

Betrodda exekveringsmiljöer för uppkopplade fordon

Slutrapport från IMY:s innovationssandlåda för dataskydd

Diarienummer
IMY-2026-5444

Datum
2026-03-30



Om innovationssandlådan

IMY:s innovationssandlåda för dataskydd är en form av fördjupad vägledning där IMY, i nära dialog med deltagande aktörer, utforskar hur dataskyddsreglerna ska tolkas och tillämpas i praktiken. Syftet är att göra det enklare att utveckla innovativa och integritetssäkra tekniska lösningar.

I innovationssandlådan får offentliga och privata aktörer vägledning genom en serie workshops tillsammans med våra specialister inom juridik, teknik och informations- och cybersäkerhet. Vi prövar dataskyddsrättsliga frågor i tydligt avgränsade projekt, vilket ger oss möjlighet att analysera specifika utmaningar på djupet. Sandlådan innebär dock inte några undantag från dataskyddsreglerna. För att fler ska kunna ta del av projektens frågor, överväganden och slutsatser sammanfattas insikterna i en rapport.

Deltagare i innovationssandlådan väljs ut genom en öppen intresseanmälan, där projekt med samhällsnytta, innovationshöjd och behov av vägledning prioriteras. På så sätt bidrar innovationssandlådan till ökad kunskap om hur dataskyddsreglerna kan tillämpas i takt med den tekniska utvecklingen – och därmed till svensk innovation och konkurrenskraft.



Innehållsförteckning

Om innovationssandlådan	2
Ordlista	4
1. Sammanfattning.....	5
1.1. Användning av betrodda exekveringsmiljöer.....	5
1.2. Slutsatser	5
2. Projektet.....	7
2.1. Bakgrund	7
2.2. Projektets mål.....	7
2.3. Deltagarna i projektet	7
2.4. Tekniken.....	8
2.5. Integritetsfrämjande tekniker	8
2.6. Dataskyddsfrågor	9
2.7. Avgränsningar	9
3. Vilka säkerhetsåtgärder kan vara lämpliga vid användning av betrodda exekveringsmiljöer?	10
3.1. Säkerhetsåtgärder och GDPR.....	10
3.2. Säkerhet vid användning av betrodda exekveringsmiljöer	10
3.3. Implementeringen av tekniken i det aktuella projektet	11
4. Är GDPR tillämplig på behandlingen?.....	15
4.1. Behandling enligt GDPR	15
5. Vilken roll enligt GDPR får tillhandahållaren av en betrodd exekveringsmiljö?..	17
5.1. Ansvarsroller enligt GDPR	17
5.2. Är tillhandahållaren personuppgiftsansvarig eller gemensamt personuppgiftsansvarig?	17
5.3. Är tillhandahållaren ett personuppgiftsbiträde?	18
6. Övriga reflektioner	23
7. Fördjupning	24

Ordlista

Användare	Den part som låter föra in och bearbetar data i en betrodd exekveringsmiljö. Användaren äger eller kontrollerar de data som ska behandlas. I detta projekt är användaren Volvo.
Betrodd exekveringsmiljö	En hårdvarubaserad, isolerad och kryptografiskt skyddad bearbetningsmiljö inom en processor som är avsedd att möjliggöra skydd av data under användning genom att utföra beräkningar i en tekniskt avgränsad och attestkontrollerad miljö. Den engelska benämningen för tekniken är "Trusted Execution Environment, TEE".
Deltagarna	CanaryBit, Ericsson och Volvo Group
EDPB	Europeiska dataskyddsstyrelsen (eng. <i>European Data Protection Board</i>)
GDPR	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning). "GDPR" är en förkortning av det engelska namnet "General Data Protection Regulation".
IMY	Integritetsskyddsmyndigheten
Kontrollantfunktion	Den part som verifierar exekveringsmiljöns integritet genom attestering och säkerställer att endast auktoriserad kod och godkända data förs in och bearbetas i miljön. I detta projekt avser Volvo att själva kontrollera denna funktion.
Tillhandahållare	Den part som tillhandahåller den tekniska tjänsten och beräkningskraften för exekveringsmiljön. I detta projekt är tillhandahållaren tänkt att vara en mobiloperatör.

1. Sammanfattning

1.1. Användning av betrodda exekveringsmiljöer

I det aktuella projektet har IMY tillsammans med deltagarna analyserat hur betrodda exekveringsmiljöer kan användas för att skydda information som behandlas utanför ett fordonets lokala datormiljö. Inom ramen för projektet avser Volvo Group (Volvo) att samla in data via kameror och sensorer som finns installerade i Volvos lastbilar. Dessa data ska överföras till och bearbetas i en betrodd exekveringsmiljö. Miljön tillhandahålls av en mobiloperatör som en teknisk tjänst inom dess infrastruktur.

Överföringen och bearbetningen i exekveringsmiljön är nödvändig eftersom fordonens egen beräkningskapacitet är begränsad och inte räcker till för att behandla all data lokalt i fordonet. Behandlingen kan omfatta personuppgifter, främst i form av videomaterial där trafikanter förekommer. Den betrodda exekveringsmiljön upprättas genom funktionaliteter som tillhandahålls av Ericsson och CanaryBit.

Syftet med behandlingen är att möjliggöra extern databehandling, det vill säga behandling som sker utanför fordonet, med en säkerhetsnivå som motsvarar den som skulle ha upprätthållits vid lokal behandling i fordonets egna system. Projektet har särskilt belyst hur betrodda exekveringsmiljöer kan bidra till ökad säkerhet och kontroll över data under användning i jämförelse med mer traditionella lösningar, såsom konventionella molntjänster.

De frågor som IMY har undersökt i projektet är vilka säkerhetsåtgärder som kan vara lämpliga vid användning av betrodda exekveringsmiljöer, om GDPR är tillämplig på behandlingen i projektet och vilken eventuell roll enligt GDPR som tillhandahållaren av en betrodd exekveringsmiljö får.

1.2. Slutsatser

Vilka säkerhetsåtgärder kan vara lämpliga vid användning av betrodda exekveringsmiljöer?

IMY framhåller att betrodda exekveringsmiljöer kan bidra till att minska de risker som är förknippade med extern behandling av personuppgifter, till exempel risken för obehörig eller oavsiktlig åtkomst. Tekniken kan därmed utgöra en skyddsåtgärd som stärker den personuppgiftsansvariges faktiska kontroll över säkerheten för data under användning. I jämförelse med konventionella molnlösningar, där tilliten i högre grad bygger på avtalsmässiga åtaganden, möjliggör betrodda exekveringsmiljöer en tekniskt verifierbar kontroll över den miljö där data bearbetas. Genom inbyggda skyddsmekanismer kontrolleras både åtkomsten till data och vilken kod som får exekveras, vilket stärker förtroendet för tillhandahållaren av tekniken. I det aktuella projektet har särskild vikt lagts vid att nyckelhanteringen och kontrollantfunktionen för den betrodda exekveringsmiljön hanteras av den personuppgiftsansvarige. Kontrollantfunktionen utför attesteringar av miljön, vilket ger tekniska bevis på att den är säker och kör rätt programkod.

Är GDPR tillämplig på behandlingen?

IMY utgår från att personuppgifter kommer att behandlas i det tilltänkta projektet, till exempel när individer fångas på videoinspelningar av Volvos lastbilars kameror. IMY bedömer att de olika stegen i processen, från det att uppgifter samlas in, till att de överförs och bearbetas i den betrodda exekveringsmiljön, typiskt sett är behandling av

den personuppgiftsansvarige enligt artikel 4.2 i GDPR. Då uppgifterna behandlas automatiserat av Volvo, omfattas behandlingen som av GDPR:s bestämmelser.

Vilken roll enligt GDPR får tillhandahållaren av en betrodd exekveringsmiljö?

Enligt IMY finns det omständigheter i det aktuella fallet som talar för att mobiloperatören, som tillhandahåller beräkningskraft och den tekniska tjänsten för miljön, inte är att betrakta som vare sig ensamt eller gemensamt personuppgiftsansvarig för behandlingen. I många kommersiella tjänster som erbjuder betrodda exekveringsmiljöer eller liknande molnbaserade lösningar är tillhandahållaren typiskt sett att betrakta som personuppgiftsbiträde. I det aktuella projektet finns dock omständigheter som talar emot personuppgiftsbiträdesansvar. Särskilt betydelsefullt är kontrollantfunktionens placering inom den personuppgiftsansvariges kontrollsfär, liksom mobiloperatörens mycket begränsade möjligheter att vidta åtgärder för att efterleva skyldigheter som personuppgiftsbiträde, exempelvis att säkerställa skyddet för registrerades rättigheter. För att en sådan bedömning ska kunna upprätthållas i praktiken behöver besluten om väsentliga medel för behandlingen i form av skyddsåtgärder och kontroll över data som behandlas i den betrodda exekveringsmiljön vila hos den personuppgiftsansvarige. Denne måste också kunna visa att de åtgärder som ska hindra mobiloperatören från att ta del av innehållet är effektiva och fungerar i praktiken.

2. Projektet

2.1. Bakgrund

Inom databehandling görs ofta en åtskillnad mellan tre tillstånd för data: under överföring (eng. *in transit*), vid lagring (eng. *at rest*) och under bearbetning (eng. *in use*). Kryptering och andra liknande skyddsmekanismer är idag väl etablerade för data som överförs och lagras.

I dagens digitala samhälle hanteras stora mängder information som ofta är känslig till sin natur, allt från särskilt skyddsvärda personuppgifter till säkerhetsinställningar och platsinformation. Behovet av att skydda information genom hela dess livscykel har därför blivit alltmer angeläget.

Även om skyddsmekanismer för data under överföring och lagring är väl etablerade kvarstår betydande utmaningar när det gäller att skydda data under användning. För att kunna bearbetas måste data normalt vara tillgänglig i ett okrypterat tillstånd, vilket innebär en ökad sårbarhet. Skydd av data under användning är därmed ett centralt och komplext område inom modern informationssäkerhet.

En av de tekniker som har utvecklats för att möta utmaningen att skydda data under användning är betrodda exekveringsmiljöer (eng. *Trusted Execution Environments, TEE*). En betrodd exekveringsmiljö kan beskrivas som ett särskilt skyddat beräkningsutrymme i en processor där information kan behandlas isolerat från resten av systemet. Endast i förväg godkänd och auktoriserad kod kan köras och få åtkomst till data som behandlas i exekveringsmiljön. Data som bearbetas i miljön är dessutom krypterade för andra utanför miljön, vilket gör det mycket svårt att kunna läsa eller manipulera innehållet även vid fysisk åtkomst eller via systemgränssnitt till enheten.

2.2. Projektets mål

Målet med projektet är att utreda hur betrodda exekveringsmiljöer kan användas för att möjliggöra säker behandling av data i situationer där beräkningskraft på en lokal enhet inte räcker till. Genom att använda betrodda exekveringsmiljöer kan databehandling utföras hos annan part utan att mobiloperatören som tillhandahåller beräkningskraften och den tekniska tjänsten för miljön faktiskt får åtkomst till data som behandlas i den. Behandlingen kan därför ske utanför den lokala datormiljön hos en extern leverantör, men skyddas som om data hade behandlats i den lokala miljön.

2.3. Deltagarna i projektet

CanaryBit är ett företag som utvecklar lösningar för säker databehandling. I projektet bistår CanaryBit med kod som används för att kunna starta upp och köra en betrodd exekveringsmiljö.

Ericsson är en leverantör inom informations- och kommunikationsteknologi och tillhandahåller tillsammans med CanaryBit den mjukvara och de funktionaliteter som krävs för driften av den betrodda exekveringsmiljön i projektet, främst i form av programvara och en kontrollantfunktion.

Volvo Group är en global fordonstillverkare och har ett brett utbud av uppkopplade tjänster. Inom ramen för projektet kommer de data som Volvos lastbilar samlar in att överföras och bearbetas i en betrodd exekveringsmiljö.

2.4. Tekniken

En betrodd exekveringsmiljö är ett skyddat område i en processor där programkod kan köras och data kan bearbetas i ett separat och skyddat minnesutrymme. Miljön är isolerad från resten av systemet och skyddas av såväl hårdvaruisolering som kryptering. Syftet är att säkerställa skydd för information även i situationer där operativsystemet eller andra delar av systemet skulle komprometteras.

Tekniskt skapas en betrodd exekveringsmiljö genom särskilda säkerhetsfunktioner i processorns hårdvara. Dessa funktioner gör det möjligt att isolera viss kod och data från övriga delar av systemet. Den kod som körs utanför den betrodda miljön saknar åtkomst till den information som behandlas i miljön och kan därför inte läsa, ändra eller manipulera den. Systemet delas på så sätt upp i två typer av miljöer: en ordinarie miljö där operativsystem och vanliga applikationer körs, och en eller flera isolerade exekveringsmiljöer där endast särskilt godkänd kod får exekveras och behandla den skyddade informationen.

En viktig funktion i betrodda exekveringsmiljöer är attestering. Det innebär att exekveringsmiljön kan skapa ett kryptografiskt bevis för vilket tillstånd miljön befinner sig i och vilken kod som körs i den. En särskild kontrollantfunktion kan använda detta bevis för att verifiera att miljön uppfyller fördefinierade säkerhetskrav innan data tillåts att behandlas i miljön.

I praktiken skickas data till exekveringsmiljön i krypterad form och avkrypteras först när de tas emot i den isolerade miljön där bearbetningen sker. Eftersom skyddet upprätthålls genom processorns hårdvara, och inte enbart av operativsystemet, kan informationen förbli skyddad även om andra delar av systemet inte är betrodda.

2.5. Integritetsfrämjande tekniker

Integritetsfrämjande tekniker (eng. *Privacy Enhancing Technologies, PET*) är ett samlingsbegrepp för tekniska lösningar som är utformade för att skydda individers personliga integritet. Ur ett dataskyddsperspektiv kan integritetsfrämjande tekniker bidra till att stärka skyddet för personuppgifter vid behandling, exempelvis genom att begränsa exponeringen av personuppgifter eller förhindra onödig eller oönskad behandling av personuppgifter.¹

Betrodda exekveringsmiljöer är en typ av integritetsfrämjande teknik. Säkerheten i dessa miljöer bygger på ett antal säkerhetsmekanismer som är inneboende i den underliggande tekniska arkitekturen, såsom isolering, åtkomstbegränsning och kryptografiska skyddsmekanismer. Dessa mekanismer bidrar till att dataskydd integreras i systemets utformning och kan därmed utgöra ett exempel på hur principen om inbyggt dataskydd kan realiseras i praktiken.²

Användningen av betrodda exekveringsmiljöer har ökat under det senaste decenniet och förekommer numera i exempelvis mobiltelefoner för att skydda biometriska data, i betaltjänster och i digitala identiteter.³ I molntjänster kan exekveringslösningar användas för att möjliggöra säker bearbetning av information utan att molnoperatören själv får insyn i användardata. Industriella processer, IoT-enheter och kantbaserade system

¹ För vidare läsning, se exempelvis ENISA, Data Protection Engineering – From Theory to Practice, och OECD, Emerging Privacy Enhancing Technologies: Current Regulatory and Policy Approaches.

² Artikel 25.1 GDPR.

³ Europeiska datatillsynsmannen, (eng. *European Data Protection Supervisor, EDPS*), Tech Sonar Report 2025–2026, s. 24 ff.

använder också säkra exekveringsmiljöer för att skapa tillit i distribuerade miljöer där flera parter interagerar utan att behöva ha full förtroende för varandra.

2.6. Dataskyddsfrågor

Deltagarna enades tillsammans med IMY om att fokusera på följande dataskyddsfrågor i det aktuella projektet:

- Vilka säkerhetsåtgärder kan vara lämpliga vid användning av betrodda exekveringsmiljöer?
- Är GDPR tillämplig på behandlingen?
- Vilken roll enligt GDPR får tillhandahållaren av en betrodd exekveringsmiljö?

2.7. Avgränsningar

I denna rapport analyseras endast behandlingen av personuppgifter från det att uppgifterna samlas in till att de överförs och bearbetas i en betrodd exekveringsmiljö. Det bör noteras att den aktuella tjänsten inte är i drift.

Denna rapport innehåller en redogörelse för IMY:s uppfattning i rättsliga frågor där det finns behov av vägledning. Bedömningarna görs mot bakgrund av nuvarande rättsläge och kan komma att ändras om det skulle komma ny lagstiftning, domstolspraxis eller vägledning från EDPB.⁴

Vägledningen i projektet har fokuserat på tre dataskyddsrättsliga frågeställningar. Utöver dessa frågeställningar finns också andra juridiska frågor som deltagarna behöver beakta innan projektet kan driftsättas, men som inte har analyserats inom ramen för detta projekt.

⁴ Läs mer om EDPB på IMY:s webbplats (<https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-eu-niva/edpb/>).

3. Vilka säkerhetsåtgärder kan vara lämpliga vid användning av betrodda exekveringsmiljöer?

3.1. Säkerhetsåtgärder och GDPR

Enligt artikel 32 GDPR ska personuppgiftsansvariga och personuppgiftsbiträden vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är adekvat i förhållande till de risker som behandlingen av personuppgifter innebär för enskildas fri- och rättigheter. Bestämmelsen bygger på en riskbaserad metod och kräver att aktörerna bland annat beaktar behandlingens art, omfattning, sammanhang och ändamål samt den tekniska utvecklingen. I detta sammanhang utgör användningen av integritetsfrämjande tekniker ett centralt verktyg för att uppfylla kraven i artikel 32, eftersom de syftar till att minimera exponeringen av personuppgifter och reducera risken för obehörig åtkomst. Korrekt implementerade kan integritetsfrämjande tekniker bidra till att skydda personuppgifter under hela livscykeln.

En betrodd exekveringsmiljö kan i sig betraktas som en särskilt relevant teknisk säkerhetsåtgärd eftersom den möjliggör isolerad och skyddad behandling av information även i miljöer där den underliggande infrastrukturen inte fullt ut kan anses vara betrodd.⁵ Betrodda exekveringsmiljöer kan implementeras i lokala enheter men också distribueras som molntjänst, där det är möjligt för kunder att köra beräkningar utan att behöva hantera den underliggande hårdvaran. Betrodda exekveringsmiljöer är en av flera integritetsfrämjande tekniker som kan användas för att skydda data under tiden de behandlas. Detta avsnitt beskriver centrala säkerhetsaspekter vid användning av betrodda exekveringsmiljöer, samt vilka åtgärder som kan vidtas för att skydda data, till exempel personuppgifter, som behandlas i sådana miljöer.

3.2. Säkerhet vid användning av betrodda exekveringsmiljöer

Säkerheten i betrodda exekveringsmiljöer bygger på ett antal säkerhetsmekanismer som är inneboende i den underliggande tekniska arkitekturen. Dessa mekanismer är grundläggande för hur betrodda exekveringsmiljöer är konstruerade och återfinns i varierande grad i olika implementationer av tekniken. Tillsammans möjliggör de ett tekniskt verifierbart skydd för data under användning. Nedan redogörs för några av de centrala mekanismer som generellt kännetecknar betrodda exekveringsmiljöer.

3.2.1. Isolering

En central egenskap hos betrodda exekveringsmiljöer är den tekniska isoleringen. Det innebär att data som bearbetas i miljön hålls åtskilda från övriga delar av systemet och inte kan nås av exempelvis driftleverantörer som tillhandahåller den underliggande infrastrukturen för miljön. Under överföring är data krypterade och avkrypteras endast inne i den isolerade miljön när de bearbetas. Kombinationen av isolering och kryptering innebär att data skyddas både under överföring och under själva bearbetningen. Ur ett dataskyddsperspektiv stärker detta konfidentialiteten och minskar risken för obehörig åtkomst, även om den omgivande infrastrukturen skulle komprometteras.

⁵ Se avsnitt 2.4. För vidare läsning, se också till exempel ANSSI, Technical Position Paper on Confidential Computing, s. 2 ff och EDPS, TechSonar Report 2025–2026 s. 24 ff.

3.2.2. Attestering

För att en användare ska kunna lita på att miljön ger det skydd som utlovas krävs verifierbarhet. Det innebär möjlighet att kontrollera att behandlingen sker i en äkta betrodd miljö, att rätt programvara används och att miljön inte har manipulerats eller komprometterats. Verifierbarheten kopplad till betrodda exekveringsmiljöer uppnås genom attesting. Attesting är en teknisk och kryptografisk process där exekveringsmiljön skapar ett bevis på sitt aktuella tillstånd. Beviset kan innehålla information om vilken kod som körs, vilka säkerhetsinställningar som gäller och om miljön befinner sig i ett betrott och oförändrat tillstånd. Detta bevis kan sedan verifieras av en särskild kontrollfunktion som kontrollerar att miljön uppfyller de förutbestämda villkoren innan data tillåts behandlas.

Till skillnad från traditionella molntjänster, där säkerheten i stor utsträckning bygger på avtal, policyer och leverantörens egna försäkringar, ger attesting ett tekniskt bevis på att miljön är i det skick som avsetts. Det är särskilt centralt när exekveringsmiljön tillhandahålls av en extern aktör och användaren inte själv har fysisk kontroll över hårdvaran och infrastrukturen.

3.2.3. Momentan och tillståndsberoende miljö

En central, men ofta mindre synlig, säkerhetsegenskap hos betrodda exekveringsmiljöer är att de är tillfälliga och strikt beroende av ett godkänt tillstånd. Det innebär att miljön endast existerar så länge den befinner sig i ett tillstånd där rätt programkod körs, där detta kan verifieras kryptografiskt och där endast behöriga komponenter har tillgång till miljön. Om detta tillstånd bryts, till exempel vid försök att köra icke-auktoriserad kod eller om underliggande säkerhetskrav inte längre uppfylls, upphör miljön omedelbart att existera. Vid en sådan nedstängning raderas all information som finns i miljön och inga data lämnar miljön i klartext. Denna mekanism kan liknas vid ett självdestruerande kassaskåp. Så länge rätt kombination används och ingen manipulation upptäcks hålls innehållet tillgängligt, men vid minsta avvikelse i miljöns konfiguration eller kodbas misslyckas attesting och kassaskåpet upphör att fungera, och innehållet förstörs.

Ur ett integritets- och säkerhetsperspektiv är detta särskilt betydelsefullt. I traditionella system kan ett intrång innebära att en angripare får möjlighet att gradvis kartlägga systemet, läsa av arbetsminne eller analysera processer över tid. I en betrodd exekveringsmiljö är både angreppsytan mer begränsad och tidsfönstret för exploatering betydligt snävare, eftersom miljön är konstruerad för att upphöra under icke-verifierbara förhållanden.

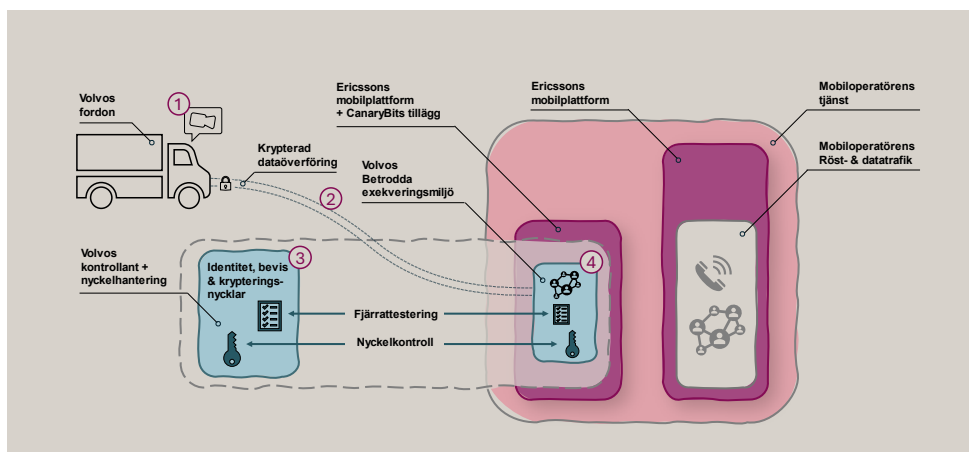
Sammantaget bidrar flera av de säkerhetsegenskaper som kännetecknar en betrodd exekveringsmiljö till att data kan behandlas under mer kontrollerade och tekniskt verifierbara former jämfört med exempelvis traditionella molnmiljöer. Teknikens bidrag till säkerheten är därutöver beroende av hur den integreras och konfigureras i den aktuella behandlingen.

3.3. Implementeringen av tekniken i det aktuella projektet

I projektet behandlas data som genereras av Volvos fordon i betrodda exekveringsmiljöer. För varje lastbil etableras en separat och unik exekveringsmiljö, som är aktiv så länge villkoren för miljön är uppfyllda. Mobiloperatören är tänkt att bistå med den tekniska tjänsten och beräkningskraften som behövs för att tillhandahålla den betrodda exekveringsmiljön. CanaryBit och Ericsson ansvarar för att tillhandahålla de

funktionaliteter, främst i form av programvara och en kontrollantfunktion, som krävs för att starta upp och köra miljön. All data i den betrodda exekveringsmiljön är krypterade vid överföringen till exekveringsmiljön och avkrypteras endast inne i miljön. Det innebär att mobiloperatören som tillhandahåller tjänsten för den betrodda miljön aldrig har eller kan bereda sig tillgång till innehållet.

Sammanfattningsvis är den planerade användningen av den betrodda exekveringsmiljön i projektet följande:



1. Volvo överför bland annat videoströmmar och positioneringsdata från lastbilens kameror och sensorer för behandling.
2. Data skickas över mobilnätet, via en krypterad uppkoppling, till en betrodd exekveringsmiljö som skapas unikt för varje fordon. En mobiloperatör tillhandahåller den tekniska tjänsten och beräkningskraften för den betrodda exekveringsmiljön, vilken är en del av mobilplattformen som levereras av Ericsson och CanaryBit.
3. Innan data kan överföras till och bearbetas i den betrodda miljön måste på förhand fastställda säkerhetsvillkor vara uppfyllda. Genom kryptografiskt baserad nyckelhantering verifieras först identitet och behörighet för lastbilens miljö. Därefter kontrolleras att exekveringsmiljön befinner sig i ett betrott och oförändrat tillstånd genom attestering. Kontrollantfunktionen säkerställer att endast auktoriserad kod och godkända data får bearbetas i miljön.
4. Först därefter kan överförda data avkrypteras och bearbetas i den betrodda miljön. Data som behandlas i miljön är skyddade från alla övriga funktioner i operativsystemet och programvaror.

När data inte längre behöver bearbetas i den betrodda miljön stängs den ner och upplöses. Den betrodda miljön stängs också ned omedelbart om en attestering inte uppfyller de förutbestämda villkoren som kontrollantfunktionen jämför med.

Den aktuella implementeringen i projektet skiljer sig från mer konventionella och kommersiella implementationer av betrodda exekveringsmiljöer i två avseenden, nämligen genom införandet av en egenstyrd kontrollantfunktion och nyckelhantering som ligger helt hos användaren av miljön. Detta har också haft särskild betydelse för IMY:s bedömning av de rättsliga frågor som är aktuella i projektet.

3.3.1. Egenstyrd eller oberoende kontrollant

En central skillnad jämfört med många generiska, molnbaserade implementationer av betrodda exekveringsmiljöer är att deltagarna i projektet avser att införa en egenstyrd kontrollantfunktion som verifierar exekveringsmiljöns integritet. I konventionella molnarkitekturer är det vanligt att molnleverantören både är infrastrukturägare och den instans som utfärdar attesteringar. Det innebär att användaren av miljön i hög grad måste förlita sig på leverantörens egna löften och säkerhetsgarantier. Den funktion som verifierar miljöns tillstånd är därmed inte organisatoriskt eller funktionellt oberoende av den aktör som driver infrastrukturen.

I det aktuella projektet ligger kontrollen i högre grad hos användaren av den betrodda exekveringsmiljön. Volvo styr och ansvarar för kontrollantfunktionen genom att fastställa vilka krav som ska uppfyllas för att en attestering ska anses giltig, exempelvis vilka komponenter som ska verifieras, vilken programkod som får köras i miljön och vilka säkerhetskfigurationer som krävs. Mobiloperatören tillhandahåller i denna modell enbart den underliggande infrastrukturen, såsom hårdvara, beräkningskapacitet och nätverksresurser, men saknar möjlighet att självständigt godkänna eller påverka attesteringen av exekveringsmiljön.

Kontrollantfunktionen kan även organiseras genom en oberoende tredje part som tillhandahåller den tekniska funktionaliteten för attestering. En sådan lösning kan ytterligare stärka funktionens oberoende och bidra till en tydligare åtskillnad mellan den aktör som tillhandahåller infrastrukturen och den som verifierar att behandlingen sker i en betrodd miljö.

Kontrollantfunktionen utför kryptografiska attesteringar av den betrodda miljön innan data låses in och bearbetas, vilket ger tekniskt bevis på att miljön verkligen är säker och kör rätt programkod. Frekvensen av attesteringen spelar en viktig roll för säkerhetsnivån. Ju tätare attesteringar, desto snabbare kan eventuella avvikelser i systemets integritet identifieras. Genom den egenstyrda kontrollantfunktionen i projektet minskar potentiella intressekonflikter avsevärt, eftersom ingen enskild aktör kan äventyra plattformen utan att det syns i attesteringen. På så vis behöver användaren av den betrodda miljön inte enbart förlita sig på avtal eller leverantörsgarantier, utan kan genom kontrollantfunktionen verifiera hela kedjan av hårdvara och mjukvara.

3.3.2. Nyckelhantering

I traditionella molntjänster hanteras ofta kryptografiska nycklar antingen av molnleverantören eller av användaren själv, vilket kan leda till sårbarheter om nycklarna exponeras eller om leverantören har teknisk möjlighet att komma åt dem. Projektets lösning implementerar istället en modell där användaren behåller kontrollen över huvudnycklarna genom att ansvara för att nycklar endast släpps in i exekveringsmiljön efter lyckad attestering. Nycklarna binds dessutom kryptografiskt till miljöns specifika tillstånd, vilket förhindrar att de kan användas i en komprometterad eller felkonfigurerad miljö. Denna modell minimerar alltså risken för nyckelläckage och säkerställer att användaren behåller kontroll över sina data.

3.3.3. IMY:s kommentar

Mot bakgrund av ovanstående redogörelse kan användningen av betrodda exekveringsmiljöer utgöra en teknisk skyddsåtgärd som stärker den personuppgiftsansvariges faktiska kontroll över säkerheten för data under användning. I jämförelse med

konventionella molnlösningar, där tilliten i hög grad bygger på avtalsmässiga åtaganden, möjliggör betrodda exekveringsmiljöer en tekniskt verifierbar kontroll över den miljö där data faktiskt bearbetas.

En central komponent för att uppnå denna kontroll är möjligheten till teknisk verifiering genom attestering. I det aktuella projektet sker denna verifiering genom en egenstyrd kontrollantfunktion som kontinuerligt granskar exekveringsmiljöns tillstånd och säkerställer att den uppfyller fördefinierade säkerhetskrav. Om miljön manipuleras eller avviker från dessa krav förblir data krypterade och exekveringsmiljön stängs ned. Det innebär att behandlingen endast kan genomföras när de tekniska förutsättningarna för behandlingen är uppfyllda, vilket inte bara stärker säkerheten i teknisk mening utan också bidrar till att den personuppgiftsansvarige kan visa att behandlingen sker under kontrollerade och verifierbara former.

Nyckelhanteringen är i detta sammanhang av betydelse för att upprätthålla faktisk kontroll över behandlingen. Om den personuppgiftsansvarige själv kontrollerar krypteringsnycklarna, eller anlitar en oberoende betrodd tredje part för detta ändamål, stärks kontrollen över åtkomsten till uppgifterna. I projektet hanteras krypteringsnycklarna inte av mobiloperatören som tillhandahåller den tekniska tjänsten och beräkningskraften för exekveringsmiljön, utan av Volvo. Detta minskar risken för att mobiloperatören får åtkomst till den data som behandlas i miljön.

Sammantaget kan betrodda exekveringsmiljöer bidra till att minska den risk för åtkomst till data som är förknippad med extern behandling av personuppgifter. Det gäller särskilt i situationer där infrastrukturen för miljön tillhandahålls av en extern aktör, såsom mobiloperatören i det aktuella projektet. Genom att tekniskt styra vem som får tillgång till data och vilken kod som får exekveras, kan förtroendet för leverantören kompletteras med tekniskt inbyggda skyddsmekanismer. På så sätt vilar säkerheten inte enbart på organisatoriska åtaganden utan även på verifierbar teknik. I förlängningen kan detta möjliggöra nya former av datadelning, liksom analys och samverkan mellan organisationer där integritetsrisker tidigare har begränsat möjligheterna att använda data. I takt med att tekniken mognar, standardiseras och integreras i allt fler hårdvaru-plattformar finns därför goda möjligheter att betrodda exekveringsmiljöer i större utsträckning kommer att användas som skydd för data under användning.

Samtidigt finns det skäl att nyansera bilden av teknikens skyddsnivå. Betrodda exekveringsmiljöer skyddar inte mot alla typer av hot. Forskning har visat att vissa typer av attacker, exempelvis sidokanalsattacker eller andra avancerade angrepp mot hårdvara och implementationer, i vissa fall kan kringgå de skyddsmekanismer som miljön erbjuder. Därtill är själva hårdvarutillverkaren den ursprungliga källan till förtroende i denna modell, eftersom det är tillverkaren som utvecklar och tillhandahåller den programvara och de mekanismer som garanterar konfidentialitet och integritet för data i exekveringsmiljön. Tilliten till tekniken är därför beroende av tilliten till leveranskedjan, vilket aktualiserar frågor om certifiering, granskning och transparens kring hur tekniken utvecklas och implementeras.

Användningen av betrodda exekveringsmiljöer garanterar därmed i sig inte regel- efterlevnad. Den faktiska säkerhets- och integritetsnivån beror i hög grad på hur tekniken implementeras och används i praktiken. Sårbarheter i applikationskod, brister i konfiguration eller otydlig ansvarsfördelning mellan aktörer kan i vissa fall undergräva de skydd som tekniken är avsedd att ge. Ur detta perspektiv bör betrodda exekveringsmiljöer inte betraktas som en universallösning, utan snarare som ett komplement till andra tekniska och organisatoriska skyddsåtgärder.

4. Är GDPR tillämplig på behandlingen?

4.1. Behandling enligt GDPR

GDPR:s tillämplighet i projektet förutsätter dels att uppgifterna utgör personuppgifter, dels att det är fråga om en behandling.

4.1.1. Personuppgifter

Personuppgifter definieras i artikel 4.1 i GDPR som varje upplysning som avser en identifierad eller identifierbar fysisk person. I skäl 26 till GDPR anges att bedömningen av om en person är identifierbar ska hänsyn tas till alla hjälpmedel som, antingen av den aktuella aktören eller av någon annan, rimligen kan komma att användas för att identifiera personen, med beaktande av bland annat kostnader, tidsåtgång och teknik. Uppgifter som inte kan hänföras till en identifierad eller identifierbar fysisk person med sådana hjälpmedel är inte personuppgifter.

Identifierbarhet behöver bedömas konkret och med hänsyn till aktörens faktiska möjligheter. Det innebär att samma informationsmängd kan vara personuppgifter för en aktör som har rimliga medel att identifiera en individ, men att bedömningen kan se annorlunda ut för en annan aktör som är effektivt avskärmd från sådana möjligheter.⁶

4.1.2. Behandling

När uppgifter i ett visst led bedöms vara personuppgifter behöver man därefter pröva om de åtgärder som vidtas i varje led utgör behandling enligt artikel 4.2 i GDPR.⁷ Begreppet behandling ska tolkas brett och teknikneutralt⁸ och omfattar varje åtgärd eller kombination av åtgärder som vidtas beträffande personuppgifter, oberoende av om de utförs automatiserat eller inte.⁹ De materiella bestämmelserna ska i princip tillämpas på behandling, det vill säga på insamling av personuppgifter, liksom på efterföljande hantering av samma uppgifter såsom lagring och överföring.¹⁰

4.1.3. IMY:s kommentar

I projektet sker insamling av data till exempel genom videoupptagningar från lastbilens kameror. Volvo har angett att inspelningarna bland annat kan innehålla uppgifter om identifierbara personer. Data som överförs från fordonet till en betrodd exekveringsmiljö verifieras av en kontrollantfunktion innan den kan avkrypteras och bearbetas i exekveringsmiljön.

Mot denna bakgrund bedöms det i projektet vara fråga om en personuppgiftsbehandling av Volvo som sker vid insamlandet av data såväl vid överföring som under bearbetning av data i den betrodda exekveringsmiljön, i den mån de uppgifter som hanteras är personuppgifter. Eftersom det är fråga om personuppgifter som behandlas automatiserat är GDPR tillämplig på samtliga led i behandlingskedjan som Volvo avser

⁶ Läs mer avseende begreppet personuppgifter i EU-domstolens domar: Europeiska datatillsynsmannen mot SRB, C-413/23 P, EU:C:2025:645 och Gesamtverband Autoteile-Handel, C-319/22, EU:C:2023:837.

⁷ EU-domstolens dom Fashion ID, C-40/17, EU:C:2019:629, p. 71–72.

⁸ Se skäl 15 GDPR.

⁹ Såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

¹⁰ Westman, D. Dataskyddsförordningen, Artikel 4.2, Karnov 2026-03-24 (JUNO).

att utföra inom ramen för projektet. Detta är relevant vid den fortsatta bedömningen av mobiloperatörens roll som tillhandahållare av den betrodda exekveringsmiljön.

5. Vilken roll enligt GDPR får tillhandahållaren av en betrodd exekveringsmiljö?

5.1. Ansvarsroller enligt GDPR

Att fastställa vilka roller aktörer har när de i varierande grad är involverade i eller verkar i anslutning till en behandling av personuppgifter är centralt. Det avgör vilket eventuellt ansvar de har för efterlevnaden av olika dataskyddsbestämmelser och klargör hur registrerade kan utöva sina rättigheter. Begreppen personuppgiftsansvarig, gemensamt personuppgiftsansvarig och personuppgiftsbiträde utgör funktionella begrepp som ska bedömas utifrån de faktiska omständigheterna för den aktuella behandlingen.¹¹ I detta projekt avses med tillhandahållare en mobiloperatör som tillhandahåller den tekniska tjänsten och beräkningskraften för exekveringsmiljön.

5.2. Är tillhandahållaren personuppgiftsansvarig eller gemensamt personuppgiftsansvarig?

5.2.1. Personuppgiftsansvarig

Enligt artikel 4.7 GDPR är en personuppgiftsansvarig den som, ensam eller tillsammans med andra, bestämmer ändamålen och medlen för behandlingen. EDPB framhåller i sina riktlinjer 07/2020 att faktisk åtkomst till uppgifterna inte är avgörande. Det centrala för bedömningen av personuppgiftsansvaret är om aktören har ett reellt inflytande över ändamål och väsentliga medel.¹²

5.2.2. Gemensamt personuppgiftsansvarig

Enligt artikel 26.1 GDPR ska två eller fler aktörer anses vara gemensamt personuppgiftsansvariga om de gemensamt fastställer ändamålen och medlen för en viss behandling. Gemensam infrastruktur eller gemensamt ekonomiskt intresse är typiskt sett inte tillräckligt i sig för att medföra ett gemensamt personuppgiftsansvar.¹³ EU-domstolen har vidare klargjort att gemensamt personuppgiftsansvar inte kräver att varje gemensamt personuppgiftsansvarig har åtkomst till personuppgifterna.¹⁴

EU-domstolen har också bekräftat att avsaknad av direkt åtkomst till uppgifterna inte i sig utesluter att en aktör kan kvalificeras som personuppgiftsansvarig eller gemensamt personuppgiftsansvarig, om aktören har ett reellt inflytande över ändamål och väsentliga medel i den aktuella delen av behandlingen.¹⁵

5.2.3. IMY:s kommentar

I det aktuella projektet beslutar Volvo ensamt om ändamål och väsentliga medel för behandlingen. Mobiloperatören deltar inte i fastställandet av vilka uppgifter som behandlas, för vilka syften eller under vilka villkor. Mobiloperatören administrerar inte kontrollantfunktionen och saknar inflytande över såväl krypteringsnycklar som vilken kod

¹¹ EDPB:s riktlinjer 07/2020, s. 10, p. 12.

¹² EDPB:s riktlinjer 07/2020, s. 19, p 45.

¹³ EDPB:s riktlinjer 07/2020, s. 23, p. 68.

¹⁴ Fashion ID, C-40/17, p. 69.

¹⁵ EU-domstolens dom den 7 mars 2024 i C-604/22, IAB Europé, p. 69.

som får exekveras i miljön. Under dessa förutsättningar är det lite som pekar mot ett gemensamt deltagande i fastställandet av ändamål eller väsentliga medel.

Mot denna bakgrund talar omständigheterna för att mobiloperatören som tillhandahållare av miljön varken är personuppgiftsansvarig eller gemensamt personuppgiftsansvarig för den behandling som sker i den betrodda exekveringsmiljön.

5.3. Är tillhandahållaren ett personuppgiftsbiträde?

5.3.1. Personuppgiftsbiträde

Enligt artikel 4.8 i GDPR är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning att anse som ett personuppgiftsbiträde. För att en aktör ska kvalificeras som personuppgiftsbiträde krävs dels att den är en separat juridisk enhet, dels att den behandlar personuppgifter för den personuppgiftsansvariges räkning och inom ramen för dennes ändamål och instruktioner.¹⁶

Utmärkande för rollen som personuppgiftsbiträde är att biträdet behandlar personuppgifter för den personuppgiftsansvariges räkning¹⁷ eller anförtros behandling.¹⁸ Det handlar alltså om att biträdet utför en behandling på uppdrag av den personuppgiftsansvarige, men utanför dennes direkta organisatoriska kontroll. Avsaknaden av direkt kontroll medför i sig en risk för att skyddet av de registrerades fri- och rättigheter blir sämre än om behandlingen hade skett i egen regi.

För att säkerställa att skyddet för registrerade inte försämras och att kraven i GDPR uppfylls vid sådan behandling åläggs därför personuppgiftsbiträden vissa självständiga skyldigheter, främst för säkerheten vid behandlingen.¹⁹ Samtidigt åläggs personuppgiftsansvariga en skyldighet att endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i GDPR och säkerställer att den registrerades rättigheter skyddas.²⁰ Vidare ställs krav på att hanteringen ska regleras genom ett avtal eller en annan bindande rättsakt, det vill säga genom ett så kallat personuppgiftsbiträdesavtal.²¹

Ett personuppgiftsbiträde ska genom lämpliga tekniska och organisatoriska åtgärder bistå den personuppgiftsansvarige i att uppfylla sina skyldigheter gentemot de registrerade. Efter det att behandlingen har avslutats ska biträdet, enligt den personuppgiftsansvariges instruktioner, radera eller återlämna samtliga personuppgifter. Detta innebär dock inte att varje tjänsteleverantör som på något sätt behandlar personuppgifter vid tillhandahållandet av en tjänst är personuppgiftsbiträde. Personuppgiftsbiträdesrollen förutsätter att leverantören faktiskt utför behandling som ingår i den personuppgiftsansvariges behandlingskedja.²²

¹⁶ EDPB:s riktlinjer 07/2020, s. 28, p. 76.

¹⁷ Eller å en personuppgiftsansvarigs vägnar, se skäl 79 och 81 i GDPR.

¹⁸ Se skäl 81 GDPR.

¹⁹ Se artikel 28.3 GDPR.

²⁰ Se artikel 28.1 GDPR.

²¹ Artikel 28.3 GDPR.

²² EDPB:s riktlinjer 07/2020, s. 29, p. 82.

5.3.2. Exempel på relationer

EDPB har i sina riktlinjer redogjort för ett flertal exempel på leverantörsrelationer som kan bidra till hur mobiloperatörens roll skulle kunna bedömas vid tillhandahållandet av den betrodda exekveringsmiljön i det aktuella fallet.

➤ *Hostingtjänster*

En internetleverantör som tillhandahåller en hostingtjänst är att bedöma som personuppgiftsbiträde för den data som kunden lagrar på servern, även i fall då data är krypterade.²³ Hostingtjänster pekar ofta mot biträdesroll när leverantören tillhandahåller en kontinuerlig lagringstjänst som del av kundens behandlingskedja, även om data är krypterade.

➤ *IT-konsult åtgärdar ett programvarufel*

En IT-konsult som anlitas av ett företag behöver få "system-åtkomst" till personuppgifter i ett uppdrag för att åtgärda en bugg. Ansvaret kan bedömas utifrån vad IT-konsulten faktiskt gör och om behandlingen sker för den personuppgiftsansvariges räkning.²⁴

➤ *Städtjänster*

En städfirma anlitas av ett företag där företaget inte har för avsikt att anlita städfirman för att behandla personuppgifter och vidtar tillräckliga säkerhetsåtgärder för att förhindra att städfirman får tillgång till personuppgifter. Städfirman och dess personal kan ses som tredje part.²⁵

Av de exempel som redogörs för ovan framgår att bedömningen av en aktörs roll ska göras utifrån vad aktören faktiskt gör och vilken roll aktören har i behandlingen som helhet. En aspekt att beakta är att behandlingen som sådan är en viktig del av den personuppgiftsansvariges beslut att anförtro ett personuppgiftsbiträde att behandla personuppgifter för sin räkning.²⁶ En ytterligare aspekt är att "tillfällig åtkomst" inte automatiskt löser rollfrågan åt något håll. Åtkomsten behöver bedömas i förhållande till uppdragets natur, åtkomstens praktiska utformning och inflytandet över väsentliga medel.²⁷

5.3.3. IMY:s kommentar

Mot bakgrund av det ovan redovisade är det tydligt att mobiloperatören utgör en separat enhet i förhållande till den personuppgiftsansvarige, det vill säga Volvo, i det aktuella projektet. Frågan blir då om mobiloperatören kan anses behandla personuppgifter för Volvos räkning och i enlighet med Volvos instruktioner. Däremot påverkar denna bedömning inte mobiloperatörens ansvar för egna behandlingar, exempelvis trafik- och kunduppgifter, där mobiloperatören kan vara personuppgiftsansvarig för uppgifter som behandlas i enlighet med lagen (2022:482) om elektronisk kommunikation.²⁸

Betrodda exekveringsmiljöer är en teknik som under senare år har fått ökad spridning i takt med behovet av säkra lösningar för data under användning. Samtidigt är vägledning avseende rollfördelning och ansvar vid behandling i sådana miljöer fortfarande

²³ EDPB:s riktlinjer 07/2020, s. 17, p. 40, se exemplet med "Hostingtjänster".

²⁴ EDPB:s riktlinjer 07/2020, s. 30, se exemplet med "IT-konsult åtgärdar ett programvarufel".

²⁵ EDPB:s riktlinjer 07/2020, s. 33, se exemplet med "Städtjänster".

²⁶ Se skäl 81 i GDPR som hänvisar till att "anförtro behandling åt ett personuppgiftsbiträde".

²⁷ EDPB:s riktlinjer 07/2020, s. 30, se exemplet med "IT-konsult åtgärdar ett programvarufel".

²⁸ Se exempelvis 9 kap. lag (2022:482) om elektronisk kommunikation.

begränsad. Bedömningen av rollfördelningen ur dataskyddssynpunkt, och särskilt om tillhandahållaren av en betrodd exekveringsmiljö är att anse som personuppgiftsbiträde, behöver därför göras utifrån etablerad generell praxis, med fokus på vad aktören faktiska gör, liksom inflytande över ändamål och väsentliga medel.

EU-lagstiftarens syfte med att vissa aktörer ska ha rollen som personuppgiftsbiträde, med de skyldigheter som följer av den rollen, är kopplat till aktörens faktiska möjligheter att bidra till skyddet för registrerades fri-och rättigheter samt i vilken utsträckning det är rimligt att ställa sådana krav på aktören.²⁹ Mot denna bakgrund är det viktigt att beakta vilka möjligheter aktören i praktiken har att bidra till detta skydd, och i vilken utsträckning det kan krävas utifrån uppdraget de har fått.

Mot denna bakgrund kan det finnas situationer där en aktör varken är personuppgiftsbiträde eller personuppgiftsansvarig, om denne har anlåtts för ett uppdrag som inte sker i syfte att behandla personuppgifter, och där behandling av personuppgifter inte ingår i de huvudsakliga uppgifterna. Det kan vara fallet om aktören saknar åtkomst till personuppgifter, eller där en eventuell åtkomst är tillfällig, mycket begränsad eller oavsiktlig och inte utgör en förutsättning för att uppdraget ska kunna utföras. Vidare kan det krävas att aktören är avtalsenligt förbjuden att behandla personuppgifter på ett obehörigt sätt. I sådana situationer är den personuppgiftsansvarige dock skyldig att säkerställa att det finns tillräckliga säkerhetsåtgärder enligt artikel 32 GDPR, inklusive sekretessplikt, för att förhindra obehörig eller oavsiktlig åtkomst.

5.3.4. Kontrollantens betydelse för biträdesbedömningen

Kontrollantfunktionen för den betrodda exekveringsmiljön, som beskrivits i avsnitt 3.3, har särskild betydelse för bedömningen av mobiloperatörens roll. Kontrollantfunktionen utför nämligen attestering av exekveringsmiljön och hanterar de behörigheter och krypteringsnycklar som krävs för att behandlingen ska kunna genomföras.

Genom kontrollantfunktionen kan Volvo i det aktuella projektet kontrollera vilken kod som får köras i miljön samt fastställa under vilka villkor behandling får ske. Kontrollantfunktionen är utformad för att avbryta och destruera miljön om villkoren för behandlingen inte längre uppfylls. Den aktör som kontrollerar denna funktion har därmed avgörande inflytande över väsentliga medel för behandlingen, bland annat genom kontroll över tillgång till data som behandlas i den betrodda exekveringsmiljön.³⁰

En ytterligare aspekt som kan få inverkan på bedömningen är att den betrodda exekveringsmiljön inte är bestående, utan startas upp genom attestering och stängs ned igen när exekvering inte längre sker. Det är till skillnad från klassiska molntjänster eller hostingtjänster inte en yta där data lagras vilande.³¹

5.3.5. Andra faktorer av betydelse

I flera kommersiella tjänsteerbjudanden avseende betrodda exekveringsmiljöer och molnliknande tjänster är leverantören typiskt att betrakta som personuppgiftsbiträde. Det beror främst på att leverantören tillhandahåller funktioner för exekvering och/eller lagring som en del av den personuppgiftsansvariges behandlingskedja, inklusive support och

²⁹ Se exempelvis artikel 28.3 c GDPR.

³⁰ EDPB anger att väsentliga medel bland annat omfattar möjligheten att bestämma vilka personer som har rätt att få tillgång till uppgifterna.

³¹ Jfr EDPB:s exempel "Hostingtjänst" där leverantören av tjänsten bedöms vara personuppgiftsbiträde eftersom lagring sker hos leverantören av tjänsten.

incidenthantering. En leverantör av en sådan tjänst får typiskt sett anses behandla personuppgifter för den personuppgiftsansvariges räkning.

Den lösning som har analyserats i projektet skiljer sig dock i vissa avseenden väsentligt från denna typ av tjänster. Implementeringen av den betrodda exekveringsmiljön är tekniskt utformad så att mobiloperatören saknar möjlighet att ta del av innehållet i miljön. Samtidigt ligger kontrollen över attestering, nyckelhantering och behörigheter hos den personuppgiftsansvarige.

Med hänsyn till syftet med rollen som personuppgiftsbiträde och vad som kännetecknar den rollen kan följande omständigheter beaktas i bedömningen av om tillhandahållaren av exekveringsmiljön är ett personuppgiftsbiträde. Om dessa omständigheter föreligger i den behandling som utförs i den betrodda exekveringsmiljön kan de vara av avgörande betydelse för bedömningen av tillhandahållaren som ett personuppgiftsbiträde.

- Kontrollantfunktionen (attestering, behörighetsstyrning och nyckelhantering) ligger helt inom den personuppgiftsansvariges kontrollfär och inte hos den externa tillhandahållaren av miljön.
- Den betrodda exekveringsmiljön etableras temporärt utifrån förutbestämda villkor och stängs ned när villkoren för miljön inte längre är uppfyllda. Behandlingen är därför inte kontinuerlig på samma sätt som en lagringstjänst. Det finns därmed inga personuppgifter som kan raderas eller återlämnas efter att uppdraget har upphört.
- Tillhandahållarens insats är begränsad till att tillhandahålla infrastruktur och beräkningskapacitet, utan att tillhandahållaren administrerar kontrollantfunktionen eller i praktiken styr vad som exekveras i den betrodda exekveringsmiljön.
- Tillhandahållaren saknar tekniska möjligheter att ta del av innehållet i exekveringsmiljön eftersom tillhandahållaren saknar krypteringsnycklar, tillgång till tekniska gränssnitt och organisatoriska rutiner som möjliggör innehållsnära behandling.
- Tillhandahållaren saknar praktiska möjligheter att bistå den personuppgiftsansvarige och uppfylla sina skyldigheter som personuppgiftsbiträde, till exempel gällande säkerställandet av skyddet för registrerades rättigheter.
- Den personuppgiftsansvarige kan visa att lämpliga säkerhetsåtgärder för behandlingen i den betrodda exekveringsmiljön upprätthålls utan att lämna instruktioner för behandlingen till tillhandahållaren.

5.3.6. Sammanvägd bedömning

En naturlig utgångspunkt är att bedöma en tillhandahållare av en tjänst för bearbetning av personuppgifter som personuppgiftsbiträde. Detta stöds av etablerad praxis för exempelvis molntjänster, där det finns omständigheter som talar för att operatören som tillhandahåller den betrodda exekveringsmiljön behandlar personuppgifter som personuppgiftsbiträde.

I det aktuella fallet finns dock omständigheter som talar för en annan bedömning. Särskilt betydelsefullt är kontrollantfunktionens placering hos den personuppgiftsansvarige som gör att mobiloperatören saknar tekniska möjligheter att ta del av data som behandlas i miljön eller påverka behandlingen, liksom att krypteringsnycklar kontrolleras helt av den personuppgiftsansvarige. En ytterligare aspekt som talar emot att mobiloperatören är personuppgiftsbiträde i det aktuella projektet är operatörens mycket begränsade möjligheter att bistå den personuppgiftsansvarige och vidta åtgärder för att säkerställa

skyddet av registrerades fri-och rättigheter, eller att säkerställa att kraven i GDPR uppfylls. Detta genom att ansvaret för de grundläggande besluten om skyddsåtgärder och kontroll över behandlingen ligger hos den personuppgiftsansvarige, som också behöver kunna visa att de åtgärder som ska förhindra mobiloperatörens åtkomst fungerar i praktiken.

De omständigheter som anges ovan kan sammantaget anses tala emot att mobiloperatören behandlar personuppgifter för den personuppgiftsansvariges räkning och således är ett personuppgiftsbiträde för behandlingen. Samtidigt behöver rollbedömningen göras utifrån vilka behandlingsmoment som faktiskt uppkommer i mobiloperatörens drift. Det måste bedömas om en tillhandahållares faktiska insats stannar vid att tillhandahålla infrastruktur och beräkningskapacitet för miljön, eller om tillhandahållaren genom drift och administration utför behandlingsmoment som innebär behandling av personuppgifter för den personuppgiftsansvariges räkning. I en sådan situation ska det heller inte finnas något behov av att den personuppgiftsansvarige lämnar instruktioner för behandlingen, eftersom tillhandahållaren saknar faktisk möjlighet att utföra dem.

Om tillhandahållarens insats i det enskilda fallet i praktiken är begränsad till att tillhandahålla infrastruktur och beräkningskapacitet, utan att tillhandahållaren utför behandlingsmoment för den personuppgiftsansvariges räkning, kan det tala emot att mobiloperatören är ett personuppgiftsbiträde. Denna bedömning kan påverkas av avtalsvillkor om tjänstens omfattning, tillsammans med hur infrastrukturen faktiskt är utformad och används i praktiken.

Avgörande blir därför om de omständigheter som anges ovan också återspeglas den faktiska driften och förvaltningen av tjänsten. Om tillhandahållaren i praktiken är effektivt hindrad från att ta del av innehållet, saknar åtkomstvägar även vid support och incidenthantering och inte administrerar kontrollantfunktionen för miljön, talar det sammantaget emot att tillhandahållaren behandlar personuppgifter för den personuppgiftsansvariges räkning och därmed emot att denne är ett personuppgiftsbiträde.

6. Övriga reflektioner

Avslutningsvis vill IMY lyfta fram den positiva utveckling som användningen av integritetsfrämjande tekniker innebär för dataskyddsområdet. Sådana tekniker kan, när de är korrekt implementerade och integrerade, bidra till att minska integritetsrisker, stärka skyddet för personuppgifter och skapa bättre förutsättningar för att uppfylla kraven på inbyggt dataskydd och dataskydd som standard, samt lämpliga säkerhetsåtgärder.

IMY ser därför positivt på initiativ som syftar till att pröva och utveckla användningen av integritetsfrämjande tekniker. Ett aktuellt exempel är den kommande utredningen om integritetsbevarande metoder för en mer datadriven och samverkande förvaltning.³² Uppdraget syftar till att identifiera rättsliga och praktiska förutsättningar för att möjliggöra ett mer effektivt informationsutbyte genom användning av bland annat sådana tekniker. IMY bedömer att integritetsfrämjande tekniker kan utgöra ett viktigt verktyg för att förena ett starkt skydd för den personliga integriteten med behovet av verksamhetsutveckling och innovation, vilket är en utveckling som enligt IMY är både nödvändig och önskvärd.

³² Dir. 2025:64, Integritetsbevarande metoder för en mer datadriven och samverkande förvaltning.

7. Fördjupning

I detta avsnitt samlas exempel på material som refererats till i rapporten och som kan vara av intresse för vidare fördjupning.

För vägledning om rollerna personuppgiftsansvarig, gemensamt personuppgiftsansvar och personuppgiftsbiträde samt gränsdragningen mellan dessa hänvisas till [EDPB:S riktlinje 07/2020 om begreppen personuppgiftsansvarig och personuppgiftsbiträde](#).

För vidare läsning om integritetsbevarande tekniker och betrodda exekveringsmiljöer (eng. *Trusted Execution Environments*), se exempelvis [ENISA, Data Protection Engineering – From Theory to Practice](#) och [OECD, Emerging Privacy Enhancing Technologies: Current Regulatory and Policy Approaches](#).

För vidare läsning om användningsområden för betrodda exekveringsmiljöer, se exempelvis [EDPS, TechSonar Report 2025–2026](#).

Nedan listas slutrapporter från projekt i IMY:s regulatoriska sandlåda om dataskydd. Hänvisningarna avser vidare läsning och fördjupning utöver vad som behandlas i denna rapport. För en uppdaterad sammanställning av publicerade sandlåderapporter, se [IMY:s innovationsportal](#).

Publicerade slutrapporter

- Federerad maskininlärning mellan två vårdgivare, 15 mars 2023 ([IMY-2023-2602](#)).
- Trygghetsmätning i offentliga miljöer med hjälp av IoT-teknik, 9 februari 2024 ([IMY-2023-15495](#)).
- Utlämnande av allmänna handlingar med hjälp av AI, 7 november 2024 ([IMY-2024-5156](#)).
- Delning av kunduppgifter mellan banker i syfte att motverka ekonomisk brottslighet, 19 maj 2025 ([IMY-2024-14275](#)).
- Vidarebehandling av personuppgifter i vårdnadsärenden för att träna en AI-modell, 9 december 2025 ([IMY-2025-23536](#)).

Detta är Integritetsskyddsmyndigheten

Integritetsskyddsmyndigheten (IMY) arbetar för att skydda alla dina personuppgifter, till exempel om hälsa och ekonomi, så att de hanteras korrekt och inte hamnar i orätta händer. Det är vi som granskar att företag, myndigheter och andra aktörer följer GDPR – dataskyddsförordningen. Vi utbildar och vägleder dem som behandlar personuppgifter. Vi vill se en hållbar och integritetsvänlig digitalisering. Vi är övertygade om att det går att värna medborgarnas trygghet och samhällets säkerhet, utan omotiverad kartläggning och övervakning. Tillsammans med övriga dataskyddsmyndigheter i EU arbetar vi för att medborgarnas personuppgifter ska ha samma skydd i hela unionen. Vi arbetar även för att kreditupplysning ska bedrivas på ett korrekt sätt.

Kontakta Integritetsskyddsmyndigheten

E-post: imy@imy.se

Webb: www.imy.se

Tel: 08-657 61 00

Postadress: Integritetsskyddsmyndigheten,
Box 8114, 104 20 Stockholm