppgett att hon efterhand förstått att kompetensen i myndigheten på säkerhetsskyddsområdet inte varit tillräcklig. Andra personer har sagt samma sak.

8.4.5 Fortsatt arbete med lösningsförslaget

Vid styrgruppsmöte den 22 mars 2017 konstateras att IBM:s lösningsförslag bör verifieras med Säkerhetspolisen tillsammans med IBM. Prisbilden har klarnat men kostnaderna blir höga. Tidplanen är även nu cirka två veckors förskjutning.

Vid styrgruppsmöte den 5 april 2017 föreslås att IBM formellt ska påbörja arbetet med transition på löpande räkning. Utredningen förstår det som att en beställning enligt detta görs. Mötet med Säkerhetspolisen har inte ägt rum och antecknas dra ut på tiden. Det konstateras också att Omtaget kommer att dra ut ytterligare på tiden och att it-ledningen behöver komma in i förhandlingen.

Det är oklart för utredningen vad anledningen är till att mötet med Säkerhetspolisen drar ut på tiden.

Vid styrgruppsmöte den 19 april 2017 antecknas att en ”ny” problematik seglat upp kring definitionen av skyddsvärd data. Det anges vidare att det är oklarheter kring det planerade mötet med

[184] Transportstyrelsens underlagsrapport *Kartlägga hanteringen av vissa uppgifter*, 2018-01-23, dnr TSR 2017–519 s. 13.

Säkerhetspolisen som ännu inte ägt rum. I anteckningarna nämns en risklista. Denna risklista har utredningen inte tagit del av. Det kan eventuellt vara samma risklista som Projekt It-drift 2.0 tog fram i februari 2016.

Som också antyds i protokollet är problematiken kring definitionen av skyddsvärd data inte en ny problematik. Enligt projektledaren för Omtaget har frågan om definition av skyddsvärd data funnits med ända sedan han kom med i projektet It-drift 2.0 (där han tidigare var projektägare under transition och transformation). Han uppger också att när IBM ställde frågan om vilka personer som behövde säkerhetskontrolleras var svaret att de personer som skulle arbete med den skyddsvärda datan behövde kontrolleras. Transportstyrelsen kunde dock inte svara på vilka dessa personer var utifrån att den skyddsvärda datan inte var definierad.

Från och med nu påbörjas alltså ett arbete med att ta fram en definition av begreppet skyddsvärd data. Detta arbete drar ut på tiden och det är svårt för myndigheten att enas kring detta begrepp. Det är oklart vilka som deltar i framtagande av denna definition och på vilken nivå i myndigheten detta arbete sker. Utredningen kan konstatera att om en definition av skyddsvärd data hade funnits innan upphandlingen startade och varit utgångspunkt för en informationsklassning av myndighetens information hade många av de problem som uppstod kunnat undvikas.

Vid styrgruppsmöte den 26 april 2017 konstateras att definitionen av skyddsvärd data fortfarande inte är överenskommen och att det är säkerhetsskyddschefen som har ansvaret för detta. Det planerade mötet med Säkerhetspolisen antecknas vara bestämt till den 2 maj 2017 med representation även från IBM.

Vid styrgruppsmöte den 3 maj 2017 antecknas att mötet med Säkerhetspolisen var ett steg framåt för alla parter men att det finns ytterligare följdfrågor att hantera för IBM. Definitionen av skyddsvärd data är inte klar.

Det framgår inte vad det är som gör att definitionen av skyddsvärd data drar ut på tiden. Den nya säkerhetsanalysen är rapporterad vid denna tidpunkt (den antas av generaldirektören i maj 2017) och borde ha kunnat vara ett stöd i framtagandet av definitionen. Uppenbarligen är det fortfarande steg som behöver tas i säkerhetsarbetet utifrån att mötet med Säkerhetspolisen gett nya följdfrågor för IBM att hantera.

Enligt uppgift från personer på Transportstyrelsen deltog bl.a. säkerhetsskyddschefen och it-säkerhetsanvarig på mötet med Säkerhetspolisen. Partneransvarig gentemot IBM har uppgett till utredningen att han ”tvingade sig in” på detta möte för att få klarhet i den komplexitet som de befann sig i. Han menar att det efter detta möte endast tog ett par veckor innan den pågående förhandlingen med IBM om en förändrad leveransmodell kunde slutföras och att denna förändring hade kunnat genomföras långt tidigare om det hade funnits ett bättre samarbete med säkerhetsfunktionen.

Utredningen noterar i detta sammanhang att internrevisionen i riskanalyser påpekat att det finns ett stuprörstänk i Transportstyrelsen och det som partneransvarig gentemot IBM beskriver om svårigheter att samarbeta mellan säkerhetsfunktionen och projektet är ett exempel på detta.[185] Troligen har svårigheterna att samarbeta också ett samband med den position och prioritet som säkerhetsfrågorna haft i organisationen, se kapitel 4.

Vid styrgruppsmöte den 10 maj 2017 anges att en reviderad kundspecifik lösning har presenterats av IBM (liknande Trafikverkets lösning) och att denna minimerar vissa risker avseende it-säkerhetsaspekter.

Vid styrgruppsmöte den 17 maj 2017 antecknas att beskrivningarna av säkerhetslösningarna nu går in i avtalsarbetet och att definitionen av skyddsvärd data nästan är klar. Vid styrgruppsmöte den 31 maj 2017 konstateras att frågorna som varit aktuella kring avtalade säkerhetskrav nu är omhändertagna. Prisförhandlingen är på mållinjen.

Enligt uppgifter från personer på Transportstyrelsen har visserligen en definition av skyddsvärd data tagits fram men hösten 2017 saknas fortfarande en informationsklassning i många delar. Det är verksamheten som ska genomföra informationsklassningen och ta fram vad som är skyddsvärt.

Av anteckningar från styrgruppsmöte den 14 juni 2017 framgår att förhandlingen gått i mål men att frågan eskalerats till generaldirektören. Avtalet skrevs under den 9 juni 2017. IBM ska ta fram en uppdragsbeskrivning för genomförandet.

Utredningen får intrycket att det uppfattats som negativt att frågan om avslut av förhandlingen eskalerats till generaldirektören. I

[185] Se t.ex. internrevisionens riskanalys, Till styrelsen för kännedom inför beslut om revisionsplan 2015, 27 april 2015.

utredningens ögon är detta tvärtom en fråga som är av sådan vikt att den ska hanteras av generaldirektören och i det läge Transportstyrelsen befann sig kanske till och med av styrelsen. Det vore inte onaturligt att anta att det förnyade avtalet var av större vikt för myndigheten.

8.5 Vad är resultatet av Omtaget?

Arbetet med Omtaget drog ut på tiden och ett reviderat avtal var klart först i juni 2017 med som utredningen har uppfattat det förändrade säkerhetskrav med innehåll att endast svensk säkerhetsprövad personal ska användas i leveransen och att detta ska vara genomfört senast den 1 januari 2018.

Enligt uppgift från personer på Transportstyrelsen bygger det nya avtalet dels på att all data anges som skyddsvärd, dels på att ingen skyddsvärd data får passera Sveriges gränser. Samma personer uppger att anledningen till att all data anges som skyddsvärd är att Transportstyrelsen inte har förmåga att ange vad som är skyddsvärt. Det finns således tveksamheter kring om myndigheten lyckats göra det arbete med identifiering av skyddsvärd data som är nödvändigt för att kunna skydda datan.

Enligt utredningens uppfattning är det inte hållbart i längden att arbeta utifrån att all data är skyddsvärd. Det blir både dyrt och komplicerat att säkerhetspröva all personal. I längden kan ett sådant förhållningssätt också urholka skyddet för det som faktiskt är skyddsvärt. En modell där myndigheten väl känner till vilken information som är skyddsvärd och utifrån detta bedriver ett säkerhetsarbete är att föredra.

Enligt företrädare på Transportstyrelsen fanns ingen utländsk personal kvar i it-driften efter den 1 oktober 2017. All personal från IBM och deras underleverantörer är nu svensk och säkerhetsprövad. Detta stämmer också med vad Transportstyrelsen angett i sin rapport till regeringen avseende kartläggningsuppdraget.[186] I oktober 2017 görs enligt uppgift från Transportstyrelsen en resning av alla

[186] Transportstyrelsens underlagsrapport *Kartlägga hanteringen av vissa uppgifter*, 2018-01-23, dnr TSR 2017–519 s. 11.

inaktuella underleverantörer och enbart underleverantörer som uppfyller kravet om att all data ska stanna inom Sveriges gränser och enbart hanteras av säkerhetsgodkänd personal får stå kvar.

Enligt ekonomidirektören är det nya avtalet med IBM på fem år och jämfört med det ursprungliga avtalet med de ändringar som har gjorts beräknas kostnaden för avtalet öka med cirka 190 miljoner kronor sammantaget under dessa fem år. Detta är enligt ekonomidirektören en lägre kostnad än vad Transportstyrelsen hade innan IBM tog över driften. Besparingen är dock inte lika stor som man beräknat från början. Utredningen saknar dock möjlighet att bedöma dessa beräkningar, men vill peka på att händelseförloppet under övergången av driften (transitionen) tagit mycket resurser i anspråk och lett till ökade kostnader inom Transportstyrelsen (se kapitel 6).

Verksamhetsmässigt får utredningen bilden av att upphandlingen av it-drift inte har gett Transportstyrelsen det som var målet med upphandlingen. Transformationen har pausats på obestämd framtid vilket innebär att det inte kan ske någon egentlig verksamhetsutveckling av driften. Enligt uppgifter från personer på Transportstyrelsen finns det ett missnöje med affären i efterhand. Det är mycket pengar och resurser som nu används för statisk förvaltning istället för verksamhetsutveckling. Det är svårt att som sammanfattande bedömning i denna del säga annat än att upphandlingen av it-drift inte blev lyckad.

8.6 Sammanfattande iakttagelser

Transportstyrelsen har inte följt sin interna rutin avseende godkännande av underleverantörer. Personal hos underleverantörer som inte har formellt godkänts av myndigheten, har tilldelats behörigheter i Transportstyrelsens it-system. Dessa personer har dessutom inte varit säkerhetsprövade.

Överföring av personuppgifter till tredje land har skett. Utredningen kan inte bedöma om tillräckliga garantier funnits för att de registrerades rättigheter skyddas men konstaterar att det är en komplicerad process att säkerställa detta vid överföring till tredje land.

Det är problematiskt att arbetet med att ta fram en definition av begreppet skyddsvärd data inleds först under Omtaget. Utredningen

kan konstatera att om en definition av skyddsvärd data hade funnits innan upphandlingen startade och varit utgångspunkt för en informationsklassning av myndighetens information hade många av de problem som uppstod kunnat undvikas.

Enligt utredningens uppfattning är det inte hållbart i längden att arbeta utifrån att all data är skyddsvärd. Det blir både dyrt och komplicerat att säkerhetspröva all personal. I längden kan ett sådant förhållningssätt också urholka skyddet för det som faktiskt är skyddsvärt.

Den säkerhetsanalys som tas fram under 2016 får inte tillräcklig spridning i organisationen, t.ex. får inte alla avdelningschefer ta del av analysdelen av säkerhetsanalysen. Detta resulterar i att åtgärdsförslagen inte får en tillräcklig förankring i verksamheten.

Det fanns egentligen inga andra alternativ för Transportstyrelsen än att omförhandla avtalet med IBM. Utredningens bedömning är att myndigheten under Omtaget gjort allt man kunnat för att säkerställa säkerhetskraven i driftsleveransen.

9 Utvärdering

9.1 Inledning

I detta kapitel redovisar vi resultaten av granskningen och de bedömningar eller reflektioner som denna föranleder. Kapitlet är indelat i fyra avsnitt. Det första presenterar utredningens sammanfattande bedömningar av varför Transportstyrelsens upphandling och outsourcing av it-driften kom att medföra brister och fel i hur hemliga uppgifter och andra skyddsvärda uppgifter hanterades. Det handlar om brister i arbetet med informationssäkerhet, en pressad tidplan och brister i kommunikationen både inom myndigheten och i förhållande till andra myndigheter. Vi diskuterar också ansvarsfrågor i denna del.

De följande tre avsnitten utgår från olika kategorier av bedömningar och utgör underlag för de sammanfattande bedömningarna som nämnts ovan. Avsnitten baseras på våra löpande iakttagelser som redovisas i rapporten. Alla dessa har inte uttryckligen kommit med i detta avslutande avsnitt, så för en samlad bild av våra iakttagelser behöver man ta del av hela rapporten.

Den första kategorin gäller upphandlingen av it-drift, bl.a. avseende hur upphandlingen genomfördes, de beslut som fattades och varför. Den andra kategorin avser hur Transportstyrelsen som myndighet har agerat och vilka faktorer som vi där kunnat iaktta som kan ha bidragit till konstaterade brister. Det gäller sådant som myndighetens organisation, styrning och interna kontroll. En tredje kategori av bedömningar är mer generella i den meningen att de kan gälla alla eller många myndigheter inom den svenska statsförvaltningen. I detta ligger bl.a. frågor om myndigheters samverkan med varandra.

Vi är väl medvetna om att andra kategorier hade kunnat väljas, att de vi valt inte utgör vattentäta skott, och att samma typ av bedöm-

ningar kan göras i flera av dem. I syfte att försöka renodla redovisningen av våra bedömningar så att de blir tydligare och lättare att diskutera har vi ändå funnit det ändamålsenligt att ge dem en struktur som är tematisk snarare än t.ex. kronologisk.

9.2 Sammanfattande bedömning

I detta avsnitt samlar vi våra slutsatser och iakttagelser och avger en samlad bedömning av det granskade händelseförloppet. I det ligger att göra en mer allmän värdering av bristerna och deras orsaker samt att peka på vem eller vilka som bär ansvar för dessa brister. Vi koncentrerar här framställningen till vad vi uppfattat vara de tre huvudsakliga brister som förekommit och deras orsaker. Som framgår senare utesluter detta inte att även andra brister förekommit, men de står alltså inte i fokus här där vi vill rikta ljuset på våra mest centrala iakttagelser.

9.2.1 Bristande kunskaper och kännedom om myndighetens information

Vår granskning leder till slutsatsen att den helt grundläggande orsaken till varför Transportstyrelsens upphandling kom att röja uppgifter gällande rikets säkerhet och hantera känsliga personuppgifter bristfälligt var att man i allt för hög grad saknade relevant kunskap om vilken information myndigheten hade, kännedom om hur denna information hanterades och vilka krav som ställdes på informationshanteringen. De flesta vid myndigheten har känt till att körkortshanteringen var känslig ur ett säkerhetsperspektiv, men i övrigt trott att myndigheten inte hanterade känslig information. Denna grundläggande brist har i sin tur berott på ett antal olika faktorer.

En första sådan faktor är att arbetet med informationssäkerhet vid myndigheten var eftersatt sedan lång tid när Transportstyrelsen beslutade sig för att outsourca it-driften. Informationsklassning hade bara gjorts för delar av verksamheten. Därmed saknades ett viktigt underlag för kunskap om dessa viktiga frågor i upphandlingen.

En andra faktor var att säkerhetsfunktionerna vid myndigheten var utspridda och saknade tillräcklig samordning. De var också svagt

bemannade, något som särskilt gäller säkerhetsskyddsfunktionen. Det är kanske inte så överraskande givet att man trodde att det inte fanns några större säkerhetsfrågor vid myndigheten och alltså dimensionerat funktionerna efter detta.

En tredje faktor som sammanhänger med den nyss nämnda är det förhållandet att de som haft kännedom och kunskap om de relevanta säkerhetsfrågorna uppfattat dessa som så pass hemliga att man inte alls velat tala om dem, inte ens i allmänna termer. Allmänt hållna invändningar om säkerhetskrav verkar därför ha ställts mot konkreta frågor som miljontals kronor i fördyrning och risk för verksamhetens genomförande. För dem i ledningen som inte var säkerhetsklassade (vilket var de flesta, inklusive styrelsen) innebar detta svårgripbara avvägningar där verksamhetskrav kom att prioriteras.

En fjärde faktor var att även de som hade viss kunskap om myndighetens hantering av känslig information inte tycks ha haft någon djupare kännedom om regelverket eller den praktiska hanteringen av detta. Det ledde till återkommande kontakter med andra myndigheter, en del missförstånd och till sist en situation som framstod som närmast ohanterlig.

9.2.2 Orealistisk tidsplan

Den andra huvudsakliga orsaken till att upphandlingen av it-driften ledde till olyckliga konsekvenser var tidsbrist. Vi har funnit att det underliggande skälet till att avstegen behövdes (oavsett om de dokumenterats eller inte) var att man inte klarade av att leva upp till vare sig lagstiftningens, de egna riktlinjernas eller avtalens krav vad gäller säkerhets- och personuppgiftshanteringen. Man kände sig därför tvungen att ”köpa” sig ytterligare tid genom att kringgå dessa krav. Att tidsplanen var orealistisk hade även det flera olika skäl.

En första faktor var att Transportstyrelsen samtidigt kom att inleda inte mindre än tre upphandlingar som alla berörde centrala delar av myndighetens funktioner. Detta innebar en stor utmaning och minsta problem eller förseningar kunde få långtgående återverkningar på verksamheten. Särskilt var den s.k. stordatormigreringen mycket tidskänslig.

En andra faktor var den snäva tidsgräns för IBM:s övertagande av it-driften som man angett i avtalet och det förhållandet att Trafikverkets leverans skulle upphöra vid årsslutet. Avtal skrevs i april 2015 med sikte på att IBM skulle ta över driften den 1 september samma år. Samtidigt hade avtalet utformats så att flera frågor var utestående och skulle lösas under den fas där IBM gradvis tog över driften. Denna period var som framgått sommaren 2015 och det borde lätt ha kunnat förutses att förseningar kunde uppstå.

En tredje faktor har med avsnittet ovan att göra. Det förhållandet att man inte hade en ordentlig genomgång och analys av befintlig information på plats vid avtalets ingång samt att dokumentationen av it-systemen var bristfällig innebar att man tvingades försöka göra detta parallellt med att kunskapsöverföringen till IBM skulle ske. Vi ser att detta var ett återkommande problem under sommaren 2015 som innebar flera månaders fördröjning i sig.

9.2.3 Bristande kommunikation

En tredje grundläggande orsak som vi kunnat identifiera gäller bristen på kommunikation såväl inom myndigheten som med andra berörda aktörer. Även denna brist beror på flera saker.

En första faktor är såvitt vi kunnat bedöma den komplexa organisation som Transportstyrelsen sjösatt i samband med upphandlingen och driftsövertagandet. Där ingick it-rådet som styrgrupp, ett s.k. core-team som ytterligare en styrnivå, en särskild grupp med fokus på problemfrågor (Framtidssäkring), utöver myndighetens säkerhetsfunktioner (som inte alla var representerade i de nämnda organen), inköpsenheten och myndighetens ledningsgrupp samt de funktioner kring generaldirektören som berördes. Vi har intrycket att organisationen i sig var ett hinder för effektiv kommunikation inom myndigheten.

En andra faktor är varför kontakt inte togs med Trafikverket för att förlänga leveransen efter årsskiftet 2015. Av intervjuerna framgår att många inblandade i myndighetens projekt hade den fasta uppfattningen att en sådan förlängning var omöjlig. Vi har dock inte kunnat finna stöd för detta och kan bara konstatera att man aldrig kontrollerade detta direkt med Trafikverket.

En tredje faktor är att Transportstyrelsens tidigare generaldirektörer brustit i sin kommunikation med styrelsen. Dels har det framgått att styrelsen inte fått information om problemen förrän i slutet av sommaren 2015, trots att det första avstegsbeslutet fattas i maj. Vi har också anledning att tro att informationen till styrelsen, delvis av skäl som hör ihop med det vi ovan noterat om hur hemlig information hanterades, inte var särskilt precis. Avstegsbesluten delgavs t.ex. inte styrelsen. Delar av styrelsen kan därför mycket väl ha haft en ganska oklar uppfattning om vad myndigheten egentligen gjort, trots att det är styrelsen som bär det yttersta ansvaret för detta. Det var knappast en idealisk situation.

En sista faktor som påverkat och som är särskilt betydelsefull är myndighetens val eller oförmåga att mer aktivt involvera regeringen i den uppkomna situationen. I viss utsträckning handlade den om att prioritera mellan olika centrala samhällsintressen – trafiklösningar av betydelse för hela samhället visavi skyddet av rikets säkerhet och skyddet av personlig integritet. Det hade då inte varit onaturligt att vända sig till regeringen vars uppgift är att styra riket (1 kap. 6 § regeringsformen) och ytterst avgöra sådana målkonflikter.

Transportstyrelsen har såvitt vi kunnat se inte varit helt tydlig med hur allvarlig den uppkomna situationen var i sin dialog med Regeringskansliet. De regelbundna kontakterna mellan myndigheten och Regeringskansliet tycks främst ha gällt mer övergripande frågor och den vitala stordatormigreringen, där brister i genomförandet kunde få politiska konsekvenser.

Det finns ett tillfälle vi kunnat belägga att Transportstyrelsen gett Regeringskansliet och Myndigheten för samhällsskydd och beredskap konkret information om allvarliga brister avseende informationssäkerheten vid myndigheten, nämligen en rapport som myndigheten lämnade i december 2015. Utredningen har inte kunnat fastställa om denna rapport föranledde några åtgärder från vare sig regeringen eller Myndigheten för samhällsskydd och beredskap.

Oviljan att vända sig till regeringen är kanske förståelig men stämmer till eftertanke avseende den svenska förvaltningsmodellens starka och svaga sidor. En tydligare och rakare kommunikation mellan myndighet och regeringen hade kanske kunnat begränsa eller förhindra de skador som upphandlingen medfört.

9.2.4 Ansvar

I denna utredning ingår inte att utkräva ansvar i formell mening, det är det andra myndigheter som gör. Enligt våra överväganden i kapitel 1 är det däremot en del av en granskning att också ange något om vem eller vilka som bör anses bära ansvaret för de iakttagna bristerna.

Alla de tre huvudsakliga brister vi identifierat leder tillbaka till myndighetens ledning. Den har det yttersta ansvaret och även om man delegerat uppgifter kan ledningen inte göra sig kvitt ansvaret för hur uppgifterna utförs. Bristerna vad gäller informations- och säkerhetshantering, tidplanen och kommunikationen vilar alla i hög grad på ledningen. Detta gäller naturligtvis de tidigare generaldirektörerna Staffan Widlert och Maria Ågren. Vi menar också att det innebär att styrelsen, trots (eller kanske på grund av) sin ringa inblandning i upphandlingen har ett ansvar för hur myndigheten varit organiserad, prioriterat sina resurser och agerat i praktiken.

Det finns också andra som bär ett ansvar. De brister vi identifierat angående bristfällig kännedom om myndighetens känsliga information, informationsklassning och liknande beror på att myndigheternas avdelningschefer inte har prioriterat dessa frågor i verksamheten. Det är också ett tydligt intryck som vi fått att säkerhetsfrågor haft betydande svårigheter att få gehör i den vardagliga verksamheten och ansvaret för det måste delvis falla på dem som ansvarat för verksamheten.

Det går vidare inte att förbise att de som lett upphandlingen och IBM:s övertagande alla verkar ha varit okunniga om säkerhetsfrågornas betydelse eller ovilliga att ta dessa på allvar. Vi har noterat att det fanns dokument som i detalj redogjorde för problematiken, t.ex. i samband med personuppgiftsbiträdesavtalet samt att flera och återkommande signaler om dessa frågor kom från de olika säkerhetsfunktionerna. Ändå verkar man inte ha kunnat ta in denna information och för detta måste även de bära ett ansvar.

Till sist kan vi inte undgå att notera att säkerhetsfunktionerna vid myndigheten bär ett ansvar för att det kunde gå så långt som det faktiskt gjorde. Allvaret i de invändningar som dessa haft har bevisligen inte gått fram. Det har, som vi förstått saken, inte enbart berott

på mottagarnas ovilja att ta till sig budskapet utan också på att säkerhetsfunktionerna uppfattats som otydliga och utan lösningar på problemen.

9.3 Upphandlingen

9.3.1 Inledning

I detta avsnitt behandlar vi de slutsatser som vi anser kan dras om själva upphandlingsförfarandet. Redovisningen sker i någon mening i en fallande skala där vi tar upp det vi uppfattat som mest viktigt och centralt först för att sedan gå över till vad som mer kan uppfattas som detaljer.

9.3.2 Brister avseende informationshantering och analys innan upphandlingen

Vi har kunnat konstatera att Transportstyrelsen inte hade gjort ett tillfredställande arbete med informationsklassning, säkerhetsanalys och dokumentation av it-system vid den tidpunkt då upphandlingen initierades. Man har inte heller tillräckligt noga övervägt frågor om hur känsliga personuppgifter ska hanteras vid en outsourcing. Detta är – som framgått av kapitel 1 – inget unikt för svenska myndigheter, men kom att leda till att Transportstyrelsens upphandling vilade på felaktiga eller bristfälliga förutsättningar om vad myndigheten hade för känslig information och hur denna skulle hanteras. Det står vidare klart att många i myndighetens ledning och på centrala poster inom myndigheten haft dessa felaktiga utgångspunkter och att det därför varit svårt att ändra förhållningssätt när väl information om annat kom fram.

Myndighetens it-försörjningsstrategi saknade mer generella överväganden kring lämpligheten att outsourca viss eller all verksamhet. Inte heller behandlade den säkerhetsfrågor. Fokus låg istället på frågor som effektivitet, kostnad och utvecklingspotential.

Detta bidrog i sin tur till att förfrågningsunderlag m.m. som togs fram för att användas i upphandlingen inte heller tog upp centrala frågor om säkerhetsskydd, sekretess och hantering av känsliga per-

sonuppgifter. Anbudsgivarna var således i viss utsträckning omedvetna om de krav som skulle komma att ställas på dem, eftersom myndigheten inte själv hade detta helt klart för sig.

Upphandlingsformen förhandlat förfarande valdes just för att ge utrymme för en gradvis precisering av vilka krav som myndigheten hade på bl.a. säkerhet. Myndigheten underskattade dock svårigheten i att göra detta och hann inte göra det i tid till att avtalet slöts. Först långt efter att IBM tagit över driften var detta på plats.

Sammantaget kan man således konstatera att det i det närmaste var ofrånkomligt att myndighetens upphandling inte skulle kunna hantera frågorna om säkerhetsskydd, informationssäkerhet, och skydd av känsliga personuppgifter eftersom förutsättningarna för att klara av detta inte fanns på plats när upphandlingen inleddes.

9.3.3 Parallella och tidspressade förfaranden

En annan starkt bidragande orsak till att upphandlingen kom att leda till besluten om avsteg från gällande lagstiftning var det sammanhang i vilken den planerades och genomfördes. Som framgått var det nämligen inte mindre än tre stora upphandlingsförfaranden avseende it-frågor som pågick parallellt.

Viktigast för myndighetens verksamhet var, som vi förstått det, den s.k. stordatormigreringen. Genom denna skulle en föråldrad teknisk lösning angående det centrala datasystemet i myndigheten bytas ut mot modern teknik. Åtgärden var såvitt framgått helt nödvändig. Behovet av en ny lösning hade varit känt under en längre tid men blev alltmer akut. Samtidigt ville Transportstyrelsen outsourca it-driften i stort och dessutom det s.k. reskontrasystemet (DUBBing).

Myndighetens fokus låg på stordatormigreringen, eftersom denna var vital för kärnverksamheten och dessutom påverkade när vissa politiska beslut angående förändringar i lagstiftningen på transportområdet skulle kunna genomföras. Upphandlingen av it-driften tycks ha uppfattats som ett ganska okomplicerat om än omfattande projekt.

Avtalet med IBM skrevs på i april 2015 och man siktade då på att företaget skulle ta över hela driften av myndighetens it-system redan

i september. Detta synes vara en mycket kort tid för ett så stort projekt. Vi har också kunnat konstatera att det redan under sommaren 2015 står klart för den ansvariga projektgruppen att en försening om en eller två månader uppstått. Det har vidare visat sig att denna försening endast delvis hade att göra med att säkerhetsfrågorna gick långsamt att lösa.

Vårt underlag tyder sammanfattningsvis på att myndigheten tog sig vatten över huvudet när man beslutade att driva tre omfattande och mycket krävande upphandlingsprojekt parallellt. Tidsplanen var dessutom för optimistisk. I efterhand framstår det pressade tidsschemat som en huvudanledning till att myndigheten fattade besluten om avsteg och att man överhuvudtaget hade svårt att väga in säkerhetsskyddsaspekter i sitt agerande eftersom dessa nästan oundvikligen innebar fördröjningar som i sin tur satte myndighetens kärnverksamhet i riskzonen.

9.3.4 Bristen på säkerhetsåtgärder i samband med outsourcingen

Den centrala frågan för detta avsnitt är om Transportstyrelsen vidtagit, eller fått tillräckliga garantier för, åtgärder som ska säkra den skyddsvärda information som myndigheten besitter.

Det första steget en myndighet måste ta för att klara av att skydda sin information är att själv skaffa sig kännedom om denna och var och hur den används. Bara då kan myndigheten ställa relevanta krav på leverantörerna. Som framgått ovan hade man inte sådan kännedom på Transportstyrelsen.

Ett andra steg är att upprätta ett väl fungerande säkerhetsskyddsavtal med samtliga leverantörer och underleverantörer. Även här har vi kunnat konstatera sådana brister som att frågan om säkerhetsskyddsavtal kom in sent i upphandlingsprocessen, att avtal inte slöts enligt tidsplan och att avtalens genomförande hos leverantörerna och underleverantörerna inte följdes upp på det sätt som det är avsett.

Säkerhetsprövning är ytterligare en del av de åtgärder som krävs för att säkra skyddet av hemliga uppgifter. Inte heller denna del kom att kunna genomföras på ett korrekt sätt. Säkerhetsprövningarna – som skulle göras av leverantören under överinseende av Transportstyrelsen – fördröjdes nämligen eller kom inte alls till stånd. Vi har

kunnat konstatera att tilldelningen av administrativa behörigheter till personal hos utländska underleverantörer skedde utan erforderlig kontroll och dokumentation. Behörighetstilldelningen har även avvikit från de interna riktlinjerna på området.

En mindre del av säkerhetsprövningen innefattar en s.k. registerkontroll och även här brast det i Transportstyrelsens hantering. Myndigheten hade inte tillräcklig kunskap om vad en sådan innebar och under vilka förutsättningar den görs. Det medförde att det tog lång tid innan man insåg att en registerkontroll av utländska medborgare som arbetar i utlandet inte kan genomföras på ett meningsfullt sätt av Säkerhetspolisen i Sverige och att denna del av säkerhetsprövningen måste lösas på ett annat sätt. Detta borde man naturligtvis ha vetat senast när avtalet slöts. Här har vår granskning också visat att kommunikationen mellan Säkerhetspolisen och Transportstyrelsen samt mellan Transportstyrelsen och Utrikesdepartementet kunde ha varit bättre.

Vi kan således konstatera att Transportstyrelsen på flera punkter, på grund av bristande kompetens, resurser och framförhållning, inte lyckades genomföra outsourcingen på ett sätt som skyddade myndighetens hemliga information på ett adekvat sätt. Av samma skäl som anförts ovan har även skyddet av känsliga personuppgifter brustit även om detta inte är lika formaliserat som skyddet av hemliga uppgifter med betydelse för rikets säkerhet (se kapitel 2).

9.3.5 Myndighetens beslutsprocess vid upphandlingen

Utredningen har kunnat visa att Transportstyrelsen initialt hade en del frågetecken kring valet av upphandlingsförfarande enligt lagen (2007:1091) om offentlig upphandling. Man kom till sist att stanna för ett s.k. förhandlat förfarande med föregående annonsering. Det ligger inte i utredningens uppdrag att göra en rättslig efterhandsprövning av detta val, men på rent allmänna grunder kan vi inte finna att detta val var felaktigt eller olämpligt.

Utredningen har kunnat konstatera att beslut om såväl inledandet av upphandlingen som dess avslutande faser (kontraktskrivande) togs av generaldirektören eller av andra personer i myndighetens ledning (främst ekonomidirektören). Vi har mot bakgrund av myndighetsförordningens (2007:515) reglering av ansvarsförhållandet

mellan styrelse och generaldirektör i en styrelsemyndighet ställt frågan om inte denna fråga var av sådan grundläggande och strategisk betydelse att den formellt borde ha beslutats av styrelsen i någon fas.

I en styrelsemyndighet ska styrelsen ansvara för ärenden av principiell karaktär eller sådana som är av större betydelse medan myndighetschefen ska sköta den löpande verksamheten. Vi har haft svårt att se att besluten om upphandling av it-drift (tillsammans med de övriga upphandlingarna på it-området, som hanterades på samma sätt) inte skulle antingen vara av principiell karaktär eller av större betydelse. Flera av våra intervjupersoner i ledande ställning har medgett att det kunde ha varit en naturlig beslutsgång om styrelsen involverats också formellt, men uppgett att det inte var något som man då reflekterade över. Vi menar sammanfattningsvis att det förhållandet att styrelsen inte formellt deltog i några beslut om upphandlingen var fel.

9.3.6 Besluten om avsteg

Vi har kunnat konstatera att det fattades ett flertal beslut om s.k. avsteg under sommaren och hösten 2015. Bakgrunden var att bl.a. säkerhetsprövningarna tog längre tid än väntat och att man med hänsyn till tidspressen ansåg sig tvungna att ”köpa sig” mer tid. Besluten är utformade så att de uttryckligen anger att det är fråga om avsteg från gällande lagstiftning. Av besluten framgår uttryckligen att de innebär risk för brott mot säkerhetsskyddslagen, personuppgiftslagen och offentlighets- och sekretesslagen. De innehåller också en intresseavvägning visavi myndighetens uppdrag.

När det gäller bakgrunden till dessa beslut är det inte helt klarlagt vad som egentligen föranledde myndigheten att fatta dem. Vissa har uppfattat dem som varningssignaler för att inte gå vidare, andra som dokumentation som gjort IBM:s övertagande av it-driften möjligt. Vad vi kunnat klarlägga är att besluten fattades som dokumentation av förfaranden som redan pågick eller som var planerade och att de var den direkt utlösande faktorn för Säkerhetspolisens tillsynsärende. Under utredningen har vi ibland mött uppfattningen att besluten var det enda fel som myndigheten begick, men det är inte korrekt.

Som redan framgått låg bristerna i att skyddsvärd information röjdes, att känsliga personuppgifter behandlades utan nödvändiga skyddsgarantier och i att lagstiftning och interna regler inte följdes. Avstegsbesluten dokumenterade bara detta och även om avstegen aldrig gjorts hade de egentliga felen bestått. Det ligger onekligen något uppseendeväckande i att en svensk myndighet fattar beslut om att bryta mot lagar. Som vi förstått händelseförloppet var dock alternativet för myndigheten inte att avstå från ett sådant agerande. Snarare var det att göra samma sak, men att inte dokumentera det. Det stämmer till viss eftertanke.

9.4 Transportstyrelsen

9.4.1 Inledning

I detta avsnitt tar vi upp och diskuterar de iakttagelser vi kunnat göra om Transportstyrelsen när det gäller organisation, styrning, policys och intern kultur vid sidan av det som specifikt gällt upphandlingen. Vårt intryck är att flera sådana myndighetsövergripande förhållanden haft en avgörande inverkan på outsourcingen och dess efterverkningar. Det är därför av vikt att också dessa förhållanden belyses.

Även i detta avsnitt har vi gjort en bedömning av vilka faktorer som hade störst inverkan och presenterar dem i fallande skala därefter.

9.4.2 Effektivisering som utgångspunkt

När Transportstyrelsen bildades var syftet att få till stånd en effektivare hantering av transportsektorn, där sammanslagningen av flera olika trafikslag i en gemensam myndighet ansågs ha potential att ge samordningsvinster, möjligheter till ömsesidigt lärande m.m. (se kapitel 3). Vi noterar också att myndigheten fick en förändrad finansieringsmodell från 2010, vilket innebar att myndigheten huvudsakligen kom att finansieras genom avgifter.

En av de bärande tankarna bakom myndighetens tillkomst var således effektivisering samtidigt som myndigheten blev mer bero-

ende av sin egen verksamhet för sin försörjning. Dåvarande generaldirektören Staffan Widlert har till utredningen sagt att han ansåg att det fanns ett tydligt uppdrag för myndigheten att göra besparingar. Myndigheten tog 2012–13 fram en plan för att minska kostnaderna. En viktig del var att man ansåg att Trafikverkets leverans låg över det marknadsmässiga priset och att man där skulle kunna göra stora besparingar.

Utredningen bedömer det sannolikt att de förhållandevis ambitiösa besparingsplanerna påverkade myndighetens beslutsfattande på ett negativt sätt när frågor om upphandlingens initierande och genomförande behandlades. Upplägget med tre parallella upphandlingar, den mycket ambitiösa tidplanen och valet av en global leveransmodell tyder alla på att kostnadseffektivitet i hög grad varit vägledande medan andra perspektiv, som t.ex. säkerhet, fått stå tillbaka.

Sammantaget har vi fått intrycket av en myndighet där man upplevt sig ha stränga besparings- och effektiviseringskrav och där synpunkter som gått på tvärs med dessa ambitioner haft svårt att vinna gehör.

9.4.3 Brister i säkerhetskulturen

En faktor som är värd att betona inledningsvis är att när vi frågat anställda vid Transportstyrelsen om säkerhetskulturen i myndigheten har flera personer i första hand reflekterat över myndighetens roll som tillsynsmyndighet på trafikområdet. Det har då framhållits att myndigheten har en god säkerhetskultur.

Vi har kunnat konstatera att samma sak inte gäller för frågorna om informationssäkerhet, skydd av känsliga uppgifter m.m. inom den egna verksamheten. De har uppfattats och hanterats som en separat del av myndighetens verksamhet och inte integrerat med kärnverksamheten. Det verkar således som att det som var en naturlig del av myndighetens arbete utåt inte hade samma självklara ställning i det interna arbetet. I sin tur har detta lett till ett reaktivt förhållningssätt till säkerhetsfrågor och risker som sammankopplas med dessa. Istället för att försöka identifiera och hantera riskerna i förväg har man tvingats agera när problem redan uppstått och då naturligtvis under betydligt större press.

En viktig del av de brister vi iakttagit som sammanhänger med säkerhetsmedvetenheten rör tilldelningen av behörigheter i myndighetens it-system. Där fanns en historia av att bevilja mycket omfattande behörigheter. Orsaken till detta var delvis den komplexa uppbyggnaden av myndighetens it-system (se kapitel 4), men berodde också delvis på mer effektivitetsrelaterade överväganden. Behörighetstilldelningen var ett känt problem inom myndigheten redan innan upphandlingen, men fick ingen lösning till när IBM skulle överta driften. Vårt intryck är att detta fortfarande är ett problem.

Till bilden hör också att myndigheten visserligen producerat ett antal riktlinjer, rekommendationer och andra vägledande dokument på området efter analyser från de ansvariga på myndigheten. Vi har fått intrycket att detta material inte kommit till praktisk användning i särskilt stor utsträckning. Utredningen har också sett att flera krav som ställs på bl.a. biträdande säkerhetsskyddschef, säkerhetsplan som baseras på säkerhetsanalys, m.m. inte uppfyllts.

En orsak till detta har varit att ledningen inte prioriterade säkerhetsfrågorna. Vi har sett att säkerhetsskyddsfunktionen hade en organisatoriskt oklar ställning, brist på beslutsmandat och på egna resurser. Den direkta tillgång till generaldirektören som säkerhetsskyddschefen ska ha enligt författning återspeglades vid tidpunkten för outsourcingen inte i arbetsordningen. Övriga säkerhetsfunktioner var utspridda och saknade samordning.

Från intervjuerna har vi kunnat förstå att medarbetare uppfattat den högsta ledningen ge uttryck för att myndigheten inte hade någon särskild skyddsvärd information, något som rimligen bidrog till hur man betraktade säkerhetsfrågorna mera generellt. Vi har också intrycket av att den organisatoriska lösningen bidragit till att den övriga verksamheten haft en oklar bild av vem som ansvarar för vad på säkerhetsområdet och att man inte fullt ut förstått vilket ansvar som låg på verksamheten.

Det förhållandet att man inte tycks ha talat särskilt mycket om säkerhetsfrågor generellt och säkerhetskyddsaspekter specifikt vid myndigheten gjorde också att dessa frågor inte fanns tydligt i medarbetarnas medvetande. Vi har fått intrycket att det fanns ett problem med osäkerhet kring vad man fick tala om. Säkerhetspolisens rådgivning uppfattades som en uppmaning att tala så lite som möjligt om de känsliga säkerhetsfrågorna. Detta kom att tolkas av de ansvariga på Transportstyrelsen som en uppmaning att inte alls tala om

dessa frågor och bidrog därmed till den okunskap och dåliga beredskap som organisationen uppvisade när frågorna sedan blev akuta.

Ytterligare en faktor som vi kunnat identifiera som bidragande till svårigheterna att rätt värdera och hantera säkerhetskänslig information vid Transportstyrelsen finns i den målkonflikt som myndigheten ställts inför när det gäller att samtidigt leva upp till kraven på moderna myndigheter vad gäller öppenhet och tillgänglighet och att skydda det som är skyddsvärt i samma ”informationsmassa”.

För utredningen har man vid flera intervjuer uppgett att strategin vid hanteringen av hemliga uppgifter vid Transportstyrelsen var att ”gömma nålen i höstacken”. Med detta torde avses att gömma ett fåtal hemliga uppgifter i ett större material av öppen information. Vi har också fått intrycket att Transportstyrelsen vid sina kontakter med intressenterna på området för kvalificerade skyddsidentiteter uppfattat att denna strategi var godtagbar eller t.o.m. rekommenderad. Detta ”hemlighetsmakeri” har såvitt utredningen kunnat bedöma bidragit till svårigheterna med att få gehör för säkerhetskyddsfrågorna under upphandlingen och genomförandet av outsourcingen. Strategin att gömma skyddsvärd information i en stor mängd öppen information framstår med tanke på dagens tekniska möjligheter till informationshantering som problematisk.

Sammanfattningsvis fanns flera brister i säkerhetskulturen som vi kunnat identifiera gällande t.ex. kunskap, informationsklassning, organisation av säkerhetsarbetet, ledningens signaler, svårigheterna att väga öppet mot skyddsvärt m.m.

9.4.4 Förvaltningskulturen vid Transportstyrelsen

I detta avsnitt ska vi ta upp några slutsatser som inte enbart rör säkerhetsfrågor och säkerhetskultur utan som kretsar kring en vidare tematik avseende förvaltningskultur. Vi använder detta begrepp för att fånga en del av de krav som ställs på statsanställda avseende förhållningssätt, regelverk och etik. Fokus ligger här på

formella krav som regelefterlevnad, dokumentation och andra förvaltningsrättsliga grundkrav, men vi kommer också att beröra andra aspekter på statstjänstemannarollen.[187]

En problematisk sammanslagning

En första iakttagelse vi gjort angående detta tema är att Transportstyrelsen fortfarande har ett arv från tiden före dess tillkomst som påverkar hur myndigheten fungerar idag. Det är ingen nyhet att det är svårt att slå ihop verksamheter och skapa nya gemensamma identiteter och värderingar för medarbetare i sådana processer. Transportsstyrelsen har en splittrad bakgrund och det förhållandet att myndighetens olika verksamheter finns på olika orter har antagligen inte underlättat bildandet av en gemensam myndighetsidentitet.

Under vår granskning har det framkommit att myndigheten i viss mån fortfarande präglas av sina avdelningars olika bakgrund och att det finns kvar ”myndigheter i myndigheten” där tidigare förhållningssätt och rutiner lever kvar. Det innebär såvitt vi kan förstå att en del av de ursprungliga tankarna med myndigheten om att möjliggöra ömsesidigt lärande och införande av bredare trafikslagsövergripande lösningar inte har kunnat realiseras fullt ut.[188]

Regelefterlevnad i praktiken och avstegskultur

Följer man myndighetens organisation från bildandet till idag ser man att den brottats med frågorna om hur man bättre ska kunna integrera de olika delarna i verksamheten med varandra. Myndigheten har också tagit fram ett ganska omfattande material avseende risk och sårbarhetsanalyser m.m. Den har alltså visat sig ha kompetens att göra analyser som identifierar konkreta risker och som innefattar förslag om åtgärder. Däremot finns det brister med att hantera dessa analyser och omvandla dem till faktisk handling.

[187] Vi använder alltså detta begrepp lite snävare än den betydelse som t.ex. Statskontoret har i sina skrifter, se Den statliga värdegrunden – professionella värderingar för en god förvaltningskultur (2018) och Ledarskapets betydelse för en god förvaltningskultur (2017).
[188] Se även Statskontorets rapport, På rätt väg? Uppföljning av Trafikverket och Transportstyrelsen, 2015:14 s. 48 ff.

Verksamhetsövergripande frågor har prioriterats ned och konsekvensen av det är att man ofta haft bra riktlinjer och analyser men inte följt dessa i praktiken.

Av delvis samma karaktär är en del iakttagelser vi kunnat göra när det gäller att följa grundläggande krav på dokumentation och ärendeberedning. Det är ofta svårt att följa vilka åtgärder som vidtagits och vilka beslut som fattats utav myndighetens dokumentation. Avstegsbesluten saknar t.ex. uppgifter om föredragande och diarienummer, trots att detta är krav som följer av myndighetsförordningen. Även andra exempel på brister i den formella hanteringen av ärenden har framkommit och vårt samlade intryck är att de förvaltningsrättsliga rutinerna i verksamheten varit svaga.

Av intervjumaterialet och en del av den övriga dokumentationen har vi kunnat se att det inom myndigheten funnits en viss ”avstegskultur” som vi tror kan ha bidragit till att de avsteg som denna granskning avser inte uppfattades som så exceptionella. Det har framkommit att man både vad gäller interna riktlinjer mer generellt och vad gäller upphandlingsfrågor mer specifikt från tid till annan beslutat om avsteg från regelverket.

Utredningen är så klart medveten om att sådana undantag från regelverket i vissa situationer är helt oproblematiska. Det gäller både när en generaldirektör beslutar om att en intern riktlinje inte behöver följas av särskilda skäl (men inte vill ändra riktlinjen) och i de fall när upphandlingsreglerna medger att man inte följer föreskrivna förfaranden. Dåvarande generaldirektören Staffan Widlert har för utredningen uppgett att han arbetade en tid just med att begränsa förekomsten av sådana avsteg, som han upplevde fattats väl lättvindigt. Vi har också från flera andra källor fått uppfattningen att det inte var ovanligt med sådana beslut om avsteg. Det finns således tecken på att Transportstyrelsen varit en organisation som vant sig vid att man kan avvika från regelverk.

Sammantaget finns anledning att tro att myndighetens allmänna kultur avseende styrande dokuments innebörd och om eller när det är godtagbart att inte följa ett regelverk kan ha haft negativa konsekvenser för det granskade händelseförloppet.

Lydnad och lojalitet

En sista tematik kring förvaltningskulturen rör hur anställda vid en myndighet ska agera när regelverk och instruktionen från överordnade inte går ihop. I en ideal situation ska det naturligtvis inte uppstå sådana konflikter men ibland är det dock oundvikligt, bl.a. för att regelverk kan tolkas olika.

Utredningen har uppfattat Transportstyrelsen som en relativt hierarkiskt ordnad organisation med klara lydnadsförhållanden mellan de olika nivåerna. Medarbetare på de olika positioner som vi har haft kontakt med har bl.a. gett uttryck för att det är svårt att öppet ifrågasätta beslut som kommer uppifrån. Vi har fått intrycket av en relativt hårt styrd linjeorganisation där lojalitet med verksamheten premieras. Vi har också noterat en attityd med innebörd av en viss ovilja att eskalera frågor till en högre nivå.

När besluten om avsteg togs så ställdes organisationen inför ett dilemma av ovan angett slag. De flesta medarbetarena utgick då, helt naturligt, från att ledningen agerat inom det som var lagligen möjligt och rättade sig därför lojalt efter besluten. Av dokumentation och intervjuer framgår att man uppfattade det som att avstegen gav ”grönt ljus” för något som annars inte hade varit tillåtet. Endast några få medarbetare ifrågasatte detta.

En fråga som inställer sig är varför inte fler medarbetare ifrågasatte besluten om avsteg. Det finns inget enkelt svar på den frågan, men den hierarkiska ledningsstrukturen bidrog sannolikt. Okunskap om regelverket och otydligheten i vad ett ”avsteg” är för något och när sådana kan komma ifråga var också faktorer av betydelse. Att avsteg förekommit tidigare i olika situationer gjorde nog också att medarbetarna inte fick helt klart för sig hur långtgående just dessa beslut var.

Utredningen har kunnat identifiera ytterligare en faktor som kan ha haft inverkan på de anställdas reaktion på avstegen. Det gäller det förhållandet att många av medarbetarna i myndighetens it-avdelning, inklusive avdelningschefen, hade bakgrund i privat sektor. Av uppgifter till utredningen har vi kunnat dra slutsatsen att en viss ”företagskultur” kan ha utvecklats inom avdelningen och att man då delvis tappat det förvaltningsrättsliga perspektivet på verksamheten. Här kan vi bara betona betydelsen av utbildning och information till

anställda som börjar arbeta på en myndighet så att den statliga anställningens särskilda villkor och förutsättningar klargörs.

Till sist vill vi också lyfta fram att vi under granskningen fått bilden att flera medarbetare vid Transportstyrelsen som på ett eller annat sätt deltagit i upphandlingen eller transitionen nu ställer frågor kring sitt eget agerande. Detta kunde myndigheten sannolikt bli bättre på att fånga upp. En del av dem som lojalt följde fattade beslut undrar nu om de gjort något fel. Utredningen vet via intervjuerna att myndigheten gått ut och informerat om möjligheten att få stöd, men det kan tänkas att ett mer uppsökande arbete är nödvändigt för att stödinsatser ska få avsedd verkan.

9.5 Generella slutsatser

I detta avsnitt presenterar utredningen slutsatser avseende några frågor som har generell bäring på de statliga förvaltningsmyndigheterna.

9.5.1 Outsourcing som fenomen i myndighetssfären

Som vi nämner i kapitel 1 är outsourcing i sig inget som måste vara problematiskt för myndigheternas verksamhet. Just it-verksamhet, som ofta är en generisk tjänst med höga krav på tekniskt kunnande och flexibilitet, är ett område där outsourcing kan tyckas naturligt för många myndigheter. Man kan då fokusera på kärnverksamheten och låta moderna marknadslösningar få genomslag vilket både kan bli billigare och bättre. Sett i ljuset av krav på effektivitet och besparingar inom myndighetssfären är det inte konstigt att myndigheter överväger sådana lösningar.

Av vår granskning har framgått att för en framgångsrik outsourcing av denna typ av funktioner förutsätts att myndigheten gjort ett systematiskt arbete med vilka funktioner som man behöver och vilken information som kan tänkas behöva skyddas om utomstående ges tillgång till de tekniska systemen. De brister som vi uppmärksammat när det gäller informationsklassning och säkerhetsmedvetenhet vid Transportstyrelsen är dock inget unikt.

Av granskningar från myndigheter som Riksrevisionen, Myndigheten för samhällsskydd och beredskap och från Statskontoret framgår att många statliga förvaltningsmyndigheter har haft liknande problem genom åren. Det är således vare sig något nytt eller specifikt, utan en utmaning som svenska myndigheter haft under längre tid och som bevisligen fortfarande är en realitet.

Ett till perspektiv på frågan om outsourcing i myndighetssfären gäller myndighetens förmåga att göra en analys av vilka delar av verksamheten som bör outsourcas. I den analysen bör det särskilt uppmärksammas att det numera inte är uteslutet med globala leveranser av avancerade it-tjänster. Det säger sig självt att om vissa centrala delar av de tekniska system som får en svensk myndighet att överhuvudtaget fungera styrs och underhålls från företag i länder långt borta så innebär det vissa risker. Även system som ska vara öppna och tillgängliga och som inte i sig innehåller någon känslig information kan vara av sådan samhällsbetydelse att det inte är lämpligt att kontrollen över dessa ligger någon annanstans än i Sverige.

9.5.2 Informationssäkerhet och förtroende

Bristande informationssäkerhet är som framgått ovan inget nytt problem för svensk statsförvaltning. Myndigheterna tycks, trots att man rimligen är väl medvetna om såväl gällande regelverk som de skyddsvärda intressen som dessa ska garantera, inte vara förmögna att leva upp till de höga krav som ställs på en modern och teknikberoende förvaltning. Vid bedömningen av vilka åtgärder som krävs är det svårt att ge förtroendekostnaderna vid brister i informationshanteringen ett eget värde och dessa frågor hamnar lätt i skymundan. I detta ligger en fara för tilltron till myndigheterna som kanske är allvarligare än de enskilda brister som kan förekomma.

I ljuset av hur vanliga och vitala olika typer av e-tjänster blivit för både medborgare och myndigheter kan nämligen ett bristfälligt hanterande av känslig information – inte minst sådan som rör personuppgifter – göra att medborgarna förlorar en del av sitt förtroende för förvaltningen. Medborgarna skulle t.ex. kunna känna tvekan inför att utnyttja myndigheternas service och tjänster och myndigheterna skulle ha svårigheter att få in information av betydelse för deras uppdrag.

Det ligger inte i vårt uppdrag att föreslå lösningar på sådana allmänna förvaltningspolitiska problem som det här diskuterade. Vi noterar dock att Riksrevisionen 2016 föreslog ett starkare operativt stöd till myndigheterna för att de ska kunna leva upp till kraven på detta område. Det är svårt att inte instämma i den rekommendationen.

9.5.3 Samverkan mellan myndigheter

Vi har i vår granskning kunnat konstatera att Transportstyrelsen levt med vissa organisatoriska uppdelningar som medfört brister i hur bl.a. säkerhetsfrågorna hanterats. Även statsförvaltningen i stort har en del sådana problem och det är något som sedan länge lyfts fram i studier av offentlig sektor.

Lite förenklat kan här skiljas på ett myndighetsperspektiv och ett helhetsperspektiv. Det förra utgår från myndighetens i författning reglerade uppgifter och hanterar frågor om samverkan med andra utifrån om det finns ett utrymme för sådana åtgärder. Det andra har staten som en enda aktör som utgångspunkt och betonar mer myndigheternas gemensamma ansvar för det staten gör. Det finns både nackdelar och fördelar med att myndigheter fokuserar på det som är deras uppgift kontra anlägger ett bredare perspektiv på vad som är statens roll. I praktiken rör det sig om avvägningar mellan dessa ytterligheter.

Svårigheterna i att finna en bra balans mellan de olika perspektiven illustreras i vår granskning av samarbetet mellan Transportstyrelsen och de myndigheter som haft direkta intressen i styrelsens hantering av känsliga uppgifter. Vi har fått en bild av att företrädare för andra myndigheter som oroat sig för Transportstyrelsens agerande inte ansett att det legat i deras uppdrag att formellt föra detta vidare, t.ex. till regeringen.

Det går inte att generellt ange i vilken utsträckning som ett helhetsperspektiv eller ett myndighetsperspektiv är det ”rätta” för ett visst förvaltningsområde eller ett specifikt händelseförlopp. Med utgångspunkt i att vi granskat ett händelseförlopp med konsekvenser för rikets säkerhet anser vi att ett för starkt betonande av varje myndighets avgränsade ansvar är olyckligt. Av utrednings-

materialet tror vi oss kunna utläsa att om fler involverade myndigheter agerat mer proaktivt hade en del av de brister och fel vi identifierat kunnat undvikas.

9.5.4 Styrelser och generaldirektörer

En sista generell slutsats som vi kan dra av granskningen berör frågan om myndighetsledningar och deras inbördes relationer samt regeringens styrning av myndigheter med olika ledningsformer.

Relationen mellan styrelser och generaldirektörer

Vi har, som nämnts ovan, sett att ansvarsfördelningen mellan styrelsen och generaldirektören i praktiken varit ganska oklar och vi menar att detta inte är något som är unikt för Transportstyrelsen. Tvärtom ligger det en inbyggd spänning i en ledningsform där såväl styrelse som generaldirektör utses av regeringen men där den förra ska utöva någon form av kontroll över den senare trots att formella befogenheter för en sådan kontroll saknas. Samtidigt sker regeringens styrning av myndigheten i hög grad via generaldirektören medan det är styrelsen som formellt sett är ansvarig för hela myndighetens verksamhet.

Vår slutsats är att det behövs tämligen ingående och löpande diskussioner mellan styrelsen och generaldirektören om hur ansvarsfördelningen ska se ut såväl principiellt som i praktiken. Alla generella utgångspunkter måste så klart anpassas till skiftande förhållanden, men utan en grundläggande och explicit hållning kan styrelsen inte ta det ansvar som myndighetsförordningen förutsätter.

Styrelsen – bolagsmodell eller intressemodell?

En närliggande fråga rör vad man från statens sida egentligen avser med att ha en styrelse i ledningen för en myndighet. Som redan nämnts är konstruktionen inte entydig och det medför bl.a. konsekvenser för hur styrelseledamöter utses.

Styrelsen kan ses som ett organ som ska representera allmänna intressen och ge viss grundläggande insyn i myndighetens verksamhet. Det skulle kunna kallas för en ”intressemodell”. Å andra sidan kan styrelsen ses som det organ som rent faktiskt utövar det styrande inflytandet över myndigheten och då ställs helt andra krav på ledamöterna. Det skulle kunna kallas för en ”bolagsmodell”.

Mot bakgrund av de oklarheter som ledningsformen medfört i detta granskningsärende – och som vi tror inte är isolerade till Transportstyrelsen – skulle vi förorda att den renodlas efter bolagsmodellen. Styrelsen i en myndighet skulle då inte bara ha det formella utan också det reella ansvaret för myndigheten, något som myndighetsförordningen utgår från. En sådan ordning skulle sannolikt ställa delvis nya krav på hur styrelseledamöter utses.

Självständighet och beroende

Vi har under granskningen reflekterat över varför Transportstyrelsens dåvarande generaldirektör Maria Ågren inte tidigare och tydligare kontaktade regeringen om de problem som uppstått vid myndigheten. Samma reflektion kan gälla andra myndighetschefer som direkt eller indirekt kommit att beröras av händelseförloppet. Vi har inte fått något direkt svar på den frågan annat än intrycket att det ska mycket till innan en generaldirektör vänder sig till regeringen för att få hjälp.

Det är något som i sig kanske inte är så konstigt, eftersom en sådan vädjan kan ses som att man inte klarar av sitt uppdrag och alltså är något som var och en skulle dra sig för att göra. Men vid sidan av sådana mer psykologiska förklaringar kan möjligen en del av den svenska statsförvaltningens särdrag bidra till att försvåra för myndighetscheferna att be om hjälp när det skulle behövas.

Det handlar om att den svenska statsförvaltningen vilar på en långt driven självständighet för myndigheterna i den vardagliga verksamheten, där normen är att myndigheterna är självgående och att regeringen endast ingriper genom formell styrning i de särskilda fall där det behövs. Myndighetscheferna förutsätts alltså klara sina uppdrag utan närmare ledning eller styrning.

Anställningen som generaldirektörer omfattas dessutom av särskilda regler där ett utmärkande drag är att anställningstryggheten är

liten och uppdragen vanligen ges på förordnanden om viss tid. Många generaldirektörer går från mindre uppdrag till större och får på så sätt över tid mer ansvar och högre prestige. Den motsatta rörelsen förekommer också. Det är inte otänkbart att de här faktorerna medverkar till att en generaldirektör kan känna tvekan att kontakta regeringen i fall när han eller hon stöter på problem och att en sådan kontakt därför tas för sent.

Sammanfattningsvis kan konstateras att rollen som myndighetschef ställer höga krav på förmågan att göra korrekta bedömningar om när regeringen ska konsulteras och inte. Det är inte uteslutet att regeringen skulle kunna stödja myndighetscheferna tydligare än idag i dessa avseenden.

9.6 Transportstyrelsen idag – vidtagna åtgärder

Utredningen ska enligt direktiven redovisa vilka eventuella åtgärder som Transportstyrelsen har vidtagit för att säkerställa att myndigheten har rätt kompetens kring it-säkerhet, informationssäkerhet, säkerhetsskydd och offentlig upphandling.

De åtgärder som vidtagits fram till och med den första delen av 2017 framgår av vår tidigare redogörelse. Transportstyrelsen har i en rapport till regeringen den 23 januari 2018 avseende uppdraget att kartlägga hanteringen av vissa uppgifter (kartläggningsuppdraget) gjort en sådan redovisning för 2017. Vi har därför bedömt att det inte är meningsfullt att också vi gör en samlad sådan redogörelse utan istället valt att avsluta vår granskning med att kort ange några iakttagelser angående vad som hänt hösten 2017 som komplettering till den nyss nämnda rapporten.

Läget när det gäller säkerhetskultur i vid mening tycks vara bättre än tidigare. Medarbetare vid myndigheten har dock under våra intervjuer hösten 2017 ändå gett uttryck för en oro att myndigheten ska behandla det inträffade som en olycklig tillfällighet eller en händelse som berott på några enskilda personers misstag snarare än på mer strukturella brister. Mot bakgrund av innehållet i denna rapport utgår utredningen från att så inte blir fallet.

En rekrytering av en säkerhetschef tillika säkerhetsskyddschef och signalskyddschef har inletts för att stärka säkerhetsorganisationen. Tanken enligt nuvarande generaldirektör Jonas

Bjelfvenstam är att denna person ska vara chef för ledningskansliet och de frågor som ligger där: krisberedskap, säkerhetsskydd och totalförsvarsfrågor. Beredning pågick vid intervjun fortfarande av hur andra frågor som skalskydd, informationssäkerhet och strategiska it-säkerhetsfrågor ska hanteras i organisationen. Mot bakgrund av resultaten i denna granskning anser vi att det bör övervägas om inte det mest ändamålsenliga är att samla så mycket som möjligt av säkerhetsfrågorna under ett gemensamt ledarskap.

Vidare kan nämnas att alla medlemmar i myndighetens ledningsgrupp numera är säkerhetsprövade. Ett arbete med att säkerhetspröva styrelsen har också inletts. Nuvarande styrelseordförande Anita Johansson uppger också till utredningen att informationsklassning pågår men att det är en stor uppgift. All information är ännu inte klassad och kommer nog inte heller att bli det i det korta perspektivet.

Utredningen har fått uppgifter av personer på Transportstyrelsen om att behörighetshanteringen ännu inte är helt åtgärdad. Det ska fortfarande vara personal på IBM som styr it-miljön och som kan lägga till och ta bort användare inklusive andra leverantörer. Denna bild bekräftas delvis av Säkerhetspolisen som uppger att de påpekat till Transportstyrelsen vid ett flertal tillfällen under uppföljningen av tillsynen att myndigheten behöver återkalla vissa behörigheter från IBM.

Sammanfattningsvis kan noteras att det vidtagits en mängd åtgärder vid Transportstyrelsen med anledning av det granskade händelseförloppet. Det återstår dock ett arbete innan hanteringen av hemliga och annars skyddsvärda uppgifter når en tillfredsställande nivå.

Uppdrag att granska Transportstyrelsens upphandling av it-drift

Regeringens beslut

Regeringen beslutar att en utredare ska granska den upphandling rörande förändrad it-drift hos Transportstyrelsen som har medfört att säkerhetskänslig och av andra skäl sekretessbelagd information har hanterats på ett sätt som strider mot svensk lag.

I uppdraget ligger att:

- Undersöka hur och varför Transportstyrelsen initierade processen att upphandla myndighetens it-drift samt vilken analys och vilka överväganden som låg till grund för myndighetens agerande. I detta ingår att klargöra beslutsordningen inför beslut att inleda upphandling, val av upphandlingsförfarande och val av potentiella leverantörer.
- Kartlägga processen från det att Transportstyrelsen beslutade att påbörja arbetet med en förändrad it-drift och it-organisation fram till i dag. Därvid ska viktiga tidpunkter, gjorda vägval, beslut som fattats på olika nivåer inom myndigheten och information som lämnats till Regeringskansliet redovisas.
- Redovisa vilka alternativ som utreddes och vilka analyser och bedömningar av konsekvenser och risker som gjordes vid olika tidpunkter under processen samt vilka typer av interna och eventuellt externa kompetenser och specialistroller som bidrog till dessa.

– Undersöka säkerhetskulturen inom Transportstyrelsen med avseende på risker med relevans för den aktuella upphandlingsprocessen. I det ligger att undersöka relevanta interna rutiner och riktlinjer samt organisationens gemensamma förhållningssätt, prioriteringar och agerande.
– Bedöma vilka åtgärder som hade kunnat vidtas för att undvika att skyddsvärd information kunde komma att hanteras felaktigt samt vilka roller och kompetenser som deltog eller saknades vid viktiga analyser och beslut.
– Redovisa vilka eventuella åtgärder som Transportstyrelsen har vidtagit för att säkerställa att myndigheten har nödvändig kompetens kring it-säkerhet, informationssäkerhet, säkerhetsskydd och offentlig upphandling.
– Utifrån granskningen redogöra för vilka lärdomar som kan dras av den aktuella upphandlingen.

Transportstyrelsen och Trafikverket ska bistå utredaren med de uppgifter som behövs för genomförandet av uppdraget.

Utredaren ska samråda med Datainspektionen, Myndigheten för samhällsskydd och beredskap, Säkerhetspolisen och Upphandlingsmyndigheten.

Uppdraget ska redovisas till Regeringskansliet (Näringsdepartementet) senast den 31 januari 2018.

Skälen för regeringens beslut

Enligt förordningen (2008:1300) med instruktion för Transportstyrelsen har myndigheten till huvuduppgift att svara för regelgivning, tillståndsprövning och tillsyn inom transportområdet. Transportstyrelsen ansvarar även för de register som behövs för att utöva denna verksamhet samt vissa uppgifter som föranleds av registerhållningsverksamheten.

Transportstyrelsen bildades den 1 januari 2009 och övertog då verksamhet från flera befintliga myndigheter, i första hand Vägverket,

Järnvägsstyrelsen, Luftfartsstyrelsen och Sjöfartsverket, bl.a. innefattande it-baserade register. Det mest omfattande registret som övertogs var vägtrafikregistret som övertogs från Vägverket. Efter Transportstyrelsens bildande skötte Vägverket, sedermera Trafikverket, it-driften av såväl vägtrafikregistersystemet som Transportstyrelsens övriga it-system.

Transportstyrelsen har beslutat att upphandla driften av myndighetens it-system av en privat extern aktör. I april 2015 tecknade Transportstyrelsen ett avtal som innebär att IBM Svenska AB ansvarar för att maskinvara, nätverk och program fungerar. IBM Svenska AB övertog driftsansvaret den 1 november 2015.

Med anledning av vissa beslut som Transportstyrelsens dåvarande ledning fattade vid upphandlingen har Säkerhetspolisen genomfört en förundersökning avseende vårdslöshet med hemlig uppgift. Transportstyrelsens dåvarande generaldirektör har enligt ett av henne godkänt strafföreläggande gjort sig skyldig till vårdslöshet med hemlig uppgift.

Med anledning av de uppgifter som har framkommit kring Transportstyrelsens it-upphandling finns det starka skäl för att kartlägga och analysera den upphandling som medfört att myndighetens ledning har fattat beslut som strider mot svensk lag.

Förteckning över intervjuade personer

Namn	Befattning
Tobias Ander	Informationssäkerhetsansvarig (nuvarande)
Rolf Annerberg	F.d. styrelseordförande (2015–2017)
Jonas Bjelfvenstam	Generaldirektör (nuvarande)
Jesper Bjärvall	Projektägare (2015–2017)
Jaana Elo	Personaldirektör (nuvarande)
Jan Engblom	Projektägare och partneransvarig vid it-avdelningen (2014–2017)
Johan Eriksson	F.d. it-säkerhetsansvarig (2013–2017)
Pär-Anders Fredriksson	Leveransansvarig mot IBM, f.d. enhetschef för drift- och infrastrukturenheten (2015)
Jacob Gramenius	F.d. stf. generaldirektör (2011–2017)
Carola Gunnarsson	F.d. styrelseordförande (2010–2014)
David Heed	It-säkerhetsansvarig (nuvarande)
Jens Johanson	Säkerhetsskyddschef (nuvarande)
Anita Johansson	Styrelseordförande (nuvarande)
Daniel Karlsson	F.d. it-direktör (2011–2017)
Michael Karlsson	Konsult, it-avdelningen
Gunnar Malm	F.d. generaldirektör Trafikverket (2010-2015)
Anders Månbrant	F.d. enhetschef för drift- och infrastrukturenheten (2012–2014)
Kristina Nilsson	Chefsjurist (nuvarande)
Annette Olofsson	Internrevisionschef (nuvarande)
Kristina Portugués	Enhetschef för inköpsenheten (nuvarande)
Mats Ringqvist	Ekonomidirektör (nuvarande)

Anders Wester	Chef för it-drift och applikationsutveckling, Trafikverket
Staffan Widlert	F.d. generaldirektör (2009–2015)
Maria Ågren	F.d. generaldirektör (2015–2017)
Sari Fröjd Åström	F.d. enhetschef för enheten för paketerade tjänster (2011–2017)
Per Ängmo	F.d. enhetschef för GD-stab (2014–2017)

Departementsserien 2018

Kronologisk förteckning

1. Genomförande av 2017 års ändringsdirektiv till EU:s vapendirektiv. Ju.
2. Reglering av mikrosimuleringsmodellen Fasit. Fi.
3. Uppbörd av böter efter EU:s dataskyddsreform. Ju.
4. En ny stödordning för säkerhetshöjande åtgärder inom det civila samhället. Ku.
5. Ny lag om koordineringsinsatser inom hälso- och sjukvården. S.
6. Granskning av Transportstyrelsens upphandling av it-drift. N.

Departementsserien 2018

Systematisk förteckning