Diarienummer
FK 2024/006423

Digitalisering på Försäkringskassan

En vägledning innehåller en samlad information om vad som gäller på det aktuella området.

En vägledning kan innehålla beskrivningar av

- författningsbestämmelser
- allmänna råd
- förarbeten
- rättspraxis
- JO:s beslut.

Vägledningarna uppdateras fortlöpande. Ändringar arbetas in i den digitala versionen. Den digitala versionen hittar du på forsakringskassan.se. Sök på ”vägledningar”.

Du som arbetar på Försäkringskassan hittar dem också på Fia.

Upplysningar: Försäkringskassan
Rättsavdelningen

Beslutad 2024-09-20

Innehåll

Sammanfattning **8**

Läsanvisningar **9**

1 Inledning **10**
1.1 Syftet med denna vägledning 10
1.2 Begrepp i vägledningen 11
1.3 Hur vägledningen förhåller sig till annat internt och externt material av särskild betydelse 12
1.4 Särskilt om juridikens och juristens roll i utvecklingsarbete 13

2 Centrala rättsprinciper och regelverk **14**
2.1 Centrala rättsprinciper 14
2.1.1 Legalitetsprincipen 14
2.1.2 Principerna om demokrati och fri åsiktsbildning 15
2.1.3 Principerna om likabehandling och objektivitet 15
2.1.4 Principen om respekt och icke-diskriminering 16
2.1.5 Principerna om effektivitet och service 17
2.1.6 Proportionalitetsprincipen 18
2.2 Centrala regelverk 18
2.2.1 SDG-förordningen 18
2.2.2 eIDAS-förordningen 19
2.2.3 Dataskyddsregelverket 19
2.2.4 Socialförsäkringsbalken 20
2.2.5 Regler om offentlighet och sekretess 22
2.2.6 Arkivrättsliga regelverket 23
2.2.7 Förvaltningslagen 24
2.2.8 DOS-lagen 24
2.2.9 Informationssäkerhet 25
2.2.10 Säkerhetsskydd 26

3 Digitala tjänster **28**
3.1 Olika slags digitala tjänster 28
3.1.1 Självbetjäningstjänster 28
3.1.2 Servicetjänster 29
3.1.3 Presentationstjänster 30
3.1.4 Bastjänster 30
3.1.5 Hjälptjänster 30
3.1.6 Eget utrymme 31
3.1.7 Digitala tjänster för informationsutbyte 32
3.2 Försäkringskassans digitala tjänster 32
3.2.1 Mina sidor för privatpersoner 32
3.2.2 Självbetjäningstjänster för förmåner och ersättningar 32
3.2.3 SSBTEK och LEFI Online 33
3.2.4 Arbetsgivartjänster 33
3.2.5 Försäkringskassans app 33
3.3 Alla har inte tillgång till digitala tjänster 33
3.3.1 Personer som saknar e-legitimation 33
3.3.2 Personer med skyddade personuppgifter (SID) 34
3.3.3 Personer med ställföreträdare 34

4 Elektronisk legitimering och underskrift 36
4.1 E-legitimation 36
4.1.1 Aktörer bakom e-legitimationen 36
4.1.2 Internationell legitimering 37
4.1.3 E-legitimering vid statliga digitala tjänster 37
4.1.4 Tillitsnivåer på e-legitimationer 38
4.1.5 EFOS 38
4.1.6 Privat e-legitimation i tjänsten 39
4.2 Elektronisk underskrift 39
4.2.1 Betrodd tjänst 40
4.2.2 Aktörer vid användning av e-underskrifter 41
4.2.3 Formkrav och underskrifter 41
4.2.4 Äkthet och bevisverkan 42
4.2.5 Allmänna handlingar, bevarande och gallring 43
4.2.6 Signeringstexter och signeringsfunktioner 44
4.2.7 Flerpartssignering 45
4.2.8 Ställföreträdare 45
4.2.9 Elektroniska underskrifter inom Försäkringskassan 46
4.3 Personuppgiftsansvar 46
4.4 Missbruk och straffrättsligt ansvar 47

5 Automatiserad handläggning och beslut 48
5.1 Tekniken vid automatisering 49
5.1.1 Regelbaserade eller maskininlärande system 49
5.1.2 Särskilt om AI 49
5.2 Rättsliga frågeställningar vid automation 51
5.2.1 Rättssäkerhet och legalitet 52
5.2.2 Grundläggande fri- och rättigheter 53
5.2.3 Demokrati och fri åsiktsbildning 54
5.2.4 Objektivitet, likabehandling och icke-diskriminering 54
5.2.5 God offentlighetsstruktur och sekretess 54
5.2.6 Behandling av personuppgifter 55
5.2.7 Transparens och dokumentation 57
5.3 Ett automatiserat förfarande i ärendehandläggningen 57
5.3.1 Utforma ansökan 58
5.3.2 Automatiska kontroller i ansökningsförfarandet 59
5.3.3 Manuella alternativ till ett automatiserat förfarande 60
5.3.4 Nudging 60
5.3.5 Utredning och kommunicering 61
5.3.6 Beslut 62
5.3.7 Krav på dokumentation vid automatiserad ärendehantering 63

6 Digitala tjänster för informationsutbyte 66
6.1 Överväganden kring sekretess 66
6.1.1 Sekretessbrytande regler 66
6.1.2 Rätten att bryta sekretess för att ställa en fråga 67
6.1.3 Sekretess gäller när mottagaren antas behandla personuppgifter i strid med dataskyddsreglerna 68
6.2 Behandling av personuppgifter 68
6.2.1 Omfattningen av personuppgiftsansvaret 68
6.2.2 Vi behöver stöd för att behandla personuppgifter i informationsutbytet 68

Källförteckning.....71

Förkortningar och ordförklaringar

Förkortning eller ord	Förklaring
AI	Artificiell intelligens
AI-förordningen	Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens)
Barnkonventionen	Förenta nationernas konvention om barnets rättigheter
BrB	Brottsbalken
Dataskyddsförordningen	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
Dataskyddslagen	Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning
Digg	Myndigheten för digital förvaltning
DOS-lagen	Lagen (2018:1937) om tillgänglighet till digital offentlig service
Ds	Departementsskrivelse
eIDAS-förordningen	Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG
eSam	eSamverkansprogrammet
Europakonventionen	Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna
EU:s rättighetsstadga	Europeiska unionens stadga om de grundläggande rättigheterna (2010/C 83/02)
FL	Förvaltningslagen (2017:900)
FKFS	Försäkringskassans föreskrifter
HFD	Högsta förvaltningsdomstolen
HSFL-FS	Gemensamma författningssamlingen avseende hälso- och sjukvård, socialtjänst, läkemedel, folkhälsa m.m.
LEFI ONLINE	Leverera förmånsinformation
JO	Justitieombudsmannen
MSB	Myndigheten för samhällsskydd och beredskap
OSL	Offentlighets- och sekretesslagen (2009:400)
Prop.	Proposition
RÅ	Regeringsrättens årsbok
RF	Regeringsformen

Förkortning eller ord	Förklaring
SAMU	Strukturerad analys av medicinska underlag
SDG-förordningen	Europaparlamentets och rådets förordning (EU) 2018/1724 av den 2 oktober 2018 om inrättande av en gemensam digital ingång för tillhandahållande av information, förfaranden samt hjälp- och problemlösningstjänster och om ändring av förordning (EU) nr 1024/2012
SOU	Statens offentliga utredningar
STL	Lagen (2008:145) statligt tandvårdsstöd
TF	Tryckfrihetsförordningen

Sammanfattning

I den här vägledningen kan du läsa om de nationella och internationella regelverk samt rättsprinciper som är av störst betydelse i arbetet med att utveckla digitala tjänster på Försäkringskassan. Även praxis och andra rättskällor på området berörs.

Vägledningen ska bidra till att de som arbetar med utveckling av digitala tjänster i Försäkringskassans kärnverksamhet ska få en större möjlighet att hantera de viktigaste och vanligaste rättsliga frågeställningarna som aktualiseras vid dessa utvecklingsinsatser.

Läsanvisningar

Vägledningen ska vara ett stöd för Försäkringskassans medarbetare vid utveckling av digitala tjänster i Försäkringskassans kärnverksamhet. Den ger rättslig vägledning genom att beskriva de rättsliga utmaningar som ofta uppkommer, relevanta regelverk och andra krav. Läs mer om syftet med vägledningen i kapitel 1.

Hänvisningar

I vägledningen finns hänvisningar till nationella och internationella regelverk, bland annat lagar, förordningar och föreskrifter. Det finns också hänvisningar till interna styrdokument, förarbeten, rättsfall, myndighetsbeslut och andra vägledningar. Dessa hänvisningar finns antingen i löpande text eller inom parentes i direkt anslutning till den mening eller det stycke den avser.

Sist i vägledningen finns en källförteckning som redovisar de lagar, förordningar, domar med mera som nämns i vägledningen.

Att hitta rätt i vägledningen

I vägledningen finns en innehållsförteckning. Den är placerad först och ger en översiktsbild av vägledningens kapitel och avsnitt. Med hjälp av fliken ”Bokmärken” i vänsterkanten kan du navigera mellan avsnitten. Det finns också en sökfunktion för att hitta enstaka ord och begrepp.

1 Inledning

Att digitalisera kan länge sägas ha handlat om en omvandling – att införa digital teknik eller att omvandla till digital form. Traditionell informationshantering och manuella arbetssätt har ersatts av eller kompletterats med digitala. Det kan exempelvis handla om elektroniska handlingar istället för handlingar i pappersform, elektroniska underskrifter istället för egenhändigt undertecknade pappershandlingar eller digitala kontaktvägar istället för papperspost, fax eller telefon.

För att hantera digital information och processer har det utvecklats olika *digitala tjänster* för ansökan eller för informationsutbyte med andra myndigheter.

Omvandlingen från det manuella eller pappersbundna till det digitala har nu pågått så pass länge att det digitala på många sätt är det normala. I framtiden kommer den digitala utvecklingen handla mindre om att byta ut något vi tidigare gjort på ett sätt till att göra det på ett annat sätt (digitalt). Det kommer i stället troligtvis handla om att med hjälp av teknikens möjligheter fortsätta utveckla, effektivisera och göra både nya och befintliga digitala tjänster mer rättssäkra. Men vi kommer också ha anledning att fråga oss om vi kan göra helt nya saker, på helt nya sätt, med hjälp av ny teknik.

Digitaliseringen skapar stora förväntningar på Försäkringskassan att utnyttja den nya teknikens möjligheter. Då är det viktigt att komma ihåg att digitalisering inte är ett mål i sig utan ett medel för att nå andra vinster – att utföra Försäkringskassans uppdrag på bästa sätt. Det finns många regelverk och principer som vi måste följa. Vi förväntas också använda våra resurser på ett korrekt och effektivt sätt.

Den här vägledningen använder genomgående begreppet *digital*, utom i de fall det i regelverk eller styrande dokument står *elektronisk*, som tidigare var det vedertagna begreppet.

1.1 Syftet med denna vägledning

Den här vägledningen ger rättslig vägledning till de medarbetare inom Försäkringskassan som arbetar aktivt med verksamhetsutveckling eller kommer i kontakt med utvecklingsfrågor. Målgruppen är särskilt jurister, verksamhetsutvecklare, och andra projektdeltagare.

Vägledningens fokus ligger på de rättsliga utmaningar som vi ofta ställs inför när vi utvecklar digitala tjänster i kärnverksamheten. Det handlar alltså primärt om digitala tjänster med koppling till handläggning av försäkringsärenden. I viss utsträckning berörs teknik och funktionalitet som i vart fall i dagsläget inte används för att utveckla digitala tjänster, men som kan förekomma i andra slags it-stöd. Ett exempel på detta är artificiell intelligens, AI, som i dagsläget inte används i tjänster som är tillgängliga externt.

Vägledningen beskriver gällande regelverk och andra krav. Den ska bidra till att öka rättssäkerheten i Försäkringskassans utvecklingsinsatser genom att hjälpa berörda medarbetare att identifiera de viktigaste och vanligaste rättsfrågorna samt att tillämpa regelverken. Den skapar också förutsättningar för att bedriva utvecklingsarbetet så effektivt som möjligt. Däremot är den *inte* en processbeskrivning eller uttömmande redogörelse av alla rättsliga frågor kopplade till utveckling av digitala tjänster på Försäkringskassan.

Digitalisering är ett område som hela tiden utvecklas. Utvecklingen medför ständigt nya juridiska utmaningar som vi behöver utreda och förhålla oss till. Det kan därför finnas frågor som vi ännu inte hunnit skriva om i den här första versionen av vägledningen.

Avsikten är att vägledningen ska revideras löpande och fortsätta utvecklas för att innehålla relevant och aktuell rättslig vägledning i de frågor vi ofta ställs inför när vi utvecklar digitala tjänster.

Den här vägledningen kan inte ge svar på alla frågor. Ibland kan det uppstå situationer där det inte finns något givet svar på en specifik rättsfråga eller det finns en osäkerhet kring hur man lämpligen bör gå tillväga för att utforma en tjänst på ett visst sätt. Det kanske inte direkt finns någon lösning, vare sig i aktuella regelverk eller i praxis. I sådana fall är avsikten att vägledningen så långt som möjligt ska beskriva den rättsliga frågeställningen och den ledning som finns att ge.

Ibland innebär befintligt regelverk eller osäkerhet kring hur regelverket ska tolkas som ett hinder mot att utveckla en digital tjänst på det sätt som verksamheten har behov av. I sådana fall kan det bli aktuellt att överväga en framställan om författningsändring för att det identifierade behovet ska kunna tillmötesgås.

Läs mer

Redan i samband med regelutveckling kan det vara aktuellt att överväga hur den aktuella författningen bör utformas för att möjliggöra digitalisering. För den intresserade finns vidare läsning på detta tema i eSams promemoria Digitaliserbar lagstiftning som handlar om digitaliserbar och digitaliseringsvänlig lagstiftning. I promemorian resoneras kring dessa begrepp och hur författning bör utformas för att vara digitaliserbar. Att författning är digitaliserbar ökar också möjligheterna till automatisering. I promemorian finns exempel på lagstiftning där det föreligger utmaningar att digitalisera och exempel på när digitalisering av rättsregler har kunnat genomföras.

Jurister från Försäkringskassan har varit delaktiga i arbetet med promemorian men den är inte direkt anpassad för Försäkringskassans verksamhet.

1.2 Begrepp i vägledningen

Vi använder många ord och begrepp när vi talar om digitalisering och it-utveckling. I vissa fall finns det etablerade definitioner för dessa begrepp, exempelvis om de definierats i en författning. Exempel på sådana begrepp är *självbetjäningstjänst*, *handling*, *allmän handling* och *personuppgift*. Andra begrepp definieras inte i författning, men förekommer i författningar och har specifika rättsliga betydelser, till exempel *uppgift*. Andra begrepp används på lite olika sätt i olika sammanhang. För att säkerställa enhetlighet används i den här vägledningen begrepp i så stor utsträckning som möjligt på det sätt som de förklaras i Rikstermbanken och på det sätt som de används i FK GEK (läs mer i avsnitt 1.3). Om det behövs förklaras begreppet.

I detta avsnitt redogör vi för de begrepp som är viktiga för den övergripande förståelsen av vägledningen och dess syfte. Övriga begrepp förklaras, vid behov, i aktuellt kapitel.

Begreppet *it-stöd* används för att beskriva alla slags tjänster. Både interna handläggningssystem och digitala tjänster är it-stöd.

Begreppet *digital tjänst* används för att beskriva alla slags externt åtkomliga tjänster. Det kan handla om tjänster där enskilda (fysiska eller privaträttsliga juridiska personer) kan ansöka, anmäla eller göra något annat hos Försäkringskassan. Det kan också handla om tjänster för informationsutbyte eller samverkan med andra myndigheter. Läs mer om digitala tjänster i kapitel 3. Där beskrivs också andra vanliga begrepp som används för att beskriva det som avses med digital tjänst.

It-tjänst är ett begrepp som används framförallt av IT-avdelningen för att beskriva en förmåga att leverera tekniskt eller kompetensrelaterat it-stöd som möjliggör en verksamhetsprocess eller tillgodoser ett verksamhetsbehov. Begreppet används sällan i vägledningen, men kan vara bra att känna till eftersom det förekommer i andra sammanhang på Försäkringskassan.

1.3 Hur vägledningen förhåller sig till annat internt och externt material av särskild betydelse

eSam har tagit fram material (checklistor med mera) med rättslig vägledning i olika frågor som delvis överlappar det som står i den här vägledningen. Det finns material som beskriver rättsliga utmaningar kopplat till utveckling av digitala tjänster mer generellt. Det finns också material som handlar om mer specifika företeelser, exempelvis AI eller *eget utrymme*. Läs mer om eget utrymme i avsnitt 3.1.6.

Den här vägledningen fokuserar på frågor som är särskilt vanliga eller utmanande på Försäkringskassan och beskriver dem utifrån förutsättningarna här. Ibland hänvisar vägledningen till eSams material som källa. I andra fall kan eSams material användas för fördjupad eller breddad läsning. Vi behöver då komma ihåg att eSams material är generellt och därför kan behöva anpassas till förutsättningarna på Försäkringskassan.

Läs mer

eSam har tagit fram material som beskriver generella juridiska frågeställningar kopplade till utvecklingsinsatser, de rättsliga kraven och hur frågorna normalt kan lösas. Bland annat *Digitalisera rätt – en praktisk juridisk vägledning* och *Checklista för jurister – Introduktion i rättsliga förutsättningar i utvecklingsinsatser.*

Vägledningen och checklistan kan användas vid utveckling av digitala tjänster på Försäkringskassan. De är dock inte är specifikt anpassade för Försäkringskassans verksamhet. Det betyder att de kan beskriva både problem och lösningar som inte är aktuella på Försäkringskassan.

Den rättsliga vägledningen och checklistan finns på eSams webbplats.

Försäkringskassans gemensamma egenskapskrav på IT-stöd (FK GEK) är ett stöddokument som samlar olika (författningsstyrda och andra) krav som gäller för utveckling med it-inslag på Försäkringskassan. Stöddokumentet fungerar primärt som en checklista. Utöver kortfattade beskrivningar av varje kravområde innehåller dokumentet bland annat information om

- hur kravet verifieras (vem som ansvarar för att säkerställa att kravet uppfylls och hur det ska uppfyllas)
- kontaktuppgifter för mer hjälp
- vilken funktion inom Försäkringskassan som ansvarar för kravområdet.

Det finns överlappningar mellan FK GEK och den här vägledningen. Båda dokumenten beskriver exempelvis krav i fråga om arkiv och gallring, personuppgiftsbehandling, förvaltningsrätt och likabehandling. Den här vägledningen ska dock, till skillnad från FK GEK, inte användas som en checklista utan beskriver istället vissa frågor rörande utveckling av digitala tjänster mer utförligt. Syftet är att ge rättslig vägledning i de viktigaste och vanligaste rättsliga utmaningarna vid utveckling av digitala tjänster på Försäkringskassan.

Läs mer
Du kan läsa mer om FK GEK på Fia-sidan *Gemensamma egenskapskrav (GEK)*. Där hittar du också själva stöddokumentet.

1.4 Särskilt om juridikens och juristens roll i utvecklingsarbete

På Försäkringskassan finns olika yrkesroller och kompetenser som samverkar för att utvecklingsinsatser ska genomföras i enlighet med gällande regelverk. De behöver därför ha övergripande kännedom om de rättsliga kraven. I många utvecklingsinsatser behövs också en jurist med fördjupad kunskap om de rättsliga kraven och kompetens att göra bedömningar kopplade till den specifika utvecklingsinsatsen.

Juristen är sällan kravställare i ett utvecklingsinitiativ eller ansvarig för de beslut som formar slutresultatet. Däremot ansvarar hen för att ge rättsligt stöd genom att identifiera rättsliga frågeställningar, bidra med fördjupad kunskap om de rättsliga kraven, göra juridiska bedömningar och beskriva vilka handlingsalternativ som är möjliga.

Juristen behöver samarbeta med andra yrkesroller med särskilda kompetenser som kan beskriva den aktuella utvecklingsinsatsen och ge underlag för juristens rättsliga stöd. För att ge rätt juridiskt stöd behöver juristen inte bara få förklarat för sig vad utvecklingsinsatsen innebär och hur olika tekniska lösningar fungerar, utan också få utvecklingsinsatsen satt i sitt sammanhang. Det kan exempelvis finnas förmånsspecifika regler eller andra slags krav och standarder som behöver beaktas. De rättsliga bedömningarna behöver fungera i ett sammanhang.

2 Centrala rättsprinciper och regelverk

Nationella och internationella regelverk samt rättsprinciper gäller precis som vanligt när vi utvecklar digitala tjänster på Försäkringskassan. Det betyder bland annat att våra digitala lösningar måste uppfylla de krav som ställs i olika internationella konventioner och fördrag, såsom till exempel Europakonventionen, fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt, EU:s rättighetsstadga och barnkonventionen.

På samma sätt måste vi, och de system vi utvecklar, leva upp till kraven i de svenska grundlagarna och alla andra lagar, förordningar, myndighetsföreskrifter och interna styrdokument.

Detta kapitel ger en samlad överblick över de allmänna rättsprinciper och de regelverk som är särskilt viktiga för digitaliseringsarbetet på Försäkringskassan. I kapitlet beskrivs också översiktligt på vilket sätt de är det. Innehållet är inte uttömmande. Det kan alltså finnas fler principer eller regelverk som är relevanta för en specifik utvecklingsinsats.

2.1 Centrala rättsprinciper

Rättsprinciperna gäller alltid, vid all verksamhet, på Försäkringskassan. De flesta av de rättsprinciper som är mest centrala för vårt digitaliseringsarbete finns i regeringsformen, som är en grundlag. Det betyder att de har företräde framför andra regler som finns i lagar och förordningar.

Flera av principerna som beskrivs i detta avsnitt ingår även i vad som kallas *grunderna för god förvaltning*. De kommer till uttryck både i grundlagstext och i 5–8 §§ förvaltningslagen (FL). De flesta ingår samtidigt i den statliga värdegrunden.

Vi måste beakta och efterleva rättsprinciperna redan när vi utvecklar en digital tjänst, men också när vi använder och följer upp och vidareutvecklar tjänsten. Är det ett system för automation måste vi också säkerställa att själva systemet efterlever principerna.

Läs mer

Läs mer om principerna och grunderna för god förvaltning i Försäkringskassans vägledning (2004:7) *Förvaltningsrätt i praktiken.* Läs mer om den statliga värdegrunden på Statskontorets webbplats.

2.1.1 Legalitetsprincipen

Legalitetsprincipen är viktig för all verksamhet som bedrivs på Försäkringskassan. Principen kommer till uttryck i både grundlag och andra författningar (se till exempel 1 kap. 1 § tredje stycket RF, 1 § andra stycket och 5 § första stycket FL och 3 § myndighetsförordningen (2007:515). Principen innebär att myndigheternas verksamhet måste ha stöd i *rättsordningen*.

Med begreppet rättsordningen avses både EU-rätt och svensk rätt på olika nivåer. Det kan handla om reglering i lag eller förordning, till exempel myndighetens instruktion. Det kan också handla om ett förvaltningsbeslut från regeringen, exempelvis i myndighetens regleringsbrev eller genom ett beslut om ett särskilt uppdrag. Principen gäller inte bara den del av verksamheten som handlar om att fatta beslut som påverkar enskilda, utan all verksamhet som en myndighet bedriver (prop. 2016/17:180, s. 58). Förutom att en

myndighet måste ha författningsstöd för sina beslut och åtgärder, måste den också kunna visa vilken regel den har använt i det konkreta fallet (SOU 2010:29, s. 146).

Legalitetsprincipen innebär att Försäkringskassan är styrd av och bunden till vad som gäller generellt och vad som framgår av Försäkringskassans instruktion, regleringsbrev och olika slags regeringsuppdrag. Utvecklingen av digitala tjänster måste grundas på vårt uppdrag och ha stöd i rättsordningen. Detsamma gäller sådan utvecklingsaktivitet som sker genom samverkan med andra myndigheter.

Legalitetsprincipen innebär bland annat att vi bara får ställa krav som det finns stöd för i lagstiftningen. Därför kan vi exempelvis inte välja att bara ta emot ansökningar i digital form om regelverket tillåter pappersansökningar (jfr. bland annat JO 2011/12 s. 413). Försäkringskassan har i dagsläget få digitala tjänster som är obligatoriska för enskilda. Den enskilde kan alltså för det mesta välja om hen vill ansöka eller anmäla på andra sätt än via en digital tjänst. Ett undantag från detta är inom tandvården och det undantaget har stöd i regelverket (jfr. 3 kap. 1 § lag [2008:145] om statligt tandvårdsstöd).

De system som tas fram måste också utvecklas och programmeras på ett sådant sätt att de inte vidtar några åtgärder utanför de givna rättsliga ramarna. Vid ett ändrat rättsläge måste också systemet gå att omprogrammera snabbt. Systemen måste vara föremål för ständig övervakning och uppföljning för att hela tiden säkerställa efterlevnaden av legalitetsprincipen. Du kan läsa mer om legalitetsprincipen i relation till utveckling och användning av automatisering och AI i avsnitt 5.2.1.

2.1.2 Principerna om demokrati och fri åsiktsbildning

Principerna om demokrati och fri åsiktsbildning följer av RF (1 kap. 1 § 1 och 2 st). Grunden för den demokratiska samhällsordningen är att människor har rätt till självstyre och att delta i beslutsprocesser som rör maktutövningen. Frågor kring demokrati aktualiseras särskilt när det gäller användning av avancerad teknik, såsom AI, för automatisering av handläggning och beslutsfattande inom den offentliga förvaltningen. Detta kan du läsa mer om i avsnitt 5.2.3.

När det gäller principen om fri åsiktsbildning spelar offentlighetsprincipen en viktig roll. Den bidrar till att garantera att medborgarna har insyn i vad myndigheterna gör och därigenom får möjlighet att kontrollera deras verksamhet. Myndigheterna ska vara öppna och transparenta och det ska gå att följa vägen till beslut. Frågan om transparens är central vid all automatisering. Det måste gå att följa vad systemet gör och varför. Det är nödvändigt att redan på förhand bedöma om de handlingar som ett system genererar är allmänna eller inte. Om handlingarna är allmänna behöver de registreras, bevaras, hanteras och gallras på det sätt som lagar, förordningar och föreskrifter kräver. Du kan läsa mer om hanteringen av allmänna handlingar och uppgifter i relation till automatisering och AI-utveckling i avsnitt 5.2.5.

2.1.3 Principerna om likabehandling och objektivitet

Principerna om likhet och objektivitet kommer till uttryck i bland annat RF (1 kap. 9 § RF), där det framgår att förvaltningsmyndigheter är skyldiga att beakta allas likhet inför lagen (likhets- eller likabehandlingsprincipen) och agera sakligt och opartiskt (objektivitetsprincipen).

Likhetsprincipen innebär ett krav på likabehandling inför lagen. Försäkringskassan får inte göra någon skillnad mellan olika individer utöver vad som kan följa av gällande rättsregler.

Objektivitetsprincipen innebär att vi ska vara sakliga och opartiska. Vi får inte låta oss vägledas av andra intressen än de som ska tillgodoses. Det är också förbjudet att fatta beslut på andra grunder än vad som framgår av reglerna i det aktuella fallet.

Principerna gäller inte bara vid handläggning av ärenden och beslutsfattande, utan också vid faktiskt handlande och rena serviceåtgärder. I praktiken innebär detta att inte bara Försäkringskassans medarbetare måste beakta allas likhet inför lagen och agera sakligt och opartiskt. Även de system vi utvecklar måste leva upp till principernas krav. Det betyder att vi inte utan sakliga skäl kan behandla kontakter som sker digitalt förmånligare än de som sker analogt (till exempel på papper). Ärenden som skickas in digitalt får inte hanteras med förtur eller ges annan förmånlig behandling enbart för att stimulera fler att använda en digital kanal (Jfr JO:s dnr 5497-2013). Att handläggning av webbansökningar kan utföras och avslutas snabbare än motsvarande ansökningar på papper bör däremot inte strida mot 1 kap. 9 § RF (eSams vägledning *Rättsliga förutsättningar för digitalt i första hand*, s. 27). Men om handläggningen av manuella ansökningar tar oproportionerligt lång tid, eller tar längre tid av skäl som inte kan motiveras sakligt, så bör det inte kunna anses vara förenligt med likabehandlingsprincipen (JO:s dnr 5796-2019 m.fl.).

Likabehandling är särskilt viktigt när vi tränar och använder avancerad teknik för maskininlärning såsom AI, eftersom vi måste säkerställa att systemet inte tränas att ta ovidkommande hänsyn. Du kan läsa mer om detta i avsnitt 5.2.4.

2.1.4 Principen om respekt och icke-diskriminering

Principen om respekt innebär att den offentliga makten ska utövas med respekt för alla människors lika värde och för den enskilda människans frihet och värdighet (1 kap. 2 § första stycket RF). Vi ska sträva efter att sköta vårt arbete med respekt för den enskilda människan och uppfylla kraven på icke-diskriminering och hänsyn till den personliga integriteten. Samma krav ställs även på våra digitala lösningar.

Principen om respekt syftar bland annat till att det allmänna ska motverka diskriminering av människor på grund av kön, hudfärg, nationellt eller etniskt ursprung, språklig eller religiös tillhörighet, funktionshinder, sexuell läggning, ålder eller andra omständigheter som gäller den enskilde som person. Regler om hur det ska gå till att nå principens mål finns till exempel i diskrimineringslagen (2008:567).

När vi utvecklar digitala tjänster på Försäkringskassan innebär principen bland annat att vi måste säkerställa att automatiserade förfaranden är fria från diskriminering. Det gör vi redan när vi utvecklar ett system, men också när det är satt i drift och vi granskar och övervakar det och när vi analyserar systemets produktionsresultat. Läs mer om icke-diskriminering i relation till automatisering och AI i avsnitt 5.2.4.

En form av diskriminering är bristande tillgänglighet. Det är när en person med en funktionsnedsättning missgynnas genom att en verksamhet inte vidtar skäliga tillgänglighetsåtgärder för att hen ska komma i en jämförbar situation med personer utan denna funktionsnedsättning. Det kan exempelvis handla om bristande tillgänglighet till våra digitala tjänster. Krav på tillgänglighet finns också i FL och i DOS-lagen. Läs mer i avsnitt 2.1.5, 2.2.7. och 2.2.8

I principen om respekt ligger även skydd för den personliga integriteten. Det finns bestämmelser till skydd för den i bland annat RF, Europakonventionen och EU:s rättighetsstadga. Det är centralt för skyddet av den personliga integriteten att myndigheter och andra organisationer hanterar och behandlar personuppgifter på ett korrekt sätt. Skyddet för personuppgifter regleras bland annat i dataskyddsförordningen och 114 kap. socialförsäkringsbalken (SFB). Dessa regelverk är centrala för all verksamhetsutveckling på Försäkringskassan. Läs mer i avsnitt 2.2.3.

Läs mer

Läs mer om förbudet mot diskriminering i vår verksamhet i Försäkringskassans vägledning (2004:7) *Förvaltningsrätt i praktiken*. Där står det också om diskrimineringslagens krav på tillgänglighet för personer med funktionsnedsättning.

I Försäkringskassans riktlinje (2019:02) *Att motverka, förebygga och åtgärda diskriminering* finns bland annat skrivningar om vem som ansvarar för att våra it-system motsvarar de krav som ställs på funktionalitet enligt diskrimineringslagen, och för att Försäkringskassans inloggade tjänster är tillgänglighetsanpassade.

Det finns mer information på Fiasidan *Digital tillgänglighet och inkluderande design*.

2.1.5 Principerna om effektivitet och service

Effektivitet handlar bland annat om att hushålla med statens medel, men även om att handlägga ärenden snabbt, enkelt och med tillräcklig kvalitet. Serviceskyldigheten handlar bland annat om att kontakterna med enskilda ska vara enkla och smidiga och att den enskilde ska få sådan hjälp att hen kan ta till vara sina intressen.

Kraven på effektivitet och service finns inte i grundlag utan i vanliga lagar och förordningar (bland annat 6 § FL och 3 § myndighetsförordningen). Det innebär att principerna i RF som du kan läsa om tidigare i detta avsnitt har företräde framför principerna om effektivitet och service. Detta betyder till exempel att även om det står klart att en utvecklingsinsats kan innebära betydande effektivitetsvinster eller förenkla kontakterna med Försäkringskassan, så får den inte realiseras om den inte samtidigt kan leva upp till kraven på till exempel legalitet och objektivitet.

Nära kopplat till serviceskyldigheten är kravet på tillgänglighet, som finns 7 § FL. Kravet innebär att myndigheter ska vara tillgängliga för allmänheten i så stor utsträckning som möjligt. Kravet är inte begränsat till vissa former av kontakter som till exempel besök, telefonsamtal, mejl eller en digital tjänst på vår webbplats (prop. 2016/17:180 s. 292), men sträcker sig ändå inte hur långt som helst. Försäkringskassan avgör till exempel själv i vilken utsträckning det är lämpligt och ändamålsenligt att vara tillgänglig via sociala medier. Frågan om vilket digitalt verktyg som är lämpligt att använda beror också på vilken typ av information det handlar om. Om det exempelvis är sekretessbelagda uppgifter som ska kommuniceras är det nödvändigt att använda ett verktyg där obehöriga inte kan komma åt uppgifterna.

Tillgänglighetskravet innebär också att Försäkringskassan inte kan kräva att allmänheten tar kontakt på ett visst sätt eller med en viss teknik, exempelvis genom ett webbformulär. Vi kan bara ställa ett sådant krav om vi har uttryckligt stöd för det, till exempel för att det framgår av en författning eller genom ett bemyndigande att meddela föreskrifter om att kontakten ska tas i en viss digital form. (Jfr von Essen 2021, s. 75).

Läs mer

Läs mer om FL:s krav på myndigheternas tillgänglighet i Försäkringskassans vägledning (2004:7) *Förvaltningsrätt i praktiken*.

2.1.6 Proportionalitetsprincipen

Proportionalitetsprincipen syftar till att hitta en rimlig balans mellan mål och medel. Den innebär förenklat att en ingripande åtgärd ska vara ägnad att tillgodose det åsyftade ändamålet, vara nödvändig för att uppnå detta ändamål och medföra fördelar som står i rimlig proportion till den skada som åtgärden förorsakar (prop. 2016/17:180 s. 61).

Proportionalitetsprincipen är central inom EU-rätten och har en framträdande roll i dataskyddsrättsliga sammanhang. Principen finns även i 5 § tredje stycket FL. Den gäller vid såväl ärendehandläggning som annan förvaltningsverksamhet och är därmed också aktuell vid olika slags digitaliseringsinitiativ på Försäkringskassan.

Att iaktta proportionalitet kräver ofta en bedömning i ett sammanhang som inte alltid kan göras redan av lagstiftaren, utan som behöver göras i det enskilda fallet. Kravet utmanar våra möjligheter att automatisera beslutsprocesser eftersom automatisering förutsätter att regelverk omsätts till standardiserade steg. (Jfr Enqvist, Naarttijärvi, s. 232ff.)

2.2 Centrala regelverk

Det finns några allmänt gällande regelverk som har stor betydelse för digitaliseringsarbetet på Försäkringskassan, till exempel offentlighets- och sekretesslagstiftningen, det dataskyddsrättsliga regelverket och förvaltningsrätten.

Inom EU finns det några rättsakter som reglerar vissa digitala företeelser specifikt, som vi också behöver ta hänsyn till i utvecklingen av olika digitala lösningar. Exempel på detta är SDG-förordningen och eIDAS-förordningen.

När vi ska göra rättsliga bedömningar inom ramen för utvecklingsarbetet kan flera rättsområden och författningar vara aktuella samtidigt. De olika regelverken kompletterar varandra. De kan ibland vara avsedda att tillämpas tillsammans på olika nivåer, men ibland ska de tillämpas parallellt. Dessutom har Försäkringskassan interna styrdokument som exempelvis beskriver vad som gäller för vårt säkerhetsarbete och hur vi får hantera verksamhetsinformation.

I det här avsnittet finns en översiktlig beskrivning av de regelverk som är viktiga för utvecklingsarbetet på Försäkringskassan.

2.2.1 SDG-förordningen

SDG-förordningen är en EU-förordning som syftar till att skapa en gemensam digital ingång inom EU/EES. SDG står för *single digital gateway*. I den digitala ingången ska privatpersoner och företag få tillgång till webbaserad information och länkar till förfaranden och tjänster som de behöver för att kunna utnyttja sin rätt till fri rörlighet. Som komplement till SDG-förordningen finns lagen (2022:126) med kompletterande bestämmelser till EU:s förordning om en gemensam digital ingång.

Med förfaranden avses det som i dagligt tal brukar benämnas digitala tjänster. Enligt SDG-förordningen är ett förfarande en sekvens av handlingar som användare måste utföra för att uppfylla kraven eller för att erhålla ett beslut från en behörig myndighet för att kunna utöva sina rättigheter på de områden av den inre marknaden som anges i bilaga I (artikel 2.2 a. och artikel 3.3).

SDG-förordningens krav på tillgång till information (artikel 4) innebär för Försäkringskassans del krav på information om rättigheter, skyldigheter och regler som gäller socialförsäkringen och vissa närliggande områden och om förfaranden inom socialförsäkringsområdet (både online och offline). Förordningen har ett tydligt

användarperspektiv och ställer omfattande kvalitetskrav på den information som lämnas, både vad gäller innehåll och form (artikel 9 och 10).

SDG-förordningens krav på tillgång till förfaranden (artikel 6) innebär bland annat att Försäkringskassan ska tillhandahålla länkar till förfaranden som erbjuds online och som omfattas av förordningens tillämpningsområde. Dessutom måste vi erbjuda vissa förfaranden online och möjlighet att lämna vissa uppgifter online. SDG-förordningen innebär också att vi behöver se till att användare i gränsöverskridande situationer får tillgång till våra onlineförfaranden på samma eller likvärdiga villkor som inhemska användare (artikel 13).

För Försäkringskassans del innebär också SDG-förordningen att tillhandahålla information om, och länkar till, de hjälp- och problemlösningstjänster som omfattas av förordningens tillämpningsområde och som Försäkringskassan ansvarar för (artikel 4 och 7).

Genom SDG-förordningen (artikel 14) inrättas också ett tekniskt system som ska ge myndigheterna i olika medlemsstater möjlighet att utbyta ”bevis” (intyg med mera) digitalt med varandra. Tanken är att användaren inte ska behöva tillhandahålla en myndighet sådana dokument eller uppgifter som en annan myndighet redan har tillgång till (engångsprincipen).

Läs mer
Myndigheten för digital förvaltning (Digg) har utsetts till nationell samordnare för SDG i Sverige. Läs mer om SDG-förordningen på Digg:s hemsida.

2.2.2 eIDAS-förordningen

eIDAS-förordningen reglerar elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på EU:s inre marknad. Syftet med förordningen är bland annat att säkerställa en väl fungerande inre marknad och att uppnå en lämplig säkerhetsnivå för medel för elektronisk identifiering och betrodda tjänster. För att uppnå detta syfte innehåller förordningen i huvudsak krav på ömsesidigt erkännande av anmälda e-legitimationer under vissa förhållanden, regler för tillhandahållande av betrodda tjänster och en rättslig ram för sådana tjänster.

Förordningen är uppdelad i två delar. En del handlar om betrodda tjänster och vilka krav som ställs på dessa tjänster, och där är Post- och telestyrelsen (PTS) ansvarig myndighet. Den andra delen handlar om elektronisk identifiering och där är Digg ansvarig myndighet.

Läs mer om vilken betydelse eIDAS-förordningen har för e-legitimering och e-underskrifter i avsnitt 4.

2.2.3 Dataskyddsregelverket

Dataskyddsförordningen är det grundläggande regelverket när det gäller skydd för personuppgifter. Förordningen gäller för alla verksamheter som hanterar personuppgifter av olika slag. Den innehåller bland annat grundläggande principer som måste efterlevas vid all personuppgiftsbehandling, krav på att behandlingen har en rättslig grund, tillförsäkrar de registrerade ett antal rättigheter och ställer krav på säkerhet vid behandlingen. Dataskyddsförordningen är direkt tillämplig i Sverige. Som komplement till den finns dataskyddslagen och förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning. Dataskyddslagen

innehåller regler av generell karaktär. Om det finns någon bestämmelse i en annan lag eller förordning som avviker från dataskyddslagen, så gäller den bestämmelsen i stället för dataskyddslagen.

För behandling av personuppgifter inom Försäkringskassans kärnverksamhet, det vill säga kopplat till handläggning av socialförsäkringsärenden, gäller också Försäkringskassans registerlagstiftning: 114 kap. SFB och förordning (2024:14) om behandling av personuppgifter vid Försäkringskassan och Pensionsmyndigheten.

De flesta utvecklingsinsatser i kärnverksamheten medför att personuppgifter behandlas eller kommer att behandlas. Ofta rör det sig dessutom om *känsliga personuppgifter*.

I de flesta fall handlar det om att vi utvecklar en digital tjänst som kommer att behandla personuppgifter när tjänsten är i drift. Oftast handlar det om att utveckla digitala tjänster som i produktion kommer att behandla personuppgifter för att handlägga ärenden. Det är i grunden oproblematiskt – vi har stöd för att behandla personuppgifter om det är nödvändigt för att handlägga ärenden.

I vissa fall innebär själva utvecklingsinsatsen att personuppgifter behandlas. Exempelvis när system testas, kvalitetssäkras eller tränas och det inte är tillräckligt att använda anonymiserade uppgifter. Läs mer om dessa ändamål i avsnitt 5.2.6.

Oavsett vilken situation som är aktuell behöver vi bedöma de personuppgiftsbehandlingar som den aktuella utvecklingsinsatsen innebär.

I Försäkringskassans registerlagstiftning finns särskilda regler som aktualiseras vid utveckling av digitala tjänster. Läs mer om sökbegränsningar i avsnitt 5.2.6 och personuppgiftsbehandling vid informationsutbyte i avsnitt **Fel! Hittar inte referenskälla.**.

Dataskyddsregelverket ställer också krav på att Försäkringskassan vidtar åtgärder som garanterar lämplig säkerhet för de personuppgifter som behandlas. Här möter dataskyddsreglerna också frågor om informationssäkerhet. Läs mer om informationssäkerhet i avsnitt 2.2.9.

Läs mer

Läs mer om behandling av personuppgifter på Försäkringskassan i vägledning (2001:3) *Offentlighet, sekretess och behandling av personuppgifter*. Där hittar du en beskrivning av regelverket i sin helhet. Där förklaras också de centrala begrepp som används i den här vägledningen, såsom *personuppgifter, känsliga personuppgifter, anonymiserade uppgifter, grundläggande principer* och *sökbegränsningar*.

Läs mer om konsekvensbedömningar i riktlinjerna (2024:02) *Bedömning av dataskydd - Grundläggande bedömning och konsekvensbedömning*.

På Fia-sidan *Behandling av personuppgifter och digitalisering* hittar du fler styrande och stödjande dokument.

2.2.4 Socialförsäkringsbalken

SFB innehåller några kapitel som är särskilt relevanta för utveckling av digitala tjänster som ska användas i kärnverksamheten. Det handlar främst om regler kopplade till ärendehandläggning, sekretess och personuppgiftsbehandling.

I 110 kap. SFB finns bland annat regler om ärendehandläggning, uppgiftsskyldigheter för såväl enskilda som myndigheter och bestämmelser om undantag från sekretess.

111 kap. SFB handlar om självbetjäningstjänster via internet och innehåller bestämmelser om vad som är en självbetjäningstjänst, när självbetjäningstjänster kan användas utan hinder av formkrav knutna till pappershantering och om, elektroniska underskrifter vid självbetjäningstjänster. Läs mer i avsnitt 3.1.1.

I 111 kap. SFB finns också en bestämmelse som beskriver när en handling eller uppgift som lämnas vid användning av en självbetjäningstjänst anses ha kommit in till Försäkringskassan i förvaltningsrättslig mening. 111 kap. 7 § SFB är en specialreglering i förhållande till 22 § FL, men principen överensstämmer med mer generella överväganden om tidpunkt för inkommande av handling till digitala tjänster generellt (jfr. prop. 2003/04:40 s. 35ff. och prop. 2016/17:180 s. 142).

111 kap. 7 § SFB

En handling eller uppgift som vid användning av en självbetjäningstjänst har översänts till Försäkringskassan eller Pensionsmyndigheten, ska anses ha kommit in till den myndighet till vilken ärendet hör när den har anlänt till den del av ett system för automatiserad behandling som anvisats som mottagningsställe för självbetjäningstjänsten.

22 § FL

En handling har kommit in till en myndighet den dag som handlingen når myndigheten eller en behörig befattningshavare.

Om en handling genom en postförsändelse eller en avi om en betald postförsändelse som innehåller handlingen har nått en myndighet eller behörig befattningshavare en viss dag, ska handlingen dock anses ha kommit in närmast föregående arbetsdag, om det inte framstår som osannolikt att handlingen eller avin redan den föregående arbetsdagen skilts av för myndigheten på ett postkontor.

En handling som finns i en myndighets postlåda när myndigheten tömmer den första gången en viss dag ska anses ha kommit in närmast föregående arbetsdag.

I 114 kap. SFB finns regler om behandling av personuppgifter inom Försäkringskassans kärnverksamhet. Läs mer i avsnitt 2.2.3.

Läs mer

Läs mer om ärendehandläggning i Försäkringskassans vägledning (2004:7) *Förvaltningsrätt i praktiken*. Där kan du bland annat läsa mer om 22 § FL.

Läs mer om uppgiftsskyldigheter, bestämmelser om undantag från sekretess och om behandling av personuppgifter i Försäkringskassans vägledning (2001:03) *Offentlighet, sekretess och behandling av personuppgifter*.

2.2.5 Regler om offentlighet och sekretess

Försäkringskassan måste följa reglerna om allmänna handlingars offentlighet i tryckfrihetsförordningen (TF) och om sekretess i offentlighets- och sekretesslagen (OSL), oavsett om den information vi hanterar är digital eller analog.

Var och en har rätt att ta del av allmänna handlingar enligt 2 kap. TF. Det finns också bestämmelser om rätt att ta del av uppgifter och information som finns hos myndigheten i OSL.

En förutsättning för att dessa regler om offentlighet ska fungera i praktiken är att vi har en god offentlighetsstruktur. Vi måste säkerställa att allmänna handlingar diarieförs eller hålls ordnade på annat sätt och att information dokumenteras. Det finns regler med krav på myndigheters hantering av och registrering (diarieföring) av allmänna handlingar i 4–6 kap. OSL och regler om dokumentation i FL och i 4 kap. 3 § OSL.

I Försäkringskassans it-system hanteras uppgifter av många olika slag. När vi utvecklar digitala tjänster för kärnverksamheten handlar det mestadels om sekretessreglerade (och ofta sekretessbelagda) uppgifter, till exempel om enskilda. Dessa uppgifter är normalt sett också allmänna handlingar i TF:s mening, eller är på väg att bli det. Uppgifterna finns som regel i digitala tabeller (”registeruppgifter” eller ”databasposter”) eller i digitala dokument. Uppgifterna kan också finnas i metadata kopplade till handlingarna eller i olika typer av loggar. Även loggar är en slags handlingar som ofta är allmänna.

I OSL finns bland annat regler om vilka uppgifter som omfattas av sekretess och sekretessbrytande regler som har stor betydelse vid bedömningen av olika slags informationsutbyten och röjande med andra myndigheter och enskilda.

De flesta digitala tjänster som vi utvecklar i kärnverksamheten innebär att uppgifter görs tillgängliga för någon utanför Försäkringskassan. Oftast handlar det om att den enskilde själv får tillgång till uppgifter om sig själv. Men det kan också handla om att andra än den enskilde får tillgång till information eller att den enskilde får tillgång till information om andra än sig själv.

Att uppgifter görs tillgängliga i en digital tjänst innebär att de lämnas ut – röjs – för den som får tillgång till uppgifterna. Det kräver att en sekretessprövning har gjorts innan uppgifterna för första gången görs tillgängliga i tjänsten. Det rör sig om en slags generell, framåtblickande, bedömning av om de uppgifter som ska lämnas ut i den digitala tjänsten alltid får lämnas ut till den eller de individer som kommer att kunna logga in i tjänsten. Antingen för att de inte omfattas av sekretess mot den som får tillgång till uppgiften, till exempel när den enskilde får ta del av uppgifter om sig själv i Mina sidor, eller för att det finns en tillämplig sekretessbrytande bestämmelse.

Om vi får kännedom om att en typiskt sett harmlös uppgift kan vara känslig i det enskilda fallet, så måste vi kunna hindra åtkomsten till den. Det kan därför vara svårt att göra digitala tjänster tillgängliga för andra än den enskilde, till exempel ombud, ställföreträdare eller vårdnadshavare. En möjlig lösning är att bygga en funktion där den enskilde kan samtycka till utlämnandet.

Läs mer om utveckling av tjänster vars primära syfte är att utbyta information i kapitel 6 *digitala tjänster för informationsutbyte*.

Läs mer

Läs mer om sekretess och röjande i Försäkringskassans vägledning (2001:3) *Offentlighet, sekretess och behandling av personuppgifter*. Där kan du också läsa sekretess i förhållande till ombud, ställföreträdare och vårdnadshavare.

2.2.6 Arkivrättsliga regelverket

I det arkivrättsliga regelverket finns bestämmelser om bevarande och gallring av allmänna handlingar. De digitala tjänster som utvecklas i kärnverksamheten innehåller i princip alltid allmänna handlingar och vi behöver därför ta hänsyn till det arkivrättsliga regelverket vid utveckling. Som utgångspunkt gäller att en allmän handling ska kunna förstås och inte får ändras, förvanskas eller göras oläslig. Det gäller under hela den tid som handlingen finns, oavsett om den ska gallras eller bevaras för framtiden.

I det arkivrättsliga regelverket finns också krav på livscykelhantering av information. Att hantera information med hänsyn till dess livscykel innebär att det krävs planerade åtgärder för när information ska framställas, överföras, dokumenteras, användas, förvaras och vårdas, under hela den tid som informationen ska finnas. Livscykelhanteringen innebär också att vi i ett tidigt skede behöver utreda om informationen ska bevaras eller gallras. Utredningens resultat påverkar planeringen av hantering och åtgärder under informationens livscykel. Om en gallrings- och bevarandeutredning inte har genomförts behöver den digitala tjänsten utformas med utgångspunkt i att informationen ska bevaras, vilket innebär högre ställda krav vid utveckling.

De åtgärder som sker med informationen under dess livscykel ska dokumenteras och följas upp i enlighet med Riksarkivets föreskrifter och allmänna råd (RA-FS 2009:1 med ändringar) om elektroniska handlingar (upptagningar för automatiserad behandling). Vi behöver också följa de tekniska krav för hantering och skapande av digital information, som finns i Riksarkivets föreskrifter och allmänna råd (RA-FS 2009:2) om tekniska krav för elektroniska handlingar (upptagningar för automatiserad behandling).

Vid utveckling av digitala tjänster är det viktigt att redan tidigt i utvecklingsinsatsen säkerställa att kraven på informationshanteringen kan uppfyllas. Kontakta därför VS Informationsförvaltning redan i planeringen av en utvecklingsinsats.

Läs mer

Läs mer om Arkivhantering och informationsförvaltning på Fia. Där hittar du olika styr- och stöddokument. Där hittar du också kontaktuppgifter till VS Informationsförvaltning som har normerings- och serviceansvar inom arkivområdet.

Läs mer om hanteringen av Försäkringskassans allmänna handlingar, arkivering och gallring i Försäkringskassans vägledning (2004:3) *Försäkringskassan och arkivhantering*. I Försäkringskassans riktlinjer (2022:01) *Gallring och bevarande av verksamhetsinformation* och Försäkringskassans anvisningar (2023:09) *Gallring och bevarande av verksamhetsinformation* kan du läsa mer om hur du ska koppla in det arkivrättsliga perspektivet tidigt i en utvecklingsinsats. I bilaga 1 till anvisningar (2023:09) finns en förenklad kravchecklista att använda vid upphandling och utveckling av it-stöd.

2.2.7 Förvaltningslagen

FL innehåller bland annat grundläggande regler om god förvaltning, ärendehandläggning och beslutsfattande. De är centrala för Försäkringskassans kärnverksamhet, även vid digital handläggning och utveckling av digitala tjänster.

Vissa av FL:s regler gäller i all verksamhet på Försäkringskassan, inte bara när vi handlägger enskilda ärenden. Det gäller bestämmelserna om grunderna för en god förvaltning, det vill säga legalitet, objektivitet och proportionalitet (5 § FL), service och tillgänglighet (6 och 7 §§ FL) och samverkan mellan myndigheter (8 § FL).

Övriga regler gäller vid handläggning av ärenden (9–49 §§ FL). Begreppet *handläggning* innefattar allt som en myndighet gör från att ett ärende inleds tills det avslutas med ett beslut. Vilka regler som gäller enligt FL beror alltså på om ett ärende har inletts och om ett ärende pågår.

Den tekniska utvecklingen och den ökade digitala ärendehanteringen kan innebära utmaningar när det gäller att fastställa ett ärendes gränser i förhållande till andra ärenden och annan information. Det finns inte alltid en teknisk motsvarighet till en pappersakt (till exempel i form av en tekniskt avgränsad enhet av information). När vi utvecklar digitala tjänster har begreppet *ärende* två betydelser:

- Ett ärende i teknisk mening, där gränserna beror på hur ett system eller en ärendeprocess har konstruerats, eller hur en mängd information lagras
- Ett ärende i rättslig mening utifrån FL:s regler.

Vi måste hantera båda dessa betydelser för att kunna säkerställa att våra digitala tjänster lever upp till FL:s krav – både vad gäller den enskildes rättigheter (till exempel rätt till partsinsyn, kommunikation och rätten att begära ett avgörande) och våra skyldigheter (att handlägga ärendet och fatta beslut).

FL har en teknikneutral utformning. Det betyder att lagen gäller både vid manuell och vid digital handläggning. Lagen innehåller också en bestämmelse som specifikt anger att beslut kan fattas automatiserat (28 §).

Läs mer

Läs mer om FL och handläggning av ärenden i Försäkringskassans vägledning (2004:7) *Förvaltningsrätt i praktiken*.

2.2.8 DOS-lagen

Lagen om tillgänglighet till digital offentlig service (DOS-lagen) innehåller krav på att offentliga aktörers webbplatser och mobila applikationer ska vara tillgängliga. Genom att följa en särskild europeisk standard kan Försäkringskassan leva upp till kraven. DOS-lagen innehåller också bestämmelser om att offentliga aktörer ska tillhandahålla en *tillgänglighetsredogörelse*, som bland annat ska beskriva hur den aktuella webbplatsen eller applikationen lever upp till kraven. DOS-lagen kompletteras av Diggs föreskrifter (2019:2) om tillgänglighet till digital offentlig service (DOS-föreskriften).

De tillgänglighetskrav som uppställs enligt DOS-författningarna ska inte förväxlas med kraven på tillgänglighet enligt 7 § FL. Läs mer om FL:s krav i avsnitt 2.1.5.

När vi utvecklar digitala tjänster för enskilda eller skapar webbsidor som används internt på Försäkringskassan ska form och funktion uppfylla kraven på digital tillgänglighet. Det grundläggande kravet är att digital offentlig service är möjlig att uppfatta, hanterbar, begriplig och robust, enligt 4 § DOS-föreskriften. Mer specificerat ska tekniken motsvara en utpekad europeisk standard, enligt 5 § samma föreskrift. Försäkringskassans arbete med webbtillgänglighet (digital tillgänglighet och inkluderande design) finns beskriven på intranätet Fia.

Det är nödvändigt att beakta tillgänglighetskraven tidigt i en utvecklingsinsats. Kraven behöver till exempel vara bedömda och formulerade så att de kan ställas vid ett eventuellt behov av upphandling. Enligt 9 kap. 2 § lagen (2016:1145) om offentlig upphandling ska de tekniska specifikationerna bestämmas med beaktande av samtliga användares behov, däribland tillgänglighet, när det som anskaffas ska användas av fysiska personer.

Bristande tillgänglighet är en form av diskriminering. Läs mer i avsnitt 2.1.4.

2.2.9 Informationssäkerhet

Informationssäkerhet är den samlade och övergripande säkerhet som ska se till att den information som finns i en organisation alltid är korrekt, tillgänglig och skyddad från obehörig åtkomst. Informationssäkerheten rör all form av information. Informationen kan till exempel utgöras av personuppgifter, tekniska beskrivningar eller ekonomiska uppgifter. Informationen finns vanligtvis i pappershandlingar och elektroniska handlingar.

Man brukar dela in informationssäkerhet i administrativ säkerhet och teknisk säkerhet. Den tekniska säkerheten delas vanligtvis in i fysisk säkerhet och it-säkerhet.

Administrativ säkerhet handlar om att ta fram policys, rutiner och anvisningar som beskriver hur medarbetare i en organisation exempelvis ska hantera information. Det kan också handla om vad som gäller kring behörigheter till olika it-system. Med teknisk säkerhet åsyftas tekniska skydd såsom brandväggar, kryptering och liknande.

It-säkerhet är en viktig del vad gäller säkerheten. Det är en del av informationssäkerheten. Till it-säkerhet hör bland annat skyddade förbindelser, intrångsdetektering och säkerhetskopiering.

Försäkringskassan måste ha en lämplig säkerhetsnivå för den information som myndigheten hanterar. Detta följer inte bara av externa regelverk som dataskyddsregelverket, utan även interna, där Försäkringskassans Säkerhetspolicy 2003:4 ger de grundläggande förutsättningarna för säkerhetsarbetet. Vad som utgör en lämplig säkerhetsnivå för olika typer av information går att utläsa ur riktlinjer (2018:13) *Säkerhetsregler.*

Myndigheten för samhällsskydd och beredskap (MSB) ger också ut föreskrifter och allmänna råd gällande informationssäkerhet. Ett exempel på detta är MSB:s föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:07).

Läs mer

I Försäkringskassans riktlinje (2018:13) *Säkerhetsregler* finns de övergripande reglerna för allt säkerhetsarbete på Försäkringskassan, inklusive övergripande regler för informationssäkerhet. Här beskrivs bland annat vad som ska gälla i fråga om informationsklassning, behörighetsstyrd åtkomst och kryptering, samt vilken/vilka organisatoriska enheter som är ansvariga för att åtgärder genomförs respektive att styrande dokument tas fram.

Försäkringskassans anvisning (2023:06) *Särskild bedömning när Försäkringskassans information ska lagras eller bearbetas i en extern tjänst* innehåller information om vilka bedömningar som behöver göras för att kunna fatta beslut om det är lämpligt att anskaffa eller fortsätta använda tjänster för bearbetning eller lagring.

Försäkringskassans anvisningar (2022:09) *Säkerhet på Försäkringskassan* innehåller anvisningar på praktisk nivå avsedda för den enskilde statsanställda. Där finns också anvisning om vilka informationsklasser (öppen/intern/känslig) som man får lov att behandla eller kommunicera på vilket sätt, vilket är viktigt att komma ihåg om man ska skapa en tjänst som på något sätt ska kommunicera med omvärlden, eller på andra sätt lagra eller behandla information.

Hur man klassar information framgår av Försäkringskassans anvisning (2022:03) *Informationsklassning*.

Informationssäkerhetsarbetet omfattar också skyddet för personuppgifter.

Läs mer

I Försäkringskassans vägledning (2001:03) *Offentlighet, sekretess och behandling av personuppgifter* finns en beskrivning av vad som gäller allmänt i förhållande till säkerhetskraven i dataskyddsförordningen. Där finns också viss vägledning kring vad som är en skyddad personuppgift, vilket är viktigt för tillämpningen av riktlinjen (2011:34) *Hantering av skyddade personuppgifter inom Försäkringskassan*. Av den riktlinjen framgår bland annat mer om vad som är en skyddad personuppgift, men framför allt hur sådana får hanteras och av vem. Det är viktigt att hänsyn tas till riktlinjen när man bygger system som ska hantera skyddade personuppgifter, så att bland annat utskick hanteras korrekt. Kom ihåg att även till exempel anställda och konsulter kan ha skyddade personuppgifter. För anställda med skyddade personuppgifter gäller riktlinjen (2024:02*) Hantering av anställdas skyddade personuppgifter inom Försäkringskassan*.

2.2.10 Säkerhetsskydd

Säkerhetsskydd handlar om att genom förebyggande arbete skydda verksamhet som är av betydelse för Sveriges säkerhet mot spionerі, sabotage, terroristbrott och vissa andra hot. Denna typ av verksamhet kallas för säkerhetskänslig verksamhet och den som bedriver sådan verksamhet har vissa grundläggande skyldigheter.

Försäkringskassans säkerhetskänsliga verksamhet beskrivs i Försäkringskassans säkerhetsskyddsanalys.

Uppgifter som rör säkerhetskänslig verksamhet kallas för säkerhetsskyddsklassificerade uppgifter och omfattas av sekretess enligt OSL.

Säkerhetsskyddet regleras i säkerhetsskyddslagen (2018:585), säkerhetsskyddsförordningen (2021:955) och kompletterande bestämmelser i form av föreskrifter. Försäkringskassan lyder under Säkerhetspolisen när det gäller säkerhetsskydd och ska därför följa Säkerhetspolisens föreskrifter och vägledningar.

Läs mer

Läs mer om säkerhetsskydd och Försäkringskassans säkerhetsskyddsanalys i Försäkringskassans stödprocess (2020:10) *Säkerhetsskydd*.

Mer information finns också på Fiasidan *Säkerhetsskydd*.

3 Digitala tjänster

I den här vägledningen används begreppet *digital tjänst* för att beskriva alla slags externt åtkomliga tjänster. Det kan handla om tjänster där enskilda (fysiska eller privaträttsliga juridiska personer) kan ansöka, anmäla eller göra något annat hos Försäkringskassan. Det kan också handla om tjänster för informationsutbyte eller samverkan med andra myndigheter.

Det finns flera begrepp som i olika sammanhang används för att beskriva det som här kallas digitala tjänster. Ibland används begreppen synonymt och ibland inte. De vanligaste begreppen utöver digital tjänst är *e-tjänst* och *självbetjäningstjänst*.

- På Försäkringskassans externa webbplats och i tjänsten Mina sidor används begreppet e-tjänst. Det är enligt Försäkringskassans termbank en tjänst som tillhandahålls via ett elektroniskt gränssnitt och som helt eller delvis utförs elektroniskt. Begreppet är också vanligt förekommande i exempelvis eSams material. Begreppet används ofta synonymt med digital tjänst.
- Begreppet självbetjäningstjänst är för Försäkringskassans del definierat i SFB och beskrivs närmare i avsnitt 3.1.1. Där framgår att självbetjäningstjänst (på Försäkringskassan) har en något snävare innebörd än digital tjänst. Begreppet används också utanför Försäkringskassan och då kan det ha en bredare innebörd.
- I SDG-förordningen används i stället begreppet *förfaranden* när man avser det som i dagligt tal brukar benämnas digitala tjänster. Läs mer om SDG-förordningen i avsnitt 2.2.1.

3.1 Olika slags digitala tjänster

Det finns inga lagregler som beskriver olika slags digitala tjänster och hur de ska utformas, med undantag för självbetjäningstjänster inom Försäkringskassan, se avsnitt 3.1.1. Däremot har det inom eSam, bland myndigheter och i utredningar utvecklats en terminologi för att beskriva olika slags digitala tjänster. Den terminologin kan ibland upplevas något inkonsekvent. En anledning till det är att en digital tjänst ofta innehåller inslag av flera olika slags digitala tjänster, till exempel både en service- och en presentationstjänst. Det är inte heller lätt att dra gränsen mellan en typ av digital tjänst eller en viss teknisk funktionalitet som kan erbjudas i en digital tjänst.

Det viktiga är inte vad en digital tjänst kallas, utan vilka funktioner tjänsten har och vad man kan göra i den. Avsnitt 3.1.1–3.1.6 beskriver olika slags digitala tjänster för att illustrera dessa olika funktionaliteter och de rättsliga frågeställningar som ofta förekommer vid utveckling av sådana tjänster.

Terminologin som används i den här vägledningen baseras bland annat på eSam:s *Juridisk vägledning för verksamhetsutveckling inom e-förvaltning 3.0*, prop. 2016/17:198 och SOU 2018:25.

3.1.1 Självbetjäningstjänster

Det finns en typ av digital tjänst som i vart fall för Försäkringskassans räkning är definierad i lag. I 111 kap. SFB finns särskilda bestämmelser som reglerar vissa av Försäkringskassans digitala tjänster (*självbetjäningstjänster*).

111 kap. 3 § SFB
Med självbetjäningstjänster avses möjligheter att via Internet få tillgång till personuppgifter och annan information samt utföra sådana rättshandlingar som anges i 4 § första stycket.

111 kap. 4 §
En enskild får, i den utsträckning som framgår av föreskrifter som meddelas av regeringen eller den myndighet som regeringen bestämmer, använda självbetjäningstjänster för att

- lämna uppgifter,
- göra anmälningar eller ansökningar,
- förfoga över rättigheter, och
- utföra andra rättshandlingar.

Sådana rättshandlingar som anges i första stycket har samma rättsverkningar som om de utförts i enlighet med de föreskrifter om formkrav som annars gäller för de förmåner och ersättningar som avses i 2 § första stycket. Föreskrifter om att uppgifter ska lämnas på heder och samvete ska dock alltid iakttas när självbetjäningstjänster används.

Med självbetjäningstjänster avses möjligheter att via Internet få tillgång till personuppgifter och annan information samt utföra vissa rättshandlingar. Enskilda kan använda sådana självbetjäningstjänster för att utföra olika slags rättshandlingar utan hinder av formkrav som gäller enligt SFB och annan författning som reglerar våra förmåner och ersättningar. Det kan exempelvis handla om att lämna uppgifter eller att ansöka om en förmån. Bestämmelser om att uppgifter ska lämnas på heder och samvete gäller däremot alltid vid användning av självbetjäningstjänster, vilket kan innebära krav på elektronisk underskrift (jfr 111 kap. 6 § SFB).

De digitala tjänster som omfattas av 111 kap. SFB är sådana som gäller socialförsäkringsförmåner samt andra förmåner och ersättningar som Försäkringskassan handlägger enligt lag eller förordning och som riktar sig till enskilda (111 kap. 2 § SFB). Det innebär att 111 kap. SFB inte är tillämpligt vid utveckling av sådana digitala tjänster som Försäkringskassan tar fram för användning inom statsförvaltningen, till exempel informationsutlämnande via LEFI Online. I begreppet *enskild* ingår också fysiska personer som driver näringsverksamhet och juridiska personer (jfr prop. 2003/04:40 s. 48 f). Det betyder att även våra digitala tjänster som riktar sig till arbetsgivare ska hanteras i enlighet med 111 kap. SFB.

Självbetjäningstjänster får bara användas i den utsträckning som är särskilt föreskrivet. Försäkringskassan har därför beslutat om föreskrifter om självbetjäningstjänster via internet (FKFS 2011:3). I föreskriften anges uttryckligen i vilka situationer den enskilde får använda självbetjäningstjänster. För att en ny självbetjäningstjänst ska kunna införas krävs därför att det som man ska kunna utföra i tjänsten finns upptaget i 1–2 §§ i den föreskriften. I annat fall krävs en föreskriftsändring. Föreskriften innehåller särskilda regleringar om hur den enskilde ska identifiera sig för att få tillgång till information och för att kunna lämna uppgifter.

3.1.2 Servicetjänster

Den definition som görs av självbetjäningstjänster i 111 kap. SFB motsvarar hur begreppet *servicetjänst* används i många andra sammanhang. Ibland förekommer

också begreppet *självservicetjänst*. I en servicetjänst kan en enskild utföra olika saker som att fylla i, signera och skicka in en ansökan.

Enligt eSam:s definition är en servicetjänst en tjänst där en innehavare av ett *eget utrymme* kan utforma utkast till handlingar i sitt utrymme, få uppgifter förifyllda eller annars utlämnade, antingen av den som tillhandahåller utrymmet eller någon annan med stöd av egen hämtning eller egen delning, skicka handlingar till en mottagningsfunktion och vidta andra nödvändiga åtgärder (se Juridisk vägledning för verksamhetsutveckling inom e-förvaltning 3.0). Försäkringskassans servicetjänster är vanligtvis inte utformade som ett eget utrymme. Läs mer om eget utrymme i avsnitt 3.1.6

3.1.3 Presentationstjänster

I en presentationstjänst sammanställs och visas information för användaren i en tjänst som kan heta Mina sidor, Min ärendeöversikt, Min pension eller liknande. Syftet är ofta att ge service genom att den enskilde på ett enkelt sätt ska kunna ta del av samlad information på ett ställe, i stället för att behöva vända sig till flera olika tjänster eller aktörer. (se prop. 2016/17:198, avsnitt 4.5).

Enligt eSam:s definition presenteras informationen i en presentationstjänst i ett *eget utrymme*. Försäkringskassans Mina sidor anses inte vara eget utrymme. Läs mer om eget utrymme i avsnitt 3.1.6

En förutsättning för korrekta presentationstjänster är att rätt person kan se informationen. En presentationstjänst måste alltså utformas så att sekretessreglerad information inte visas för obehöriga.

Presentationstjänster kan utformas så att informationen som presenteras är sammanställd från flera olika aktörer. Då är det viktigt att utforma tjänsten så att den myndighet som tillhandahåller tjänsten inte kan anses ha fått del av informationen. Läs mer i eSams vägledning *Juridisk vägledning för verksamhetsutveckling inom e-förvaltning 3.0* om utformning av presentationstjänster.

3.1.4 Bastjänster

En bastjänst syftar till att möjliggöra smidigt maskinellt utbyte och sammanställning av information. Försäkringskassan ansvarar till exempel för teknisk förvaltning och drift av bastjänsten SSBTEK (sammansatt bastjänst ekonomiskt bistånd), som är en bastjänst för att lämna ut uppgifter från ett antal myndigheter till socialtjänsten.

Det finns mer information om rättsliga aspekter vid utformning av bastjänster i eSams vägledning *Juridisk vägledning för verksamhetsutveckling inom e-förvaltningen 3.0*.

3.1.5 Hjälptjänster

För att uppfylla kravet på serviceskyldighet har myndigheter tagit fram olika typer av stöd för att hjälpa den enskilde. Det kan handla om publicerade frågor och svar, eller en möjlighet att tala med en handläggare för att få stöd när man fyller i ett webbformulär. Det kan också handla om beräkningstjänster, där man får automatiserad hjälp att beräkna ett belopp.

I många fall kan användaren få hjälpen utan att vara är inloggad, till exempel genom att hen fyller i uppgifter och får ett automatiserat svar eller hjälp att beräkna ett belopp. I andra fall behöver användaren ett mer anpassat stöd i inloggat läge, när hen använder en digital tjänst.

Beräkningsfunktioner och andra liknande hjälptjänster måste utformas så att svaren inte framstår som ett förhandsbesked eller en bedömning av rätten till ersättning.

Förhandsbesked inför en ansökan får bara förekomma om det finns stöd i regelverket. Det finns exempel på detta i 4 kap. 5, 5 a, 6 och 7 §§ lagen (2008:145) om statligt tandvårdsstöd. Hjälptjänster handlar i stället om att ge service i form av exempelvis anpassad information och vägledning om reglerna.

Det finns uttalade regler om hjälptjänster i bland annat art 2.2 c, art 7, art 11 och bilaga III SDG-förordningen (se avsnitt 2.9). Dessa regler gäller endast vissa utpekade områden och för Försäkringskassans del har myndigheten gjort bedömningen att det endast omfattar en skyldighet att ge tillgång till – och information om – den hjälptjänst som Försäkringskassan tillhandahåller som nationell kontaktpunkt för gränsöverskridande hälso- och sjukvård i enlighet med patientrörlighetsdirektivet.

Räkna på föräldrapenning och *Räkna på bostadsbidrag* är exempel på oinloggade hjälptjänster, alltså tjänster där man inte behöver logga in.

3.1.6 Eget utrymme

Digitala tjänster kan utformas så att de uppgifter den enskilde vill lämna till en myndighet sparas som ett utkast i en skyddad teknisk miljö, ett *eget utrymme*. Eget utrymme är alltså snarare en teknisk funktionalitet eller en rättsfigur, snarare än en slags digital tjänst.

Innebörden av eget utrymme är att den enskilde ska kunna fylla i uppgifter i en digital tjänst, utan att uppgifterna anses vara inkomna till en myndighet. Den enskilde ska alltså kunna känna sig trygg med att uppgifterna inte är tillgängliga för någon annan innan hen själv har valt att skicka in dem. Eget utrymme är ett begrepp som ofta förekommer vid tjänsteutveckling, men som inte är definierat i författning.

Vid införandet av en utvidgad bestämmelse om tystnadsplikt vid teknisk bearbetning och lagring, i 40 kap. 5 § OSL, anförde regeringen att det är ”rimligt att enskilda ska kunna förvänta sig att uppgifter som de lämnar på ett eget utrymme på en myndighets server via en digital tjänst skyddas såväl mot insyn från allmänheten som mot obehörigt utnyttjande från dem som har teknisk tillgång till uppgifterna” (prop. 2016/17:198, s. 17). Detta är alltså något som myndigheten bör beakta vid utformningen av digitala tjänster.

Försäkringskassans digitala tjänster är vanligtvis inte utformade som ett eget utrymme. Information (utkast) sparas därför inte från ett inloggningstillfälle till ett annat, förutom i ett fåtal digitala tjänster. I vissa ärendetyper är det nödvändigt att fler än en person signerar en ansökan, till exempel om bostadsbidrag eller merkostnadsersättning. För den hanteringen har Försäkringskassan utvecklat en lösning som baseras på eget utrymme.

Den informationshantering som föregår inlämningen till myndigheten anses vara en form av teknisk lagring för den enskildes räkning där handlingen inte blir att anse som allmän innan den har ”skickats in”, enligt 2 kap. 13 § första stycket TF. För att Försäkringskassan ska kunna tillhandahålla digitala tjänster i form av eget utrymme krävs alltså att tjänster utformas så att de kan anses vara teknisk lagring och bearbetning enligt TF.

Det är nödvändigt att ha genomtänkta regler för det egna utrymmet, så att uppgifter inte lagras där för länge eller att det är möjligt att spara olämpligt material.

Läs mer
eSam har tagit fram rättsliga vägledningar och designprinciper för eget utrymme, som rekommenderas för den som vill läsa hur en digital tjänst bör utformas för att kunna anses vara ett eget utrymme. Se till exempel *Eget utrymme hos en myndighet – en vidareutveckling, 2021* och *Vägledning Designprinciper och krav för eget utrymme, 2022*.

3.1.7 Digitala tjänster för informationsutbyte

Det finns inget etablerat begrepp för att samlat benämna tjänster för informationsutbyte. En tjänst för informationsutbyte kan vara en tjänst vars primära syfte är att utbyta information (exempelvis LEFI Online) eller en del av exempelvis en självbetjäningstjänst. Begreppet ”fråga/svar-tjänster” används ibland för att beskriva tjänster med fördefinierade frågor och svar.

I den här vägledningen använder vi begreppet *digital tjänst för informationsutbyte* för att beskriva en tjänst för att utbyta information digitalt med någon utomstående, det vill säga andra myndigheter, individer eller företag. Läs mer i kapitel 6.

3.2 Försäkringskassans digitala tjänster

Försäkringskassan har flera digitala tjänster som privatpersoner, företag och andra myndigheter kan använda.

För andra myndigheter tillhandahåller Försäkringskassan även it-tjänster för att stödja en samverkande statsförvaltning. Mycket av det görs inom ramen för uppdraget om SSSID (samordnad och säker statlig it-drift).

3.2.1 Mina sidor för privatpersoner

På Mina sidor samlas olika digitala tjänster riktade till enskilda. Där kan man efter inloggning bland annat få tillgång till information om sina ärenden och se sina utbetalningar. Den information som visas är densamma som Försäkringskassan har lagrad i andra system. I den här delen är Mina sidor en presentationstjänst.

Delar av Mina sidor har också karaktär av en självbetjäningstjänst. Den enskilde kan lämna vissa uppgifter om sig själv och exempelvis ange hur hen vill bli kontaktad av Försäkringskassan. Hen kan också lämna in bilagor och svara på meddelanden.

Via Mina sidor kan den enskilde också nå andra självbetjäningstjänster för bland annat anmälan och ansökan.

Det finns också sådant som snarare är hjälptjänster, exempelvis *Planera föräldrapenning*, och presentationstjänster som *Föräldrakalendern* (som visar vab-historik).

3.2.2 Självbetjäningstjänster för förmåner och ersättningar

Försäkringskassan har många självbetjäningstjänster där enskilda bland annat kan ansöka, anmäla och lämna uppgifter kopplade till Försäkringskassans förmåner och ersättningar.

3.2.3 SSBTEK och LEFI Online

Försäkringskassan har ett antal digitala tjänster för informationsutbyte, till exempel SSBTEK och LEFI Online.

SSBTEK är en bastjänst för att lämna information från bland annat Försäkringskassan, Pensionsmyndigheten och Skatteverket till kommunernas socialtjänster. Tidigare utfördes detta arbete till stor del manuellt. SSBTEK innebär en förenklad och säkrare hantering av informationen (prop. 2016/17:198 s. 7). Försäkringskassan ansvarar för teknisk förvaltning och drift av tjänsten.

I LEFI Online kan medarbetare vid vissa myndigheter och organisationer, företrädesvis kommuner, Kronofogdemyndigheten och försäkringsbolag, ställa frågor om person- och förmånsinformation som finns hos Försäkringskassan.

Läs mer om utveckling av digitala tjänster för informationsutbyte i kapitel 6.

3.2.4 Arbetsgivartjänster

Arbetsgivartjänster, ofta kallade e-tjänster för arbetsgivare, är självbetjäningstjänster för juridiska personer, där de kan lämna uppgifter och anmäla. Försäkringskassan har cirka tio sådana tjänster för arbetsgivare, bland annat *Sjukanmälan från dag 15* och *Lämna svar på inkomstförfrågan*.

För att använda arbetsgivartjänsterna behöver arbetsgivaren först ansluta till de digitala tjänsterna och ange vilka som är behöriga att företräda företaget mot Försäkringskassan. De behöriga personerna loggar in med e-legitimation vid varje användning. Några uppgifter om de anställda visas inte i tjänsterna, utöver de som arbetsgivaren anger vid varje tillfälle.

3.2.5 Försäkringskassans app

Försäkringskassan erbjuder några digitala tjänster via appen Försäkringskassan. Den enskilde kan ansöka om VAB, följa sina ärenden, se utbetalningar samt visa förmånsintyg vid sjuk- eller aktivitetsersättning. Appen är anpassad för att uppfylla sådana tillgänglighetskrav som beskrivs i avsnitt 2.2.8.

3.3 Alla har inte tillgång till digitala tjänster

Vissa personer kan ha svårt att få tillgång till digitala tjänster på Försäkringskassan. Det kan bero på att de saknar e-legitimation och därför inte kan logga in i tjänsterna, att de har skyddade personuppgifter eller att de har ställföreträdare, till exempel god man eller förvaltare.

3.3.1 Personer som saknar e-legitimation

En grundläggande förutsättning för att kunna använda digitala tjänster är att man kan identifiera sig för att få tillgång till uppgifter och signera en anmälan eller ansökan digitalt. För att det ska vara möjligt behöver man en e-legitimation.

Några har svårt att få en e-legitimation som kan användas i Försäkringskassans digitala tjänster. Den e-legitimation som har varit dominerande i Sverige har förutsatt att den enskilde varit kund hos vissa banker. Numera finns det alternativa leverantörer av e-legitimationer. Det kan fortfarande vara svårt för personer som saknar svenskt personnummer eller inte är folkbokförda i Sverige att ha tillgång till en e-legitimation som kan användas i Försäkringskassans digitala tjänster.

Det här betyder att det är nödvändigt att säkerställa att det finns möjlighet för alla som är målgrupp för en digital tjänst att väcka sitt anspråk hos Försäkringskassan. Om det inte är möjligt att använda en digital tjänst så måste det finnas en alternativ digital eller analog väg att lämna in en ansökan eller anmälan.

Även *användare i gränsöverskridande situationer* kan ha svårigheter att logga in och signera med de e-legitimationer som de vanligtvis använder. I och med SDG-förordningen (se avsnitt 2.2.1) finns det rättsliga krav på att det ska vara möjligt att logga in i Försäkringskassans digitala tjänster med e-legitimationer som är anmälda till eIDAS-systemet, art 13.1 c. Försäkringskassan arbetar för att ansluta till eIDAS-systemet och möjliggöra sådan inloggning.

3.3.2 Personer med skyddade personuppgifter (SID)

Personer med skyddade personuppgifter har inte tillgång till alla digitala tjänster hos Försäkringskassan. Detta gäller personer med sekretessmarkering och skyddad folkbokföring. Personer med fingerade personuppgifter berörs inte av dessa begränsningar. De hanteras ”som vanligt” i systemet, eftersom de skyddas genom den nya identiteten.

Att tillgången är begränsad för personer med sekretessmarkering och skyddad folkbokföring beror på att deras uppgifter är sekretessreglerade. Den enskilde har rätt att se sin egen information. Försäkringskassan har dock vissa digitala tjänster där uppgifter visas för andra än den som uppgiften gäller, till exempel uppgifter om barn, en annan vårdnadshavare eller en sambo.

Försäkringskassan har gått igenom alla digitala tjänster för att kontrollera att uppgifter inte visas för någon annan än den som SID-markeringen gäller. De digitala tjänster där det inte finns något hinder ur ett sekretessperspektiv har därför blivit tillgängliga.

Läs mer
Läs mer om skyddade personuppgifter i Försäkringskassans riktlinjer (2011:34) *Hantering av skyddade personuppgifter inom Försäkringskassan.*

Läs mer om sekretess och skyddade personuppgifter i Försäkringskassans vägledning (2001:3) *Offentlighet, sekretess och behandling av personuppgifter*.

3.3.3 Personer med ställföreträdare

Personer med ställföreträdare kan ha svårt att använda digitala tjänster på Försäkringskassan. Ställföreträdare är ett samlingsbegrepp för god man och förvaltare.

Den som har god man har rätt att själv utföra rättshandlingar i en digital tjänst genom att legitimera sig och sedan signera en ansökan eller anmälan. Den som har förvaltare får däremot inte själv ansöka om en förmån utan att förvaltaren har lämnat sitt samtycke.

Det är svårt att i förväg bedöma vad en god man eller förvaltare har rätt att göra eller ta del av i huvudmannens ärenden. Det beror bland annat på ställföreträdarens uppdrag. Regelverken kring sekretess och dataskydd begränsar också möjligheterna. Det kan därför vara möjligt för ställföreträdaren att få tillgång till uppgifter om sin huvudman i ett enskilt fall, men det kan vara svårt att göra digitala tjänster tillgängliga för ställföreträdaren.

Tillgång till personuppgifter genom direktåtkomst är i kärnverksamheten bara tillåtet i den utsträckning det anges i lag eller förordning. Varken lag eller förordning medger någon rätt för en ställföreträdare att ha direktåtkomst till en huvudmans personuppgifter. Detta innebär i praktiken att ställföreträdare inte kan få direktåtkomst till personuppgifter om sin huvudman via Försäkringskassans digitala tjänster. Läs mer om dataskydd och direktåtkomst i avsnitt 6.2.2. samt om sekretessbedömningen i avsnitt 2.2.5

Det är möjligt för en ställföreträdare att ansöka om ersättning för sin huvudman eller beställa årsredovisningar i vissa digitala tjänster. Då visas inte någon annan information om huvudmannen än den som ställföreträdaren själv har angett.

Läs mer om ställföreträdares åtkomst till digitala tjänster som kräver e-legitimation i avsnitt 4.2.8.

Läs mer

Läs mer om ställföreträdare i Försäkringskassans vägledning (2004:7) *Förvaltningsrätt i praktiken*.

Läs mer om sekretess och sekretess i förhållande till ställföreträdare i Försäkringskassans vägledning (2001:3) *Offentlighet, sekretess och behandling av personuppgifter*.

4 Elektronisk legitimering och underskrift

Elektronisk legitimering och elektronisk underskrift är centrala funktioner för att kunna erbjuda säkra digitala tjänster. Det är viktigt att Försäkringskassan släpper in rätt personer i myndighetens digitala tjänster och att rätt person skriver under en ansökan. Därför finns det även särskilda krav på legitimering och underskrifter för Försäkringskassans självbetjäningstjänster i 111 kap. SFB.

I det här avsnittet används begrepp som utgår från *legitimering* och *underskrift*. Avsikten är att enbart översiktligt beskriva de tekniska delarna i den utsträckning som är nödvändig för att tydliggöra de juridiska frågeställningarna.

Läs mer

eSam har tagit fram en juridisk vägledning om e-legitimering och e-underskrifter. Vägledningen är mer omfattande än detta kapitel och kan användas för en fördjupning i ämnet. Men vägledningen har inte uppdaterats sedan 2018. Sedan dess har det hänt mycket inom områdena elektronisk legitimering och underskrift, både vad gäller teknik och regelverk. Det betyder att vägledningstexten måste läsas med försiktighet. Texterna är inte heller specifikt anpassade för Försäkringskassans verksamhet. Det betyder att vägledningen kan innehålla problem och lösningar som inte är aktuella på Försäkringskassan.

Ta del av *Juridisk vägledning för införande av e-legitimering och e-underskrifter 1.1* på eSams webbplats.

4.1 E-legitimation

E-legitimation är en elektronisk id-handling som används för att legitimera sig på ett säkert sätt på exempelvis en webbplats eller i en app. Legitimering är i många fall nödvändig för att säkerställa att rätt person får tillgång till en digital tjänst. Legitimationen kan också användas för att skapa elektroniska underskrifter.

I den här vägledningen används begreppet *legitimering* eftersom det är vanligast, framförallt bland svenska myndigheter. I vissa sammanhang används däremot begreppet *identifiering* för att beskriva samma sak. Det begreppet används inom EU men också i Sverige, exempelvis av privata aktörer.

4.1.1 Aktörer bakom e-legitimationen

Det är en kedja av aktörer inblandade vid användningen av e-legitimation. Utgångspunkten är att varje aktör ansvarar för sin del och att respektive aktör även är personuppgiftsansvarig för sin del (läs mer i avsnitt 4.3). Ansvarsfördelningen kan framgå av lagstiftning, till exempel eIDAS-förordningen, eller avtal mellan aktörerna.

Användaren kan vara en privatperson som behöver identifiera sig för att använda någon av Försäkringskassans digitala tjänster eller en medarbetare som ska identifiera sig i en digital miljö. Id-handlingen kan finnas lagrad i exempelvis användarens dator, telefon eller i ett chip i ett fysiskt kort. Uppgifterna som syftar till att identifiera användaren är personuppgifter.

Utfärdaren förser användaren med e-legitimationen och ansvarar för de stödfunktioner som krävs för att ge ut, verifiera och spärra e-legitimationer. Utfärdaren kan ansöka hos

Digg om att få kvalitetsmärket Svensk e-legitimation som anger att e-legitimationen är kvalitetsgranskad. Än så länge är det bara privata aktörer som utfärdar e-legitimation för privatpersoner i Sverige. Digg har på uppdrag av regeringen lämnat förslag om att ta fram och drifta en statlig e-legitimation (En säker och tillgänglig statlig e-legitimation. Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas [I2022/01335]). Regeringen har därefter tillsatt en särskild utredare att bland annat utreda och lämna förslag på hur staten kan utfärda en e-legitimation på högsta nivå (Säker och tillgänglig digital identitet [Dir. 2022:142]). Utredningen lämnade sitt slutbetänkande En säker och tillgänglig statlig e-legitimation (SOU 2023:61) i oktober 2023.

När en användare har valt en legitimeringslösning som hen ska använda i en digital tjänst, skickar tjänsten användaren vidare till *utställaren* eller *leverantören av identitetsintyg* för en identitetskontroll. Det är vanligt att det är utfärdaren som även har den här funktionen (funktionen faller inom utfärdarens ansvar för den som har kvalitetsmärket Svensk e-legitimation). Den granskar vem som har legitimerat sig och skickar ett identitetsintyg till den förlitande parten där det framgår vem som har legitimerat sig.

Försäkringskassan, eller någon annan som tillhandahåller en digital tjänst, är *den förlitande parten* som kontrollerar att det utfärdade identitetsintyget är äkta och att det kommer från en leverantör som den digitala tjänsten litar på samt ger användaren tillträde till tjänsten med rätt behörigheter.

4.1.2 Internationell legitimering

Offentliga aktörer inom EU och EES ska ge användare tillgång till digitala tjänster på ett icke-diskriminerande sätt genom att tillhandahålla information och digitala tjänster på ett officiellt unionsspråk som förstås av så många som möjligt. Offentliga aktörer ska erkänna elektroniska identiteter från andra länder inom området. Utländska e-legitimationer från EU- och EES-länder ska kunna användas för inloggning i Försäkringskassans digitala tjänster. Det här regleras i eIDAS-förordningen och SDG-förordningen. Läs mer om förordningarna i avsnitt 2.2.2 och 2.2.1.

Systemet för legitimering med elektronisk id-handling mellan medlemsstater bygger på att det finns kontaktpunkter i varje land, så kallade noder. I Sverige är Digg ansvarig för att tillhandahålla den svenska eIDAS-noden, Sweden Connect. För att möjliggöra användning av utländska e-legitimationer i svenska e-tjänster ska tjänsterna anslutas till Sveriges eIDAS-nod. Den som tillhandhåller en tjänst, den förlitande parten, tecknar avtal med Digg om anslutning till Sweden Connect. Vid e-legitimering över medlemsgränserna, är det alltså ytterligare aktörer involverade.

Vilka utländska e-legitimationer som godtas i Sverige och vilka svenska e-legitimationer som ska godtas i andra länder framgår av Digg:s webbplats. I dagsläget (2024) fungerar ett visst antal utländska e-legitimationer för att identifiera sig hos Försäkringskassan. Cirka 70 av Försäkringskassans digitala tjänster finns tillgängliga med utländska e-legitimationer (Svar på regeringsuppdrag FK 2021/014418).

4.1.3 E-legitimering vid statliga digitala tjänster

Den förlitande parten kan, i stället för att själv upphandla funktioner för e-legitimering, använda auktorisationssystemet för elektronisk identifiering som Digg tillhandahåller. Det är ett system där Digg godkänner ansökningar om anslutning från utfärdare av e-legitimationer och ingår avtal med dem. Myndigheter kan sedan använda de godkända tjänsterna för e-legitimering i sin verksamhet (Auktorisationssystem i fråga om tjänster för elektronisk identifiering och digital post, prop. 2023/24:6). Auktorisationssystemet ersätter det tidigare valfrihetssystemet i fråga om tjänster för elektronisk identifiering.

Auktorisationssystemet regleras i lag (2023:704) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post samt i tillhörande förordning (2023:709) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post.

Läs mer

På Digg:s webbplats kan du läsa mer om auktorisationssystemet och om regelverket.

4.1.4 Tillitsnivåer på e-legitimationer

Med tillitsnivå menas grad av säkerhet och tillförlitlighet. Ju högre tillitsnivå en e-legitimation har desto säkrare är den, både när det gäller teknisk och administrativ säkerhet.

Den som tillhandahåller en digital tjänst där användaren ska legitimera sig digitalt behöver bestämma sig för vilken tillitsnivå, eller skyddsnivå, på e-legitimationen som tjänsten ska kräva.

Tillitsnivån i *Tillitsramverk för Svensk e-legitimation* graderas från 2 till 4. Tillitsnivåerna för e-legitimering över landsgränserna enligt eIDAS benämns låg, väsentlig och hög. Båda bygger på den internationella standarden ISO/IEC 29115 som definierar fyra olika nivåer, men där den lägsta nivån varken används i det svenska tillitsramverket eller i eIDAS-förordningen.

Tillitsnivån bestäms utifrån hur stor skadan riskerar att bli om fel person får tillgång till tjänsten. Bland annat ska konsekvensen bedömas av om känsliga uppgifter kan röjas för obehöriga. Ju högre tillitsnivå en e-legitimation har, desto högre krav ställs på säkerheten och kontrollen av att personen som använder e-legitimationen verkligen är den hen utger sig för att vara. Valet av tillitsnivå påverkar hur användaren kan logga in i tjänsten. Den som tillhandahåller tjänsten behöver därför balansera riskerna med att ställa för låga krav mot onödiga kostnader och svårigheter att använda tjänsten.

I dagsläget använder Försäkringskassan e-legitimationer med tillitsnivå 3 vid inloggning och underskrifter i de digitala tjänsterna. Tidigare har det enbart funnits privata e-legitimationer på tillitsnivå 3, men allteftersom börjar det utfärdas även på andra nivåer.

Läs mer

Digg granskar och godkänner svenska e-legitimationer utifrån *Tillitsramverk för Svensk e-legitimation*. Tillitsramverket syftar till att etablera gemensamma krav för utfärdare av godkända svenska e-legitimationer.

På Digg:s webbplats kan du läsa mer om tillitsramverket. Du kan också se vilka e-legitimationer som har godkänts.

4.1.5 EFOS

E-identitet för offentlig sektor, EFOS, är en tjänst för e-legitimering (och elektronisk underskrift) som Försäkringskassan tillhandahåller för sina medarbetare och för andra myndigheter. En medarbetare på Försäkringskassan legitimerar sig med EFOS

tjänstekort bland annat i it-miljön och kommer därmed åt de system och funktioner som hen har behörighet till.

EFOS e-legitimation är godkänd enligt det statliga kvalitetsmärket Svensk e-legitimation, med smartkort tillitsnivå 3 och 4 och mobilt EFOS tillitsnivå 3.

Vid användning av EFOS är det Försäkringskassan som utfärdar e-legitimationen. EFOS används även av andra myndigheter och då behöver ansvarsfördelningen tydliggöras mellan Försäkringskassan och den anslutande myndigheten.

EFOS är en *e-legitimation i tjänsten*, en *e-tjänstelegitimation*. Den måste skiljas från *privat e-legitimation*. En *e-legitimation i tjänsten* är en e-legitimation som arbetsgivaren anskaffar och som arbetstagaren använder för att legitimera sig i tjänsten. En privat e-legitimation används för att legitimera sig som privatperson och är det som exempelvis används av enskilda för att logga in Försäkringskassans självbetjäningstjänster. Det förekommer också att privat e-legitimation används i tjänsten. Läs mer i avsnitt 4.1.6

4.1.6 Privat e-legitimation i tjänsten

Ibland är det nödvändigt för medarbetare att använda sin privata e-legitimation för inloggning i exempelvis digitala möten med flera parter eller för att få tillgång till dokument där avsändaren använt speciella kommunikationslösningar. Det finns inget förbud mot att använda privat e-legitimation i tjänsten, men användningen kan aktualisera aspekter som ska beaktas i form av personuppgiftsbehandling, efterlevnad av användarvillkor och informationssäkerhet. Användning av privat e-legitimation bör därför enbart förekomma när det inte är möjligt att använda tjänstelegitimationen för att fullgöra en arbetsuppgift (SOU 2021:62 Användning av e-legitimation i tjänsten i den offentliga förvaltningen).

Försäkringskassan har bedömt att arbetsgivare i offentlig förvaltning ska förse sina medarbetare med e-legitimationer om de behöver använda e-legitimationer inom ramen för sin tjänsteutövning. En arbetsgivare kan inte spärra en privat e-legitimation som har använts i tjänsten och användaren kan därför fortsättningsvis ha tillgång till tjänster som hen inte ska komma åt. (Remissvar för Vem kan man lita på? Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen – SOU 2021:9 FK dnr 2021/006292).

Det är svårt att direkt påverka andra myndigheters eller parters e-legitimationslösningar. Däremot behöver vi ha i åtanke vilka risker som finns med att utomstående kan legitimera sig med privat e-legitimation i Försäkringskassans egna tjänster.

För att underlätta för medarbetare att använda arbetsgivarens e-legitimation i andra organisationers tjänster erbjuder Digg ett avtal som kopplar ihop e-tjänstelegitimationer med digitala tjänster. Läs mer på Digg:s webbplats.

Vi måste skilja på *privat e-legitimation* som beskrivs i det här avsnittet, och *e-legitimation i tjänsten (e-tjänstelegitimation)*. Läs mer om e-legitimation i tjänsten i avsnitt 4.1.5.

4.2 Elektronisk underskrift

Elektroniska underskrifter är den elektroniska motsvarigheten till att skriva under ett papper, exempelvis en ansökningshandling, med en penna. Enligt eIDAS-förordningen är en elektronisk underskrift uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra uppgifter i elektronisk form och som undertecknaren använder för att skriva under. Det här avsnittet tar upp frågor som är av betydelse för elektroniska underskrifter inom Försäkringskassans kärnverksamhet.

Underskrifter kan ha olika juridiska funktioner. En underskrift kan användas för att identifiera en person kopplat till en viss handling. Underskriften kan också ha en avslutningsfunktion som innebär att innehållet är fullständigt och förenligt med undertecknares vilja och heller inte ändrats efter att det skrivits under. Det kan handla om att någon ansöker om en förmån i en digital tjänst och genom att skriva under ansökan digitalt, på heder och samvete, garanterar att uppgifterna är korrekta.

Det finns olika typer av elektroniska underskrifter. Underskrifterna kan kategoriseras i *avancerade*, *kvalificerade* och *enkla*. Ursprunget till beskrivningarna finns i eIDAS-förordningen.

En avancerad elektronisk underskrift ska vara unikt knuten till den som har skrivit under handlingen och personen som skrivit under ska kunna identifieras genom underskriften. Den avancerade elektroniska underskriften ska vara skapad på ett sådant sätt att den som har skrivit under har kontroll över underskriften. Det ska också gå att upptäcka ändringar i underskriften. Underskriften som användaren gör i Försäkringskassans digitala tjänster är en avancerad elektronisk underskrift.

En *kvalificerad elektronisk underskrift* är en avancerad elektronisk underskrift som skapas med hjälp av en kvalificerad anordning för underskriftsframställning och som är baserad på ett kvalificerat certifikat för elektroniska underskrifter. Kvalificerade elektroniska underskrifter används inte på Försäkringskassan i dag, eftersom det inte finns någon utfärdare av sådana underskrifter i Sverige.

En elektronisk underskrift som inte uppfyller kraven på avancerad eller kvalificerad nivå är en *enkel elektronisk underskrift*. Det kan vara en inskannad namnteckning som klistrats in ett dokument. Enkla elektroniska underskrifter används inte i Försäkringskassans digitala tjänster.

Vilken typ av underskrift som ska användas i Försäkringskassans digitala tjänster avgörs inte i varje utvecklingsinsats utan gemensamt. Det handlar bland annat om att det finns krav i 111 kap. 5 och 6 §§ SFB på elektronisk underskrift när ansökningar görs eller vissa uppgifter lämnas i Försäkringskassans självbetjäningstjänster.

4.2.1 Betrodd tjänst

En betrodd tjänst är en tjänst som skapar, kontrollerar, validerar och bevarar elektroniska underskrifter. Det är alltså själva tjänsten med vilken användaren skriver under ett dokument.

En betrodd tjänst används för att skriva under något digitalt. Betrodda tjänster kan även användas för elektroniska stämplar, certifikat för autentisering av webbplatser, elektroniska tidsstämplingar eller för tjänster för rekommenderade leveranser och certifikat med anknytning till dessa tjänster. Detta ska skiljas från en e-legitimation, som används för digital legitimering.

Vissa tjänster, till exempel bank-id, tillhandahåller både tjänster för e-legitimation och för elektroniska underskrifter. När bank-id används för att skapa elektroniska underskrifter är tjänsten en betrodd tjänst.

Det ställs säkerhetskrav på betrodda tjänster. Kraven regleras i eiDAS-förordningen.

I Försäkringskassans digitala tjänster används bara betrodda tjänster.

Läs mer
Du kan läsa mer om betrodda tjänster på PTS hemsida.

PTS ansvarar för tillsyn över de regler i eIDAS-förordningen som rör betrodda tjänster. PTS ansvarar också bland annat för att bedöma företag som vill bli kvalificerade tillhandahållare av betrodda tjänster. PTS har däremot ingen officiell förteckning över alla företag som levererar betrodda tjänster.

4.2.2 Aktörer vid användning av e-underskrifter

På motsvarande sätt som vid e-legitimering är det ett antal olika aktörer inblandade i kedjan för att en elektronisk underskrift ska kunna användas. Ansvaret för respektive aktör kan framgå av lagstiftning och av avtal parterna emellan.

Användaren är den som skriver under exempelvis en ansökan med en e-underskrift. Användaren behöver vara identifierad med en e-legitimation innan hen skriver under.

Den som står bakom en betrodd tjänst benämns *tillhandahållare eller leverantör*. Det är ofta samma aktör bakom både e-legitimationen och den betrodda tjänsten för e-underskrift. I tjänsten länkas uppgifterna om användaren ihop med innehållet och tidpunkten för underskriften. Det här sker med hjälp av krypteringsnycklar. De uppgifter som undertecknas sammanställs till ett underlag i form av ett unikt *hashvärde*. Till det följer ett underskriftscertifikat som länkar ihop en användare med de uppgifter hen har använt sin underskrift för. Certifikatet har en viss giltighetstid. Det går att läsa mer om det tekniska förfarandet i exempelvis e-Sams vägledning för införande av e-legitimering och e-underskrifter.

Numera finns det ett antal olika leverantörer för e-legitimation och e-underskrift. Det förekommer att enskilda och andra aktörer som Försäkringskassan kommer i kontakt med använder andra leverantörers tjänster för e-legitimation än dem som Försäkringskassan använder i sina digitala tjänster. Det kan exempelvis handla om att enskilda skriver under fullmakter eller medicinska intyg i en fristående tjänst för elektronisk underskrift och skickar in den digitalt underskrivna handlingen till Försäkringskassan. I sådana fall är det viktigt att kunna avgöra om underskriften kan godtas. För att kunna avgöra det måste vi dels veta att det är en betrodd och kvalificerad underskrift, dels kunna verifiera själva underskriften. Läs mer i avsnitt 4.2.3.

Den som förlitar sig på en digital identifiering, till exempel Försäkringskassan som tar emot en ansökan, är på motsvarande sätt som vid e-legitimationer, *den förlitande parten* (eller *mottagaren*). Underskriften är inte läsbar för mottagaren men kan tolkas av en dator eftersom den består av digital information.

4.2.3 Formkrav och underskrifter

Ett *formkrav* är ett krav på att en handling ska ha en viss form, ett särskilt innehåll eller tillkomma på ett särskilt sätt för att ha en viss rättsverkan. När det gäller underskrifter kan formkrav i vissa fall innebära ett hinder mot digitala lösningar.

Det finns inte något enhetligt synsätt på hur formkrav såsom ”undertecknad”, ”namnteckning” och ”underskriven”, ibland kombinerat med termen ”egenhändigt”, ska uppfyllas. I många fall har denna typ av formkrav endast ansetts kunnat uppfyllas med penna på papper. I vissa fall anses dock motsvarande uttryck ha en teknikoberoende innebörd, det vill säga att undertecknandet också kan göras digitalt. För att bedöma om det rör sig om ett formkrav som hindrar elektronisk underskrift måste man bedöma varje

bestämmelse där formkravet förekommer. (Se till exempel Ds 2003:29 s. 87–91, prop. 2021/22:40 s. 6–7, prop. 2010/11:165 s. 346 och prop. 2017/18:126 s. 22).

Det finns inget allmänt krav på att handlingar som ges in till en myndighet måste vara underskrivna, utan det gäller bara om det finns ett författningsreglerat krav på det. I så fall krävs en underskrift för att formkravet ska vara uppfyllt. Enligt eIDAS-förordningen ska elektroniska underskrifter godtas. Om det däremot finns formkrav i nationell rätt som innebär ett krav på undertecknande så har ett sådant krav företräde framför reglerna i eIDAS-förordningen om elektroniska underskrifters rättsliga verkan (art. 2.3, 25.1 och 2).

Inom Försäkringskassans kärnverksamhet finns det särskilda formkrav för den enskildes ansökan och visst slags uppgiftslämnande (110 kap. 4 och 13 §§ SFB samt 111 kap. SFB). Dessa formkrav gäller för förmåner som handläggs enligt SFB och i vissa andra fall när det framgår av särskilda regler för ersättningar som regleras utanför SFB. I korthet kan sägas att det går att ansöka om en förmån eller lämna uppgifter enligt 110 kap. 13 § SFB med en egenhändigt undertecknad ansökningshandling (i pappersform) eller inloggad i Försäkringskassans självbetjäningstjänster (med elektronisk underskrift). Läs mer om självbetjäningstjänster i avsnitt 3.

För båda underskriftsformerna gäller att de ska vara i original för att uppfylla formkravet, det vill säga kopior av egenhändigt undertecknade ansökningshandlingar (i pappersform) eller elektronisk underskrivna handlingar godtas inte. Vad gäller digitalt underskrivna handlingar följer av 111 kap. 4 § SFB att elektronisk underskrift ska göras i Försäkringskassans självbetjäningstjänster för att godtas.

När det gäller andra handlingar (än sådana ansökningar och sådant uppgiftslämnande som ska undertecknas inne i Försäkringskassans självbetjäningstjänster) kan det vara möjligt att uppfylla eventuella formkrav genom att skriva under handlingen digitalt och skicka in den till Försäkringskassan. Utöver att det aktuella regelverket ska tillåta elektronisk underskrift, måste vi ta ställning till vilka krav som ställs på den underskriften. Exempelvis ska läkarintyg undertecknas med en avancerad elektronisk underskrift enligt 6 kap. 9 § *Socialstyrelsens föreskrifter och allmänna råd om att utfärda intyg i hälso- och sjukvården* (HSLF-FS 2018:54). Handlingen som skickas in ska också kunna kontrolleras, så att äktheten kan säkerställas. Många handlingar som skickas in till Försäkringskassan har dock inga författningsreglerade formkrav. Däremot kan handlingarnas bevisverkan påverkas av om de är underskrivna. Läs mer om äkthet och bevisverkan i avsnitt 4.2.4.

Läs mer

Läs mer om de formkrav som gäller för ansökan och uppgiftslämnande på Försäkringskassan i Försäkringskassans vägledning (2004:7) *Förvaltningsrätt i praktiken* och i de förmånsspecifika vägledningarna.

4.2.4 Äkthet och bevisverkan

När en handling som innehåller text har försetts med en underskrift kopplas handlingens innehåll ihop med den person som skrivit under. En digitalt underskriven handling består dels av själva informationen som ges in i till exempel en ansökan, dels olika former av valideringsdata (exempelvis identitetsintyg, en e-underskrift, uppgift om certifikat) som är information om själva underskriften. Informationen tillsammans med valideringsdata kommer in i flera olika filer som är sammanhållna i ett datapaket.

En elektronisk signatur från en betrodd tjänst kan ge ett minst lika starkt skydd mot manipulation som en underskrift på papper. Eftersom principen om fri bevisprövning

tillämpas av svenska domstolar görs det ingen skillnad i bevisverkan mellan elektroniska signaturer och namnteckningar (SOU 2021:9 s. 56).

Underskrifter i original har som regel ett högre bevisvärde än kopior. En namnteckning på en pappershandling är ett sätt att säkra potentiella behov av att kunna bevisa identiteten och avsikten hos den som skrev under handlingen, liksom kopplingen mellan hen och den undertecknade handlingens innehåll.

Det är inte alltid lätt att avgöra vad som är en originalhandling i digital miljö. Ett original är inte knutet till en unik fysisk bärare på det sätt som text och underskrift är knutna till ett pappersark. Ett elektroniskt original kan definieras som en elektronisk handling som har försetts med en elektronisk utställarangivelse så att det kan kontrolleras med ett tekniskt förfarande om handlingen är äkta (E-delegationens vägledning *Elektroniska original, kopior och avskrifter*).

Det händer att enskilda och andra aktörer skickar in handlingar till Försäkringskassan som skrivits under digitalt med en e-legitimation som levereras av olika privata aktörer. För att en sådan handling ska kunna betraktas som ett original måste vi kunna kontrollera om handlingen är äkta.

Ett inskannat dokument med underskrift är inte ett original. En sådan handling kan däremot ha en viss funktion som bevis även om den inte är ett original, precis som när det gäller kopior av pappershandlingar som skrivits under med penna. Den elektroniska motsvarigheten av en kopia av en underskriven fullmakt kan vara en elektroniskt underskriven fullmakt som skannats in och mejlats till Försäkringskassan och som Försäkringskassan inte kan verifiera. Fullmakt är en sådan handling som inte behöver ges in med originalunderskrift, men där det finns möjlighet att kräva original om man anser att det behövs. Läs mer i vägledning 2004:7.

4.2.5 Allmänna handlingar, bevarande och gallring

En handling som skrivits under digitalt innehåller dels själva informationen i handlingen, dels olika former av valideringsdata med information om underskriften. Det rör sig om flera olika filer som är sammanhållna i ett datapaket och som tillsammans är en sådan handling som avses i 2 kap. 3 § TF.

Uppgifter som lämnas i Försäkringskassans digitala tjänster för ansökan blir allmänna handlingar när de kommer in till Försäkringskassan. Underskriften är en del av den inkomna handlingen och ska bevaras som andra inkomna handlingar, om det inte följer av föreskrifter eller beslut att de får gallras.

När en handling som skrivits under digitalt har kommit in till Försäkringskassan kan ytterligare handlingar upprättas om till exempel utfallet av en äkthetskontroll och när den äkthetskontrollern gjordes. Nya valideringsdata och handlingar upprättas dessutom om Försäkringskassan till exempel stämplar en handling eller på andra sätt verifierar äktheten hos underskriften.

När vi utvecklar digitala tjänster på Försäkringskassan behöver vi även ta ställning till hur länge det finns rättsliga krav på att kunna validera en underskrifts giltighet, för att kunna verifiera äktheten, till exempel för att kunna bevisa brott, hantera tvister eller uppfylla någon annan form av lagstiftning.

En grundläggande problematik med elektroniska underskrifter är att certifikaten är tidsbegränsade eller kan spärras och det skydd krypteringen ger minskar med tiden. Krypteringsnycklar och algoritmer försvagas nämligen över tid. Möjligheten att validera underskriften försvinner efter att certifikatet löpt ut.

Därför måste vi så tidigt som möjligt validera giltigheten och dokumentera resultatet av valideringen – äkta eller oäkta. Detta kan ske antingen genom manuella rutiner eller genom valideringsintyg (se Diggs *Valideringstjänst*). Valideringen av underskriften bör i de allra flesta fall ske i samband med att en elektroniskt underskriven handling kommer in till Försäkringskassan, särskilt om handlingen ligger till grund för någon form av myndighetsutövning, avtal eller överenskommelse.

Skyddet av handlingens autenticitet och äkthet behöver säkerställas även efter att ett certifikat löpt ut, men detta kan ske med andra tekniska och administrativa metoder än det ursprungliga skydd som certifikat har gett. Till stor del handlar detta även om att informationsägare behöver säkerställa skydd för handlingarna i de verksamhetssystem där de förvaras och ta fram dokumentation om handlingarna med stöd av eSam:s juridiska vägledning.

Det måste vara säkerställt att inte hela eller delar av den digitalt underskrivna handlingen gallras utan att det finns ett gallringsbeslut.

Läs mer

Läs mer om gallring och bevarande av verksamhetsinformation i Försäkringskassans riktlinjer (2022:01) om gallring och bevarande av verksamhetsinformation och vägledning (2004:3) *Försäkringskassan och arkivhantering*.

Enheten Informationsförvaltning på Avdelningen för verksamhetsstöd normerar och stödjer i frågor om bevarande och gallring på Försäkringskassan.

4.2.6 Signeringstexter och signeringsfunktioner

När en ansökningshandling undertecknas eller uppgifter ska lämnas till Försäkringskassan i kärnverksamheten handlar det i praktiken inte bara om en ensam underskrift, utan underskriften görs i anslutning till en text (kallas i fortsättningen *signeringstext*). På Försäkringskassan används olika signeringstexter. De är formulerade utifrån vad som gäller för den förmån och den rättshandling som det är fråga om. Texterna innehåller regelmässigt dels ett intygande av samtliga uppgifter (exempelvis ”i ansökan” eller ”som jag lämnar”) på heder och samvete, dels information (om straffbarhet och skyldigheten att meddela FK om uppgifter ändras). Informationen är en form av service till den som undertecknar, eftersom reglerna om straffbarhet och återkrav gäller oavsett om man får informationen eller inte. Ibland förekommer också annan text i signeringstexten, exempelvis annan information. Läs mer om det i följande stycken.

Det är naturligt att det förekommer olika signeringstexter i olika förmåner, eftersom de rättsliga kraven kan vara olika om förmånen hanteras enligt SFB eller en annan författning, till exempel när det gäller att intyga på heder och samvete och skyldigheten att anmäla ändrade förhållanden. Signeringstexter kan även skilja sig något när en rättshandling företas i olika format, exempelvis mellan en pappersblankett och en digital tjänst.

Som utgångspunkt ska Försäkringskassan hantera digitala förfaranden och pappersförfaranden likadant. De rättsliga kraven för förmånen ska styra hur intygandet och informationen utformas. Den enskilde ska alltså som huvudregel göra samma intygande och få samma information oavsett formen för rättshandlingen (papper, digital blankett eller digital tjänst). Det här är viktigt inte minst ur ett likabehandlingsperspektiv

för att inte riskera att diskriminera någon som bara kan ansöka genom ett visst förfarande.

Själva kärnan i signeringstexten ska alltså vara densamma, men det är möjligt att göra tillägg eller utforma signeringen annorlunda. Ibland handlar det om att signeringsvyn i sig innebär att texten måste omdisponeras, exempelvis finns olika utrymme på en pappersblankett eller e-blankett jämfört med i en app-tjänst på mobiltelefonen. I andra fall handlar det om att den digitala tjänsten ger möjligheter att lägga till information eller förtydliganden som inte pappersförfarandet gör.

När vi utvecklar digitala tjänster på Försäkringskassan behöver vi ta ställning till om det är motiverat att göra tillägg till signeringstexten eller utforma signeringen på ett annorlunda sätt. De rättsliga kraven och användarvänligheten avgör om det är motiverat. En tjänst kan till exempel behöva anpassas för att bli mer tillgänglig (se avsnitt 2.1.4, 2.1.5 och 2.2.8). Vilken information som behövs kan variera beroende på vilken form för ansökan vi väljer. Det kan till exempel finnas anledning att ha olika information i en enkel digital tjänst och en traditionell pappers- eller en e-blankett, för att den ska upplevas som tydlig och användarvänlig. Den som exempelvis ansöker om en förmån måste få den information som hen behöver för att kunna göra rätt.

Det finns digitala tjänster där utvalda uppgifter presenteras särskilt i samband med att den enskilde ska intyga att uppgifterna stämmer. Syftet är att uppmärksamma hen på uppgifter som är särskilt viktiga för rätten till den aktuella förmånen, eller uppgifter som ofta blir fel vid ansökan om just den förmånen. Det handlar då om att uppmärksamma den enskilde på uppgifterna för att säkerställa att de blir rätt och i förlängningen för att undvika felaktiga utbetalningar och återbetalningskrav. Men det måste samtidigt vara tydligt för den enskilde att hen intygar *samtliga* uppgifter och inte bara de särskilt angivna. Ett alternativ till att endast presentera vissa utvalda uppgifter i signeringsstadiet är att i steget före presentera exempelvis ett pdf-dokument där samtliga uppgifter i ansökan framgår.

Det finns ibland texter som uppmanar den enskilde att kontrollera uppgifterna innan hen signerar. Det är ett sätt att säkerställa att uppgifterna är korrekta och det kan hjälpa den enskilde att göra rätt. Sådana texter kan vara särskilt hjälpsamma i tjänster med förifyllda uppgifter, till exempel i en ansökan. Även sådana uppgifter anses lämnade av den enskilde och intygas på heder och samvete.

4.2.7 Flerpartssignering

Ansökan om förmåner kan i vissa fall göras av fler än en person, till exempel bostadsbidrag. Samtliga personer som omfattas av ansökan behöver därför skriva under ansökan innan den skickas in till Försäkringskassan. För att flera personer ska kunna skriva under en digital ansökan är en sådan tjänst utformad som ett *eget utrymme* (läs mer i avsnitt 3.1.6). Det innebär att Försäkringskassan tillhandahåller utrymmet, men har inte tillgång till mer uppgifter än vad som är nödvändigt för teknisk bearbetning och lagring av uppgifterna i ett första skede av ansökan.

Ansökan kan skrivas under av personerna vid olika tillfällen, genom att de legitimerar sig för den digitala tjänsten och skriver under. Först när samtliga personer som omfattas av ansökan har skrivit under kan de skicka in den, och först då kommer den in till Försäkringskassan.

4.2.8 Ställföreträdare

En god man eller förvaltare (ställföreträdare) kan i vissa förmåner använda digitala tjänster för att ansöka för sin huvudmans räkning. Ställföreträdaren kan då legitimera sig i Försäkringskassans digitala tjänst med sin egen e-legitimation och välja att fylla i en

ansökan för sin huvudman. Ställföreträdaren kan, när ansökan är färdigifylld, signera den på heder och samvete. Det är då, precis som när ansökan undertecknas med penna på papper, ställföreträdaren som intygar de faktiska omständigheterna på heder och samvete.

Genom att en ställföreträdare har möjlighet att lämna in uppgifter förhindrar Försäkringskassan att hen använder sin huvudmans e-legitimation för göra det.

Ställföreträdare kan inte ta del av huvudmannens personuppgifter i tjänsten. Det beror på att ställföreträdare inte får ha direktåtkomst till personuppgifter om huvudmannen. Direktåtkomst är bara är tillåtet om det anges i lag eller förordning och det finns ingen bestämmelse som ger ställföreträdare rätt till direktåtkomst till uppgifter om sina huvudmän. Läs mer i avsnitt 3.3.3 och 6.2.2.

4.2.9 Elektroniska underskrifter inom Försäkringskassan

Beslut som fattas inom Försäkringskassans kärnverksamhet undertecknas inte om handläggningen sker elektroniskt.

Läs mer
Läs mer om beslut inom kärnverksamheten i Försäkringskassans vägledning (2004:7) *Förvaltningsrätt i praktiken* och Försäkringskassans riktlinjer (2005:14) *Kommuniceringsbrev och beslutsbrev i Försäkringskassan*.

4.3 Personuppgiftsansvar

De personuppgifter som hanteras under legitimerings- och underskriftsprocesserna passerar ett flertal aktörer. Det är vanligt att respektive aktör är personuppgiftsansvarig för sin del i processen. Det kan också förekomma situationer eller leveranser där någon kan bedömas vara personuppgiftsbiträde.

Läs mer
Läs mer om personuppgiftsansvar och personuppgiftsbiträde i Försäkringskassans vägledning (2001:3) *Offentlighet, sekretess och behandling av personuppgifter*.

Försäkringskassan är utpekad förvaltningsmyndighet för socialförsäkringen och personuppgiftsansvarig för den personuppgiftsbehandling som sker i verksamhet som gäller förmåner enligt SFB och andra förmåner som Försäkringskassan ska handlägga (114 kap. 2 och 7 §§ SFB). Mot den bakgrunden är Försäkringskassan personuppgiftsansvarig för den personuppgiftsbehandling som sker direkt kopplat till den digitala tjänst som myndigheten erbjuder. Den eller de som utfärdar e-legitimationen och utför legitimationskontroll är i sin tur personuppgiftsansvarig för den behandling som den eller de utför inom legitimeringsprocessen. På motsvarande sätt är leverantören av en betrodd tjänst som används för e-underskrift personuppgiftsansvarig för det som sker inom dennes ansvarsområde. Om det är en gränsöverskridande legitimering eller underskrift kan den personuppgiftsansvarige därmed finnas i ett annat land.

När Försäkringskassan tillhandahåller EFOS till andra myndigheter har Försäkringskassan bedömts vara personuppgiftsbiträde till den anslutande myndigheten. Försäkringskassan kan därför ha olika roller inom det här området.

4.4 Missbruk och straffrättsligt ansvar

En elektronisk handling som har upprättats som bevis eller annars är av betydelse som bevis och som har en utställarangivelse som kan kontrolleras på ett tillfredsställande sätt är en *urkund* (14 kap. 1 § BrB). En e-legitimation är alltså en urkund och de e-legitimationer som Försäkringskassan godtar har urkundskvalitet.

Missbruk av e-legitimationer jämställs med missbruk av andra sätt att legitimera sig eller intyga något och är ett brott. Det kan till exempel vara *urkundsförfalskning* (14 kap. 1 § BrB), *osant intygande* (15 kap. 11 § BrB) eller *missbruk av urkund* (15 kap. 12 § BrB). Att använda någon annans e-legitimation eller att låta någon annan använda ens egen e-legitimation är ett brott. Det spelar ingen roll om den som legitimationen tillhör har samtyckt till att någon annan använder den.

Förutom att det är brottsligt att använda någon annans e-legitimation eller låta någon annan använda ens egen, är det samtidigt ett avtalsbrott mot den som har utfärdat legitimationen.

Det kan vara svårt att upptäcka att det inte är rätt person som använt en e-legitimation eller gjort en elektronisk underskrift. Digitala tjänster kan i vissa fall utformas så att någon annan som är behörig kan lämna uppgifter i ett ärende som rör den enskilde. På så sätt kan Försäkringskassan tillhandahålla en säker digital tjänst som underlättar för användarna och möjliggör ett lagligt sätt att lämna uppgifter digitalt. De enkla digitala tjänsterna som ställföreträdare kan använda är exempel på sådana.

5 Automatiserad handläggning och beslut

Digitalisering och *automatisering* är begrepp som hänger samman och vars innebörd delvis överlappar. I inledningen till den här vägledningen används begreppet digitalisering för att beskriva en slags omvandling – att analoga underlag övergår i elektronisk form respektive att manuell hantering blir datorunderstödd. Att manuell hantering blir datorunderstödd kan också uttryckas som att den *automatiseras*.

Automatisering innebär alltså att en maskin eller en teknik utför ett arbete i stället för att en handläggare gör det manuellt. Automatisering kan ske i delar av ärendehanteringen eller av hela ärendet.

När både handläggning och beslutsfattande görs helt utan att någon befattningshavare på Försäkringskassan har varit inblandad kan man tala om en *helautomatiserad* process. Det är dock mer vanligt att automatiseringen avser vissa moment. I dessa fall kan processen kallas för *semiautomatiserad*, eftersom ärendehanteringen utförs i samverkan mellan handläggare och it-system. Det kan handla om att automatisera vissa led i handläggningen, som att göra kontroller av om ansökan är komplett och stämma av uppgifter i ansökan mot andra uppgifter. Det kan också handla om att it-system skapar förslag till beslut baserat på resultaten från olika automatiska kontroller eller utredningsåtgärder. Förslagen presenteras för handläggare som fattar beslut.

Automatisering i olika former är sedan länge ett viktigt stöd i vår verksamhet. I dag är det svårt att föreställa sig en utvecklingsinsats som inte inkluderar något moment där en maskin eller en teknik utför ett arbete. Ofta innebär detta en möjlighet att effektivisera, förbättra och förenkla handläggningen av ärenden. Automatisering leder ofta till att den enskilde får beslut snabbare utan att förvaltningskostnaderna ökar. Automatisering leder generellt sett också till en mer likställd ärendehantering än vid manuell handläggning. Sett ur dessa perspektiv kan automatisering skapa en ökad rättssäkerhet i ärendehanteringen. Samtidigt finns det risker med automatisering, exempelvis kopplat till nya avancerade tekniker som AI.

Det här kapitlet beskriver rättsliga frågeställningar som aktualiseras när vi automatiserar ärendehanteringen på Försäkringskassan. Oftast handlar det om att automatisera delar av ärendehanteringen, men det blir allt vanligare med frågor kring möjligheten att automatisera i större utsträckning eller helautomatisera handläggningsprocesser i socialförsäkringsärenden. Det finns också ett växande intresse för de möjligheter som nya avancerade tekniker som AI kan ge.

Läs mer

Redan i samband med regelutveckling kan det vara aktuellt att överväga hur den aktuella författningen bör utformas för att möjliggöra automatisering. För den intresserade finns vidare läsning på detta tema i eSams promemoria Digitaliserbar lagstiftning (jfr avsnitt 1.1). Att författning är digitaliserbar ökar också möjligheterna till automatisering. I promemorian finns bland annat exempel på hur författning kan omsättas till programmering och vilka metoder som kan användas.

Jurister från Försäkringskassan har varit delaktiga i arbetet med promemorian men den är inte direkt anpassad för Försäkringskassans verksamhet.

5.1 Tekniken vid automatisering

När vi ställer rättsliga krav på automatiserade system måste vi ha viss kunskap om den teknik som används. Det krävs för att vi ska kunna förstå vilka förutsättningar tekniken har att efterleva de rättsliga krav vi ställer på den. Det handlar både om att förstå vad system kan göra och – kanske främst – vad de *inte* kan göra. Felaktiga föreställningar riskerar att leda till felaktiga kravställningar och i slutändan till bristfällig ärendehantering eller beslut.

Det kan vara vanskligt att beskriva en teknik som ständigt utvecklas och förändras. Det viktiga är därför egentligen inte vad tekniken kallas utan vad den gör. Det här avsnittet beskriver vissa aspekter av den teknik som används vid automatisering och som är viktiga att förstå för att kunna analysera och ställa rättsliga krav vid automatisering.

5.1.1 Regelbaserade eller maskininlärande system

På Försäkringskassan använder vi sedan länge framförallt det som kallas *regelbaserade* system för automation.

Regelbaserade system kännetecknas av att regler eller andra hänsyn har översatts till maskinellt läsbara kriterier, samt att systemen inte kan utföra andra uppgifter än de som de har programmerats för att utföra.

Ett sådant system kan till exempel programmeras för att steg för steg kontrollera om en ansökan är komplett eller om den enskilde uppfyller villkoren för en viss förmån. Det är alltså vi som programmerar systemet som bestämmer mot vilka villkor systemet ska kontrollera ansökan. Vi säger åt systemet på förhand vad som ska anses vara en komplett ansökan eller vilka villkor som krävs för att ansökan ska anses uppfylla villkoren för en viss förmån. Systemets motsvarighet till att bedöma om den enskilde har rätt till en förmån är att jämföra de uppgifter som hen har lämnat i ansökan eller som finns tillgängliga på annat sätt (i andra interna system eller hos andra myndigheter) med villkoren för förmånen. På Försäkringskassan har vi dock få förmåner som är uppbyggda på ett sätt som möjliggör detta. Läs mer om bedömningsutrymme i avsnitt 5.2.1.

Maskininlärande system bygger på en annan slags logik än regelbaserade. Ett maskininlärande system tränas med hjälp av exempelvis tidigare fattade beslut eller bedömningar. De är inte bundna till att utföra samma förprogrammerade processteg varje gång. Man skulle kunna säga att systemet, till skillnad från ett regelbaserat system, gör en slags egen bedömning baserad på sannolikhet. Vi vet faktiskt inte med full säkerhet *hur* maskininlärande system fattar beslut och når sina slutsatser. Men vi kan konstatera att tillvägagångssättet inte kan likställas med de tillvägagångssätt (i form av rättsliga slutledningar eller rättsliga metoder) som människor ägnar sig åt. Systemet saknar också sådana mänskliga egenskaper som ofta förknippas med rättstillämpning och beslutsfattande, som ansvarstagande. På Försäkringskassan använder vi maskininlärande system, men inte för att bedöma rätten till ersättning eller för att fatta beslut i förmånsärenden. Läs mer i avsnitt 5.1.2.

Maskininlärande system består av två led: ett lärandeled (utveckling) och ett prestationsled (tillämpning). I lärandeledet tränas systemet för att förbättra prestationsledet. Utveckling av den här typen av system förutsätter tillgång till stora mängder data av god kvalitet. Typen av data som systemet tränas på har stor betydelse för utfallet i prestationsledet.

5.1.2 Särskilt om AI

AI har länge saknat en allmänt accepterad definition. Det har snarare kunnat beskrivas som ett slags paraplybegrepp som rymmer olika tekniker och metoder.

Numera definieras AI-system i artikel 3.1 i den nya AI-förordningen (läs mer om AI-förordningen under rubriken *AI-förordningen*). AI-system är enligt AI-förordningen ett maskinbaserat system som är utformat för att fungera med varierande grad av autonomi, som kan uppvisa anpassningsförmåga efter införande och som, för uttryckliga eller underförstådda mål, på grundval av de indata det tar emot, drar slutsatser om hur utdata såsom förutsägelser, innehåll, rekommendationer eller beslut som kan påverka fysiska eller virtuella miljöer ska genereras.

Ett exempel på AI-teknik är maskininlärning, som ofta används när man utvecklar system som ska hantera komplexa arbetsuppgifter.

Ibland förekommer det att AI-teknik beskrivs ha förmåga att visa människoliknande drag – som intelligens, resonerande och kreativitet. AI-tekniken beskrivs ibland ha förmåga att lära sig själv och bli bättre över tid, och visa intelligent beteende genom att analysera sin miljö och vidta åtgärder med viss grad av självständighet. (Se bland annat eSam, Checklista Juridik vid användning av AI, s. 6 med hänvisning) Den här beskrivningen av AI-teknik stämmer inte överens med den som Försäkringskassan använder.

Den (maskininlärande) AI-teknik som Försäkringskassan använder kan beskrivas som att den tränas att göra en slags egen bedömning genom att skapa svar utifrån sannolikhetsbedömningar. Det handlar alltså mer om matematik och logik än om mänsklig intelligens i form av kreativitet och självständighet. Vi använder metoden *övervakad inlärning* för att träna systemet. Det betyder att vi människor formulerar facit och rättar modellen därefter. Med den här metoden har man mer kontroll över träningsledet och därmed också vad systemet gör och varför. Systemet blir snävare och mindre självständigt.

Försäkringskassan använder i nuläget inte mer avancerade tekniker såsom AI för att bedöma rätten till ersättning eller för att fatta beslut i förmånsärenden. AI-teknik används däremot i vissa it-stöd avsedda att stödja försäkringsutredare vid handläggning och inför beslut. Exempel på sådana är metodstöd för strukturerad analys av medicinska underlag (SAMU) och identifiering av enskildas ärenden med hög risk för felaktig utbetalning inom olika förmåner (”urvalsprofiler”).

Läs mer
eSam har tagit fram en checklista över olika rättsliga frågeställningar vid användning av AI. Syftet med checklistan är att belysa vilka rättsliga frågor som särskilt behöver beaktas vid användning av AI (*Checklista Juridik vid användning av AI*, eSam, ES2022-08). Där beskrivs vissa rättsområden som inte tas upp i denna vägledning, som skadestånd, konkurrensfrågor och upphandling.

AI-förordningen

En ny EU-förordning med regler för AI – AI-förordningen, trädde i kraft den 2 augusti 2024. Förordningen börjar som huvudregel tillämpas först den 2 augusti 2026, men vissa delar börjar tillämpas redan den 2 februari 2025, och andra delar betydligt senare. Arbete pågår inom Rättsavdelningen med att analysera den nya förordningen och vad den betyder för Försäkringskassan.

Syftet med den nya förordningen är att harmonisera reglerna för AI inom EU och att främja pålitlig AI kontrollerad av människor, men också att skydda människors säkerhet, hälsa och grundläggande rättigheter. Förordningen kommer att få stor betydelse för myndigheters AI-användning. Den kommer att styra vad myndigheter får respektive inte

får göra när det gäller AI. AI-förordningen behöver därför beaktas även om den ännu inte har börjat tillämpas i alla delar.

Förordningen använder ett riskbaserat angreppssätt för att dela upp olika typer av AI-system och deras användning, där vissa är förbjudna och andra är tillåtna men med restriktioner och krav i form av bland annat tillsyn och registrering hos ansvarig myndighet. De AI-system som inte innebär någon eller liten risk får användas utan restriktioner.

Förordningen ställer däremot långtgående krav på AI-användning som klassificeras som hög risk. För att få använda högrisksystem krävs bland annat att systemet har genomgått en granskningsprocess av en behörig offentlig aktör och fått en CE-märkning.

Vissa tekniska lösningar som Försäkringskassan redan använder kan komma att nå upp till definitionen av hög risk enligt AI-förordningen. Den anger att AI-system som är avsedda att användas av myndigheter eller för offentliga myndigheters räkning för att utvärdera fysiska personers rätt till väsentliga förmåner och tjänster i form av offentligt stöd samt för att bevilja, dra ner på, återkalla eller återkräva sådana förmåner och tjänster ska anses utgöra så kallade högrisksystem. (Bilaga III 5 a) AI-förordningen.)

AI-förordningen innehåller högre administrativa sanktionsavgifter än dataskyddsförordningen. Storleken på sanktionsavgiften beror på vilket brott mot förordningen som skett. Det är även upp till medlemsstaterna att besluta hur höga sanktionsavgifter som ska kunna tas ut av myndigheter i den staten. Sverige har inte kommit med något förslag i frågan än, och vi vet alltså inte hur höga sanktionsavgifter som kan drabba Försäkringskassan. EU-kommissionen har även föreslagit ett direktiv om skadeståndsansvar som gäller AI.

De bakomliggande skälen till AI-förordningen är i stora delar samma som den Europeiska kommissionens expertgrupp på hög nivå för AI-frågor (AI-expertgruppen) redogjorde för i publikationen *Etiska riktlinjer för tillförlitlig AI*. Där förklaras exempelvis att människor och samhällen behöver kunna lita på teknikens utveckling och dess tillämpningar. Om inte AI-systemen – och människorna bakom dem – är uppenbart tillförlitliga kan de ge oönskade konsekvenser och försvåra dess spridning, vilket innebär att det inte går att utnyttja de samhälleliga och ekonomiska fördelarna med AI-system.

Enligt de etiska riktlinjerna för tillförlitlig AI krävs att följande principer efterlevs:

- Den bör vara *laglig* och garantera respekt för alla gällande lagar och förordningar.
- Den bör vara *etisk* och säkerställa efterlevnad av etiska principer och värden.
- Den bör vara *robust*, både ur tekniskt och samhälleligt perspektiv eftersom AI-system även med de bästa intentioner kan orsaka oavsiktliga skador.

5.2 Rättsliga frågeställningar vid automation

Automatisering kan innebära olika slags rättsliga utmaningar. Vilka utmaningar det handlar om och hur påtagliga de är beror bland annat på vilken automatiseringsteknik det rör sig om. Vilken typ av teknik det handlar om sätter ramarna för vilka förutsättningar systemet har att efterleva de rättsliga krav vi ställer på den (läs mer i avsnitt 5.1). Men det handlar också om i vilken rättslig kontext automatiseringen sker.

I Försäkringskassans kärnverksamhet finns det möjligheter att använda automatisering som stöd för vissa moment vid handläggning av ärenden. Möjligheterna är däremot mer begränsade när det handlar om stöd vid bedömning eller beslutsfattande. För att avgöra

om vi får eller bör använda teknikens möjligheter måste vi göra rättsliga, demokratiska och etiska överväganden. Dessa frågor går delvis in i varandra.

I följande avsnitt beskrivs de viktigaste rättsliga frågorna som vi behöver ta ställning till. I viss utsträckning beskrivs också viktiga demokratiska och etiska frågor i den mån de går in i de rättsliga frågorna och är avgörande för våra möjligheter att använda oss av tekniken.

När det gäller avancerad teknik som AI finns många frågor där det ännu inte finns några säkra svar. Juridiken på området är fortfarande under utveckling. När det gäller bland annat AI-förordningen pågår arbete inom Rättsavdelningen med att analysera den nya förordningen och vad den betyder för Försäkringskassan.

5.2.1 Rättssäkerhet och legalitet

Det krävs stöd i rättsordningen för alla åtgärder och beslut. Det innebär att all utveckling och automatisering på Försäkringskassan måste ha stöd i vårt uppdrag och den lagstiftning vi tillämpar. Systemen måste programmeras och tränas så att de inte vidtar några åtgärder eller beslut som leder till att Försäkringskassan agerar i strid med lag eller beslutar på ett sätt som inte kan godtas utifrån gällande rätt. Systemet måste kunna kategorisera och identifiera både lika fall och olika fall och hantera båda korrekt enligt lag.

En svårighet är att systemet kan sakna förmåga att identifiera, förstå och ta hänsyn till nya oförutsedda omständigheter. Det kan leda till att systemet drar en felaktig slutsats och därmed vidtar en åtgärd i strid med lagstiftningen. Vid ett ändrat rättsläge måste det också gå att omprogrammera systemet för att anpassa det till det nya rättsläget.

Det finns olika förutsättningar för automatisering beroende på hur lagstiftningen är utformad. Om den är utformad med ett eller några få kriterier där det handlar om relativt enkla omständigheter som ska vara uppfyllda, till exempel ålder och födelseår, så går det att automatisera handläggningen och beslutsfattandet på ett rättssäkert sätt i större utsträckning. Försäkringskassan använder sådan automatisering med regelbaserad teknik redan i dag.

Ju mer komplexa reglerna är och ju mer avancerade systemen blir, desto mer resurskrävande och svårare blir det att granska, övervaka och följa upp systemen. I förmåner med ett större bedömningsutrymme finns det fler rättsliga och faktiska hinder och det medför fler risker som behöver hanteras. Det blir helt enkelt svårare att säkerställa att det finns lagstöd för varje åtgärd och beslut. En korrekt tillämpning av bedömningsutrymmet i varje enskilt fall är en förutsättning för att vi ska leva upp till legalitetsprincipen. Läs mer om den i avsnitt 2.1.1.

Vi får inte skapa större förutsebarhet än vad lagstiftningen medger. Automatisering kräver en förenkling, standardisering eller schablonisering av vilka omständigheter som ska tillmätas betydelse och vilket utfall de ska ge vid bedömningen av om den enskilde har rätt till en förmån. Om Försäkringskassan använder automatisering vid förmåner som har ett bedömningsutrymme finns det en risk att vi genom att införa sådana schabloniseringar i praktiken ställer upp villkor som begränsar eller utvidgar bedömningsutrymmet, det vill säga ändrar eller ställer upp nya gränser i själva lagstiftningen. En sådan tillämpning skulle kunna utgöra otillåten normgivning i strid med den formella lagkraftens princip i 8 kap. 18 § RF.

Den formella lagkraftens princip innebär att en föreskrift som en gång beslutats som lag inte kan ändras eller upphävas på annat sätt än genom en ny lag. Kravet på uttryckligt författningsstöd för kvalificerande (och därmed begränsande) villkor har i HFD:s praxis ställts relativt högt i socialförsäkringsrätten, se bland annat RÅ 2004 ref. 91, HFD 2022

ref 34, HFD 2013 ref 9, RÅ 2002 ref 98, RÅ 2010 ref. 5, RÅ 2010 ref. 37, RÅ 2000 ref. 51. Se även JO:s dnr 2367-2011. Försäkringskassan har alltså inte mandat att skapa större förutsebarhet än vad lagstiftningen medger genom att beskriva exakt vilka omständigheter som ger rätt till ersättning. En förutsebarhet som skapas på det sättet skulle inte innebära ökad rättssäkerhet.

När det handlar om förmåner med större bedömningsutrymme är möjligheterna att helautomatisera begränsade, eftersom den grad av standardisering eller schablonisering som skulle krävas sannolikt skulle innebära en hantering som saknar stöd i rättsordningen. I sådana förmåner skulle det behövas lagändringar för att kunna automatisera beslutsprocessen i högre grad.

En helt automatiserad beslutsprocess med regelbaserad teknik förutsätter att samtliga omständigheter som kan bli aktuella har beaktats när systemet programmerats. Med dagens teknik kan systemet inte i tillräcklig utsträckning ta hänsyn till nya omständigheter, placera dem i sitt sammanhang och värdera dem utifrån syftena med lagstiftningen. I förmåner med stort bedömningsutrymme är detta svårt eftersom det inte går att förutse och beskriva alla tänkbara situationer och kombinationer som kan uppkomma.

Maskininlärande system som AI kan *inte* lösa dessa svårigheter. Eftersom AI tränas att göra sina bedömningar på exempelvis tidigare beslut, så kommer de svar som AI:n ger att baseras på sannolika utfall utifrån dessa beslut. AI:n kan inte ta hänsyn till nya omständigheter.

I förmåner med bedömningsutrymme kan det dock vara möjligt att automatisera vissa led i handläggningen. Exempelvis för att göra kontroller av om ansökan är komplett, stämma av uppgifter i ansökan mot andra uppgifter och på andra sätt vara ett stöd för handläggaren. På så sätt kan automatiserade och manuella förfarande komplettera varandra, läs mer i avsnitt 5.3.3.

En annan aspekt av rättssäkerhet och legalitet är att vi behöver säkerställa tillräcklig mänsklig kontroll och inflytande. Det krävs transparens kring systemet så att vi kan förstå och förklara vad systemet gör och varför (läs mer i avsnitt 5.2.7). Helautomatiserade system måste följas upp och kunna förklaras, men detta är viktigt också vid semiautomatiserade processer exempelvis när systemet gör uträkningar eller lämnar förslag till beslut. Handläggaren måste granska systemets bedömning och pröva den mot sin egen. Om handläggaren inte granskar och vid behov korrigerar systemets förslag finns det risk för felaktig hantering. Det är därför viktigt att vi inte följer de förslag som systemet lämnar helt okritiskt.

5.2.2 Grundläggande fri- och rättigheter

Användningen av AI och annan avancerad teknik berör flera grundläggande fri- och rättigheter enligt EU:s rättighetsstadga, Europakonventionen och regeringsformen. Det rör sig bland annat om integritet, dataskydd, icke-diskriminering och tillgång till rättslig prövning. Vilken inverkan användningen av avancerad teknik får på de grundläggande fri- och rättigheterna beror på graden av automatisering och på hur avancerat systemet är. För att säkerställa möjligheten till insyn och för att motverka kränkningar av människors grundläggande fri- och rättigheter eller andra negativa och oönskade konsekvenser, måste vi ställa upp krav på bland annat transparens och öppenhet när vi utvecklar avancerade system på Försäkringskassan, och efterleva kraven när vi använder systemen.

Till stor del saknas det kunskap om hur grundläggande rättigheter påverkas av de nya teknologierna (se bland annat rapporten *Getting the future right – Artificial intelligence and fundamental rights*).

5.2.3 Demokrati och fri åsiktsbildning

Avancerad teknik som AI väcker frågor om i vilken utsträckning vi är beredda att överlämna den offentliga demokratiska maktutövningen till en maskin, det vill säga att låta den analysera, dra slutsatser och fatta beslut.

Med den nya avancerade tekniken inträder en ny dimension av självständighet hos systemet. Processen är mindre transparent och svårare för en människa att förstå och därmed minskar möjligheten att granska, utvärdera, ifrågasätta och bilda sig en åsikt om den.

Grundläggande i ett demokratiskt samhälle är också möjligheten för enskilda att utkräva ansvar hos beslutsfattare. Det måste finnas en utpekad människa på Försäkringskassan som är ansvarig för det som systemet gör och det behöver klarläggas vem som har det ansvaret.

5.2.4 Objektivitet, likabehandling och icke-diskriminering

Kraven på saklighet innebär bland annat att omständigheter som är irrelevanta för frågan om rätten till en förmån inte får läggas till grund för ett beslut om förmånen. Civilstånd, hemlän, eller tidigare uttag av föräldrapenning får exempelvis inte läggas till grund för bedömningen av rätten till sjukpenning eftersom dessa omständigheter är irrelevanta för att bedöma om den enskilde har en sjukdom som medför nedsatt arbetsförmåga.

Hela handläggningsprocessen, inklusive de delar som är automatiserade och eventuellt utförs av AI-system eller annan avancerad teknik, måste vara fria från diskriminering. En speciell utmaning vid användningen av AI-teknik är kopplad till vad vi människor tror att AI kan göra. Det finns en risk med att vi människor ibland systemet som objektivt och tänker oss att AI skulle kunna fatta objektiva beslut när tillämpning av AI i själva verket endast är en förlängning av subjektiv, mänsklig verksamhet. AI-systemet kan i princip bara göra det som människan har instruerat det att göra och kan endast veta det som människan har talat om för det eller lagt in i systemet. Om data inte är objektiva kan AI-systemet reproducera och intensifiera diskriminerande och skadliga processer när AI:n används i exempelvis sociala trygghetssystem.

Vi behöver därför säkerställa hög kvalitet på de data som används på Försäkringskassan och att systemen byggs så att de kan granskas, analyseras och bedömas utifrån samtliga diskrimineringsgrunder innan de tas i bruk. Vi behöver också övervaka och följa upp hur datan används för att motverka risker för diskriminering.

5.2.5 God offentlighetsstruktur och sekretess

En god ordning i hanteringen av Försäkringskassans information och handlingar är viktig för allmänhetens möjlighet att ta del av allmänna handlingar och uppgifter. Vi måste säkerställa att allmänna handlingar diarieförs eller hålls ordnade på annat sätt och att information dokumenteras. Behovet av bevarande och gallring måste utredas och efterlevas. Detta gäller också när vi utvecklar och testar automatiserade system.

När vi utvecklar behöver vi bedöma om de handlingar som uppstår är allmänna eller inte. Exempelvis kan systemdokumentation och programkod vara allmän handling. Vi måste också bedöma om tränings- och valideringsdata blir nya allmänna handlingar eller om de utgör kopior av tidigare allmänna handlingar.

Systemdokumentation och programkod kan omfattas av sekretess enligt exempelvis 18 kap. 8 § 3 och 18 kap. 9 § OSL. Uppgifter som används för att träna och testa automatiserade system kan också omfattas av sekretess. Om det rör sig om uppgifter

om enskilda kan socialförsäkringssekretessen i 28 kap. 1 § OSL bli aktuell. Den gäller visserligen i första hand i ärenden, men kan också gälla utanför förmånsärendet i strikt bemärkelse. Om det rör sig om uppgifter om metoder, modeller och riskfaktorer som hänför sig till dataanalyser och urval för att förebygga, förhindra och upptäcka felaktiga utbetalningar kan sekretess gälla enligt 17 kap. 1b § OSL.

Läs mer

Läs mer om offentlighetsprincipen, allmänna handlingar och om sekretess i Försäkringskassans vägledning (2001:3) *Offentlighet, sekretess och behandling av personuppgifter.* Läs mer om gallring och bevarande i Försäkringskassans riktlinjer (2022:01) *Gallring och bevarande av verksamhetsinformation* och Försäkringskassans anvisningar (2023:09) *Gallring och bevarande av verksamhetsinformation*.

5.2.6 Behandling av personuppgifter

När automatiseringen innebär att personuppgifter behandlas aktualiseras bland annat bestämmelserna i dataskyddsregelverket.

Det måste till exempel finnas en rättslig grund för behandlingen och uppgifterna får endast behandlas för uttryckliga, på förhand angivna, berättigade ändamål. Detta gäller även när personuppgifterna behandlas för att utveckla automatiserade system, exempelvis för att testa och för att träna mer avancerade system.

Försäkringskassan framförde i sin hemställan om nya regler för personuppgiftsbehandling i kärnverksamheten att det behövs ett särskilt primärt ändamål för utvecklingsåtgärder. Det handlade bland annat om att det skulle bli tydligt att Försäkringskassan har stöd för det omfattande utvecklingsarbete som pågår och förväntas pågå framöver samt för mer innovativa utvecklingsåtgärder (Hemställan om ändringar i 114 kap. SFB och förordningen (2003:766) om behandling av personuppgifter inom socialförsäkringens administration, s. 85f.). Något sådant ändamål infördes dock inte i det nya 114 kap. SFB.

I propositionen skriver regeringen bland annat följande om it-utveckling (prop. 2023/24:29 s. 45).

> ”Myndigheter ska bedriva en effektiv verksamhet och fortlöpande utveckla den. Försäkringskassan och Pensionsmyndigheten bedriver verksamhets- och it-utveckling både på eget initiativ och med anledning av olika uppdrag. Myndigheterna behöver t.ex. ha adekvata system för ärendehantering, digitala lösningar för informationsutbyte och effektiva analysverktyg. Arbetet med it-utveckling kan handla både om att säkerställa och förbättra befintliga lösningar och om att ta fram nya lösningar och ny funktionalitet. Förvaltning, utveckling och underhåll av myndigheternas it-system förutsätter ofta testning. […]
>
> Testning kan ofta göras med hjälp av avidentifierade uppgifter som saknar koppling till individer. Sådan anonym information är inte personuppgifter och omfattas därmed inte av dataskyddslagstiftningens krav. I vissa fall kan dock tester med personuppgifter vara en förutsättning för att personuppgifter ska behandlas på ett korrekt sätt i den faktiska verksamheten.”

It-utveckling i form av testverksamhet berörs uttryckligen i förarbetena. Där framgår att testverksamhet har ett sådant samband med Försäkringskassans verksamhet i övrigt att det inte behövs någon särskild ändamålsbestämmelse. (prop. 2023/24:29 s. 45f.)

Testverksamhet anses alltså kunna ske med stöd av bestämmelserna i 114 kap. SFB, antingen genom ett av ändamålen i 8 § eller att det görs en bedömning enligt finalitetsprincipen (att ändamålet inte är oförenligt med det ändamål för vilket uppgifterna samlades in) i 10 §.

Det betyder inte att testverksamhet alltid är tillåten på Försäkringskassan. Vi behöver alltid bedöma om den aktuella testningen behövs för att vi ska kunna utföra vårt uppdrag. Personuppgiftsbehandlingen måste vara nödvändig för det identifierade ändamålet. Testverksamheten måste också utföras i enlighet med övriga bestämmelser om dataskydd, exempelvis bestämmelserna om sökbegränsningar och begränsningar i fråga om tillgång till personuppgifter. (Jfr prop. 2023/24:29 s. 45f.)

Mer innovativ it-utveckling och exempelvis träning av AI-modeller berörs inte uttryckligen i förarbetena. Precis som med all personuppgiftsbehandling måste vi göra samma bedömningar som beskrivs i föregående stycke, bland annat om personuppgiftsbehandlingen behövs för att vi ska kunna utföra vårt uppdrag och identifiera ett ändamål.

Vid träning av en AI-modell har mängden träningsdata betydelse för att ge korrekt och önskat resultat i produktion. I vissa fall kan mängden träningsdata vara avgörande för hur bra modellen presterar. Om datamängden innehåller personuppgifter kan AI-modellens behov av stora mängder data komma i konflikt med dataskyddsregelverkets principer om bland annat uppgifts- och lagringsminimering. Å ena sidan finns kravet i dataskyddsförordningen på att minimera uppgiftsmängder och å andra sidan AI-modellens behov av en större uppgiftsmängd för ett korrekt utfall.

Utvecklingsinsatser med automatiserade inslag inom kärnverksamheten förutsätter ofta att it-systemen kan söka, sortera och strukturera information genom sökningar. Då aktualiseras sökbegränsningarna i 114 kap. 12 § SFB.

Vi får inte göra sökningar *i syfte* att få fram ett urval av personer grundat på känsliga personuppgifter. Vi får däremot göra det för de primära ändamålen (i 114 kap. 8 § SFB) i syfte att få fram ett urval av personer grundat på känsliga personuppgifter om hälsa, om uppgiften avser förmån eller ersättning. Vi får också göra sökningar i syfte att få fram ett urval av personer grundat på andra känsliga personuppgifter om hälsa än förmån och ersättning, om urvalet ska användas för att vidta åtgärder i handläggningen, planera, följa upp eller utvärdera handläggningen eller för kontrollåtgärder. Andra känsliga personuppgifter om hälsa än förmån och ersättning kan exempelvis vara uppgift om diagnos.

Sökbegränsningsregeln hindrar alltså inte automatisering som kräver sökningar på uppgift om förmån och ersättning eller på exempelvis diagnos om det handlar om att automatisera ärendehandläggningen. (prop. 2023/24:29 s. 67)

En grundläggande princip i dataskyddsförordningen är att den personuppgiftsansvarige (i detta fall Försäkringskassan) ska vidta åtgärder som säkerställer lämplig säkerhet för personuppgifterna. Vid mer långtgående automatisering och användning av avancerad teknik kommer det många gånger att finnas sådana risker för enskildas fri- och rättigheter så att vi behöver göra en konsekvensbedömning.

Läs mer

Läs mer om konsekvensbedömningar i riktlinjerna (2024:03) *Bedömning av dataskydd - Grundläggande bedömning och konsekvensbedömning*.

De registrerades rättigheter enligt dataskyddsförordningen behöver säkerställas, till exempel information till de registrerade, rättelse och radering. Dataskyddsförordningen ställer också krav på dokumentation för att möjliggöra transparens. Det måste gå att följa vilken information systemet har hämtat, varifrån den har hämtats och hur systemet har dragit sina slutsatser för att säkerställa korrekthet. Vi behöver alltså ta fram ett sätt att dokumentera vad det automatiserade systemet gör och klarlägga vad som är en tillräcklig grad av förklarbarhet. Samtidigt får inte personuppgifter behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen.

5.2.7 Transparens och dokumentation

När man talar om transparens vid automatisering menar man i allmänhet möjligheten till insyn i vad systemet gör och hur det fungerar. Transparens förutsätter dokumentation.

Det finns många regler som påverkar behovet av transparens och skyldigheten till dokumentation. I FL, OSL och dataskyddsförordningen ställs krav på viss dokumentation och information vid ärendehandläggning. Andra rättsliga krav påverkar behovet av dokumentation av it-systemen i sig, såsom dataskyddsförordningens krav på dokumentation för att möjliggöra transparens och den föreslagna AI-förordningens krav på teknisk dokumentation.

I grunden handlar dessa regler om att det måste gå att förstå och förklara vad systemet gör och varför. Det är en förutsättning för att parter och registrerade ska kunna få den insyn de har rätt till och bevaka sin rätt på ett meningsfullt sätt. Det krävs för att Försäkringskassan ska ha kontroll över sin information och sin ärendehantering, bland annat för att kunna upptäcka och åtgärda risker för felaktigheter och diskriminering. Det krävs också för att överinstanser och tillsynsmyndigheter ska kunna göra sitt jobb.

Transparens har alltså rättslig betydelse för enskilda ärenden och individer, men också på en övergripande nivå. Att kunna säkerställa att vår ärendehandläggning går rätt till och är rättssäker (i betydelsen formell rättssäkerhet) är en förutsättning för ansvarstagande, för allmänhetens förtroende och för socialförsäkringens legitimitet.

Mer avancerade system för automation såsom maskininlärande system innebär särskilda utmaningar när det gäller transparens. Om vi inte fullt ut kan förstå och förklara hur systemet gör sina bedömningar är det svårt att bedöma rättsenligheten i systemet. Det handlar framförallt om den formella rättssäkerheten, det vill säga hur systemet kommer till sina slutsatser.

5.3 Ett automatiserat förfarande i ärendehandläggningen

I grunden är det samma regelverk som styr hur ärenden ska handläggas, oavsett om handläggningen sker automatiserat eller om en handläggare utför den manuellt. Ett ärende ska i båda fallen handläggas enligt FL och eventuell avvikande lagstiftning, till exempel SFB. Vi ska ta emot en ansökan, handlägga den och därefter fatta beslut. Det är viktigt att ha med sig när ny teknik öppnar möjligheter för förbättringar, förenklingar och effektiviseringar.

Det finns vissa särskilda regler för automatiserade förfaranden. Det finns en särskild regel om automatiserat beslutsfattande (se avsnitt 5.3.6). Det finns också särskilda regler i SFB för elektroniska ansökningar och uppgiftslämnande som har betydelse vid automatiserade förfaranden (se 111 kap. SFB). Dessa regler påverkar däremot inte de allmänna förvaltningsrättsliga kraven, som i grunden handlar om rättssäkerhet, utan syftar till att ta bort eventuella rättsliga hinder mot digitala förfaranden.

Det är uppkommer ofta rättsliga frågeställningar när ett automatiserat förfarande ska införas. En anledning till det är att stegen i det automatiserade förfarandet måste

bestämmas på förhand så att systemet kan programmeras för att utföra stegen. För att ta ställning till vad systemet ska programmeras att utföra måste de rättsliga kraven utredas. Rättsliga frågeställningar kan också uppstå av andra anledningar. Det kan exempelvis handla om att tekniken öppnar möjligheter att testa nya lösningar för att öka effektiviteten eller att minska risken för felaktiga utbetalningar.

Om vi vid en utvecklingsinsats överväger att införa nya funktioner måste vi först ta ställning till om det är möjligt och lämpligt, utifrån de regler och övriga förutsättningar som gäller för den aktuella förmånen. De tekniska möjligheterna och övriga skäl som talar för nya lösningar måste vägas mot regelverket. Ibland blir regelverket ett hinder mot utveckling av nya lösningar. Då är det viktigt att komma ihåg att regelverket finns där av en anledning, vanligen för att värna om den enskildes rättssäkerhet.

Läs mer
Läs mer om de förvaltningsrättsliga kraven som gäller generellt vid ärendehandläggning på Försäkringskassan i Försäkringskassans vägledning (2004:7) *Förvaltningsrätt i praktiken* och i de förmånsspecifika vägledningarna.

5.3.1 Utforma ansökan

För att ett automatiserat förfarande ska fungera ändamålsenligt måste ansökan och den mottagningsfunktion som tar emot ansökan utformas på ett sätt som möjliggör automatiserad handläggning. Kompletteringar och utredning kräver ofta manuell handläggning. Det är därför exempelvis en fördel om ansökan innehåller alla uppgifter som behövs, utan att behöva kompletteras.

När ett automatiserat förfarande ska införas uppstår det ofta önskemål om att utforma och på det sättet ställa krav på ansökningar för att ärendet ska kunna handläggas automatiserat i så stor utsträckning som möjligt. Exempel på frågor som kan uppkomma är om det är möjligt att

- införa obligatoriska fält i en digital ansökan
- bara tillåta digitala ansökningar i det automatiserade förfarandet (det vill säga inte ta emot pappersansökningar som handläggs helt manuellt)
- bygga mottagningsfunktionen så att bara ansökningar som är kompletta eller som uppfyller vissa andra krav tas emot.

När det gäller mottagningsfunktioner finns det vissa rättsliga principer som alltid måste följas. En sådan är att Försäkringskassan är skyldig att ta emot och handlägga ansökningar om sådan ersättning som regelverket ger rätt till och på det sätt som regelverket ger rätt till. Det innebär att vi inte får utforma mottagningsfunktioner som bara tar emot ansökningar som uppfyller vissa krav (exempelvis att de är komplett ifyllda), om det inte följer av regelverket att det är så ärendet ska hanteras. Vi kan inte heller välja att bara ta emot digitala ansökningar, om regelverket tillåter pappersansökningar (jfr. bland annat JO 2011/12 s. 413).

Försäkringskassan får alltså inte ställa mer krav än som följer av regelverket eller på annat sätt direkt eller indirekt hindra enskilda från att ansöka. Det förvaltningsrättsligt korrekta är att ta emot alla framställningar från enskilda och hantera dem, manuellt eller automatiserat. Otydliga framställningar ska förtydligas eller kompletteras inom ramen för Försäkringskassans serviceskyldighet, med undantag för framställningar som är i sådant skick att vi över huvud taget inte förstår vad som avses eller vem avsändaren är. Om vi konstaterar att det rör sig om en ansökan om ersättning och att ett ärende därmed har

inletts på Försäkringskassan, så ska det ärendet handläggas och sedan avslutas med ett ställningstagande till ansökan, det vill säga ett beslut.

5.3.2 Automatiska kontroller i ansökningsförfarandet

När vi bygger digitala tjänster på Försäkringskassan där enskilda kan göra ansökningar, anmäla uppgifter med mera kan vi samtidigt skapa kontroller som stämmer av de uppgifter som ges in i den digitala tjänsten, exempelvis för att kontrollera om ansökan är komplett ifylld. Sådana kontroller är vanliga i automatiserade förfaranden och kan ur ett rättsligt perspektiv motiveras med att de är en digital tillämpning av Försäkringskassans *serviceskyldighet* enligt FL.

Många kontroller är oproblematiska. De underlättar både för enskilda och myndigheter. Exempel på kontroller av ett okontroversiellt slag är avstämningar av att uppgifter i ansökan är korrekt eller komplett ifyllda, eller enkel logik som att summeringar är rätt. Exempelvis kan systemet uppmärksamma den sökande på att hen glömt att fylla i en uppgift eller fyllt i ett födelsenummer som inte är möjligt. Genom sådana kontroller får den enskilde stöd att rätta till brister innan hen lämnar in sin ansökan i stället för att behöva komplettera ansökan i efterhand. Denna typ av kontroller kan alltså underlätta för enskilda att göra rätt i kontakten med Försäkringskassan och skapa bra förutsättningar för effektiv ärendehandläggning.

Det finns dock gränser för hur omfattande kontroller som kan byggas in i en digital tjänst. Kontrollerna kan nämligen påverka hur den enskilde kan använda tjänsten och hur den enskilde kan rättshandla i förhållande till Försäkringskassan. Exempelvis kan kontrollerna styra den enskilde när hen ska lämna information till Försäkringskassan – genom att bara tillåta viss information, genom obligatoriska fält eller genom att göra automatiska beräkningar som den enskilde godtar utan att ta ställning till. Det är i de sammanhangen nödvändigt att dra gränsen för vilken service som är möjlig och när en service övergår till att bli för styrande i förhållande till den enskildes vilja.

Det är inte helt tydligt var den gränsen går, det vill säga hur styrande kontrollerna kan vara och fortfarande anses vara en serviceåtgärd. Det finns förarbetsuttalanden som talar för att lagstiftaren ansett att vissa typer av hindrande kontroller är möjliga (prop. 2014/15:10, s. 27).

Kontroller som hindrar den enskilde från att lämna in en ansökan med den information som hen vill ange, exempelvis genom att hen hindras från att slutföra ett digitalt ansökningsförfarande utan att komplettera vissa uppgifter, kan vara problematiska. Man kan då diskutera om det egentligen handlar om ett avvisnings-, avskrivnings- eller avslagsbeslut. Sådana beslut måste uppfylla kraven i FL. Om systemet inte tar emot en ansökan, eventuellt kompletterat med ett enkelt felmeddelande, innebär det inte att ett förvaltningsrättsligt korrekt beslut om avvisning eller avskrivning har fattats. Alla former av negativa beslut ska nämligen som huvudregel dokumenteras och motiveras. Den sökande ska också underrättas om beslutet och få information om hur det kan överklagas.

Försäkringskassan har övervägt, men avstått från, hindrande kontroller som innebär en bedömning av sakomständigheter vid en ansökan om merkostnadsersättning. Den sökande skulle i det fallet stoppas från att lämna in ansökan i en digital tjänst om de uppgifter som hen angav indikerade att hen inte hade rätt till förmånen. Försäkringskassan har däremot infört kontroller av framförallt formalia vid vårdgivares begäran om utbetalning av tandvårdsstöd. Det statliga tandvårdsstödet skiljer sig från många andra förmåner, bland annat merkostnadsersättning, eftersom regelverket bygger på en utpräglad digitalisering och automatisering samt utgör en form av schabloniserad masshantering.

När Försäkringskassan överväger att skapa kontroller i en digital tjänst ska vi alltså först ta ställning till vad kontrollerna får för konsekvenser för användaren. Sedan måste vi ta ställning till om kontrollerna är möjliga och lämpliga att införa enligt regelverket.

5.3.3 Manuella alternativ till ett automatiserat förfarande

Det behövs alternativa, manuella, förfaranden för dem som är förhindrade att kommunicera digitalt eller av olika skäl inte vill använda det utpekade digitala ansökningsförfarandet.

Det kan också behövas manuella förfaranden för att hantera sådana delar av handläggningen som inte är rättsligt möjliga eller lämpliga att automatisera. Ofta handlar det om vissa utredningsåtgärder eller bedömningar som en handläggare behöver göra, till exempel ärenden som kräver omfattande utredning eller skönsmässiga bedömningar för att avgöra rätten till ersättning.

I många fall behöver automatiserade förfaranden alltså kompletteras med manuell handläggning. Oftast finns det parallella förfaranden från början, med en digital ansökan och en pappersansökan. De förfaranden som inleds digitalt brukar sedan ha en manuell hantering i delar av förfarandet, till exempel om systemet identifierar vissa kriterier.

Ett praktiskt exempel från Försäkringskassans verksamhet är hanteringen av SGI-ärenden. När frågan om att fastställa SGI väcks tar systemet först ställning till om det finns anledning att utreda frågan om SGI. Om SGI:n inte behöver utredas fastställs den maskinellt i det förmånsärende där frågan om SGI aktualiserats. Om frågan om SGI behöver utredas startas ett ärende i handläggningssystemet. I det ärendet kan handläggningen ske automatiserat, delvis automatiserat eller helt manuellt beroende på vad det rör sig om för ärende.

- De ärenden där vi kan få ett tillräckligt beslutsunderlag genom automatiserade kontroller hanteras helt eller delvis automatiserat:
  - Systemet stämmer av uppgifterna om årsinkomst i ansökan mot uppgifter från Skatteverket. Om uppgifterna i ansökan stämmer överens med uppgifterna från Skatteverket fattas beslut om SGI automatiserat. Avstämningen och bedömningen dokumenteras i ärendet.
  - Systemet stämmer av uppgifterna om årsinkomst i ansökan mot uppgifter från Skatteverket. Om uppgifterna skiljer sig åt eller systemet identifierar vissa andra kriterier för manuell hantering (exempelvis att det saknas uppgifter att stämma av mot hos Skatteverket) lämnas ärendet över för manuell hantering. Avstämningen och bedömningen dokumenteras i ärendet. En handläggare utreder sedan ärendet vidare, exempelvis frågan om varför inkomsten varierar, och bedömer vilken SGI som den enskilde har rätt till.
- De ärenden där vi inte kan få ett tillräckligt beslutsunderlag genom automatiserade kontroller handläggs helt manuellt.

Om det finns sådan manuell hantering som alternativ bör det finnas större utrymme att bygga effektiva, användarvänliga och utpräglat eller helt automatiserade förfaranden med den typen av funktioner som har getts exempel på tidigare i avsnittet. Då har nämligen alla möjlighet att ansöka om den aktuella förmånen, även om inte alla kan ansöka digitalt.

5.3.4 Nudging

Vi ska hjälpa den sökande att förtydliga eller komplettera otydliga framställningar, främst som ett led i Försäkringskassans serviceskyldighet. Men vi kan också ge service utanför ett enskilt ärende, innan den enskilde har ansökt.

Ett sätt att hjälpa den enskilde att utforma sin ansökan så komplett och korrekt som möjligt är att använda sig av *nudging*. Det kan definieras som en ”knuff” i en viss riktning, utan att minska individens valfrihet. Genom att arrangera en valsituation på ett visst sätt och belysa konsekvensen av de val som den enskilde gör, får hen möjlighet att göra informerade val som är positiva för hen själv. Det kan till exempel handla om att göra det lättare att lämna korrekt information genom hjälptexter som förklarar vad ett visst fält är tänkt att innehålla.

När Försäkringskassan använder nudging handlar det framför allt om att hjälpa den enskilde att göra rätt, inte att påverka hen att göra på ett sätt som passar vår handläggning bäst. Det är därför viktigt att nudging görs på ett transparent sätt så att den enskilde själv kan överblicka konsekvenserna av sina val.

Allt vi gör måste vara förankrat i lagstiftningen. Vi får inte påverka människors beteende, till exempel vilka uppgifter de lämnar i en ansökan, utan att först analysera vilka konsekvenserna skulle kunna bli för den enskilde. Vi ska exempelvis inte påverka den enskilde i en riktning som får negativa konsekvenser för hen.

Vi måste särskilja nudging från en situation då det, till exempel inom ramen för en tjänst, finns ett obligatoriskt fält som måste fyllas i för att en ansökan ska kunna skickas in. Ett sådant fält innebär visserligen att användaren "knuffas” i rätt riktning, men har mer karaktären av ett krav på hur ansökan ska fyllas i än ett hjälpmedel.

5.3.5 Utredning och kommunicering

I avsnitt 5.3.1–5.3.4 framgår att det förvaltningsrättsligt korrekta är att ta emot alla framställningar från enskilda och hantera dem. När någon ansöker om ersättning inleds ett ärende på Försäkringskassan. Inom ramen för ärendet vidtas sedan handläggningsåtgärder, såsom att kontrollera att uppgifter stämmer, hjälpa den sökande att komplettera sin ansökan med de uppgifter eller intyg som behövs och att vidta egna utredningsåtgärder. Det är samma åtgärder som blir aktuella när en ansökan hanteras automatiserat som när en handläggare hanterar den manuellt. Hur det görs kan dock i vissa fall skilja sig åt på grund av de möjligheter som ett digitalt handläggningssätt erbjuder. Detta gäller särskilt vid automatisering.

Samma krav gäller vid utredning av ärenden genom automatiserad och manuell handläggning. Det är också samma beviskrav som gäller. Det betyder att Försäkringskassan ska utreda ärendena på samma sätt och ställa samma krav för att en ansökan ska kunna bifallas. Det automatiserade förfarandet måste dock konstrueras på förhand och har inte samma möjlighet till avvägningar i det enskilda fallet som vid manuell handläggning. Det är därför sällan möjligt att använda helt automatiserade förfaranden inom ramen för ett ärende i socialförsäkringsärenden. Eftersom automatisering kräver att de omständigheter som avgör utgången i ett ärende standardiseras och schabloniseras är ett helautomatiskt förfarande problematiskt för förmåner med ett större bedömningsutrymme. Läs mer om automatisering och bedömningsutrymme i avsnitt 5.2.1.

Även om Försäkringskassan sällan kan ha helt automatiserade förfaranden är det möjligt att göra dem delvis automatiserade. Då handläggs ärendet i samverkan mellan handläggaren och it-systemet. Vi kan använda automatiserade kontroller som stämmer av inlämnade uppgifter mot interna uppgifter eller uppgifter som hämtas in från en annan myndighet. Många utredningsåtgärder kan göras enklare och mer effektivt när de automatiseras, till exempel inom SGI. Läs mer i avsnitt 5.3.3.

Om information stäms av mot uppgifter från en annan myndighet handlar det om en slags *digital tjänst för informationsutbyte*. Du kan läsa mer om dem i kapitel **Fel! Hittar inte referenskälla.**.

Det är också möjligt att fatta beslut med stöd av maskinellt framställda underlag eller rekommendationer. Exempelvis kan automatisering användas för att kontrollera om en ansökan är komplett ifylld eller för beräkningar utifrån uppgifter i ärendet.

Oavsett om handläggningen av ett ärende sker manuellt eller automatiserat måste den enskilde få rätt till kommunikation enligt FL. Om en automatiserad handläggning innebär att utredning i större utsträckning hämtas in på Försäkringskassans initiativ utan den enskildes inblandning, så ökar behovet av att kommunicera det inhämtade materialet med den enskilde.

När det handlar om automatiserade förfaranden talar vi ofta om att systemet *kontrollerar* något, när vi i ett manuellt förfarande skulle tala om att en handläggare *utreder* något. De kontroller som utförs innan ärendet avslutas handlar dock också om utredningsåtgärder, oftast att utreda rätten till ersättning. Att begreppet kontroller används i detta sammanhang ska alltså inte förväxlas med de kontroller som görs efter att ett ärende avslutats, exempelvis för att kontrollera om ersättning betalats ut felaktigt. När ärendet handlagts klart avslutas det med ett ställningstagande till ansökan, det vill säga ett beslut.

5.3.6 Beslut

Beslut kan fattas av en tjänsteperson eller automatiserat. En tjänsteperson kan fatta beslut med stöd av maskinellt framtagna underlag, men det är fortfarande tjänstepersonen som fattar beslutet. När beslut fattas maskinellt utan att någon tjänsteperson tar aktiv del i själva beslutsfattandet i det enskilda fallet talar vi om *automatiserade beslut* (prop. 2016/17:180 s. 315). Att sådant beslutsfattande är tillåtet framgår numera uttryckligen i 28 § FL.

Det finns också bestämmelser om automatiserat beslutsfattande i dataskyddsförordningen.

Enligt artikel 22.1 i dataskyddsförordningen ska den registrerade ha rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripet profilering, vilket har rättsliga följder för hen eller på liknande sätt i betydande grad påverkar hen. Profilering definieras i dataskyddsförordningen som automatisk behandling av personuppgifter för att bedöma vissa personliga egenskaper hos en person, i synnerhet för att förutsäga bland annat pålitlighet. Automatiserat beslutsfattande hos myndigheter som innebär behandling av personuppgifter för att analysera eller förutse till exempel pålitlighet, beteende, arbetsprestation, hälsa eller dylikt kan därför vara otillåtet enligt förordningen (Se eSam, Checklista Juridik vid användning av AI, s. 15).

Det är oklart hur artikel 22.1 i dataskyddsförordningen ska tolkas och i vilken utsträckning automatiserat beslutsfattande är tillåtet enligt bestämmelsen. Det är bland annat oklart om bestämmelsen innebär ett generellt förbud mot automatiserat beslutsfattande eller om den innebär en rätt för den registrerade (den enskilde) att invända. Det är också oklart om bestämmelsen handlar om alla former av automatiserat beslutsfattande eller bara automatiserat beslutsfattande som innebär profilering.

I artikel 22.1.b i dataskyddsförordningen finns ett undantag som ger medlemsstaterna möjlighet att i nationell lag godkänna automatiserat beslutsfattande om den nationella lagen fastställer lämpliga åtgärder till skydd för den registrerades rättigheter, friheter och berättigade intressen. Den svenska regeringen anser att FL innehåller sådana skyddsåtgärder som krävs i dataskyddsförordningen och att automatiserat beslutsfattande med stöd av 28 § FL därför är tillåtet. (Se bland annat prop. 2017/18:95 s. 100, prop. 2017/18:112 s. 64-65, prop. 2017/18:115 s. 31, prop. 2017/18:254 s. 55

och prop. 2018/19:33 s. 164 samt eSam, *Rättsligt uttalande om automatiserade beslut* 2018-03-19).

I artiklarna 13 och 14 i dataskyddsförordningen finns bestämmelser om att den registrerade ska få särskild information om förekomsten av automatiserat beslutsfattande enligt artikel 22.

När Försäkringskassan använder automatiserat beslutsfattande måste vi alltså följa FL:s krav på handläggnings- och beslutsprocessen. Reglerna i FL om dokumentation, kommunikation och beslutsmotivering gäller även vid automatiserade beslut. Enskilda måste också få särskild information om att det förekommer automatiserat beslutsfattande.

Kraven på beslutsmotivering i FL innebär att automatiserade beslut framförallt blir aktuellt i fråga om positiva beslut. De krav som ställs på beslutsmotiveringen vid negativa beslut kan nämligen vara svåra att leva upp till utan mänsklig involvering. (Jfr JO:s dnr 6744-2020).

Försäkringskassan fattar i dagsläget inga automatiserade beslut som grundas på profilering i dataskyddsförordningen mening. När vi fattar ett automatiserat beslut som rör en förmån sker det en automatiserad bedömning av en persons personliga egenskaper. Det görs till exempel en automatiserad bedömning av personens specifika förhållanden och andra omständigheter. Bedömningen syftar dock inte till att förutsäga någons ekonomiska situation eller att analysera några andra personliga egenskaper. Syftet är inte heller att placera vederbörande i en viss kategori eller grupp. I stället fattas dessa beslut utifrån objektiva och förutbestämda kriterier för förmånen. Systemet bearbetar endast lämnade och befintliga uppgifter om exempelvis ålder och inkomst. Profilering används däremot vid urval för kontroll, men i samband med det fattas inget beslut.

Läs mer
Läs mer om beslut på Försäkringskassan i Försäkringskassans vägledning (2004:7) *Förvaltningsrätt i praktiken.* Den beskriver bland annat vad som gäller i fråga om dokumentation, kommunikation och beslutsmotivering.

5.3.7 Krav på dokumentation vid automatiserad ärendehantering

Dokumentation i ärenden
De allmänna kraven på dokumentation i ärenden enligt FL gäller även vid automatiserad handläggning. Dessa beskrivs i Försäkringskassans vägledning (2004:7) *Förvaltningsrätt i praktiken*. Det finns också en specifik regel om att elektronisk information ska tillföras ärendet i läsbar form om sådan information används för att för att handlägga ett ärende. Det framgår av 4 kap. 3 § OSL. Undantaget är om det finns särskilda skäl mot det.

Skyldigheten att dokumentera gäller i första hand uppgifter som lämnas muntligt till Försäkringskassan, eller som vi får på annat sätt än genom en handling, och som kan ha betydelse för ett beslut i ett pågående ärende. Men vi måste också dokumentera andra relevanta händelser i ärendet. Det kan exempelvis handla om kontakter med parter, andra personer eller myndigheter. Det kan också handla om handläggningsåtgärder och andra händelser som rör ärendets gång, även om de inte tillför något i sak till ärendet. En fullständig och ordnad dokumentation i ett ärende är en

förutsättning för att man ska kunna följa och förstå ärendets gång. (JO:s beslut dnr 4367-2005. JO:s beslut dnr 5365-2005, JO:s beslut dnr 1982-2006 och JO:s beslut dnr 1739-2004)

Om det är uppenbart att en uppgift kommer att sakna betydelse för ärendet behöver den inte dokumenteras. Ett exempel på uppgiftsinhämtning som kan sakna betydelse för ärendet och därför inte behöver dokumenteras är upprepade automatiserade avstämningar av registeruppgifter. En sådan automatisk kontroll kan göras när ett ärende kommer in till Försäkringskassan. Om ärendet sedan faller ut för ett manuellt handläggningssteg och den automatiserade processen därefter återupptas, kan samma kontroll behöva göras på nytt. I den situationen är det främst den information som inhämtas senast som är relevant för ärendet och som behöver sparas. I de fall en kontroll görs flera gånger är det alltså informationen från den kontroll som påverkar resultatet i ärendet som behöver dokumenteras.

De olika typer av uppgifter som kan behöva dokumenteras är

- uppgifter som lämnas av eller hämtas in från den enskilde, en annan person eller en myndighet
- kontroller som görs av systemet i handläggningen
- utfallet av kontrollerna
- ställningstaganden som påverkar ärendets gång
- andra åtgärder som vidtas i ärendet, både manuella handläggningsåtgärder och verkställighetsåtgärder.

Det finns inte några regler om i vilken form som dokumentationen ska göras. Men det ska framgå vem som har dokumenterat och när. Dokumentationen ska också vara begriplig och bestående.

Dokumentationen kan till exempel göras i en elektronisk journalanteckning:

- Inom den automatiserade hanteringen av SGI stämmer systemet av uppgifter i ansökan mot uppgifter hos Skatteverket och dokumenterar vad det har gjort i journalen: ”*Den försäkrade har lämnat uppgift om årsinkomst på XX kronor. Begär in uppgifter från Skatteverket för att kunna kontrollera att den försäkrade haft inkomster sex månader i följd och kunna göra en bedömning av den lämnade årsinkomsten. Period: MÅN ÅÅÅÅ – MÅN ÅÅÅÄ.”*
- Systemet stämmer också av om det, baserat på utredningen i ärendet, kan gå till beslut själv eller om ärendet ska gå till en handläggare för fortsatt utredning. Då gör systemet en bedömning som dokumenteras i journalen: *”Inkomstuppgifterna från Skatteverket för (period) är (summa för respektive månad) kronor. Summan av inkomsterna har räknats om till årsinkomst för att kunna jämföras. (summa/6 x 12 = z kronor). Skillnaden mellan den lämnade årsinkomsten och den omräknade årsinkomsten är för stor för att den försäkrades uppgift ska kunna godtas. Bedömer att ärendet behöver utredas vidare”.*

Även beslut ska dokumenteras. Hos Försäkringskassan fattar vi beslut i huvudsak på två olika sätt: antingen i ett beslutsbrev eller i ärendets journal. Det gäller både beslut som fattas av en handläggare och beslut som fattas automatiserat. I vissa fall sparas informationen om beslut som fattas automatiserat i en digital handling som kan tas fram vid behov. Läs mer om hur vi dokumenterar och motiverar beslut i Försäkringskassans vägledning (2004:7) *Förvaltningsrätt i praktiken*.

Information som är specifik för ett visst ärende behöver finnas i ärendet. Det beror på att ärendet måste kunna stå för sig själv. Informationen måste vara begriplig så att en part

eller exempelvis en extern granskare kan följa och förstå vad som hänt i ärendet. Det måste vara tydligt vilken information som en part har särskild rätt att ta del av med stöd av den partsinsyn som regleras i FL och OSL. Om ärendet överklagas måste det också vara tydligt vilken information som ska skickas till överinstansen. Det är dessutom, i ett längre perspektiv, inte säkert att ärendet kommer att lagras i samma system som det skapades och handlades i. Det innebär att informationen i ärendet måste hänga ihop för att kunna läsas tillsammans och förstås i efterhand, om och när det blir aktuellt. Lagen säger däremot inget om hur detta ska lösas rent tekniskt.

För att uppfylla kraven på dokumentation i ett ärende kan information sparas i löpande journalanteckningar, loggar, eller ett samlingsdokument med information om kontroller och resultat. Detta leder fram till att informationen i ärendet kan dokumenteras på flera sätt och på olika platser eller nivåer, rent tekniskt. Informationen kan lagras dels på ett sätt som är direkt läsbart, till exempel en journal och i handlingar i ärendet, dels i till exempel tabeller som fogas till ärendet. Ett exempel på detta är datastrukturer som beskriver handläggningen i ett ärende; vad systemet har gjort, vilken information som har använts och hur utfallet har blivit i varje steg.

Dokumentation av system

När ärenden handläggs automatiserat finns den information som gör att det går att följa och förstå ärendets gång dokumenterad dels i själva ärendet, dels i den dokumentation som beskriver hur systemet fungerar. Dokumentationen av systemet kan till exempel bestå av programkod, användarhandledningar eller dokument som beskriver de krav som ställts vid programmeringen. Programkoden och annan dokumentation visar på de många val som har gjorts under systemets utveckling och innehåller både rättsliga och praktiska överväganden.

Det finns olika regelverk som styr kraven på dokumentation av våra system. Det handlar om dataskyddsregelverkets regler om rätt till information, kraven i AI-förordningen och om informationssäkerhet samt arkivrättsliga krav. Vi kan också ta ledning av Digitaliseringsrättsutredningens förslag om dokumentation av system, som däremot inte lett till lagstiftning (SOU 2018:25, Juridik som stöd för förvaltningens digitalisering). I dagsläget är det svårt att säga exakt vad sådan dokumentation behöver innehålla. Klart är dock att den behöver vara tillräckligt tydlig för att Försäkringskassan ska kunna lämna klargörande information om hur vi använder algoritmer eller datorprogram vid handläggning av ärenden.

Försäkringskassans system behöver dokumenteras för att elektroniska handlingar och annan digital information ska kunna förstås i framtiden, eftersom dokumentationen beskriver kontexten i vilka de en gång hanterades.

Läs mer

Läs mer om krav på dokumentation av system, och vad sådan dokumentation kan bestå av i Försäkringskassans anvisningar (2023:09) *Gallring och bevarande av verksamhetsinformation*.

6 Digitala tjänster för informationsutbyte

En digital tjänst för informationsutbyte är en tjänst för att utbyta information digitalt med någon utomstående, det vill säga andra myndigheter, individer eller företag.

Det här kapitlet handlar framförallt om tjänster vars primära syfte är att utbyta information. Ett exempel på en sådan tjänst är LEFI Online. Men information utbyts också i andra fall. De flesta digitala tjänster som vi utvecklar i kärnverksamheten innebär nämligen att uppgifter görs tillgängliga för någon utomstående. Det kan handla om att den enskilde kan läsa uppgifter om sig själv eller en annan individ, exempelvis en familjemedlem. Men det kan också handla om att Försäkringskassan utbyter information med en annan myndighet som ett led i handläggningen av ett ärende, för att kontrollera uppgifter. Till exempel en självbetjäningstjänst vars primära syfte är att hantera ansökan om en förmån, innehåller normalt sett en funktion för informationsutbyte. Många delar av detta kapitel är relevanta även för sådana tjänster.

I det här kapitlet redovisas de frågor och de lagrum som är viktigast utifrån reglerna om sekretess och dataskydd när vi utvecklar en digital tjänst för informationsutbyte på Försäkringskassan.

Kapitlet behandlar inte frågor som rör den förvaltningsgemensamma digitala infrastrukturen för informationsutbyte (se närmare om Ena - Sveriges digitala infrastrukturer på digg.se). Kapitlet behandlar inte heller specifika frågor om *informationsdelning/datadelning* och *interoperabilitet*.

- Med informationsdelning/datadelning menas i allmänhet att en organisation gör information tillgänglig för andra att använda.
- Interoperabilitet handlar om två eller flera systems förmåga att utbyta information och att använda informationen som de får från varandra.

Läs mer

Försäkringskassans behov av information för handläggning av ärenden behandlas också i förmånsvägledningarna

Läs mer om loggar och andra säkerhetsaspekter i Försäkringskassans riktlinje (2018:13) *Säkerhetsregler*.

6.1 Överväganden kring sekretess

6.1.1 Sekretessbrytande regler

När vi utvecklar digitala tjänster för informationsutbyte i Försäkringskassans kärnverksamhet handlar det oftast om sekretessreglerade (och ofta sekretessbelagda) uppgifter. Exempelvis uppgifter om enskilda personer.

Socialförsäkringssekretessen förutsätter en bedömning i det enskilda fallet för att avgöra om de uppgifter som träffas av bestämmelsen (som är sekretessreglerade) också omfattas av sekretess (är sekretessbelagda) mot den de ska lämnas ut till. När en digital tjänst för informationsutbyte ska skapas blir det i stället fråga om en slags generell, framåtblickande, sekretessbedömning. Om det finns en risk för att sekretessbelagda uppgifter kommer att röjas i tjänsten behöver vi en bestämmelse som bryter sekretessen. I praktiken finns det i princip alltid en sådan risk. Det betyder att vi i

praktiken behöver ha en sekretessbrytande bestämmelse när *sekretessreglerade* uppgifter ska överföras. Oftast handlar det om en specifikt formulerad uppgiftsskyldighet, som samtidigt är sekretessbrytande enligt 10 kap. 28 § OSL.

Sekretessbrytande bestämmelser som förutsätter bedömningar i det enskilda fallet, exempelvis generalklausulen, är inte en långsiktig eller lämplig lösning i digital tjänst för informationsutbyte. Specifikt formulerade uppgiftsskyldigheter ger däremot stöd för överföring av den kategori av uppgifter som bestämmelsen avser.

Ibland uppstår ett behov av att utbyta information utan att det finns ett tydligt stöd för att lämna ut uppgifterna. Då får vi överväga om behovet motiverar en framställan om författningsändring.

Läs mer
I Försäkringskassans vägledning (2001:3) *Offentlighet, sekretess och behandling av personuppgifter* kan du läsa mer om sekretess. Bland annat om de sekretessbestämmelser som oftast är tillämpliga på Försäkringskassan och om olika sekretessbrytande bestämmelser. Där finns också mer information om den restriktiva tillämpningen av generalklausulen vid rutinmässigt informationsutbyte.

På Fia-sidan Uppgiftsskyldigheter finns en förteckning över bestämmelser som handlar om att Försäkringskassan ska lämna uppgifter till andra myndigheter och aktörer, eller att de ska lämna uppgifter till Försäkringskassan.

6.1.2 Rätten att bryta sekretess för att ställa en fråga

I många fall behöver Försäkringskassan lämna uppgifter för att kunna få uppgifter från någon annan. Vi kan till exempel behöva ange vilken individ vi behöver information om för att en annan myndighet ska kunna lämna uppgifter om den individen till oss. Många uppgiftsskyldigheter handlar exempelvis om att uppgifter ska lämnas ”på begäran”. De förutsätter en fråga för att det ska kunna lämnas ett svar. Tjänster som hanterar sådana typer av informationsutbyten kallas ofta för ”fråga/svar-tjänster”.

I ”fråga/svar-tjänster” behövs stöd för informationsutbytet i båda riktningar. I dessa fall handlar det om en tvåvägskommunikation.

När Försäkringskassan ställer frågor till andra kan den sekretessbrytande regeln i 10 kap. 2 § OSL aktualiseras. Bestämmelsen ska tolkas restriktivt. Effektivitetsskäl räcker inte för att bryta sekretessen. Sekretessen får bara brytas om det är en *nödvändig* förutsättning för att vi som utlämnande myndighet ska kunna fullgöra vår verksamhet. Ett exempel på när det anses nödvändigt är när vi behöver lämna uppgift om personnummer för att ange vilken individ vi behöver uppgifter om, när det finns en uppgiftsskyldighet för en annan myndighet att lämna uppgifter, på begäran, till Försäkringskassan. (Prop. 1979/80:2 s. 465, prop. 2008/09:150 s. 368, SOU 2023:52 s. 397, Ds 2023:15 s. 308, Enqvist, s. 232ff.)

Läs mer
I Försäkringskassans vägledning (2001:3) *Offentlighet, sekretess och behandling av personuppgifter* kan du läsa om i vilka situationer det kan anses nödvändigt att Försäkringskassan bryter sin sekretess och hur restriktiv den regeln är.

6.1.3 Sekretess gäller när mottagaren antas behandla personuppgifter i strid med dataskyddsreglerna

När det handlar om att Försäkringskassan ska lämna ut information i form av personuppgifter till någon annan måste vi bedöma om bestämmelsen i 21 kap. 7 § OSL är tillämplig. Det gäller sekretess för personuppgifterna enligt den bestämmelsen om det kan antas att personuppgifterna efter utlämnandet kommer att behandlas i strid med dataskyddsregelverket. Bestämmelsen tillåter alltså utlämnande om mottagarens behandling lever upp till kraven i dataskyddsregelverket.

Det är inte möjligt med en individuell prövning när det handlar om en digital tjänst för informationsutbyte. En sådan bedömning måste göras generellt, på förhand.

Om mottagaren av Försäkringskassans personuppgifter är en myndighet styrs personuppgiftsbehandlingen vanligtvis av en registerlagstiftning med bestämmelser som bland annat reglerar för vilka ändamål myndigheten får behandla personuppgifter. I dessa fall får vi utgå från att den mottagande myndigheten följer sitt regelverk.

Att Försäkringskassan får behandla personuppgifter i sin kärnverksamhet när de tas emot från någon utomstående framgår av flera bestämmelser i 114 kap. SFB.

Läs mer
I Försäkringskassans vägledning (2001:3) *Offentlighet, sekretess och behandling av personuppgifter* finns en detaljerad beskrivning av hur prövningen enligt 21 kap. 7 § OSL ska gå till.

6.2 Behandling av personuppgifter

6.2.1 Omfattningen av personuppgiftsansvaret

Personuppgiftsansvarig är enligt artikel 4 i dataskyddsförordningen den som bestämmer ändamålen och medlen för behandlingen av personuppgifter. I en digital tjänst för informationsutbyte ansvarar normalt sett varje aktör för sin personuppgiftsbehandling. Vanligtvis kan det utan större problem slås fast vem som är personuppgiftsansvarig för vilka delar. Ibland anlitas en fristående aktör för att distribuera, ta emot, eller på annat sätt hantera informationen. Då kan det bli aktuellt att upprätta ett personuppgiftsbiträdesavtal.

Läs mer
Läs mer om personuppgiftsansvar och personuppgiftsbiträdesavtal i Försäkringskassans vägledning (2001:3) *Offentlighet, sekretess och behandling av personuppgifter* och Försäkringskassans riktlinjer (2019:01) Personuppgiftsbiträdesavtal.

6.2.2 Vi behöver stöd för att behandla personuppgifter i informationsutbytet

När vi utvecklar digitala tjänster för informationsutbyte i Försäkringskassans kärnverksamhet handlar det oftast om personuppgifter, till exempel om försäkrade personer. Vi måste ha stöd för att behandla personuppgifterna i den digitala tjänsten. Det finns bestämmelser om detta i 114 kap. SFB, som är vår registerförfattning. Den

skiljer också på olika former av digitalt utlämnande: genom *direktåtkomst* och andra sätt för digitalt utlämnande.

Digitala tjänster för informationsutbyte handlar ofta om att fullgöra olika bestämmelser om uppgiftslämnande, exempelvis en bestämmelse om uppgiftsskyldighet. I sådana fall får vi behandla personuppgifter som behandlas för de *primära ändamålen* i 114 kap. 8 § SFB för att kunna utbyta information i enlighet med uppgiftsskyldigheten. Det framgår av de *sekundära ändamålen* i 114 kap. 9 § SFB.

Informationsutbytet kan också handla om att Försäkringskassan behöver inhämta uppgifter som bedömts vara nödvändig för handläggningen av ett ärende i kärnverksamheten. Det är en sådant primärt ändamål som vi får behandla personuppgifter för. Oftast handlar det i dessa fall om funktioner för informationsutbyte som är en del av eller knutna till exempelvis en självbetjäningstjänst.

I de regler som gällde före den 15 februari 2024 var det inte helt tydligt om det gick att stödja ett digitalt utlämnande på exempelvis generalklausulen i 10 kap. 27 § OSL eller ett sekretessbrytande samtycke från den enskilde. Försäkringskassans nya registerförfattning öppnar upp för detta i 114 kap. 9 § SFB. Det är dock framförallt aktuellt för enstaka informationsutbyten. Det är inte lämpligt att bygga en digital tjänst för informationsutbyte med stöd av generalklausulen eller ett sekretessbrytande samtycke. Det beror framför allt på att det inte är en långsiktig eller lämplig lösning för att utbyta uppgifter som är sekretessreglerade. Läs mer i avsnitt 6.1.1.

Direktåtkomst är en form av digitalt utlämnande som är särskilt reglerad i 114 kap. SFB. Direktåtkomst är bara tillåtet om det uttryckligen framgår av i lag eller förordning att det är tillåtet (114 kap. 14 § SFB). Det kan exempelvis framgå i förordning (2024:14) om behandling av personuppgifter vid Försäkringskassan och Pensionsmyndigheten.

Begreppet *direktåtkomst* innebär att någon utomstående har direkt tillgång till uppgifter som behandlas hos en myndighet. Den utomstående kan på egen hand ta fram uppgifter och på så sätt få uppgifter utlämnade till sig. Prövningen av om ett utlämnande är förenligt med OSL måste därför göras redan när uppgifterna görs tillgängliga för direktåtkomst. Den faktiska begränsningen av direktåtkomsten görs sedan med hjälp av olika tekniska lösningar.

I många sammanhang används begreppet *medium för automatiserad behandling* för att skilja direktåtkomst från andra slags former för digitalt utlämnande. Båda utlämnandeformerna var tidigare uttryckligt reglerade i 114 kap. SFB. Numera omnämns inte medium för automatiserad behandling. I förarbetena till den nya registerförfattningen talar man i stället om *annat elektroniskt utlämnande än direktåtkomst* (prop. 2023/24:29 s. 83f.). Begreppet täcker en rad olika tekniker och förfaranden att lämna ut uppgifter, till exempel via mejl eller sms, på usb-minne, genom webbtjänster eller filöverföring (Jfr. prop. 2023/24:29 s. 83 med hänvisningar). Utlämnandet kan göras på begäran av mottagaren eller på eget initiativ av den utlämnande myndigheten som förfogar över uppgiften och bestämmer om den ska lämnas ut eller inte.

I vissa fall är det enkelt att avgöra vilket slags digitalt utlämnande det är fråga om, till exempel när det gäller mejl. I andra fall är det mer komplicerat. Den tekniska utvecklingen har inneburit att skillnaden mellan direktåtkomst och andra sätt för utlämnande har blivit hårfin. Det har bidragit till att begreppen uppfattats som oklara, vilket har gett upphov till olika problem vid tillämpningen. Vanligtvis innebär ”fråga/svar-tjänster” annat elektroniskt utlämnande än direktåtkomst (jfr. exempelvis prop. 2023/24:29 s. 83). Man kan dock inte alltid utgå från att det är så, för det beror på hur tjänsten utformas.

Rättsfall

Högsta förvaltningsdomstolen har klargjort hur gränsen ska dras mellan de olika formerna för digitalt utlämnande i det så kallade LEFI Online-målet (HFD 2015 ref. 61). Domstolen fann i det målet att Försäkringskassans tjänst LEFI Online utgör utlämnande på medium för automatiserad behandling. De myndigheter som begär uppgifter via tjänsten kan inte söka information på egen hand, utan ett utlämnande förutsätter att Försäkringskassan reagerar på en begäran. Myndigheterna anses därför inte ha sådan teknisk tillgång till upptagningarna som avses i 2 kap. 6 § första stycket TF, varför förfarandet inte är att betrakta som direktåtkomst enligt bestämmelserna i SFB.

Det finns olika risker kopplade till direktåtkomst. Det bör därför bara användas när det inte finns andra alternativ som kan lösa behovet av informationsförsörjning.

Som huvudregel utformas Försäkringskassan digitala tjänster för informationsutbyte så att det inte rör sig om direktåtkomst. (Prop. 2023/24:29 s. 77f.)

Läs mer

Läs mer om personuppgiftsbehandling i Försäkringskassans vägledning (2001:3) *Offentlighet, sekretess och behandling av personuppgifter*. Där kan du bland annat läsa mer omförutsättningarna för digitala utlämnanden.

I eSam:s vägledning *Elektroniskt informationsutbyte – en vägledning för utlämnande i elektronisk form* (2016) beskrivs utlämnande genom medium för automatiserad behandling och direktåtkomst. Här beskriver eSam vilka förutsättningar som behöver uppfyllas för att informationsutbytet ska anses vara ett utlämnande av automatiserad behandling och inte en direktåtkomst.

I eSam:s vägledning *Digitalisera rätt*, (2019) beskrivs ännu mer utförligt funktioner och moment som är aktuella vid informationsutbyte. Den vägledningen kan i tillämpliga delar användas som stöd eller referens.

Källförteckning

Författningar

EU:s lagar och regler

Fördraget om Europeiska unionen

Fördraget om Europeiska unionens funktionssätt

Europeiska unionens stadga om de grundläggande rättigheterna (2010/C 83/02) (EU:s rättighetsstadga)

Europaparlamentets och rådets förordning (EU) 2018/1724 av den 2 oktober 2018 om inrättande av en gemensam digital ingång för tillhandahållande av information, förfaranden samt hjälp- och problemlösningstjänster och om ändring av förordning direktiv 1024/2012 (SDG-förordningen)

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 (dataskyddsförordningen, GDPR)

Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (eIDAS-förordningen)

Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens)

Förslag till Europaparlamentets och rådets direktiv om anpassning av reglerna om utomobligatoriskt skadeståndsansvar vad gäller artificiell intelligens (direktivet om skadeståndsansvar gällande AI), COM (2022) 496

Internationella regelverk

Förenta nationernas konvention om barnets rättigheter (barnkonventionen)

Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen)

Grundlagar

Regeringsformen

Tryckfrihetsförordningen

Yttrandefrihetsgrundlagen

Lagar

Brottsbalken

Socialförsäkringsbalken

Lagen (2022:126) med kompletterande bestämmelser till EU:s förordning om en gemensam digital ingång

DOS-lagen (2018:1937)

Säkerhetsskyddslagen (2018:585)

Dataskyddslagen (2018:218)

Förvaltningslagen (2017:900)

Offentlighets- och sekretesslagen (2009:400)

Diskrimineringslagen (2008:567)

Lagen (2008:145) om statligt tandvårdsstöd

Arkivlagen (1990:782)

Förordningar

Förordning (2024:14) om behandling av personuppgifter vid Försäkringskassan och Pensionsmyndigheten

Säkerhetsskyddsförordningen (2021:955)

Förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning

Förordningen (2009:1174) med instruktion för Försäkringskassan

Myndighetsförordningen (2007:515)

Arkivförordningen (1991:446)

Föreskrifter

Myndigheten för samhällsskydd och beredskaps föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:07)

Myndigheten för digital förvaltnings föreskrifter om tillgänglighet till digital offentlig service (MDFFS 2019:2)

Socialstyrelsens föreskrifter och allmänna råd om att utfärda intyg i hälso- och sjukvården (HSLF-FS 2018:54)

Försäkringskassans föreskrifter (FKFS 2011:3) om självbetjäningstjänster via Internet

Riksarkivets föreskrifter och allmänna råd (RA-FS 2009:2) om tekniska krav för elektroniska handlingar (upptagningar för automatiserad behandling).

Riksarkivets föreskrifter och allmänna råd (RA-FS 2009:1 med ändringar) om elektroniska handlingar (upptagningar för automatiserad behandling).

Förarbeten

Propositioner

Prop. 2023/24:29 En ny dataskyddsreglering på socialförsäkringsområdet

Prop. 2021/22:40 Ett teknikneutralt krav på underskrift av regeringsbeslut

Prop. 2019/20:113 En mer ändamålsenlig dataskyddsreglering för studiestödsverksamheten

Prop. 2018/19:33 Behandling av personuppgifter samt registrering och användning av fordon på vägtrafikområdet

Prop. 2017/18:299 Genomförande av webbtillgänglighetsdirektivet

Prop. 2017/18:126 Digital hantering av domstolsavgörande, strafföreläggande och ordningsbot

Prop. 2016/17:198 Utökat sekretesskydd i verksamhet för teknisk bearbetning och lagring

Prop. 2016/17:180 En modern och rättssäker förvaltning – ny förvaltningslag

Prop. 2015/16:65 Utlänningsdatalag

Prop. 2014/15:10 Förbättringar av husavdragets fakturamodell

Prop. 2010/11:165 Skatteförfarandet

Prop. 2008/09:150 Offentlighet- och sekretesslag

Prop.1979/80:2 med förslag till sekretesslag m.m.

Statens offentliga utredningar

SOU 2023:61 En säker och tillgänglig statlig e-legitimation

SOU 2023:52 Ett stärkt och samlat skydd av välfärdssystemen

SOU 2021:62 Användning av e-legitimation i tjänsten i den offentliga förvaltningen

SOU 2021:9 Vem kan man lita på? Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen

SOU 2018:25 Juridik som stöd för förvaltningens digitalisering

SOU 2010:29 En ny förvaltningslag

Departementsskrivelser

Ds 2003:29 Formel Formkrav och elektronisk kommunikation

Ds 2023:15 Fler verktyg i socialtjänsternas arbete för att förebygga brott och stärka skyddet för barn

Domar och beslut

Högsta förvaltningsdomstolen

HFD 2022 ref. 34

HFD 2013 ref. 9

RÅ 2010 ref. 37

RÅ 2010 ref. 5

RÅ 2004 ref. 91

RÅ 2002 ref 98

RÅ 2000 ref. 51

Justitieombudsmannen
JO:s beslut dnr 6744-2020

JO:s beslut dnr 5497-2013

JO:s beslut dnr 2367-2011

JO:s beslut dnr 2155-2009

JO:s beslut dnr 1982-2006

JO:s beslut dnr 4367-2005

JO:s beslut dnr 5365-2005,

JO:s beslut dnr 1739-2004

Litteratur

von Essen, Arbete i offentlig förvaltning, 2021, JUNO version 3

Enqvist, En myndighet i samverkan – Försäkringskassans rättsliga förutsättningar att samverka med Arbetsförmedlingen samt hälso- och sjukvården. Akademisk avhandling, Juridiska institutionen vid Umeå universitet 2019

Interna styr- och stöddokument

Vägledning (2004:7) Förvaltningsrätt i praktiken

Vägledning (2004:3) Försäkringskassan och arkivhantering

Vägledning (2001:3) Offentlighet, sekretess och behandling av personuppgifter

Riktlinjer (2024:03) Bedömning av dataskydd - Grundläggande bedömning och konsekvensbedömning

Riktlinjer (2022:01) Gallring och bevarande av verksamhetsinformation

Riktlinjer (2019:01) Personuppgiftsbiträdesavtal

Riktlinjer (2018:13) Säkerhetsregler

Riktlinjer (2011:34) Hantering av skyddade personuppgifter inom Försäkringskassan

Riktlinjer (2008:25) Registervård (rättelse, radering och begränsning enligt EU:s dataskyddsförordning)

Riktlinjer (2008:11) Hantering av information till den registrerade (registerutdrag)

Riktlinjer (2005:14) Att skriva kommuniceringsbrev och beslutsbrev i Försäkringskassan

Anvisningar (2023:09) Gallring och bevarande av verksamhetsinformation

Anvisningar (2022:09) Säkerhet på Försäkringskassan

Anvisningar (2022:03) Informationsklassning

Stödprocess (2020:10) Säkerhetsskydd

Säkerhetspolicy (2003:4)

Övrigt

eSam, Digitaliserbar lagstiftning, ES2023-09

eSam, Designprinciper och krav för eget utrymme, ES 2022-04, 2022

eSam, Checklista Juridik vid användning av AI, ES2022-08, 2022

eSam, Eget utrymme hos en myndighet – en vidareutveckling, 2021

Getting the future right – Artificial intelligense and fundamental rights, Europeiska unionens byrå för grundläggande rättigheter, 2020

eSam, Digitalisera rätt – En praktisk juridisk vägledning, 2019

Europeiska kommissionens expertgrupp på hög nivå för AI-frågor, Etiska riktlinjer för tillförlitlig AI, 2019

eSam, Juridisk vägledning för införande av e-legitimering och e-underskrifter 1.1, 2018

eSam, Rättsliga förutsättningar för digitalt i första hand, 2018

eSam, Juridisk vägledning för verksamhetsutveckling inom e-förvaltning 3.0, 2018

eSam, Rättsligt uttalande om automatiserade beslut, VER 2017:57, 2018-03-19

eSam, Elektroniskt informationsutbyte – en vägledning för utlämnande i elektronisk form, 2016

E-delegationen, Elektroniska original, kopior och avskrifter, 2012-06-07

Hemställan om ändringar i 114 kap. SFB och förordningen (2003:766) om behandling av personuppgifter inom socialförsäkringens administration, Försäkringskassans dnr FK 2020/001747