E-bevis – Försäkringskassans behov av författningsreglering av vissa frågor rörande tillhandahållande av teknisk lösning

Innehållsförteckning

Sammanfattning

Försäkringskassan har fått i uppdrag att drifta och förvalta en teknisk lösning som möjliggör för av tjänsteleverantörer utsedda verksamhetsställen och rättsliga ombud (i denna framställning kallade tjänsteleverantörer) att ansluta sig och få åtkomst till det decentraliserade it-systemet enligt EU:s förordning om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis (e-bevisförordningen) på ett säkert sätt från och med den 18 augusti 2026. I utförandet av uppdraget har Försäkringskassan identifierat ett brådskande behov av författningsstöd på fem områden:

- Försäkringskassans uppdrag behöver fastställas i författning.
- Försäkringskassan behöver ett bemyndigande att utfärda föreskrifter om vilka operativa och tekniska krav som tjänsteleverantörer ska uppfylla i samband med anslutning till och användning av den tekniska lösningen.
- Försäkringskassan behöver författningsstöd för att tillfälligt kunna stänga av tjänsteleverantörer som äventyrar säkerheten i systemet.
- En sekretessbrytande regel behövs för att Försäkringskassan exempelvis ska kunna underrätta Åklagarmyndigheten och Post- och telestyrelsen om tjänsteleverantörer som inte uppfyller kraven för att kunna anslutas till systemet och om eventuella incidenter orsakade av en tjänsteleverantör.
- Ansvarsförhållandena ur ett dataskyddsrättsligt perspektiv behöver regleras.

Försäkringskassan ger i denna framställning förslag på en förordning om den tekniska lösningen för åtkomst till det decentraliserade it-systemet i enlighet med EU:s förordning om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis där de ovan nämnda punkterna regleras.

Försäkringskassans önskemål är att förordningen, framför allt bestämmelsen som ger Försäkringskassan bemyndigande att utfärda föreskrifter om vilka operativa och tekniska krav som tjänsteleverantörer ska uppfylla i samband med anslutning till och användning av den tekniska lösningen, träder i kraft den 15 juni 2026. Försäkringskassan kommer inte att kunna ansluta tjänsteleverantörer till den tekniska lösningen förrän föreskrifterna har trätt i kraft. Om den föreslagna bestämmelsen med bemyndigande för Försäkringskassan att besluta föreskrifter inte träder i kraft förrän den 18 augusti 2026 eller senare kommer Försäkringskassan inte att kunna besluta föreskrifter om operativa och tekniska krav förrän samma dag. Föreskrifterna kommer då inte att kunna träda i kraft förrän tidigast två till fyra veckor senare.

1 Författningsförslag

1.1 Förslag till förordning om den tekniska lösningen för åtkomst till det decentraliserade it-systemet i enlighet med EU:s förordning om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis

Regeringen föreskriver följande.

1 § Denna förordning innehåller bestämmelser som kompletterar Europaparlamentets och rådets förordning (EU) 2023/1543 av den 12 juli 2023 om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden (e-bevisförordningen), Kommissionens genomförandeförordning (EU) 2025/1550 av den 28 juli 2025 om fastställande av tekniska specifikationer och andra krav för det decentraliserade it-system som avses i Europaparlamentets och rådets förordning (EU) 2023/1543 (genomförandeförordningen) och lagen (2026:XXXX) om utsedda verksamhetsställen och rättsliga ombud för inhämtning av elektroniska bevis.

Förordningen är meddelad med stöd av 8 kap. 7 § regeringsformen.

2 § Ord och uttryck i denna förordning har samma betydelse som i EU-förordningarna och lagen om utsedda verksamhetsställen och rättsliga ombud för inhämtning av elektroniska bevis.

3 § Försäkringskassan ska tillhandahålla en teknisk lösning som möjliggör för sådana verksamhetsställen och rättsliga ombud, som omfattas av lagen om utsedda verksamhetsställen och rättsliga ombud för inhämtning av elektroniska bevis, att få åtkomst till det decentraliserade it-systemet i enlighet med artikel 19 i e-bevisförordningen.

4 § Försäkringskassan får meddela föreskrifter om vilka operativa och tekniska åtgärder som tjänsteleverantörerna ska vidta för att säkerheten och tillgängligheten i den tekniska lösningen ska kunna upprätthållas.

5 § Försäkringskassan får tillfälligt stänga av en tjänsteleverantör från åtkomst till det decentraliserade it-systemet om tjänsteleverantören agerar på ett sådant sätt att säkerheten eller tillgängligheten i den tekniska lösningen äventyras.

6 § Försäkringskassan får, utan hinder av sekretess, underrätta Åklagarmyndigheten om en tjänsteleverantör åsidosätter skyldigheter enligt artikel 13.4 e-bevisförordningen.

Försäkringskassan får, utan hinder av sekretess, underrätta Post- och telestyrelsen om förhållanden som har betydelse för Post- och telestyrelsens tillsyn och för verksamhetsställens och rättsliga ombuds åtkomst till det decentraliserade it-systemet enligt 3 §.

7 § [Dataskyddsbestämmelse, se avsnitt 4.6]

Denna författning träder i kraft den 15 juni 2026.

2 Bakgrund

2.1 E-codexsystemet eller det decentraliserade it-systemet

Genom två förordningar, den s.k. digitaliseringsförordningen[1] och den s.k. e-Codexförordningen, har EU skapat förutsättningar för ett system för gränsöverskridande elektroniskt utbyte av uppgifter inom de straff- och civilrättsliga områdena.

E-Codexsystemet bygger på att aktörer i olika EU-länder kommunicerar direkt med varandra via nationella åtkomstpunkter. Systemet kallas därför även för det decentraliserade it-systemet.

Försäkringskassan har haft regeringens uppdrag att inrätta, drifta och förvalta en gemensam åtkomstpunkt för svenska aktörer till e-Codex.[2] Målet med uppdraget var att ett antal särskilt utpekade myndigheter skulle kunna ansluta sig senast i maj 2025. Försäkringskassan tillhandahåller den gemensamma åtkomstpunkten och ansluter aktörer vartefter behov uppstår.

2.2 E-bevis

Vilka uppgifter som ska utbytas inom e-Codexsystemet preciseras genom digitaliseringsförordningen och andra EU-rättsakter. En av dessa rättsakter är den s.k. e-bevisförordningen. E-bevisförordningen gör det möjligt för en myndighet i en medlemsstat att beordra en tjänsteleverantör som är etablerad i en annan medlemsstat att lämna ut eller bevara elektronisk bevisning. Tjänsteleverantörerna är skyldiga att vara ansluta till det decentraliserade it-systemet (art. 19) och de är också skyldiga att vidta de senaste operativa och tekniska åtgärder som krävs för att säkerställa konfidentialiteten, sekretessen och integriteten för de uppgifter som omfattas (art 13.4).

Närmare tekniska specifikationer och andra krav fastställs i Kommissionens genomförandeförordning. EU-kommissionen ansvarar även för e-bevissystemets officiella databas över tjänsteleverantörer och behöriga myndigheter (CDB).

Det s.k. e-bevisdirektivet syftar till att säkerställa att medlemsstaterna ser till att de tjänsteleverantörer som omfattas av e-bevisförordningens regelverk utser verksamhetsställen eller rättsliga ombud som ansvarar för att en order om att lämna ut eller bevara elektronisk bevisning verkställs. De tjänsteleverantörer som omfattas är i huvudsak företag som erbjuder elektroniska kommunikations- och informationstjänster samt it-infrastrukturtjänster som till exempel ip-adresser och domännamn. Elektroniska bevis kan enligt e-bevisförordningen vara exempelvis namn- och adressuppgifter, kontonummer och telefonnummer eller det faktiska innehållet i skriftlig eller muntlig kommunikation.

Regeringen har föreslagit en ny lag med kompletterande bestämmelser till e-bevisförordningen och en ny lag som genomför e-bevisdirektivet (lagen om utsedda verksamhetsställen och rättsliga ombud för inhämtning av elektroniska bevis).[3]

Enligt föreslagna 3 kap. 1 § lagen om utsedda verksamhetsställen och rättsliga ombud för inhämtning av elektroniska bevis är den myndighet som regeringen bestämmer centralmyndighet enligt e-bevisdirektivet. Regeringen avser att i förordning utse Post- och telestyrelsen till svensk centralmyndighet enligt e-bevisdirektivet. Det innebär att Post- och telestyrelsen bland annat är ansvarig för att ta emot underrättelser från tjänsteleverantörer om bl.a. kontaktuppgifter till utsedda verksamhetsställen och rättsliga

[1] För exakta namn på de EU-rättsakter som tas upp, se avsnitt 3 Gällande rätt.
[2] Regeringsuppdrag med dnr Ju2024/01093, Försäkringskassans dnr FK 2024/011223
[3] Proposition 2025/26:147 Effektivare gränsöverskridande inhämtning av elektroniska bevis

ombud. Post- och telestyrelsen ska vidare ombesörja den administration som är nödvändig för att tjänsteleverantörerna ska kunna anslutas till den tekniska lösningen. Enligt föreslagna 3 kap. 2 § lagen om utsedda verksamhetsställen och rättsliga ombud för inhämtning av elektroniska bevis ska centralmyndigheten, det vill säga Post- och telestyrelsen, ha tillsyn över att lagen och de föreskrifter som meddelats i anslutning till lagen följs.

Regeringen föreslår att Åklagarmyndigheten utses till verkställande myndighet enligt e-bevisdirektivet (se föreslagna 3 kap. 1 § lagen med kompletterande bestämmelser till EU:s förordning om europeiska utlämnande order och europeiska bevarandeorder för elektroniska bevis). Det innebär bland annat att Åklagarmyndigheten ska ta ut sanktionsavgifter av tjänsteleverantörer som åsidosätter någon av sina skyldigheter (se föreslagna 4 kap. 1 §).

Regeringen har gett Försäkringskassan i uppdrag[4] att inrätta, drifta och förvalta en teknisk lösning som möjliggör för tjänsteleverantörer att ansluta sig och få åtkomst till det decentraliserade it-systemet. Enligt uppdraget ska tjänsteleverantörer kunna ansluta sig till den tekniska lösningen från och med den 18 augusti 2026. Med teknisk lösning avses – enligt Försäkringskassans tolkning av e-bevisförordningen – en webbtjänst, alternativt ett applikationsgränssnitt för de tjänsteleverantörer som önskar integrera sina interna lösningar i stället för att använda webbtjänsten.[5] .

I uppdraget ingår att Försäkringskassan ska genomföra en analys av vilka specifika tekniska och säkerhetsmässiga krav som ska ställas på tjänsteleverantörer. Försäkringskassan ska även lämna förslag på hur dessa krav ska dokumenteras och regleras och vid behov lämna förslag till författningsändringar.

Den information som ska utbytas är europeiska utlämnande- och bevarandeorder samt elektroniska bevis. Försäkringskassan kommer att inrätta den tekniska lösningen (en webbtjänst och ett applikationsgränssnitt som bygger på EU-kommissionens tillhandahållna referensprogramvara) i enlighet med kraven i e-bevisförordningen och genomförandeförordningen.

[4] Regeringsbeslut 2025-10-30, dnr Ju2025/02279
[5] Se artikel 19 p. 2 och 3 e-bevisförordningen samt genomförandeförordningens bilaga punkt 2.6, 2.8, 2.9, 3.1 och 4.6

3 Gällande rätt

EU-rätt

- Europaparlamentets och rådets förordning (EU) 2023/2844 av den 13 december 2023 om digitalisering av rättsligt samarbete och tillgång till rättslig prövning i gränsöverskridande frågor på privaträttens och straffrättens område och om ändring av vissa rättsakter inom området för rättsligt samarbete (digitaliseringsförordningen)

- Europaparlamentets och rådets förordning (EU) 2022/850 av den 30 maj 2022 om ett datoriserat system för gränsöverskridande elektroniskt utbyte av uppgifter på området civil- och straffrättsligt samarbete (e-Codex-systemet) och om ändring av förordning (EU) 2018/172 (e-Codexförordningen)

- Europaparlamentets och rådets förordning (EU) 2023/1543 av den 12 juli 2023 om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden (e-bevisförordningen)

- Kommissionens genomförandeförordning (EU) 2025/1550 av den 28 juli 2025 om fastställande av tekniska specifikationer och andra krav för det decentraliserade it-system som avses i Europaparlamentets och rådets förordning (EU) 2023/1543 (genomförandeförordningen)

- Europaparlamentets och rådets direktiv (EU) 2023/1544 av den 12 juli 2023 om fastställande av harmoniserade regler för att utse utsedda verksamhetsställen och rättsliga ombud för insamling av elektroniska bevis i straffrättsliga förfaranden (e-bevisdirektivet)

- 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), här kallad dataskyddsförordningen

4 Överväganden och förslag

4.1 Inledning

För att Försäkringskassan ska kunna utföra sitt uppdrag att drifta och förvalta en teknisk lösning som möjliggör för tjänsteleverantörer att ansluta sig och få åtkomst till det decentraliserade it-systemet enligt e-bevisförordningen på ett säkert sätt från och med den 18 augusti 2026 har ett brådskande behov av författningsstöd på fem områden identifierats:

- Försäkringskassans uppdrag behöver fastställas i författning.
- Försäkringskassan behöver ett bemyndigande att utfärda föreskrifter om vilka operativa och tekniska krav som tjänsteleverantörer ska uppfylla i samband med anslutning till och användning av den tekniska lösningen.
- Försäkringskassan behöver författningsstöd för att tillfälligt kunna stänga av tjänsteleverantörer som äventyrar säkerheten i systemet.
- En sekretessbrytande regel behövs för att Försäkringskassan ska kunna underrätta Åklagarmyndigheten och Post- och telestyrelsen exempelvis om tjänsteleverantörer som inte uppfyller kraven för att kunna anslutas till systemet och om eventuella incidenter orsakade av en tjänsteleverantör.
- Ansvarsförhållandena ur ett dataskyddsrättsligt perspektiv behöver regleras.

Enligt 8 kap. 7 § regeringsformen får regeringen bland annat meddela föreskrifter om verkställighet av lag. Med detta avses dels tillämpningsföreskrifter av rent administrativ karaktär, dels föreskrifter som i och för sig kompletterar en lag i materiellt hänseende men inte tillför något väsentligt nytt. När det gäller verkställighetsföreskrifter likställs EU-förordningar med svensk lag. Regeringen anses därför ha rätt att meddela verkställighetsföreskrifter till EU-förordningar.[6] Enligt Försäkringskassans bedömning kan de frågor som omfattas av denna framställning regleras i förordning eftersom de kompletterar e-bevisförordningen och Kommissionens genomförandeförordning, utan att tillföra något väsentligt nytt.

4.2 Försäkringskassans uppdrag

Försäkringskassans förslag: Försäkringskassans uppgift att tillhandahålla en teknisk lösning, som möjliggör för tjänsteleverantörer att ansluta sig och få åtkomst till det decentraliserade it-systemet i enlighet med artikel 19 i e-bevisförordningen, fastställs i förordning.

Skälen för förslaget: Försäkringskassan fick i oktober 2025 i uppdrag av regeringen att bland annat inrätta, drifta och förvalta en teknisk lösning som möjliggör för tjänsteleverantörer att ansluta sig och få åtkomst till det decentraliserade it-systemet i enlighet med artikel 19 i e-bevisförordningen. Uppdraget ska slutredovisas den 1 september 2027. Driften och förvaltningen av den inrättade tekniska lösningen är dock tänkt att fortlöpa även efter det att uppdraget har slutredovisats. Försäkringskassan behöver därför ett mer långsiktigt uppdrag att tillhandahålla den tekniska lösningen.

Post- och telestyrelsen har i egenskap av centralmyndighet ett författningsreglerat uppdrag som anknyter till Försäkringskassans uppdrag. För att gränsdragningen mellan myndigheternas uppdrag ska bli tydlig, bör även Försäkringskassans uppdrag regleras i författning.

[6] Myndigheternas föreskrifter SB PM 2025:4, s. 16–17

Försäkringskassan har dessutom behov av en tydlig rättslig grund för den personuppgiftsbehandling som är nödvändig med anledning av uppdraget (artikel 6.3 i dataskyddsförordningen). En sådan rättslig grund tillgodoses genom ett uppdrag till myndigheten.

Bestämmelsen föreslås formuleras så att Försäkringskassan får i uppdrag att *tillhandahålla* den tekniska lösningen. Formuleringen har sin förebild i 1 § lagen (2020:272) om konto- och värdefackssystem. Begreppet *tillhandahålla* får anses innebära detsamma som att *drifta och förvalta* den tekniska lösningen.

4.3 Bemyndigande för Försäkringskassan

Försäkringskassans förslag: Försäkringskassan ska få meddela föreskrifter om vilka operativa och tekniska åtgärder som tjänsteleverantörerna ska vidta för att säkerheten och tillgängligheten i den tekniska lösningen ska kunna upprätthållas.

Skälen för förslaget: Tjänsteleverantörer är skyldiga att vara anslutna till det decentraliserade it-systemet (art. 19 i e-bevisförordningen) och de är också skyldiga att vidta de senaste operativa och tekniska åtgärder som krävs för att säkerställa konfidentialiteten, sekretessen och integriteten för de uppgifter som omfattas (art 13.4). I punkt 5 i bilagan till genomförandeförordningen framgår vilka tekniska åtgärder som ska vidtas för att säkerställa efterlevnad av minimistandarder för it-säkerhet i samband med utbyte av information via det decentraliserade it-systemet.

Enligt artikel 9.3 i e-Codexförordningen ska dock ansvaret för eventuella skador som uppstår till följd av driften av en auktoriserad e-Codexåtkomstpunkt och eventuella anslutna system bäras av den enhet som driver den auktoriserade åtkomstpunkten. Försäkringskassan tillhandahåller den nationella e-Codexåtkomstpunkten och den tekniska lösningen för anslutning till e-Codexsystemet. Försäkringskassan bedömer att denna tekniska lösning sannolikt utgör ett sådant anslutet system som omfattas av artikel 9.3. Försäkringskassan har ett uppdrag att inrätta en säker och tillgänglig lösning i enlighet med e-bevisförordningen och genomförandeförordningen. Eftersom Försäkringskassan således har ansvar för att den tekniska lösningen är säker och tillgänglig och för eventuella skador som uppstår i systemet, behöver Försäkringskassan kunna ställa krav på tjänsteleverantörer att vidta nödvändiga operativa och tekniska åtgärder i samband med deras anslutning till och användning av den tekniska lösningen.

Försäkringskassan föreslår därför att regeringen ger Försäkringskassan rätt att meddela föreskrifter om vilka operativa och tekniska åtgärder som tjänsteleverantörerna ska vidta för att säkerheten och tillgängligheten i den tekniska lösningen ska kunna upprätthållas.

Fördelarna med att uppställa krav i föreskriftsform är att reglerna blir allmänt tillgängliga på Försäkringskassans webbplats (lagrummet.forsakringskassan.se) och att det blir transparent för alla berörda vilka krav som gäller. Försäkringskassan kan också vid behov relativt enkelt ändra föreskrifterna utan att behöva involvera regeringen eller någon annan aktör. En nackdel med att använda sig av föreskrifter är att det rör sig om omfattande, tekniska bestämmelser på ett område som inte hör till Försäkringskassans kärnverksamhet och som Försäkringskassan inte har erfarenhet av att reglera på detta sätt. Försäkringskassan anser dock att föreskriftslösningen ändå är att föredra framför alternativen (se nedan i avsnitt 5.2 Alternativa lösningar).

4.4 Tillfällig avstängning

Försäkringskassans förslag: Försäkringskassan ska få tillfälligt stänga av en tjänsteleverantör från åtkomst till det decentraliserade it-systemet om tjänsteleverantören agerar på ett sådant sätt att säkerheten eller tillgängligheten i den tekniska lösningen äventyras.

Skälen för förslaget: Försäkringskassan tillhandahåller den nationella e-Codexåtkomstpunkten och den tekniska lösningen för det anslutande systemet i enlighet med e-bevisförordningen och bär ansvaret för eventuella skador som uppstår till följd av driften. I e-bevisförordningen och genomförandeförordningen uppställs krav på att den tekniska lösningen ska vara säker och tillgänglig. Enligt punkt 5.7 i bilagan till genomförandeförordningen ska medlemsstaterna, Eurojust och Europeiska åklagarmyndigheten inrätta robusta mekanismer för upptäckt av hot och incidenthantering för att säkerställa snabb identifiering, begränsning och återhämtning från säkerhetsincidenter, i enlighet med deras relevanta policyer, för de it-system under deras ansvar som ingår i det decentraliserade it-systemet.

För att kunna tillhandahålla en säker och tillgänglig tjänst samt kunna begränsa skador i samband med driften behöver Försäkringskassan, utöver rätten att genom föreskrifter kunna ställa upp operativa och tekniska krav för anslutning till och användning av den tekniska lösningen (se ovan i avsnitt 4.3 Bemyndigande för Försäkringskassan), få rätt att tillfälligt stänga av en tjänsteleverantör som inte uppfyller de uppställda kraven och därigenom hotar säkerheten och tillgängligheten i den tekniska lösningen. En möjlighet för Försäkringskassan att tillfälligt stänga av tjänsteleverantörer får anses utgöra en del av sådana robusta mekanismer för begränsning av och återhämtning från säkerhetsincidenter som medlemsstaterna ska inrätta enligt genomförandeförordningen. Så snart som tjänsteleverantören har vidtagit nödvändiga åtgärder och säkerheten och/eller tillgängligheten är återställd ska Försäkringskassan återansluta denne till it-systemet.

Det bör noteras att en avstängning av en tjänsteleverantör sannolikt är att se som ett förvaltningsbeslut med de följder som det innebär.

En tjänsteleverantör som inte vidtar de åtgärder som krävs för att säkerställa konfidentialiteten, sekretessen och integriteten enligt 13.4 i e-bevisförordningen, i vilket innefattas att efterleva operativa och tekniska krav för anslutning och användning av den tekniska lösningen, kan åläggas en sanktionsavgift av Åklagarmyndigheten, se vidare nedan i avsnitt 4.5 Underrättelse till Åklagarmyndigheten och Post- och telestyrelsen.

4.5 Underrättelse till Åklagarmyndigheten och Post- och telestyrelsen

Försäkringskassans förslag: Försäkringskassan ska få möjlighet att, utan hinder av sekretess, underrätta Åklagarmyndigheten om att en tjänsteleverantör åsidosätter sina skyldigheter enligt artikel 13.4 i e-bevisförordningen.

Försäkringskassan ska få möjlighet att, utan hinder av sekretess, underrätta Post- och telestyrelsen om förhållanden som har betydelse för Post- och telestyrelsens tillsyn och för verksamhetsställens och rättsliga ombuds åtkomst till det decentraliserade it-systemet enligt 3 §.

Skälen för förslaget: Tjänsteleverantörer är skyldiga att vidta de senaste operativa och tekniska åtgärder som krävs för att säkerställa konfidentialiteten, sekretessen och

integriteten för de uppgifter som omfattas av e-bevisförordningen (art 13.4 i e-bevisförordningen). I detta ingår att följa de operativa och tekniska krav för anslutning till och användning av den tekniska lösningen som Försäkringskassan har ställt upp. Försäkringskassan har inga möjligheter att ålägga en tjänsteleverantör som bryter mot denna skyldighet några sanktioner. Enligt föreslagna 4 kap. 1 § lagen med kompletterande bestämmelser till EU:s förordning om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis, som föreslås träda i kraft den 18 augusti 2026, ska dock Åklagarmyndigheten ta ut en sanktionsavgift av en tjänsteleverantör som åsidosätter någon av de skyldigheter som följer av artikel 10, 11 eller 13.4 i e-bevisförordningen. Om Försäkringskassan upptäcker att en tjänsteleverantör hotar konfidentialiteten, sekretessen eller integriteten i systemet enligt artikel 13.4 behöver Försäkringskassan således kunna underrätta Åklagarmyndigheten om detta, så att Åklagarmyndigheten kan ta ut en sanktionsavgift av tjänsteleverantören.

Post- och telestyrelsen föreslås få ett långtgående tillsynsansvar över tjänsteleverantörer enligt lagen om utsedda verksamhetsställen och rättsliga ombud för inhämtning av elektroniska bevis. Post- och telestyrelsen föreslås också få ett ansvar för att ansluta de utsedda verksamhetsställena och rättsliga ombuden till Försäkringskassans tekniska lösning. Om Försäkringskassan upptäcker att en tjänsteleverantör inte uppfyller de operativa och tekniska kraven för anslutning till och användning av den tekniska lösningen kan det ha betydelse för Post- och telestyrelsens tillsyn. Post- och telestyrelsen kan också ha behov av support från Försäkringskassan vid anslutningen samt information om eventuella brister i systemet. Försäkringskassan bör därför ha möjlighet att underrätta Post- och telestyrelsen om förhållanden som har betydelse för Post- och telestyrelsens tillsyn och för verksamhetsställens och rättsliga ombuds åtkomst till det decentraliserade it-systemet enligt 3 §.

Sekretess gäller för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs och åtgärden avser bl.a. telekommunikation eller system för automatiserad behandling av information samt behörighet att få tillgång till upptagning för automatiserad behandling eller annan handling (18 kap. 8 § 3 och 4 offentlighets- och sekretesslagen [2009:400] – OSL). Uppgifter om på vilket sätt en tjänsteleverantör hotar konfidentialiteten, sekretessen eller integriteten i Försäkringskassans system kan vara sådana uppgifter som bidrar till upplysning om säkerhets- eller bevakningsåtgärd.

Om den information som tjänsteleverantörerna skickar via det decentraliserade systemet hanteras av Försäkringskassan som ett led i en teknisk bearbetning eller teknisk lagring för tjänsteleverantörernas räkning på det sätt som avses i 2 kap. 13 § första stycket tryckfrihetsförordningen, omfattas eventuella uppgifter om en enskilds personliga eller ekonomiska förhållanden av sekretess enligt 40 kap. 5 § OSL (se avsnitt 4.6 om när sekretessbestämmelsen eventuellt inte är tillämplig).

För att Försäkringskassan utan hinder av sekretess ska kunna underrätta Åklagarmyndigheten om att en tjänsteleverantör åsidosätter sina skyldigheter enligt artikel 13.4 i e-bevisförordningen, krävs en sådan sekretessbrytande bestämmelse som avses i 10 kap. 28 § OSL. Detsamma gäller för att Försäkringskassan ska kunna underrätta Post- och telestyrelsen om att en tjänsteleverantör bryter mot de operativa och tekniska kraven.

En underrättelse bör kunna omfatta både uppgiften att en tjänsteleverantör åsidosätter sina skyldigheter och bakgrundsuppgifter.

En förutsättning för en sekretessbrytande bestämmelse bör vara att uppgifter som är sekretessbelagda hos Försäkringskassan omfattas av sekretess även hos mottagaren. Det bör därför utredas vilken sekretess som kan vara aktuell hos mottagaren.

4.6 Dataskydd

Försäkringskassans bedömning: Ansvarsfördelningen ur dataskyddsrättslig synpunkt mellan Försäkringskassan och tjänsteleverantörer bör fastställas i författning.
Om Försäkringskassan ska vara personuppgiftsbiträde krävs även kompletterande reglering som motsvarar ett personuppgiftsbiträdesavtal.

Skälen för bedömningen

Ansvarsfördelningen

Försäkringskassan har i tidigare svar på regeringsuppdrag bedömt att myndighetens befattning med de meddelanden som skickas via den gemensamma nationella åtkomstpunkten enligt e-codexförordningen får anses ske som ett led i en teknisk bearbetning eller teknisk lagring på det sätt som avses i 2 kap. 13 § första stycket TF (FK 2024/011223). Det innebär att de uppgifter som skickas via åtkomstpunkten inte blir allmänna handlingar hos Försäkringskassan. När personuppgifter skickas via åtkomstpunkten, behandlar Försäkringskassan dem i egenskap av personuppgiftsbiträde.

Försäkringskassan kommer, med anledning av det nu aktuella uppdraget, endast att vidta de åtgärder som är nödvändiga för att kunna vidarebefordra information via den tekniska lösningen för elektroniska bevis och åtkomstpunkten (jfr. prop. 2022/23:97 s. 16–17). Försäkringskassan kommer inte att använda informationen för egen räkning. Försäkringskassan kommer således ur ett offentlighets- och sekretessperspektiv att hantera informationen som ett led i en teknisk bearbetning eller teknisk lagring. Personuppgiftsbehandlingen kommer därmed att ske för de utfärdande myndigheternas respektive tjänsteleverantörernas räkning. Det innebär att Försäkringskassan, baserat på faktiska förhållanden, får anses vara personuppgiftsbiträde i förhållande till de utfärdande myndigheterna och de anslutna tjänsteleverantörerna.

En biträdesroll kan dock ge upphov till säkerhetsrisker för Försäkringskassan (se särskilt artikel 28.3 h i dataskyddsförordningen). Det gäller i synnerhet om Försäkringskassan är personuppgiftsbiträde till privata tjänsteleverantörer. Det talar emot att Försäkringskassan ska ges rollen som personuppgiftsbiträde i förhållande till privata tjänsteleverantörer.

Eftersom ändamål och medel för Försäkringskassans personuppgiftsbehandling regleras i e-bevisförordningen och genomförandeförordningen bör det vara möjligt att i nationell rätt utse Försäkringskassan som personuppgiftsansvarig för den begränsade behandling som myndigheten utför (artikel 4.7 i dataskyddsförordningen). Det är dock tveksamt om Försäkringskassan bör vara personuppgiftsansvarig för en personuppgiftsbehandling som myndigheten enbart utför för någon annans räkning. Det är också tveksamt om en myndighet i egenskap av personuppgiftsansvarig kan anses behandla uppgifter för enbart teknisk bearbetning eller teknisk lagring. Det innebär i så fall bland annat att uppgifterna blir allmänna handlingar hos Försäkringskassan och att uppgifterna inte kommer att omfattas av sekretess.

Sammantaget finns behov av att regeringen avgör om Försäkringskassan ska agera som personuppgiftsansvarig eller personuppgiftsbiträde.

Det krävs reglering i författning
Eftersom de faktiska förhållandena talar för att Försäkringskassan är personuppgiftsbiträde, krävs att personuppgiftsansvaret fastställs i författning om Försäkringskassan ska anses vara personuppgiftsansvarig (artikel 4.7 i dataskyddsförordningen). Relationen mellan Försäkringskassan, i egenskap av personuppgiftsansvarig, och en personuppgiftsansvarig tjänsteleverantör behöver inte regleras.

Om regeringen anser att Försäkringskassan ska agera som personuppgiftsbiträde åt personuppgiftsansvariga tjänsteleverantörer, måste relationen med tjänsteleverantörerna regleras i författning. Normalt sett regleras en sådan relation i ett avtal. Eftersom tjänsteleverantörernas anslutning till det decentraliserade it-systemet inte bygger på frivillighet, är det emellertid inte möjligt att reglera hanteringen och ansvarsfördelningen genom att upprätta biträdesavtal mellan tjänsteleverantörerna och Försäkringskassan. Hanteringen måste därför framgå av unionsrätten eller av nationell rätt, som är bindande för personuppgiftsbiträdet med avseende på den personuppgiftsansvarige och anger vissa uppgifter och krav (artikel 28.3 i dataskyddsförordningen).

Försäkringskassan bedömer att e-bevisförordningen och genomförandeförordningen, tillsammans med ett uppdrag för Försäkringskassan att tillhandahålla aktuell teknisk lösning, får anses utgöra sådan unionsrätt och nationell rätt som enligt artikel 28.3 i dataskyddsförordningen kan ersätta ett biträdesavtal. En stor del av de tekniska kraven på lösningen, inklusive standarder för säkerhet och tillgänglighet, är reglerad i e-bevisförordningen och genomförandeförordningen. Det finns dock behov av kompletterande reglering för att regleringen sammantaget ska kunna ersätta ett biträdesavtal. En sådan kompletterande reglering bör bland annat avse krav på Försäkringskassan i enlighet med artikel 28.3 b–h i dataskyddsförordningen.

Till skillnad från vad som gäller i fråga om personuppgiftsansvar, framgår det inte av dataskyddsförordningen att ett personuppgiftsbiträde kan utses i nationell rätt (artikel 4.7 jämfört med artikel 4.8 i dataskyddsförordningen). När uppgifter behandlas av ett biträde kan hanteringen dock regleras antingen genom ett avtal eller genom unionsrätt eller nationell rätt (artikel 28.3 i dataskyddsförordningen). Försäkringskassan noterar också att biträdesrollen har fastställts i artikel 23.3 i Europaparlamentets och rådets förordning (EU) 2023/969 av den 10 maj 2023 om inrättande av en samarbetsplattform till stöd för gemensamma utredningsgruppers funktion och om ändring av förordning (EU) 2018/1726. Biträdesrollen har där fastställts i enlighet med Europaparlamentets och rådets förordning (EU) 2018/1725 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter, och inte i enlighet med dataskyddsförordningen. Definitionen av biträdesrollen är dock densamma i båda EU-förordningarna. Mot den bakgrunden bedömer Försäkringskassan att det är möjligt att i författning utpeka Försäkringskassan som biträde. För att Försäkringskassans roll som biträde ska bli tydlig och ostridig föreslår Försäkringskassan därför, om regeringen bedömer att Försäkringskassan ska vara personuppgiftsbiträde, att biträdesrollen ska framgå av författning.

När Försäkringskassan behandlar personuppgifter av andra skäl än för att hantera sådan information som skickas via den tekniska lösningen för utfärdande myndighets eller tjänsteleverantörs räkning, kommer Försäkringskassan att vara personuppgiftsansvarig. Det kan vara aktuellt exempelvis vid administration med anledning av uppdraget. Detta behöver inte regleras särskilt.

4.7 Ikraftträdande

Försäkringskassans förslag: Den föreslagna bestämmelsen med bemyndigande för Försäkringskassan att meddela föreskrifter om vilka operativa och tekniska åtgärder som tjänsteleverantörerna ska vidta för att säkerheten och tillgängligheten i den tekniska lösningen ska kunna upprätthållas ska träda i kraft den 15 juni 2026.

Skälen för förslaget: I Försäkringskassans uppdrag ingår att åtkomsten till den tekniska lösningen ska finnas tillgänglig för tjänsteleverantörer från och med den 18 augusti 2026. Eftersom Försäkringskassan har ansvar för att den tekniska lösningen är säker och tillgänglig och för eventuella skador som uppstår i systemet, behöver Försäkringskassan kunna ställa krav på tjänsteleverantörer att vidta nödvändiga operativa och tekniska åtgärder innan de kan ges åtkomst till den. Försäkringskassans föreskrifter om vilka operativa och tekniska åtgärder som tjänsteleverantörerna ska vidta för att säkerheten och tillgängligheten i den tekniska lösningen ska kunna upprätthållas behöver därför träda i kraft senast samma dag som den tekniska lösningen görs tillgänglig för tjänsteleverantörerna.

En författning som kungörs i en tryckt författningssamling, som Försäkringskassans författningssamling är, ska om möjligt ges ut så att den är författningssamlingens abonnenter till handa i god tid innan den träder i kraft (22 § författningssamlings-förordningen [1976:725]). Ikraftträdandedatumet bör normalt sättas så att författningen kan komma ut från trycket minst fyra veckor före ikraftträdandet, så att de som berörs får tillräckligt med tid för att anpassa sig till de nya bestämmelserna. En författning bör endast i speciella undantagsfall komma ut från trycket senare än två veckor före ikraftträdandet.[7] Fyra veckor före den 18 augusti 2026 är den 21 juli 2026. För att ge tid för tryckning av föreskrifterna behöver beslut fattas senast den 15 juli 2026. Detta är således det senaste datum som bemyndigandet för Försäkringskassan att besluta föreskrifterna behöver träda i kraft om åtkomst till den tekniska lösningen ska finnas tillgänglig för tjänsteleverantörer från och med den 18 augusti 2026. Försäkringskassan anser inte att det är lämpligt att i detta fall tillämpa undantagsregeln om att en författning i speciella undantagsfall kan komma ut från trycket två veckor före ikraftträdandet, eftersom det rör sig om tvingande, betungande regler som berör en stor grupp enskilda (företag).

Den 15 juli 2026 är dock mitt i sommaren och med tanke på behovet av att före den 18 augusti 2026 hinna informera alla berörda tjänsteleverantörer om dessa tvingande och betungande regler, anser Försäkringskassan att föreskrifterna bör kungöras före midsommar. Försäkringskassans önskemål är därför att bestämmelsen med bemyndigande för Försäkringskassan att meddela föreskrifter om vilka operativa och tekniska åtgärder som tjänsteleverantörerna ska vidta för att säkerheten och tillgängligheten i den tekniska lösningen ska kunna upprätthållas träder i kraft senast den 15 juni 2026. Då skulle Försäkringskassan kunna fatta beslut om föreskrifterna samma dag och föreskrifterna kunna komma ut från trycket den 18 juni 2026. Föreskrifterna skulle då kunna träda i kraft den 16 juli 2026. Detta skulle ge mer tid för att informera om bestämmelserna och för berörda företag att anpassa sig till dem till den 18 augusti 2026.

Om bestämmelsen med bemyndigande för Försäkringskassan att meddela föreskrifter om vilka operativa och tekniska åtgärder som tjänsteleverantörerna ska vidta för att säkerheten och tillgängligheten i den tekniska lösningen ska kunna upprätthållas inte träder i kraft förrän den 18 augusti 2026 eller senare blir konsekvensen att

[7] Myndigheternas föreskrifter, SB PM 2025:4, s. 90

Försäkringskassan inte kan genomföra sitt uppdrag att ansluta tjänsteleverantörer till det decentraliserade it-systemet från och med den 18 augusti 2026. Om beslut om föreskrifterna fattas den 18 augusti 2026, kan de, om huvudregeln följs, tidigast träda i kraft den 18 september 2026. Om man anser att det finns skäl att frångå huvudregeln kan tidsperioden mellan beslut och ikraftträdande kortas, men då kortas också tidsperioden för att informera berörda företag om de beslutade föreskrifterna.

Post- och telestyrelsen har ansvar för kommunikation med tjänsteleverantörer om sådant som gäller möjligheten att ansluta till och använda det decentraliserade it-systemet.[8] Försäkringskassan kommer därför att samarbeta med Post- och telestyrelsen för att bidra med information om vilka operativa och tekniska åtgärder som tjänsteleverantörerna ska vidta för att säkerheten och tillgängligheten i den tekniska lösningen ska kunna upprätthållas.

Övriga föreslagna bestämmelser behöver också träda i kraft senast samma dag som Försäkringskassan ger tjänsteleverantörerna åtkomst till den tekniska lösningen.

[8] Regeringens uppdrag till Post- och telestyrelsen att hantera administration, kommunikation och kontakter med andra aktörer än myndigheter med uppkoppling till e-Codex, dnr Ju2025/02286

5 Konsekvensutredning

5.1 Syftet med förslagen

Syftet med förslagen i denna framställning är att ge Försäkringskassan rättsliga förutsättningar att utföra sitt uppdrag att drifta och förvalta en teknisk lösning som möjliggör för tjänsteleverantörer att ansluta sig och få åtkomst till det decentraliserade it-systemet e-Codex i enlighet med artikel 19 i e-bevisförordningen från och med den 18 augusti 2026.

5.2 Alternativa lösningar

5.2.1 Försäkringskassan uppdrag

Om Försäkringskassans uppdrag inte regleras i författning kommer det att råda osäkerhet om var ansvaret för personuppgiftsbehandlingen ligger, vilket kan leda till ifrågasättanden från tjänsteleverantörernas sida. Vidare kommer gränsdragningen mellan Försäkringskassans och Post- och telestyrelsens uppdrag att vara fortsatt otydlig. Därtill kommer myndigheten att sakna ett generellt stöd för sitt arbete när det innevarande regeringsuppdraget slutrapporteras år 2027, eftersom e-Codex inte omfattas av myndighetens instruktionsenliga uppdrag.

5.2.2 Bemyndigande till Försäkringskassan

Försäkringskassan har övervägt de alternativa sätt som finns för att uppställa krav på alla tjänsteleverantörer som omfattas. Villkoren för anslutning kan inte regleras genom avtal mellan Försäkringskassan och respektive tjänsteleverantörer, eftersom tjänsteleverantörer är skyldiga att ansluta sig till den tekniska lösningen och det således inte rör sig om frivilliga överenskommelser. Försäkringskassan bedömer att det inte heller är lämpligt att villkoren fastställs i beslut om anslutning av respektive tjänsteleverantörer. Skälet för detta är framför allt att något beslutsförfarande vad gäller anslutningen till den tekniska lösningen inte finns beskrivet eller reglerat i det författningspaket genom vilket Sverige ansluter sig till EU:s system för gränsöverskridande inhämtning av elektroniska bevis. Ett annat skäl är att det skulle vara mycket administrativt krävande för Försäkringskassan att fatta dessa beslut och att fatta nya beslut avseende varje tjänsteleverantörer när det uppstår behov av att ändra villkoren.

Om Försäkringskassan inte kan uppställa operativa och tekniska krav på tjänsteleverantörer i samband med deras anslutning och användning av den tekniska lösningen medför det en risk för att Försäkringskassan inte kan tillhandahålla en säker och tillgänglig tjänst enligt kraven i e-bevisförordningen och genomförandeförordningen, samt en ökad risk för att skador uppstår vid användning av systemet. Ansvaret för dessa skador bärs av Försäkringskassan, vilket kan innebära ekonomiska konsekvenser för myndigheten, till exempel i form av skadestånd. Det kan också innebära ökad risk för cybersäkerhets- och personuppgiftsincidenter.

Ett alternativ till att ge Försäkringskassan rätt att besluta föreskrifter om vilka operativa och tekniska åtgärder som tjänsteleverantörerna ska vidta för att säkerheten och tillgängligheten i den tekniska lösningen är att ge någon annan myndighet, till exempel Post- och telestyrelsen, ett sådant bemyndigande. Eftersom det är Försäkringskassan som ansvarar för att tillhandahålla en säker och tillgänglig tjänst enligt e-bevisförordningen och genomförandeförordningen anser Försäkringskassan dock att det är lämpligare att Försäkringskassan ges rätt att besluta föreskrifterna.

5.2.3 Tillfällig avstängning

Om Försäkringskassan inte ges möjlighet att tillfälligt stänga av tjänsteleverantörer som hotar säkerheten och tillgängligheten i den tekniska lösningen kan Försäkringskassan inte utföra sitt uppdrag att tillhandahålla en säker och tillgänglig tjänst enligt e-bevisförordningen och genomförandeförordningen. Det skulle medföra en ökad risk för att skador uppstår för andra tjänsteleverantörer vid användning av den tekniska lösningen. Ansvaret för dessa skador bärs av Försäkringskassan, vilket kan innebära ekonomiska konsekvenser, till exempel i form av skadestånd. Det kan också innebära ökad risk för cybersäkerhets- och personuppgiftsincidenter.

5.2.4 Underrättelse till Åklagarmyndigheten och Post- och telestyrelsen

En alternativ lösning för att se till att tjänsteleverantörer, som inte vidtar de operativa och tekniska åtgärder som krävs, åläggs sanktioner är att Försäkringskassan ges en rätt att besluta om sanktionsavgifter. En sådan rätt kräver dock reglering i lag. Regeringen har också redan föreslagit att Åklagarmyndigheten får rätt att besluta om sanktioner vid brott mot artikel 13.4 i e-bevisförordningen. Försäkringskassan anser därför att den lämpligaste lösningen är att Försäkringskassan ges möjlighet att underrätta Åklagarmyndigheten om en tjänsteleverantör inte uppfyller sina skyldigheter enligt artikel 13.4, så att Åklagarmyndigheten kan besluta om sanktionsavgift.

Om Försäkringskassan inte ges möjlighet att underrätta Åklagarmyndigheten blir konsekvensen att tjänsteleverantörer kan undgå sanktioner och att det inte finns något påtryckningsmedel för att förmå dem att följa de uppställda tekniska kraven.

Om Försäkringskassan inte ges möjlighet att underrätta Post- och telestyrelsen blir konsekvensen att tillsynen över lagen riskerar att försvagas på grund av att Post- och telestyrelsen inte får information om att en tjänsteleverantör bryter mot de tekniska kraven eller annan väsentlig information som Försäkringskassan får kännedom om. Det kan också påverka tjänsteleverantörernas anslutning till Försäkringskassans tekniska lösning, eftersom Post- och telestyrelsen administrerar anslutningen.

5.2.5 Dataskyddsregel

Oavsett om Försäkringskassan ska agera personuppgiftsansvarig eller personuppgiftsbiträde krävs reglering i författning. Det framgår av artikel 4.7 respektive 28.3 i dataskyddsförordningen. En reglering som motsvarar kraven i artikel 28.3 i dataskyddsförordningen är nödvändig när ett personuppgiftsbiträde behandlar personuppgifter. Viss reglering finns i e-bevisförordningen och genomförandeförordningen men den behöver kompletteras.

Om Försäkringskassans biträdesroll inte fastställs i författning finns risk för viss osäkerhet och ett utrymme att ifrågasätta ansvarsförhållandena.

5.3 Integritetsanalys

Det nu aktuella regeringsuppdraget innebär att Försäkringskassan kommer att behandla sådana personuppgifter som skickas via Försäkringskassans tekniska lösning. Flertalet förslag i den här framställningen medför ingen utökad personuppgiftsbehandling i förhållande till den behandling som regeringsuppdraget medför. Försäkringskassan gör ingen integritetsanslys avseende den personuppgiftsbehandling som följer av regeringsuppdraget.

Förslaget som avser en möjlighet att utan hinder av sekretess lämna underrättelser till Åklagarmyndigheten och Post- och telestyrelsen innebär en nyhet i förhållande till

uppdraget och kan komma att medföra personuppgiftsbehandling. En uppgift om att en tjänsteleverantör inte har fullgjort sina skyldigheter är visserligen i de flesta fall en uppgift om en juridisk person, dvs. inte en personuppgift. En tjänsteleverantör skulle dock teoretiskt sett även kunna vara en enskild firma, vilket innebär att en uppgift om firman då är en personuppgift. En underrättelse bör vidare kunna omfatta information om vad som föranleder Försäkringskassan att lämna en underrättelse och sådan bakgrundsinformation kan komma att omfatta personuppgifter. Det innebär att förslagen i framställningen kan komma att medför en viss utökad personuppgiftsbehandling i förhållande till vad som följer av regeringsuppdraget.

I regeringsformen finns grundläggande bestämmelser till skydd för den personliga integriteten. Var och en är gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden (2 kap. 6 § andra stycket RF). I förarbetena till regeringsformen anges att vid bedömningen av om en åtgärd innebär kartläggning ska åtgärdens effekter snarare än det huvudsakliga syftet med åtgärden beaktas. Det anges vidare att ett betydande intrång bland annat avgörs utifrån uppgifternas karaktär och omfattning samt ändamålet med behandlingen (prop. 2009/10:80 s. 181 och 184). Det förväntade utbytet av personuppgifter är begränsat, både i fråga om omfattning och antalet individer. Till Åklagarmyndigheten kommer Försäkringskassan företrädelsevis att lämna uppgifter om omständigheten att en tjänsteleverantör inte har uppfyllt kraven på säkerhet. Uppgifterna skulle kunna omfatta uppgifter om ett rättsligt ombud. I enstaka fall skulle eventuell bakgrundinformation också kunna omfatta personuppgifter. Uppgiftsutbytet med Post- och telestyrelsen förväntas främst röra tjänsteleverantörers anslutning, vilket också kan omfatta uppgifter om rättsliga ombud. Den utökade underrättelseskyldigheten bedöms endast marginellt påverka Åklagarmyndighetens respektive Post- och telestyrelsens förmåga att kartlägga enskilda. Förslagen i promemorian innebär således inte ett sådant betydande intrång i den personliga integriteten att 2 kap. 6 § andra stycket RF blir tillämplig.

För Försäkringskassans personuppgiftsbehandling gäller bestämmelserna i dataskyddsförordningen. Bestämmelserna i 114 kap. SFB, som är Försäkringskassans registerförfattning, gäller endast i verksamhet som avser förmåner och ersättningar. Försäkringskassan kommer att behandla personuppgifter med anledning av förslagen i framställningen med stöd av artikel 6.1 c och e i dataskyddsförordningen. Den rättsliga grunden för personuppgiftsbehandling i den tekniska lösningen finns i uppdraget att tillhandahålla den tekniska lösningen, som för närvarande är fastställt i regeringsuppdraget men som behöver permanentas enligt förslagen i framställningen. Den rättsliga grunden för att lämna uppgifter till Åklagarmyndigheten och Post- och telestyrelsen finns i den föreslagna underrättelsemöjligheten.

Den nationella rätt som fastställer grunden för en personuppgiftsbehandling ska uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas (artikel 6.3 andra stycket sista meningen i EU:s dataskyddsförordning). En bestämmelse om underrättelsemöjlighet avser att uppfylla syftet med e-bevisförordningen genom att skapa dels förutsättningar för Åklagarmyndigheten att besluta om sanktioner, dels förutsättningar för Post- och telestyrelsen att administrera anslutning till Försäkringskassans tekniska lösning. Underrättelsemöjligheten omfattar sådana uppgifter som är nödvändiga för att Åklagarmyndigheten och Post- och telestyrelsen ska kunna utföra sina uppdrag. Personuppgiftsbehandlingen får anses proportionerlig i förhållande till målet att skapa en fungerande administration för hanteringen enligt e-bevisförordningen.

När personuppgifter delas mellan flera myndigheter, får fler personuppgiftsansvariga och enskilda användare åtkomst till uppgifterna. En spridning av personuppgifter utgör i

sig en integritetsrisk. Överföringen av personuppgifter ska därför ske på ett säkert sätt. Den personuppgiftsansvariga myndigheten ansvarar för att genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken samt för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen. Vissa personuppgifter kan omfattas av sekretess hos Försäkringskassan, vilket framgår av avsnitt 4.5. Under förutsättning att eventuellt sekretessbelagda uppgifter även skyddas av sekretess hos mottagaren får den personuppgiftsbehandling som möjliggörs av förslagen anses utgöra en godtagbar inskränkning av skyddet för den personliga integriteten.

5.4 Ekonomiska konsekvenser

5.4.1 Konsekvenser för Försäkringskassan

Försäkringskassan kommer att ha vissa kostnader för att ta fram och publicera föreskrifter, men dessa kostnader bedöms rymmas inom anslaget. Försäkringskassan räknar med att det ingår i Post- och telestyrelsens uppdrag att informera tjänsteleverantörerna om de operativa och tekniska krav som ställs på dem, varför Försäkringskassan inte kommer att ha några kostnader för detta.

5.4.2 Konsekvenser för andra myndigheter

Åklagarmyndigheten och Post- och telestyrelsen kommer att ha vissa kostnader för att ta hand om underrättelser från Försäkringskassan om att tjänsteleverantörer bryter mot tekniska krav. Dessa kostnader bedöms dock bli mycket små.

5.4.3 Konsekvenser för försäkringsutgifterna

Förslagen rör inte socialförsäkringen och har därför inga konsekvenser för försäkringsutgifterna.

5.4.4 Konsekvenser för enskilda

De tekniska krav som i förlängningen kommer att ställas på tjänsteleverantörerna genom föreskrifter beslutade av Försäkringskassan, kan medföra kostnader för de tjänsteleverantörer som inte redan uppfyller dem.

5.5 Förenlighet med EU-rätten

Försäkringskassan bedömer att förslagen inte strider mot EU-rätten.

Beslut i detta ärende har fattats av rättschef Ingrid Utne i närvaro av avdelningschef Peter Haglind och rättsliga experterna Emma Boman och Hélène Runsten, de senare som föredragande.

INGRID UTNE

Emma Boman

Hélène Runsten