

05:02

Vägledning för hantering av inkommande elektroniska handlingar





Vägledning för hantering av inkommande elektroniska handlingar

Denna Vägledning för hantering av inkommande elektroniska handlingar (e-nämnden 05:02) har fastställts av e-nämnden den 11 maj 2005. Gustaf Johnssén, kansliansvarig, deltog i den slutliga handläggningen.

Alf Nilsson

/Gustaf Johnssén

Innehåll

| | | |
|----------|----------------------------------------------------------------------------------|-----------|
| 1 | Inledning | 5 |
| 2 | Tillgång till en e-tjänst | 6 |
| 3 | Service via en e-tjänst | 7 |
| 3.1 | En enskild mellanlagrar ett utkast | 7 |
| 3.2 | Myndighetens informationssystem skapar och överför ett utkast | 7 |
| 3.3 | Stöd i serviceskedet för att avhjälpa fel och sända in felfria handlingar | 7 |
| 3.4 | Tydliga användargränssnitt | 7 |
| 4 | Inkommen handling | 9 |
| 4.1 | Regleringen | 9 |
| 4.2 | En tydlig punkt för inkommande | 9 |
| 4.3 | Hjälpregeln | 9 |
| 4.4 | Mottagningsfunktionens placering | 9 |
| 4.5 | Fel adress, anrop eller format | 10 |
| 4.6 | Skydds- eller kontrollåtgärder | 10 |
| 4.7 | Kvittenser och felmeddelanden | 10 |
| 4.8 | Registrera händelser | 10 |
| 5 | Myndighetens hantering av elektronisk legitimering och inkomna handlingar | 11 |
| 5.1 | Tidsstämpling | 11 |
| 5.2 | Myndigheten bör kontrollera e-legitimationer och underskrifter automatiserat | 11 |
| 5.3 | Spärrkontroll | 11 |
| 5.4 | Information som myndigheten behöver vid automatiserade kontroller | 11 |
| 5.5 | Information vid manuella kontroller | 12 |
| 5.6 | Ytterligare kontroller | 12 |
| 5.7 | Samordnade föreskrifter | 12 |
| 5.8 | Åtgärder när ett fel eller en brist föreligger | 12 |
| 5.9 | Manuella åtgärder och bedömningar | 13 |
| 6 | Kommentar | 14 |
| 6.1 | Inledning | 14 |
| 6.2 | Inkommen handling | 15 |
| 6.2.1 | Regleringen | 15 |
| 6.2.2 | Är försändelser med fel elektronisk adress eller format att anse som inkomna? | 16 |
| 6.2.3 | Leder kontroller till att försändelserna anses inkomna? | 17 |
| 6.2.4 | Undantag för kontroller som utgör ett typiskt led i en ärendehandläggning | 18 |
| 6.2.5 | Fördelningen av risken vid befordran av handlingar | 18 |
| 6.3 | Kvittenser och felmeddelanden | 19 |
| 6.4 | Serviceverksamhet | 20 |
| 6.4.1 | Mellanlagring och utkast från myndighet | 20 |
| 6.4.2 | Kontroller under serviceskedet | 21 |
| 6.5 | Tydliga användargränssnitt m.m. | 22 |
| 6.6 | Tillträde till e-tjänster | 22 |

| | | |
|-----|---------------------------------------------------------------------------|----|
| 6.7 | Myndighetens hantering av elektronisk legitimering och inkomna handlingar | 23 |
|-----|---------------------------------------------------------------------------|----|

1 Inledning

Myndigheter lämnar upplysningar och annan service via webbplatser. Där finns också e-tjänster. De används för att skriva och ge in handlingar. En e-tjänst brukar ha funktioner för att

1. begränsa tillträdet till tjänsten (kap. 2),
2. ge service (kap. 3),
3. ta emot handlingar (kap. 4), och
4. kontrollera att inkomna handlingar är äkta (kap. 5).

Det är viktigt att veta när en handling kommer in till en e-tjänst enligt 10 § förvaltningslagen (1986:223; FL). Denna vägledning ger

1. en juridisk grund för den bedömning som varje myndighet får göra utifrån den egna verksamhetens förutsättningar, och
2. underlag för att samordna myndigheternas e-tjänster så att de tillgodoser enskildas behov av rättssäkerhet.

Denna vägledning gäller för e-tjänster som används med e-legitimationer som omfattas av Statskontorets upphandling.¹ Termer och uttryck har samma betydelse här som i den grundläggande vägledningen.

Myndigheter har flera kanaler för att ge in handlingar och flera mottagningsfunktioner, t.ex. för e-tjänster och för e-post. Samma rättssäkerhetsgarantier bör gälla för dem. Riktlinjerna i kap. 4 för inkommen handling och i kap. 5 för myndighetens hantering av inkomna handlingar gäller även för e-post.

Den slutliga bedömningen av när en handling har kommit in enligt 10 § FL görs av domstol. I denna vägledning behandlas inte när en handling är inkommen enligt 2 kap. 6 § tryckfrihetsförordningen (TF) eller andra frågor om allmänna handlingar (jfr dock avsnitt 4.4 och 6.2.5). Här behandlas inte heller frågor om spam eller om e-tjänster där PIN-koder används istället för e-legitimationer. Vägledningen kan dock i många fall ge motsvarande stöd på dessa områden.

¹ Dessa följer e-nämndens *grundläggande vägledning* för myndigheternas användning av e-legitimationer och elektroniska underskrifter samt e-nämndens *vägledning för användargränssnitt* som uppfyller legala krav (e-nämnden 04:02 och 04:03).

2 Tillgång till en e-tjänst

En myndighet kan av sakligt motiverade administrativa skäl eller säkerhets-
skäl begränsa tillgången till en e-tjänst eller tillgången till en funktion för att
skicka in handlingar. Tillgången kan begränsas så att endast den person som
godkänts på förhand av myndigheten eller legitimerat sig elektroniskt kan
använda e-tjänsten eller funktion för att skicka in handlingar; se även kap. 5.
Kommentaren s. 23.

3 Service via en e-tjänst

Den person som använder en e-tjänst får hjälp och stöd på ett sätt som liknar den hjälp som en handläggare ger vid ett personligt besök hos myndigheten. I det skedet – serviceskedet – kan utkast till elektroniska handlingar skapas och förvaras i myndighetens informationssystem utan att utkastet anses ha sänts in för att inleda ett ärende.

3.1 En enskild mellanlagrar ett utkast

När en elektronisk handling förvaras i myndighetens informationssystem som en service, utan att handlingen har sänts in för att inleda ett ärende (mellanlagring), bör meddelandet inte anses inkommet enligt 10 § FL. I dessa fall har handlingen inte nått myndighetens mottagningsfunktion; dvs. den funktion för automatiserad behandling som myndigheten anvisat som mottagningsställe för försändelser av detta slag (jfr kap. 4). Kommentaren s. 20.

3.2 Myndighetens informationssystem skapar och överför ett utkast

När en enskild person ska granska en färdig text i en e-tjänst kan myndighetens informationssystem skapa ett utkast och föra över utkastet till den dator som den enskilde använder. Detta stöd bör bedömas som en automatiserad service. Något ärende inleds inte genom att utkastet tas fram och förs över till den enskildes dator. Kommentaren s. 20.

3.3 Stöd i serviceskedet för att avhjälpa fel och sända in felfria handlingar

En myndighet kan som service innan en enskild sänder in en handling, av sakligt motiverade administrativa skäl eller säkerhetsskäl, använda automatiserade kontroller via en e-tjänst för att

1. ge stöd när handlingen skapas, och
2. undvika att handlingar ges in om det finns brister som upptäcks genom sådana kontroller; jfr dock 4.2 om kontroller efter serviceskedet.

Sådana kontroller bör inte leda till att handlingen anses inkommen enligt 10 § FL. Detta eftersom handlingen inte har nått myndighetens mottagningsfunktion. Om det stöd som en myndighet ger som service för att avhjälpa fel medför att en viss handling inte kan sändas in via e-tjänsten bör det finnas möjlighet för användaren att enkelt kunna kommunicera med myndigheten på annat sätt; jfr 5 § andra stycket FL. Kommentaren s. 21.

3.4 Tydliga användargränssnitt

Redan när en användare börjar använda en e-tjänst bör det framgå hur tjänsten används. Användargränssnittet bör utformas tydligt så att enskilda inte när service ges

1. tror sig ha varit "inne hos" myndigheten och överlämnat en handling till en handläggare eller ha sänt handlingen till myndighetens mottagningsfunktion, och inte heller
2. av misstag skickar in en handling. Kommentaren s. 22.

4 Inkommen handling

En myndighet kan ha flera mottagningsfunktioner, t.ex. en för en e-tjänst och en för e-post. Detta kapitel gäller om inte annat framgår för båda dessa kanaler.

4.1 Regleringen

Reglerna i 10 § FL om inkommande handlingar är tillämpliga även i elektronisk miljö. Men om en annan lag eller en förordning innehåller någon bestämmelse som avviker från förvaltningslagen gäller den bestämmelsen. Kommentaren s. 15.

4.2 En tydlig punkt för inkommande

Huvudregeln för inkommande handlingar bör tolkas så att en elektronisk handling anses ha kommit in när den har nått den funktion för automatiserad behandling som myndigheten har anvisat som mottagningsställe för försändelser av aktuellt slag (mottagningsfunktionen).

Om en handling som har nått myndighetens informationssystem stoppas till följd av kontroller som utgör ett typiskt led i en ärendehandläggning bör det material som stoppas anses ha nått mottagningsfunktionen. Exempel på sådana kontroller är granskning av om en inlaga är äkta eller undertecknad av en behörig person, Kommentaren s. 18. Detsamma bör gälla om en handling har kommit till myndighetens informationssystem, vid en viss tidpunkt som går att fastställa, men satts i karantän eller annars fördröjts som en följd av myndighetens skydds- eller kontrollåtgärder i anknytning till mottagningsfunktionen. Kommentaren s. 18.

4.3 Hjälpregeln

Den hjälpregel som gäller när det kan antas att en handling har anlänt till myndigheten en viss dag bör kunna tillämpas även på en elektronisk handling. En förutsättning är att det kan antas att handlingen nått myndighetens mottagningsfunktion en viss dag och att den kommer en behörig tjänsteman till handa närmast följande arbetsdag, t.ex. genom att vara tillgänglig i det verksamhetssystem som tjänstemannen använder. Kommentaren s. 16.

4.4 Mottagningsfunktionens placering

Den som ger in en elektronisk handling bär risken om försändelsen inte kommer fram till mottagningsfunktionen. Därför bör en myndighet placera sin mottagningsfunktion så att risken för den som ger in en handling begränsas så mycket som möjligt. Detta gäller särskilt för fel eller brister i behandlingarna efter det att en försändelse har lämnat allmänna kommunikationsnät och nått myndighetens informationssystem utan att ha nått fram till en mottagningsfunktion. Kommentaren s. 19.

Frågan om var mottagningsfunktionen placeras och vilka behandlingar som är möjliga innan funktionen nås är viktiga också för frågor om handlings-

offentlighet enligt 2 kap. TF och för bevarande och gallring. Kommentaren s. 19.

4.5 Fel adress, anrop eller format

Om ett meddelande sänds till

1. fel elektronisk adress, eller
2. rätt adress men med fel anrop eller format; t.ex. till rätt server men till en okänd s.k. port eller sida som är stängd av säkerhetsskäl

bör meddelandet inte anses inkommet enligt 10 § FL. Detta bör gälla även när hindret finns i adressatens system. Kommentaren s. 16.

4.6 Skydds- eller kontrollåtgärder

En försändelse bör inte anses ha kommit in enligt 10 § FL om den hindras från att nå en mottagningsfunktion på grund av brandväggar, virusprogram, intrångsdetekteringssystem eller andra skydds- och kontrollåtgärder.

Kommentaren s. 17.

4.7 Kvittenser och felmeddelanden

När det är möjligt med rutinbetonade åtgärder bör myndigheternas system för kvittenser och felmeddelanden utformas så att enskilda personer får meddelande om att en handling har kommit in eller om fel uppkommit under överföringen. Kommentaren s. 19.

4.8 Registrera händelser

Myndigheten bör löpande registrera händelser som kan tyda på fel i myndighetens system för mottagning av elektroniska handlingar. Kommentaren s. 19.

5 Myndighetens hantering av elektronisk legitimering och inkomna handlingar

När elektroniska handlingar kommer in till en myndighet enligt 10 § FL behöver myndigheten vidta åtgärder för att registrera handlingarna och kontrollera att de är äkta. Om en handling försetts med en elektronisk underskrift som stöds av en e-legitimation behövs särskilda åtgärder. Myndigheterna bör samordna åtgärderna så att enskilda personer kan förutse vilka risker de löper, t.ex. i anknytning till utgången av en frist. Detta gäller även för e-post.

5.1 Tidsstämpling

En myndighet bör så snart en elektronisk handling nått myndighetens mottagningsfunktion logga inkommandet och förse handlingen med uppgift om när handlingen kom in till myndigheten enligt 10 § FL. Kommentaren s. 19.

5.2 Myndigheten bör kontrollera e-legitimationer och underskrifter automatiserat

Myndigheten bör genom automatiserade behandlingar kontrollera att

1. den elektroniska legitimeringen för tillträde eller för uppgiftslämnande kan kopplas till angiven e-legitimation,
2. underskriften eller stämpeln kan kopplas till angiven e-legitimation,
3. att underskriven eller stämplad text inte har ändrats,
4. att den som utfärdat e-legitimationen uppfyller de säkerhetskrav som den förlitande parten ställer, och

att den e-legitimation som använts är giltig och lämplig för det aktuella användningsområdet. Kommentaren s. 23

5.3 Spärrkontroll

Myndigheten bör kontrollera att en e-legitimation som stöder en legitimering, en underskrift eller en stämpel inte har spärrats. Sådana kontroller sker genom en automatiserad

1. spärrkontrollfråga till en ID-tjänst, eller
2. kontroll mot spärrlistor. Kommentaren s. 23.

5.4 Information som myndigheten behöver vid automatiserade kontroller

Tillhandahållare av ID-tjänster som utfärdar e-legitimationer bör göra följande information tillgänglig för att anslutna myndigheter ska kunna utföra automatiserade kontroller enligt 5.2 och 5.3;

1. utfärdarens e-legitimation för att underteckna eller stämpla
 - a. personliga e-legitimationer, tjänstelegitimationer, webbserverlegitimationer eller e-legitimationer för myndighetens elektroniska stämpel,

- b. spärllistor m.m., t.ex. svar på frågor om spärr till en ID-tjänst,
2. användarens e-legitimation för legitimering eller underskrift vid kommunikation med en myndighet (om e-legitimationen inte har bifogats en försändelse till myndigheten eller om en bifogad e-legitimation har förkommit eller skadats) och uppgift om eventuell spärr av e-legitimationen och tidpunkten för spärr. Kommentaren s. 23.

5.5 Information vid manuella kontroller

Om automatiserade kontroller enligt 5.2 eller 5.3 av inkomna handlingar inte fungerar eller visar att fel föreligger bör manuella kontroller utföras. Kommentaren s. 23.

Vid manuella kontroller bör uppgifterna presenteras för en handläggare i direkt läsbar form på ett överskådligt och tydligt sätt. Det bör framgå om

1. e-legitimationen är spärrad och när den spärrades,
2. e-legitimationens giltighetstid har gått ut och i så fall när,
3. utfärdaren av e-legitimationen inte är känd av myndigheten,
4. legitimationen inte hör till de legitimationer från en viss utfärdare som myndigheten godtar vid sina automatiserade kontroller,
5. en tjänst för giltighetskontroll inte är tillgänglig,
6. e-legitimationen används för fel ändamål, t.ex. om underskrift har skett med en privat nyckel för legitimering, och om innehållet i den undertecknade handlingen har ändrats. Kommentaren s. 23.

5.6 Ytterligare kontroller

När det finns skäl för ytterligare kontroller, t.ex. om tekniska fel uppkommit eller om en handling eller e-legitimations äkthet ifrågasätts, bör myndigheten se till att den har rätt att från utfärdaren få de handlingar och uppgifter som behövs för sakens prövning. Kommentaren s. 23.

5.7 Samordnade föreskrifter

Myndigheter bör se till att med sina föreskrifter samordna de avtal som sluts med utfärdare som tillhandahåller ID-tjänster. Kompletterande handlingar och uppgifter ska få lämnas ut när de behövs för en säker identifiering eller kontroll av en underskrift.

Föreskrifter och avtal bör för andra fall begränsa utlämnande och användning så att otillbörligt intrång i den enskildes personliga integritet inte uppkommer. Kommentaren s. 23.

5.8 Åtgärder när ett fel eller en brist föreligger

Visar en kontroll av en elektronisk underskrift enligt 5.2 – 5.3 eller 5.5 att en handling har en brist bör myndigheten genom en handläggare göra en manuell bedömning av om

1. handlingen till följd av andra kontrollåtgärder t.ex. efter samtal med angiven utställare eller bekräftelse på elektronisk väg, kan godtas som äkta,
2. ett föreläggande bör utfärdas om bekräftelse genom en egenhändigt undertecknad handling eller på annat alternativt sätt,
3. handlingen inte föranleder någon ytterligare åtgärd av myndigheten till följd av att den är gravt ofullständig eller oläsbar eller en avsändare som kommunikation kan ske med inte anges, eller
4. förutsättningar föreligger för att gallra handlingen.

Detsamma bör gälla vid legitimering för uppgiftslämnande. Kommentaren s. 23.

5.9 Manuella åtgärder och bedömningar

Manuella åtgärder och bedömningar som innefattar ärendehandläggning får normalt inte utföras av annan än den myndighet till vilken en handling har inkommit. Kommentaren s. 24.

6 Kommentar

6.1 Inledning

När en myndighet lämnar upplysningar, vägledning, råd och annan service via en e-tjänst och användare kan upprätta och sända in elektroniska handlingar via samma kanal² ställs myndigheten inför nya juridiska och administrativa frågor. För att lösa dessa behövs tydliga gränser mellan vad som utgör

- *serviceverksamhet*, där enskilda
 - ges hjälp och stöd med att fylla i handlingar m.m., på motsvarande sätt som vid ett personligt besök hos en myndighet, och
 - av tekniska skäl³ eller för mellanlagring⁴ får utkast till handlingar förvarade i myndighetens informationssystem⁵, utan att handlingarna ges in,
- *ingivande*, när en enskild med stöd av e-tjänsten sänder en elektronisk handling till myndighetens mottagningsfunktion (den funktion för automatiserad behandling som myndigheten har anvisat som mottagningsställe) och
- *ärendehandläggning*, när en myndighet vidtar åtgärder med handlingar som har nått mottagningsfunktionen eller annars är att anse som inkomna i förvaltningsrättslig mening.

Myndigheternas elektroniska serviceverksamhet kan beskrivas så att användare loggar in i ett elektroniskt ”besöksrum” där myndighetens personal har ersatts med automatiserat stöd. I nästa steg, när en användare är färdig och vill ge in en handling, lägger han eller hon försändelsen på en elektronisk motsvarighet till Postens brevlåda, för befordran på avsändarens risk till myndighetens elektroniska ”brevinkast”.

De rättsliga bedömningarna av dessa tjänster behöver samordnas så att enskildas behov av rättssäkerhet tillgodoses på ett enhetligt sätt. Som exempel kan nämnas att myndigheternas rutiner för att kontrollera om en undertecknad elektronisk handling är äkta behöver samordnas.

I e-nämndens vägledning för service och hantering av inkommande handlingar, m.m. (”Vägledningen”) sorteras dessa frågor utifrån de stadier

² Med kanal menas den elektroniska kommunikationsväg som används, t.ex. via en viss webbplats.

³ Jfr en handling som förvaras hos myndighet endast som ett led i teknisk bearbetning eller teknisk lagring för annans räkning (2 kap. 10 § TF).

⁴ Med mellanlagring menas att meddelandet förvaras i myndighetens informationssystem som en serviceåtgärd, utan att handlingen sänts in för att anhängiggöra ett ärende.

⁵ Med informationssystem menas här organisationens hela IT-miljö, även de delar som ligger utanför e-tjänster och mottagningsfunktioner.

Hit hör också organisationens externa IT-miljö avgränsad vid en router ansluten till Internet.

som en e-tjänst och anknytande elektroniska rutiner kan användas. Dessa är (1) tillträde, (2) upprättande av handlingar, (3) ingivning och (4) myndighetens kontroller av inkomna handlingar. Denna kommentar ("Kommentaren") tar i stället sin utgångspunkt i vissa centrala rättsfrågor som e-tjänsterna aktualiserar. Den som direkt vill nå kommentarer till vissa delar kan nå dem via länkar i Vägledningen.

6.2 Inkommen handling

6.2.1 Regleringen

Bestämmelserna om inkommande handlingar i 10 § FL, 44 § förvaltningsprocesslagen (1971:291) och 33 kap. 3 § rättegångsbalken är i sak samordnade. Dessa regler är normalt tillämpliga även i elektronisk miljö (4.1).⁶ Om det beträffande en förvaltningsmyndighets handläggning av förvaltningsärenden finns avvikande regler i en annan lag än förvaltningslagen eller i en förordning gäller dock den bestämmelsen.⁷

I de olika led som en e-tjänst kan användas återkommer frågan om och i så fall när en handling ska anses inkommen i förvaltningsrättslig mening. Av hänsyn till arbetets behöriga gång behöver berörda regler kunna tolkas enkelt och snabbt, oberoende av i vilken form och via vilken kanal som en handling når en myndighet. Förutsättningarna för dessa bedömningar skapas till stor del genom standardisering och allmänt vedertagna systemkonstruktioner. I myndigheternas arbete med mottagningsfunktioner för e-tjänster behöver IT-systemens och infrastrukturens funktionssätt utformas på ett sätt som harmonierar med gällande rätt.

Huvudregeln, att en handling anses komma in den dag då den anländer till myndigheten, bör i elektronisk miljö tolkas så att en elektronisk handling har kommit in när den nått den funktion för automatiserad behandling som myndigheten har anvisat som mottagningsställe; en s.k. *mottagningsfunktion* (4.2 första stycket). Denna tolkning bör gälla oavsett om en försändelse når en myndighet via en e-tjänst, e-post eller någon annan elektronisk "kanal" där försändelsen kan tas emot. I praktiken bör därmed, i de allra flesta fall, den punkt där en elektronisk handling anses ha anlåtit till en myndighet kunna knytas till den punkt där teknisk registrering sker i den mottagningsfunktion som utgör myndighetens "brevlåda" för att ta emot sådana meddelanden; jfr nedan om kontroller av underskrifter.

Visserligen kan en e-tjänst vara utformad så att den elektroniska adressen till mottagningsfunktionen är dold för användaren, som endast ser ett grafiskt element i form av en knapp för att skicka in handlingen. Detta hindrar emellertid inte en tillämpning av den förordade huvudregeln för inkommande. Ett uttalande i den förvaltningsrättsliga doktrinen⁸ att ett

⁶ Se prop. 1985/86:80 s. 57 och Ds 2003:29 s. 35 f.

⁷ Se 3 § FL, 2 kap. 5 § tullagen (2000:1281) och 4 § lagen (2004:115) om självbetjäningstjänster via Internet inom socialförsäkringens administration.

⁸ Hellners/Malmqvist, Förvaltningslagen med kommentarer, 2003, s. 113 och 122.

elektroniskt meddelande kommer in först när någon behörig företrädare för myndigheten tar hand om det, t.ex. genom att ta del av meddelandets innehåll på en bildskärm eller göra en utskrift, torde ha sin grund i ett missförstånd. I nu aktuella e-tjänster sker handläggningen helt automatiserat och helt elektroniskt, så att det normalt inte är någon människa som läser eller skriver ut materialet. Myndigheten kan knappast påbörja handläggningen av ett ärende om handlingen inte har kommit in.

Den *hjälpregel* som gäller för det fall att det kan antas att en handling har anlänt till en myndighet viss dag bör också kunna tillämpas, om handlingen kan antas ha nått myndighetens mottagningsfunktion en viss dag och kommit en behörig tjänsteman till handa närmast följande arbetsdag. De system som används av myndigheter som tillhandahåller e-tjänster är utformade så att meddelanden som kommit till mottagningsfunktionen görs tillgängliga i ett verksamhetssystem som handläggare har tillgång till, på motsvarande sätt som när pappershandlingar läggs i handläggares aktskåp eller på deras skrivbord (4.3).

Om en handling når en myndighet via en annan kanal, som inte har anvisats som myndighetens mottagningsfunktion för e-tjänsten och inte heller som mottagningsfunktion för andra försändelser till myndigheten, bör handlingen anses inkommen när den kommit en behörig tjänsteman till handa. Detta har inte angetts i Vägledningen eftersom kommunikationen då sker utanför e-tjänsten.

Frågan om när en handling är att anse som inkommen enligt reglerna om offentlighetsinsyn får inte blandas samman med frågan om inkommande enligt förfaranderegler i förvaltningslagen, förvaltningsprocesslagen och rättegångsbalken.

6.2.2 Är försändelser med fel elektronisk adress eller format att anse som inkomna?

Om en avsändare, som använder en mottagningsfunktion som inte är knuten till en e-tjänst, använder fel anrop bör detta meddelande inte anses inkommet i förvaltningsrättslig mening (4.5). Som exempel kan nämnas om en användare sänder en handling till den server som myndigheten använder som mottagningsfunktion men till en okänd s.k. port eller sida, som dessutom kan vara ”stängd” av t.ex. säkerhetsskäl, så att meddelandet ”studsar”.

Detta kan jämföras med att fel adress anges på ett vanligt kuvert så att en försändelse antingen kommer fel (och därför inte kommer in) eller kommer rätt men uppfattas som feladresserat (och därför skickas vidare eller lämnas obehandlat).⁹ Myndigheternas system för kvittenser och felmeddelanden m.m. bör som framgått utformas så att den enskilde får besked om misstag av detta slag. En handling bör inte anses vara inkommen bara för att en teknisk kontroll skett som lett till ett felmeddelande.

⁹ Jfr rättspraxis för vanliga försändelser där det krävs, för att en försändelse ska anses ha kommit in, att adressaten är så tydligt angiven att försändelsen kan uppfattas vara ställd till denne (RH 1996:45; jfr dock RH 1991:3).

Skulle ett meddelande ha fel format bör detta på motsvarande sätt kunna jämföras med att i pappersmiljö försöka stoppa en alldeles för stor försändelse i en myndighets brevkast och – när åtgärden misslyckas – ställa försändelsen utanför dörren så att den kommer bort innan någon hos myndigheten hunnit ta hand om den. Ett meddelande som inte följer vedertagna standarder, som myndigheten använder för att ta emot via den aktuella kanalen, bör alltså inte anses inkommet om bostämnerna för med sig att systemet inte kan ta emot meddelandet. Även här bör systemen, så långt det är praktiskt möjligt, utformas så att en enskild får besked om fel av detta slag.

I praktiken är de tekniska systemen emellertid utformade så att felmeddelanden ofta inte kan lämnas. På motsvarande sätt som myndigheten inte har vetskap om en försändelse som ställts utanför myndighetens dörr men kommer bort, saknar myndigheten vetskap om elektroniska försändelser som faller ur de sedvanliga funktionerna för kommunikation. Rutinerna bygger såväl i pappersmiljö som i elektronisk miljö på att det är avsändaren som står risken för att meddelanden, under befordran till mottagningsfunktionen, försenas eller inte kommer fram.

6.2.3 Leder kontroller till att försändelserna anses inkomna?

Många uppfattar det så att det skulle finnas en förutbestämd väg från avsändaren till mottagaren, t.ex. via ett externt system, till en router där mottagande myndighets nät tar vid, genom en brandvägg för vidare transport via viruskontroller m.m. till mottagningsfunktionen och därifrån till myndighetens verksamhetssystem. Denna tanke utifrån en sådan förutbestämd väg stämmer dock ofta inte. Den tekniska verkligheten är mera komplicerad. Informationssystemen kan struktureras och fördelas på olika sätt, så att vissa funktioner – t.ex. viruskontrollen – flyttas till den dator där det för tillfället finns ledig kapacitet. En grundregel där endast hela filer eller en viss server pekas ut för att en handling ska anses inkommen kan därmed vara svåra att förena med den tekniska verkligheten. De meddelanden som skapas i e-tjänsten och sänds iväg kan dessutom brytas ned till olika typer av paket och distribueras olika vägar men ändå nå adressaten och komma in, packas upp och sätts samman hos adressaten.

Åtgärder som en myndighet vidtar endast för att skydda sig mot datavirus, intrång i informationssystem eller liknande bör inte anses leda till att en handling kommit in redan till följd av kontrollerna. En annan sak är att t.ex. viruskontroller kan ske både före och efter det att ett meddelande nått mottagningsfunktionen, dvs. både på icke inkomna och inkomna handlingar. Låter en myndighet ”intelligenta” brandväggar, t.ex. s.k. intrångsdetekteringsystem ”öppna” meddelanden av systemsäkerhetsskäl, bör meddelandet inte anses inkommet redan till följd av denna åtgärd (4.6). Detta bör gälla även om åtgärden sker i den dator där myndighetens mottagningsfunktion körs, om meddelandet stoppas eller behandlingarna faller på annat sätt, innan handlingen registreras i mottagningsfunktionen. Meddelanden som t.ex. har felaktigt format eller innehåller ett virus och

därför ”fastnar” eller ”rensas bort” genom de automatiserade skydds- eller kontrollåtgärderna ska därför inte ses som inkomna, även om de faktiskt har lagrats i myndighetens system, t.ex. i en logg över intrång eller en ”karantän” för virusinfekterade meddelanden. Detta synsätt kan jämföras med vissa typer av kontroller av vanlig post som sker innan en försändelse når fram – t.ex. ett s.k. hundsök för att finna narkotika, sprängämnen eller andra skadliga eller otillåtna ämnen i brev och paket. Om en brevbomb sprängs av säkerhetsskäl under transporten, så att en inlaga förstörs, kommer inlagan inte in till myndigheten. Detsamma bör gälla för virusmittade elektroniska försändelser som stoppas eller raderas. I den mån det kan ske med rutinbetonade åtgärder bör enskildas rättssäkerhet dock tillgodoses och myndighetens serviceskyldighet uppfyllas genom tydliga felmeddelanden och uteblivna kvittenser; se vidare nedan under rubriken ”Kvittenser och felmeddelanden”.

Undantag bör dock göras för vissa fall där myndigheten har fått problem med sitt informationssystem och därför stoppat eller fördröjt försändelser vid en viss tidpunkt som går att fastställa som en följd av tillfälliga skydds- eller kontrollåtgärder i anknytning till mottagningsfunktionen – t.ex. vid en krissituation. Finns handlingen kvar och når fram på vanligt sätt efter att myndigheten hävt sina kontroll- eller skyddsåtgärder bör handlingen anses inkommen redan när den kom till myndighetens informationssystem och sattes i karantän, om det går att fastställa denna tidpunkt (4.2 andra stycket andra meningen).

Syftet med detta är att felfria meddelanden som avsänts på ändamålsenligt sätt och nått myndighetens informationssystem inte ska anses ha kommit in för sent till följd av t.ex. en virusattack eller brister i myndighetens informationssystem. Motsatt synsätt skulle kunna leda till rättsförluster för den enskilde, trots att myndigheten i många fall med enkla medel kan kontrollera när meddelandet fördröjdes i myndighetens system – t.ex. genom kontroll av loggar eller liknande.

6.2.4 Undantag för kontroller som utgör ett typiskt led i en ärendehandläggning

Undantag bör dock göras för kontroller som utgör ett typiskt led i en ärendehandläggning, t.ex. en granskning av om en inlaga är äkta eller behörigen undertecknad eller om de uppgifter som lämnats uppfyller lagens krav för att bifalla framställningen. Sådana åtgärder bör anses ske på material som har nått mottagningsfunktionen (4.2 andra stycket första meningen).

6.2.5 Fördelningen av risken vid befordran av handlingar

Vid en ytlig granskning av förordade synsätt kan riskfördelningen uppfattas som alltför förmånlig för myndigheten eftersom den enskilde står risken till dess handlingen når myndighetens mottagningsfunktion; dvs. även för viss del av den befordran som sker i myndighetens system. Skälen för denna fördelning har dock framgått. Myndigheterna bör emellertid, för att begränsa den enskildes risk för rättsförluster, ge varje mottagningsfunktion en sådan plats och utformning i mottagande myndighets informationssystem

att hans eller hennes risk begränsas, om fel skulle uppkomma efter det att en försändelse har lämnat allmänna kommunikationsnät och nått myndighetens informationssystem, men inte nått ända fram till myndighetens mottagningsfunktion (4.4).

I detta sammanhang behöver också reglerna i 2 kap. TF om allmänna handlingars offentlighet uppmärksammas. Myndigheter bör inte utforma sina system så att upptagningar i ett serviceskede, innan de nått myndighetens mottagningsfunktion, blir tillgänglig med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att de kan läsas, avlyssnas eller på annat sätt uppfattas. En sådan avgränsning är en förutsättning för att kunna upprätthålla en god offentlighetsstruktur på området. Myndigheterna bör vidare utforma sina system så att det integritetsskydd och skydd för företagsuppgifter m.m. som ingivare med fog kan förvänta sig inte sätts åt sidan. Dessa komplexa frågor får behandlas närmare i annan ordning (4.4).

6.3 Kvittenser och felmeddelanden

Elektroniska handlingar kan inte läsas utan tekniska hjälpmedel. Därför bör en teknisk registrering göras så snart en handling har nått myndighetens mottagningsfunktion, så att myndighetens handläggare kan se om en handling har kommit in (5.1). Sådan *tidsstämpling* för att stödja en förvaltningsrättslig bedömning av inkommandefrågan får inte förväxlas med registrering av allmänna handlingar enligt 15 kap. 1 § sekretesslagen (1980:100), där det dessutom för flera fall föreskrivs att registrering får underlåtas. Med tidsstämplig menas här att förse handlingen med uppgift om när handlingen kom in till myndigheten (jfr att detta begrepp i standardiseringssammanhang kan ha en närmare teknisk innebörd). För användarna är det på motsvarande sätt viktigt att få veta att en handling nått mottagningsfunktionen. Genom kvittenser på mottagna dokument och felmeddelanden kan risken begränsas för att enskilda drabbas av rättsförluster. Myndigheterna bör därmed utforma varje e-tjänst och mottagningsfunktion så att en enskild – om det kan ske med rutinbetonade åtgärder – får besked när det uppstått ett fel vid överföringen av en handling (4.7). I den mån besked kan lämnas bör användarna också informeras om vilka brister som finns i en handling som inte nått fram, så att avsändaren kan rätta och sända in en ny handling.¹⁰

Myndigheterna bör dessutom löpande registrera händelser som kan tyda på fel i system för mottagning av elektroniska handlingar (4.8). Detta underlag är viktigt för att myndigheten ska kunna ge information till enskilda om vad som kan ha hänt med handlingar som inte nått mottagningsfunktionen och för att fel och brister snabbt ska bli åtgärdade.

¹⁰ Jfr 10 § lagen (2002:562) om elektronisk handel och andra informationssamhällets tjänster.

6.4 Serviceverksamhet

6.4.1 Mellanlagring och utkast från myndighet

De e-tjänster som myndigheter tillhandahåller består till stor del av sådan service som avses i 4 § FL, t.ex. när information ges på en myndighets webbplats. Servicen kan här bestå i hjälp via t.ex. en webbplats för att fylla i och kontrollera uppgifter elektroniskt.¹¹ Serviceverksamheten kan resultera i färdiga elektroniska handlingar som användaren ger in till myndighetens mottagningsfunktion för att anhängiggöra ett ärende. Elektronisk service kan också innebära att en användare innan ingivning sker sänder utkast eller delar av utkast till myndighetens informationssystem för mellanlagring, antingen tillfälligt i ett arbetsminne (så sker t.ex. när en deklaration skapas via Skatteverkets e-tjänst) eller för längre tid t.ex. på en hårddisk i myndighetens system (t.ex. vid upprättande av registreringshandlingar via Bolagsverkets e-tjänst).

Vid bedömningen av om en handling ska anses inkommen enligt förvaltningslagen eller om endast serviceverksamhet ska anses föreligga bör det beaktas om användaren har sänt uppgifter till myndighetens mottagningsfunktion i avsikt att ge in en handling eller om användaren endast avsett att mellanlagra uppgifter eller kontrollera dem maskinellt. På grund av materialets omfattning kan det vara så att den enskilde laddar ned endast delar av detta till sin dator för att granska och ändra, när det behövs. Hela detta förfarande påminner om ett besök i myndighetens lokaler, där användaren förses med blanketter och får hjälp av en handläggare med att fylla i och kontrollera dem men inte ger in något till myndigheten. I pappersmiljö leder sådana åtgärder inte till att en handling anses ingiven; den granskas bara över disk, utan att tas emot. Att en enskild mellanlagrar ett utkast i myndighetens informationssystem bör inte anses leda till att handlingen kommer in i förvaltningsrättslig mening eftersom den inte når myndighetens mottagningsfunktion (3.1). En jämförbar situation i fysisk miljö skulle kunna vara om en enskild som besöker myndigheten inte hinner färdigställa sina inlagor och får löfte att lämna kvar sina papper till nästa dag, när den enskilde återkommer och fortsätter sitt arbete. Den omständigheten att väskan med handlingarna förvaras i myndighetens lokaler medför inte att handlingarna anses inkomna i förvaltningsrättslig mening. Först senare vidtar användaren åtgärder för att ge in handlingarna så att de kommer in i förvaltningsrättslig mening.

På motsvarande sätt bör en myndighets åtgärd, att i en e-tjänst skapa och överföra ett utkast till den enskildes dator för t.ex. elektronisk underskrift, bedömas som ren service där inget ärende anhängiggörs; jfr att en tjänsteman vid ett personligt besök av en enskild hjälper denne att fylla i en blankett som han eller hon tar med sig från myndighetens lokaler (3.2). Först i ett senare led vidtar användaren en åtgärd i avsikt att ge in en

¹¹ Se bestämmelserna i 4 och 5 §§ FL om serviceskyldighet i myndigheters förvaltningsverksamhet, 15 kap. 4 och 10-12 §§ sekretesslagen om upplysningar som myndigheter ska lämna till enskilda och 13 § förordningen (2003:234) om tiden för tillhandahållande av domar och beslut, m.m.

handling. Detta gäller även för e-tjänster där handlingen sänds genom ett kommando för elektronisk underskrift.

Förordade tolkningar av reglerna i förvaltningslagen, förvaltningsprocesslagen och rättegångsbalken, enligt vilka en handling anses inkommen först när den når myndighetens mottagningsfunktion, ger därmed även en naturlig avgränsning mot ren service för att stödja användare när de upprättar handlingar. Enligt gällande rätt torde en handling som en person bär med sig och visar för en handläggare för att få råd om hur den ska fyllas i inte anses inkommen redan till följd av att den finns i myndighetens lokaler. Detta anses gälla även om omfattande hjälp ges så att en handläggare, som en serviceåtgärd, gör ingående kontroller av om kraven är uppfyllda för att en handling ska kunna läggas till grund för ett beslut. På motsvarande sätt bör elektronisk kommunikation kunna äga rum till (och från) en e-tjänst, inom ramen för myndighetens serviceverksamhet, utan att något ärende anses bli anhängiggjort. Den interaktiva processen via en e-tjänst kan göras mycket lik det stöd som ges vid ett personligt besök hos myndigheten.

6.4.2 Kontroller under serviceskedet

Inom ramen för den service som ges via en e-tjänst bör en myndighet, av sakligt motiverade administrativa skäl, få införa automatiserade kontroller, innan en handling sänds in, så att användaren får stöd när handlingen upprättas och att myndigheten inte får in handlingar om det finns brister som kan upptäckas genom automatiserade kontroller (3.3). Som exempel på sådana kontroller kan nämnas att en uppgift finns i ett visst fält, att uppgiften har rätt format, exempelvis består av siffror eller bokstäver och att en angiven uppgift har ett korrekt samband med en uppgift i ett annat fält, exempelvis postnummer och postort. Även mera långtgående kontroller kan emellertid komma i fråga, motsvarande en sådan granskning som skulle kunna ha gjorts av en handläggare om användaren personligen hade besökt myndigheten och en handläggare hjälpt till med en granskning utan att handlingen getts in så att något ärende anhängiggjorts.

Med sakligt motiverade administrativa skäl (för att införa kontroller innan en handling sänds in) menas begränsningar med hänvisning till arbetets behöriga gång, resursernas omfattning eller andra organisatoriska skäl, t.ex. vilka möjligheter det finns att fortsätta handläggningen elektroniskt om underlaget behöver kompletteras. Sådana kontroller bör inte medföra att handlingen anses inkommen enligt 10 § FL eftersom handlingen inte har nått myndighetens mottagningsfunktion. Detta synsätt bör även gälla för kontroller av underskrifter inom ramen för service i en e-tjänst; jfr att en handläggare vid ett personligt besök tittar igenom en handling och granskar att den är korrekt undertecknad – t.ex. granskar att undertecknaren är behörig – och sedan lämnar tillbaka handlingen till besökaren som tar den med sig från myndigheten.

En särskild fråga är om en myndighet får bygga in tvingande kontroller i en e-tjänst så att dessa kontroller måste ha utfallit positivt för att användaren ska kunna sända in handlingen via den kanalen; jfr 3.2 andra stycket. I praktiken kan en sådan utformning av e-tjänster, med långtgående

ingivningshinder, leda till att uppgiftslämnandet kontrolleras med avseende även på det materiella innehållet, exempelvis om näringsförbud föreligger så att ansökan inte kan bifallas eller om uppgifter i något annat register som myndigheten har åtkomst till visar att hinder mot bifall kan föreligga. Den som upprättar inlagan kanske inte ens känner till att myndigheten har åtkomst till dessa uppgifter och skulle – vid en sådan utformning av systemet – i praktiken sakna möjlighet att inom ramen för en (elektronisk) ärendehandläggning invända mot eventuella brister i registret; jfr 29 § personuppgiftslagen (1998:204). Enda möjligheten för användaren blir att välja en annan kanal för att kommunicera med myndigheten, t.ex. e-post.

I 4 § FL regleras myndigheternas skyldighet att ge service i form av upplysningar, vägledning, råd och annan sådan hjälp, här service i e-tjänstens funktion för att upprätta inlagor. I denna servicefas kan en myndighet, så som i fysisk miljö, ge ett långtgående stöd utan att någon handling anses inkommen. Nu är frågan i stället på vilka sätt och i vilken omfattning en myndighet som tillhandahåller en e-tjänst måste vara tillgänglig för allmänheten genom att göra det möjligt att sända det material som tas fram till e-tjänstens mottagningsfunktion. Denna fråga regleras i 5 § andra stycket FL så att myndigheterna ska se till att det är möjligt för enskilda att kontakta dem med hjälp av telefax och elektronisk post och att svar kan lämnas på samma sätt. I lagmotiven, som skrevs efter det att flera e-tjänster som stöds av ID-tjänster tagits i drift, förklarade regeringen att andra metoder än e-post och fax inte kan anses vara så etablerade att det finns anledning att föra in dem i förvaltningslagens serviceregler.

Det finns alltså inte några författningsregler som innebär en skyldighet för en myndighet att ta emot meddelanden via e-tjänstens mottagningsfunktion. Eftersom en myndighet som tillhandahåller en e-tjänst för att upprätta och ge in inlagor går utöver den miniminivå som gäller för serviceskyldigheten enligt 5 § andra stycket FL bör begränsningar kunna göras i e-tjänstens funktioner för att ge in handlingar. Detta förutsatt att miniminivån enligt 5 § FL upprätthålls, t.ex. genom att den enskilde – när hinder uppstår i e-tjänsten – kan kommunicera via e-post.

6.5 Tydliga användargränssnitt m.m.

De tolkningar av gällande rätt som ligger till grund för Vägledningen förutsätter att e-tjänsterna utformas så att användaren kan se och förstå när det är fråga om service och inte ges skäl att tro att en handling sänts till myndighetens mottagningsfunktion när så inte är fallet eller ges skäl att tro sig redan ”vara inne” hos myndigheten och ”ge in” en handling. Därför måste användargränssnitten vara tydliga (3.4). Det bör redan när en användare börjar bruka en e-tjänst framgå hur tjänsten används (e nämnden 04:03). Dessa frågor om begriplighet och användbarhet blir ofta avgörande även för den juridiska bedömningen av enskildas agerande via e-tjänster.

6.6 Tillträde till e-tjänster

Av sakligt motiverade administrativa skäl eller säkerhetsskäl bör en myndighet kunna begränsa tillträdet till en e-tjänst eller en mottagningsfunktion så att endast den som har godkänts av myndigheten på förhand eller legiti-

merat sig elektroniskt ges tillträde till tjänsten (avsnitt 2). Detta får inte leda till någon inskränkning i allmänhetens rätt till anonymitet vid en begäran om att få ut en allmän handling (2 kap. 14 § tryckfrihetsförordningen). Inte heller får det hindra enskildas möjlighet att kontakta myndigheten med hjälp av telefax eller elektronisk post (5 § andra stycket FL). Med sakligt motiverade administrativa skäl enligt 2 (för att begränsa åtkomsten till en e-tjänst eller en funktion för att skicka in handlingar) menas begränsningar med hänvisning till arbetets behöriga gång, resursernas omfattning eller andra organisatoriska skäl, t.ex. omfattningen av och inriktningen på en enskilds kontakter med myndigheten.

6.7 Myndighetens hantering av elektronisk legitimering och inkomna handlingar

Frågan om vad som bör innefattas i de kontroller som myndigheterna gör av mottagna e-legitimationer och andra handlingar behandlas i 5.2 och 5.3. Vidare redovisas i 5.4. vilken information myndigheten bör ha tillgång till vid dessa kontroller. Visar de automatiska kontrollerna att det finns en brist i en inkommen handling bör myndigheten genom en handläggare göra en manuell bedömning av om handlingen till följd av andra kontrollåtgärder t.ex. efter samtal med angiven utställare eller bekräftelse på elektronisk väg, kan godtas som äkta (5.5 och 5.9). Vid sådana kontroller behöver uppgifterna presenteras för handläggaren i direkt läsbar form på ett överskådligt och tydligt sätt; se 5.6 där det också anges vilka uppgifter som bör presenteras.

Ytterligare information kan behövas från en utfärdare av e-legitimationer för sakens prövning och denna information bör kunna göras tillgänglig (5.7). Till detta hör att myndigheter som tillhandahåller e-tjänster bör samordna sina föreskrifter med de avtal som sluts med utfärdare som tillhandahåller ID-tjänster. Genom samordningen kan säkerställas att kompletterande handlingar och uppgifter får lämnas ut när de behövs för en säker hantering av elektroniska underskrifter och elektronisk identifiering. Samtidigt bör myndigheterna beakta behovet av skydd mot otillbörligt integritetsintrång (5.8). Den förlitade partens kontroller bör inte försvåras eller fördröjas på grund av att det fordras en talan om editionsföreläggande vid allmän domstol för att få ut underlaget eller att avtalsvillkor om tystnadsplikt inte på ett balanserat sätt tillgodoser behovet av att kunna utföra kontroller av elektroniska underskrifters äkthet.

Vid de manuella kontrollerna kan en handläggare behöva göra en manuell bedömning av om ett föreläggande bör utfärdas om bekräftelse genom en egenhändigt undertecknad handling eller på annat alternativt sätt. Med annat alternativt sätt kan exempelvis avses att bekräftelse sker genom ytterligare en elektronisk underskrift eller att annan eller kompletterande e-legitimation används. Handläggare bör även bedöma om handlingen inte föranleder någon ytterligare åtgärd av myndigheten till följd av att den är gravt ofullständigt eller oläsbar eller om ingen avsändare som kommunikation kan ske med anges, eller om förutsättningar föreligger för att gallra handlingen (5.9). I vissa fall är en bekräftelse nödvändig, t.ex. när egenhändigt undertecknande är föreskrivet i författning och elektroniska signaturer inte godtas

enligt praxis. I en framtid när kvalificerade elektroniska signaturer tagits i bruk kan 17 § lagen (2000:832) om kvalificerade elektroniska signaturer hindra en sådan begäran om bekräftelse. Det får i övrigt från fall till fall avgöras om bekräftelse av en elektronisk handling ska införas (jfr prop. 1993/94:190 s. 107-109 och 121).

När en myndighet får tekniskt stöd av annan, t.ex. genom outsourcing av vissa funktioner, är det viktigt att de manuella åtgärderna för ärendehandläggning inte utförs av annan än den myndighet till vilken handlingen har kommit in (5.10)¹²;

¹² jfr 11 kap. 6 § regeringsformen, lagen (2004:543) om samtjänst vid medborgarkontor och Samsetrapport 2002:1, Infratjänster för 24-timmarsmyndigheterna.