Digitalisera rätt

En praktisk juridisk vägledning

eSam, juni 2019

eSam

Innehåll

1. Inledning

1.1 Bakgrund

Digitaliseringen är den mest samhällsomvälvande förändringen sedan industrialiseringen. Digital samverkan innebär helt nya förutsättningar, behov och villkor för individ och samhälle, för företag och offentlig sektor, för arbetsliv och utbildning och för civilsamhället. För att ta tillvara digitaliseringens möjligheter behöver hela det offentliga Sverige gå i takt och ha arbetssätt och tekniker som drar nytta av innovationskraften hos företag och andra externa aktörer.

Digitaliseringen innebär att myndigheter ersätter sin traditionella informationshantering med nya digitala arbetssätt där kända och inarbetade hanteringsformer ersätts med elektroniska handlingar (e-handlingar), elektroniska[1] underskrifter (e-underskrifter), elektroniska stämplar (e-stämplar) och anknytande funktioner för att kontrollera och bevara e-handlingar i ursprungligt skick. I samband med digitaliseringen pågår också en utveckling där själva informationen och automatiserade möjligheter att hantera den kan betraktas som en tillgång i sig.

De begrepp som har använts för att beskriva dessa funktioner har ofta framstått som mångtydiga, vaga och svåra att tillämpa. För att undgå detta tog E-delegationen fram en vägledning för elektroniska original, kopior och avskrifter. Vidare har eSam beskrivit konsekvenserna av att digitalisering numera är huvudregel och publicerat vägledningar och uttalanden om hur information kan dokumenteras, ges in och i övrigt hanteras digitalt.[2]

I dessa vägledningar och uttalanden har tolkningar av gällande rätt gjorts. Ett stort antal myndigheter och organisationer har ställt sig bakom dessa tolkningar och lagt dem till grund för utformningen av sina it-baserade tjänster. Däremot har varken E-delegationen eller eSam närmare analyserat hur uppgifter bör hanteras digitalt i myndigheternas egen verksamhet för att handlägga ärenden. På liknande sätt finns ”vita fläckar” i eSams och E-delegationens beskrivningar av hur uppgifter bör hanteras innan de har kommit in till

[1] Använda begrepp har i denna vägledning samma innebörd som i eSams juridiska vägledning för verksamhetsutveckling inom e-förvaltning 3.0. Digital och elektronisk är därmed synonymer.
[2] Se bland annat eSams juridiska vägledningar om rättsliga förutsättningar för digitalt i första hand, verksamhetsutveckling inom e-förvaltning 3.0, eget utrymme, införande av e-legitimering och e-underskrifter (nu i version 1.1), Elektroniskt informationsutbyte och outsourcing samt eSams uttalanden om eget utrymme, ankomstdag för e-handlingar och röjande enligt offentlighets- och sekretesslagen. Se även SKL:s cirkulär 11:46 Rapport till vägledning vid införandet av e-tjänster.

en myndighet enligt förvaltningslagen och tryckfrihetsförordningen och om handlingar kan expedieras digitalt istället för på papper. Som exempel på andra frågor som behöver belysas närmare kan nämnas om e-underskriften har en för människa läsbar form, om metadata anses ingå i en viss e-handling och om digitala data helt kan ersätta pappershandlingar.

1.2 En ny vägledning för en fullständig digitalisering

Eftersom digitala tjänster[3] numera ska vara förstahandsval vid myndigheters kontakter med andra har verksamhetsutvecklingen inriktats på helt digitaliserade och automatiserade interna och externa procedurer. För att stödja en rättsenlig och ändamålsenlig utveckling av funktioner för en sådan fullständig digitalisering har eSam tagit fram denna praktiska juridiska vägledning för att digitalisera rätt. Vägledningen ska göra det möjligt att överblicka de frågor som uppkommer och att få en ingång till bedömningar och synsätt som etablerats.

1.3 Syfte

Vägledningen ska stödja myndigheterna i arbetet med att införa en helt digital hantering av information, dels i myndighetens verksamhetssystem, dels i generella stödfunktioner för bland annat kommunikation av meddelanden, e-legitimering, e-underskrifter, e-arkiv och eget utrymme. Dessa funktioner behöver användas samordnat och etableras på ett rättsenligt sätt[4] inom de miljöer som med en populär term bland utvecklare brukar kallas den digitala förvaltningens ekosystem.[5]

Vägledningen berör myndighetens interna informationshantering som sker digitalt för att handlägga ärenden eller för myndighetens faktiska handlande. För förvaltningsmyndigheter är det normalt förenligt med författningsregleringen att dokumentera myndighetsbeslut i endast digital form[6], oberoende av

[3] Begreppet ”digital tjänst” omfattar i denna vägledning även funktioner där kommunikationen sker maskin till maskin, det vill säga utan användargränssnitt för en fysisk person.
[4] Huvudspåret var tidigare manuella rutiner, baserade på egenhändigt underskrivna pappershandlingar. Myndigheternas digitaliseringsarbete inriktades då på skanning av mottagna handlingar för att ärendehandläggningen skulle kunna ske via bildskärm med hjälp av digitala akter. Erfarenheten har visat att det som bevarats på papper sällan återsökts eftersom det digitala materialet i praktiken varit tillräckligt. Någon närmare analys av hur frågan om gallring av de pappersexemplar som i praktiken aldrig används skulle kunna hanteras på ett i praktiken fungerande sätt synes inte ha genomförts. Tvister om handlingarnas äkthet där ett pappersoriginal kan behöva åberopas är mycket ovanliga. På liknande sätt skrevs beslutsdokumenten ofta ut på papper och undertecknades med bläck, för att i många fall åter ges digital form så att handlingarna kunde tillgängliggöras via nät. Vanligtvis bevarades alla pappershandlingar, trots att de nästan aldrig blev brukade efter att ha lagts i arkiv.
[5] Med digitalt ekosystem menas sammanhållen funktionalitet för offentlig förvaltning där samverkan kan ske automatiserat utifrån gemensamma synsätt och rättsenliga tillvägagångssätt. Detta begrepp används bland annat av OECD, exempelvis i en rapport från Forum on Tax Administrations.
[6] Se vidare punkt 6.3 eSams juridiska vägledning för införande av e-legitimering och e-underskrifter.

om ansökningshandlingar och annat underlag har getts in i på papper eller digitalt. Denna hantering kan förenklas om data kommer till myndigheten i rätt format och med korrekt innehåll (eget utrymme behöver vara ändamålsenligt utformat). Format och metoder för underskrifter och stämplar måste också kunna hanteras av myndigheten (bland annat behöver e-legitimationer kunna kontrolleras med redan införda metoder). Slutligen behöver beslut och andra handlingar kunna expedieras elektroniskt, med stöd av till exempel Mina meddelanden, även när handlingen har producerats på papper.

Vägledningens ändamål är att ge praktisk juridisk vägledning för en rättsenlig hantering av dessa funktioner genom att informera om vilka juridiska utmaningar som brukar uppkomma och hur de vanligtvis kan lösas.

1.4 Metod

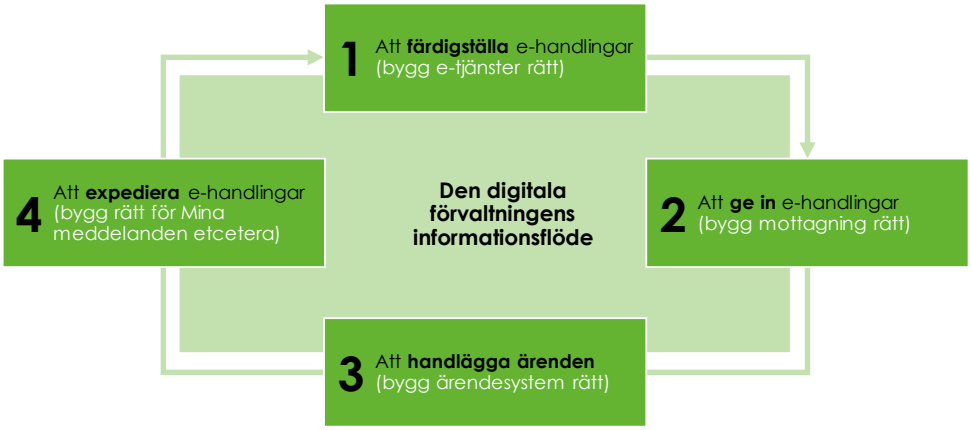
När en fullständig digitalisering ska genomföras, från ax till limpa, kan de vägledningar och rättsliga uttalanden som eSam tidigare utarbetat framstå som ett lapptäcke. Här tas frågorna upp från ett helhetsperspektiv med sikte på att växla över från fysiska dokument och blanketter till en juridisk utgångspunkt från själva informationsinnehållet.[7] Vid en fullständig digitalisering behövs strategier för hur myndigheter ska kunna expediera, motta, återanvända och bevara information på ett rättsenligt sätt. En juridisk bedömning av e-handlingar, e-underskrifter och e-stämplar utgår här från färdiga handlingar med eller utan underskrifter och stämplar. Handlingar som blivit allmänna genom att myndigheten tagit emot eller upprättat dem ska vara tillförlitliga, autentiska och åtkomliga, samt konverterbara, läsbara och möjliga att tolka till dess de gallras eller tas om hand i ett e-arkiv. Samtidigt behöver gränser i traditionell miljö mellan myndigheter och enskilda återskapas i form av logiska avgränsningar baserade på till exempel kryptografiskt skydd.

Vi beskriver denna hantering som fyra övergripande led i informationsflödet i ärendeprocessen där det som äger rum inom en myndighets verksamhetssystem inte går att isolera från de funktioner för service som myndigheten tillhandahåller för att färdigställa och skicka information. För detta utvecklingsarbete behövs jurister, verksamhetsutvecklare, arkitekter och arkivarier som

[7] I juridiska sammanhang sker också en övergång från att tänka i termer av dokument och blanketter till att se själva uppgiften som objektet för en reglering, till exempel vid bedömningen av om en uppgift i en handling är sekretessreglerad, om en sammanställning av uppgifter är en allmän handling och om en personuppgift föreligger som omfattas av regler om dataskydd (jfr om en ”sammanställning av uppgifter ur en upptagning för automatiserad behandling” respektive en färdig elektronisk handling ska anses föreligga, det vill säga en sådan e-handling som av utställaren getts en bestämd, fixerad form som kan återskapas gång på gång (2 kap. 6 § TF). Se också offentlighets- och sekretesslagen (2009:400) som utgår från ”uppgift” i stället för ”handling”.

kan uppfatta e-handlingen som en slags paketering av digitala data som ska kunna omvandlas till läsbar form, kommuniceras och förvaras i olika exemplar hos skilda aktörer.[8] Vår metod för att ge ett konkret stöd utgår därför från de fyra övergripande led i den ärendeprocess som beskrivs i följande figur.

Figur 1: Fyra övergripande led i den digitala förvaltningens informationsflöde



Hanteringen går typiskt sett till så att en person färdigställer en handling (Led 1) och sänder den till en myndighet (Led 2). Myndigheten tar emot handlingen och handlägger det ärende som väcks på grund av informationen i handlingen (Led 3). Slutligen expedierar myndigheten ett föreläggande, ett beslut eller någon annan handling till den enskilde (Led 4), som i sin tur kan upprätta ett svar, en begäran om omprövning eller ett överklagande (Led 1) och skicka handlingen (Led 2). Handlingen har ett innehåll som leder till ärendehandläggning (Led 3), varefter informationsflödet kan fortsätta på samma sätt.

Varje myndighet behöver analysera och ha kontroll över förfaranden inom den egna verksamheten. Förutsättningarna för en digitalisering måste klarläggas. Denna vägledning kan tas tillvara även för digitalisering som inte innefattar ärendehandläggning. För sådan faktisk hantering används visserligen inte det ärendeflöde som vi har beskrivit. Det är emellertid möjligt att med stöd av vägledningens struktur finna de råd och hänvisningar till annat material som blir relevanta i det enskilda fallet (se kap. 6). Myndigheten behöver också ha förmåga att hantera de komponenter som är nödvändiga för att detta

[8] Juridiska kommentarer och läroböcker brukar istället utgå från det rättsområde och de lagar och förordningar som berörs, medan myndigheter i sina utvecklingsprojekt tar sin utgångspunkt i beskrivningar av de processer som ska digitaliseras och de förmågor eller värden processerna ska stödja. Eftersom de digitala processerna äger rum i informationssystem betraktas även e-handlingar, e-underskrifter och e-stämplar som (delar av) processer. Jurister betraktar istället dessa e-handlingar, med eller utan e-underskrifter och e-stämplar, som digitala produkter – ofta utan att fråga efter de system och förlopp där de uppkommit. Handlingarna ses som skriftliga bevis.

informationsflöde ska fungera ändamålsenligt och rättsenligt.[9] De utmaningar som detta för med sig behöver sorteras närmare och beskrivas på ett ändamålsenligt sätt i en praktisk juridisk vägledning. Vi har därför delat in varje övergripande led i ”Att göra-punkter”, se följande figur.

Figur 2: Att göra-punkter för varje övergripande led i informationsflödet

Flera av de frågor som berörs är generella och behöver bedömas övergripande innan ett utvecklingsprojekt inleds, exempelvis om en funktion ryms inom myndighetens uppdrag och om en lämplig skyddsnivå upprätthålls. Vissa frågor aktualiseras i mer än ett av de övergripande leden eller hör hemma under flera Att göra-punkter. Myndigheten behöver exempelvis göra en risk- och sårbarhetsanalys för berörd it-miljö och ta ställning till om en konsekvensbedömning avseende dataskydd enligt artikel 35 i EU:s dataskyddsförordning behöver genomföras. Även principerna om inbyggt dataskydd och dataskydd som standard enligt artikel 25 i dataskyddsförordningen måste beaktas. Vår indelning är emellertid ändamålsenlig för att ge praktisk juridisk vägledning när den målgrupp som anges i nästa avsnitt ska genomföra en fullständig digitalisering. För den som överväger ett utvecklingsprojekt där flera myndigheter är inblandade hänvisas till eSams checklista för jurister.

Vid all digital hantering av personuppgifter som förekommer i myndigheters verksamhet måste såväl EU:s dataskyddsförordnings grundläggande principer för behandling av personuppgifter som framgår av artikel 5 som resten av de

[9] Till denna arkitekturella förmåga, dvs. vad en viss myndighet behöver kunna göra, hör de resurser, processer och it-system samt den information och de verksamhetsregler som är nödvändiga för att på ett ändamålsenligt och rättsenligt sätt etablera en papperslös myndighet.

krav som förordningen uppställer efterlevas. Den här vägledningen gör endast nedslag i dataskyddsregelverket i förhållande till automatiserat beslutsfattande. Det finns också andra regelverk som kan vara relevanta i förhållande till den information som hanteras digitalt, exempelvis regler om säkerhetsskydd.

1.5 Målgrupp

Vägledningen ska fungera som en bro mellan teknik och juridik. För att utveckla och införa funktioner som är juridiskt riktiga krävs samarbete, inte bara mellan verksamhetsutvecklare, säkerhetsansvariga, arkitekter, arkivarier och jurister utan även med alla som på något sätt verkar för att ta fram en lösning (till exempel beställare, chefer, controllers, kommunikatörer och projektledare). Alla dessa yrkeskategorier är därför målgrupp för denna vägledning.

Vägledningen kommer dessutom vara av betydelse för externa leverantörer som behöver anpassa sina tjänster till en fullständig digitalisering. Genom att vara väl insatt i de tekniska och juridiska förutsättningarna blir det möjligt för dem att ta fram nya enhetliga it-baserade tjänster och förbättra de tjänster som redan finns i drift.

1.6 En del i ett svenskt ramverk för digital samverkan

För att underlätta en effektiv samverkan mellan svenska organisationer har eSams expertgrupp för arkitektur utarbetat Svenskt ramverk för digital samverkan. Med digital samverkan menas förmågan hos organisationer att interagera i en gemensam riktning mot ömsesidigt fördelaktiga och överenskomna mål. Det svenska ramverket tar sin utgångspunkt i ett europeiskt interoperabilitetsramverk (EIF), som ger förutsättningar för en sammanhållen hantering där offentliga organisationer genom ökad transparens får förmåga att samverka med varandra, företag och privatpersoner.

Det svenska ramverket för digital samverkan omsätter nationella och internationella styrdokument till grundläggande gemensamma principer som ska ge stöd för en samordnad riktning i digitaliseringsarbetet. Utifrån dessa principer rekommenderar ramverket vad offentliga organisationer behöver göra för att kunna verka tillsammans på ett effektivt sätt. Ramverkets rekommendationer behöver kompletteras med ett konkret juridiskt stöd. Det är här den följande praktiska juridiska vägledningen för att digitalisera rätt kommer in som ett stöd för att genomföra ramverkets principer.

1.7 Medverkande

Arbetet med att ta fram vägledningen har genomförts av eSams rättsliga expertgrupp. Ledamöter i expertgruppen är Johan Bålman, Eva Maria Broberg, Malgorzata Drewniak, Per Furberg, Gustaf Johnssén, Jan Sjösten, Gunnar Svensson, Mikael Westberg, Staffan Wikell, Tomas Öhrn, Christina Wikström och Erik Janzon. Adjungerade ledamöter i expertgruppen är Veronica Eckerby, Nils Fjelkegård och Linn Kempe. I arbetet har även eSams rättsliga referensgrupp och expertgrupperna för säkerhet och arkitektur deltagit.

1.8 Läsanvisning

För den som inte tidigare arbetat med området kan det vara lämpligt att först ta del av de begrepp och användningssätt som eSam har redovisat i den juridiska vägledningen för verksamhetsutveckling inom e-förvaltning. Här används samma begrepp och synsätt. Därefter presenteras i kap. 2 denna vägledning den informationshantering och vissa av de rättsfrågor som en fullständig digitalisering för med sig. Vissa frågor som kräver en närmare analys planeras att redovisas i bilagor, som beslutas av eSams juridiska expertgrupp.

För att konkretisera de åtgärder som bör vidtas vid en fullständig digitalisering inleds respektive avsnitt i kap. 2–5 med en ”Att göra-ruta” där de frågor anges som kräver särskild vaksamhet – se följande exempel.

> Att göra 1: En myndighet som planerar en tjänst för att enskilda ska kunna upprätta och ge in uppgifter eller handlingar digitalt eller en funktion för att själv upprätta och expediera e-handlingar behöver undersöka om det finns formkrav och i så fall tolka dem för att bedöma om formkraven hindrar den planerade hanteringen.

Under respektive ruta ges en allmän genomgång av de juridiska kraven, det material som finns, hur myndigheten bör förfara inom området och följderna av att underlåta detta. Eftersom beskrivna informationsflöden ingår som led i service eller ärendehandläggning enligt förvaltningslagen eller särreglering inom området redovisas de digitala processerna från ett ärendeperspektiv. Där kan följande moment särskiljas.

1. Service och tillgänglighet innan ett ärende inleds.
2. Hur ett ärende inleds.
3. Hur ett ärende bereds;

a. dokumentation av uppgifter,
b. kommunikation med part i ärende, och
c. kommunikation genom remiss till annan myndighet och annan enskild.

4. Myndighetens beslut och expediering.
5. Omprövning och överklagande.

Dessa moment och de tekniska och administrativa funktioner som beskrivs i vägledningen utgör, tillsammans med övriga skyldigheter enligt förvaltningslagen och särreglering för vissa förvaltningsområden, grunden för myndigheternas digitala informationshantering. Regleringen i förvaltningslagen (2017:900; FL) är i högre grad än äldre regler anpassad för att vara neutral i förhållande till den omfattande och kontinuerligt ökande digitala förvaltningen (prop. 2016/17:180 s. 68). När digitalisering nu sker från ax till limpa finns emellertid ”vita fläckar” där juridiska utmaningar uppstår.

Vägledningen kan som framgått också användas utanför den ärendeprocess som beskrivs i avsnitt 1.4. Då innefattar hanteringen inte alla led i ärendeprocessen och hanteringsordningen varierar. Att göra-punkternas rubricering kan dock leda läsaren rätt tillsammans med de kortfattade beskrivningarna i en ruta för varje punkt (se vidare kap. 6).

2. Att färdigställa e-handlingar

Tänk på att:

En myndighet kan tillhandahålla en funktion där en användare kan färdigställa handlingar på egen hand. Funktionen kan användas av enskilda för att upprätta handlingar innan och under ett ärende, och funktionen kan användas av myndigheten för att upprätta eller hantera e-handlingar. En sådan funktion kan införas av myndigheten för att erbjuda service och tillgänglighet.

Det första övergripande ledet i hanteringen av uppgifter för att etablera en helt digital förvaltning (se figur 1 i avsnitt 1.4) omfattar de funktioner som en myndighet behöver tillhandahålla för att enskilda ska kunna ta del av underlag och färdigställa handlingar på ett ändamålsenligt sätt, samt de juridiska förutsättningarna för myndigheten att skapa sådana funktioner.

I funktionen ger myndigheten enskilda sådan hjälp att de kan ta till vara sina intressen innan ett ärende har inletts. I praktiken brukar det ske genom att myndigheten skapar en teknisk lagringsyta, ett s.k. eget utrymme, åt den enskilde. Det kan också vara myndigheten själv som upprättar handlingar i sin verksamhet, exempelvis för att inleda ett ärende.

En funktion för att färdigställa handlingar tillhandahålls av en myndighet som en service åt enskilda. I eget utrymme kan myndigheten inrätta en funktion där den enskilde själv hämtar uppgifter från andra (se avsnitt 4.7). Funktioner av detta slag ska normalt tillgodose enskildas behov innan ett ärende har väckts. Myndigheten utför då sina uppgifter i fråga om service enligt 6 § FL och tillgänglighet enligt 7 § FL. En sådan funktion kan emellertid också underlätta kommunikation i ett pågående ärende, till exempel när en komplettering begärs enligt 20 § FL av en ansökan eller när den enskilde ska yttra sig över vad som har anförts av någon annan i ett ärende.

2.1 Formkrav (Att göra 1)

Att göra 1: En myndighet som planerar en tjänst för att enskilda ska kunna upprätta och ge in uppgifter eller handlingar digitalt eller en funktion för att själv upprätta och expediera e-handlingar behöver undersöka om det finns formkrav och i så fall tolka dem för att bedöma om formkraven hindrar den planerade hanteringen.

När en helt papperslös tjänst för att ställa ut och ge in e-handlingar eller en funktion för att själv upprätta och expediera e-handlingar planeras behöver det säkerställas att det inte finns hinder i lag, förordning eller myndighetsföreskrifter mot denna hantering. Med formkrav menas att en handling, för att ha en viss rättsverkan, ska ha viss form eller visst innehåll eller ska tillkomma eller annars hanteras på visst sätt. Formkrav i detta sammanhang, att hantera handlingar i ett ärende digitalt, kan vara att det finns regler som kräver handpåläggning, till exempel krav i författning på underskrift.

Allmänt om kraven: Om det finns formkrav kan de hindra att en e-handling med e-underskrift får juridisk verkan. Här är frågan alltså om en enskild får färdigställa och ge in handlingar, såsom deklarationer och ansökningshandlingar, i digital form och om en myndighet får upprätta förelägganden, beslut och andra liknande handlingar i digital form. Måste handlingarna i så fall på grund av formkrav skrivas under, får underskriften ha digital form och vilken nivå av skydd ska krävas?[10] Ett exempel på hindrande formkrav är att handlingen avser köp av fast egendom. Här får en e-handling med e-underskrift inte juridisk verkan.

Det finns normalt inte juridiska hinder mot att enskilda och myndigheter använder it för att producera utkast, så länge de grundläggande kraven på skydd för informationssäkerheten och persondata uppfylls. När utkast ska färdigställas kan de dock på grund av formkrav behöva skrivas ut på papper och undertecknas med bläck. Varken i förvaltningslagen eller myndighetsförordningen finns emellertid något krav på att handlingar ska vara pappersbaserade eller undertecknade. Där finns inte heller krav på att beslut och andra handlingar ska vara på papper eller undertecknade. Sådana formkrav följer

[10] E-underskrifter och e-stämplar kan dessutom, oberoende av formkrav i författning, behövas av rättssäkerhets- eller informationssäkerhetsskäl.

snarare av speciallagstiftning eller myndighetens interna hanteringsregler. Myndighetsbeslut får dessutom normalt fattas automatiserat.[11]

Termerna ”handling” och ”skriftlig” medger normalt digitala rutiner (se Ds 2003:29 s. 12). Krav på ”underskrift” av handlingar som ges in till en myndighet gäller endast om detta följer av författning. Sådana föreskrifter finns för vissa förvaltningsområden. Termen ”beslut” anses när den används i lag, förordning eller myndighetsföreskrifter inte hindra digitala rutiner. Detta följer numera redan av att beslut enligt 28 § FL kan fattas automatiserat (jämför Ds 2003:29 s. 98). Krav på att beslut och andra handlingar ska vara undertecknade gäller bara när det föreskrivs i författning. Sådana krav är inte vanliga. Finns de i en myndighetsföreskrift kan myndigheten själv ändra regeln så att en digitalisering kan ske.

Det material som finns: En grundlig genomgång har gjorts av regeringens FORMEL-grupp och resultatet har redovisats i en departementspromemoria (Ds 2003:29). Till promemorian hör en bilaga där varje departement gjort en genomgång och kommenterat sina författningar.[12] De bedömningar som redovisats där återger vad som allmänt brukar betraktas som gällande rätt.[13] Dessutom har eSam i en juridisk vägledning för införande av e-legitimering och e-underskrifter (kap. 6) berört under vilka förutsättningar e-underskrifter får användas. Det finns också en matris över några krav på underskrift i en rapport den 31 oktober 2011 till vägledning av Sveriges kommuner och landsting vid införandet av e-tjänster (Cirkulär 11:46). Se även eSams checklista för jurister, avsnitt 5.1.2.

Gör så här: Läs igenom de lagar, förordningar och myndighetsföreskrifter som är tillämpliga inom det rättsområde där den nya tjänsten ska införas. Leta efter krav på underskrift, namnteckning, undertecknande eller liknande. I undantagsfall kan andra krav som förutsätter papper eller traditionell fysisk distribution finnas. Sådana krav brukar kunna identifieras med sunt förnuft, om läsaren har kunskap och erfarenhet inom området och närmare överväger vilka praktiska förfaranden som reglerna kräver. Eftersom en pappersbaserad hantering med

[11] Se 28 § FL och Att göra 21. Det föreskrivs visserligen i 21 § myndighetsförordningen (2007:515) att det för varje beslut i ett ärende ska upprättas en handling som visar dagen för beslutet, beslutets innehåll, vem som har fattat beslutet, vem som har varit föredragande och vem som har varit med vid den slutliga handläggningen utan att delta i avgörandet. Uppgifter om föredragande, beslutsfattare och liknande får emellertid utelämnas när ingen sådan individ har agerat.

[12] För upphävda författningar finns ofta en äldre att jämföra med. Det kan på så sätt gå att hitta vägledning även för vad som gäller enligt en nyare författning till vilken en formföreskrift förts över.

[13] Dock används begreppet undertecknad teknikneutralt i skatteförfarandelagen (2011:1244) så att kravet kan uppfyllas både genom undertecknande på papper och med digitala medel (se 38 kap. 1 och 2 §§ och prop. 2010/11:165 s. 857). Andra sådana skillnader finns också i undantagsfall.

underskrifter framstod som självklar när äldre lagar och förordningar kom till går det vanligtvis inte att finna ledning i gamla motiv till författningar.

Hittar ni inga formkrav eller kan de krav som finns tolkas så att digitaliserade förfaranden inryms är det i normalfallet möjligt att införa e-handlingar, e-underskrifter och e-akter i stället för pappersbaserade rutiner, när andra krav såsom de på integritetsskydd och informationssäkerhet tillgodoses.[14] En utveckling pågår i riktning mot att mera självklart acceptera digitala ersättare för pappershandlingar. – Krävs dokumentation på papper är en viss digitalisering ändå möjlig. I sådana situationer blir resultatet varken helt digitalt eller helt pappersbaserat, se avsnitt 3.6 och 4.4.

Följden av att en formföreskrift inte följs är vanligtvis att en rättshandling eller en annan åtgärd inte får rättslig verkan. Bristen kan resultera i en rättsförlust eller ett kompletteringsföreläggande, exempelvis att skriva under samma text på papper.

2.2 Myndighetens uppdrag (Att göra 2)

> Att göra 2: En myndighet som planerar en digital tjänst måste undersöka om det faller inom ramen för myndighetens uppdrag att tillhandahålla den, det vill säga om myndigheten har stöd i gällande rätt för att tillhandahålla en sådan tjänst.

När en papperslös tjänst för att ställa ut och ge in e-handlingar planeras behöver det säkerställas att tjänsten faller inom ramen för myndighetens uppdrag (legalitet), eftersom myndigheter inte får företa åtgärder som saknar stöd i författning.

Allmänt om kraven: Regeringen lämnar sina uppdrag till förvaltningen på olika sätt. I 5 § första stycket FL föreskrivs att en myndighet endast får vidta åtgärder som har stöd i rättsordningen. Bestämmelsen ger uttryck för legalitetsprincipen och tar sikte på de källor som tillsammans bildar rättsordningen i vidsträckt mening. Bestämmelsen innebär att det måste finnas någon form av normmässig förankring för all typ av verksamhet som en myndighet bedriver. Exempel på sådant författningsstöd kan vara allmänna bestämmelser i lag eller detaljerade regler i speciallagstiftning. Det kan också vara fråga om allmänna

[14] En genomgång av nya lagmotiv där frågor om e-förvaltning tas upp tyder också på att en utveckling ägt rum mot att mera självklart tolka in användningen av digitala ersättare för pappersbaserade handlingar, se till exempel hur frågan om inkommande av e-handlingar behandlas i propositionen till den nya förvaltningslagen (prop. 2016/17:180 s. 141).

eller särskilda bestämmelser i myndighetens instruktion eller myndighetsförordningen eller i någon annan förordning som regeringen har beslutat. Så kan till exempel vara fallet i fråga om befogenheten för en myndighet att ingå civilrättsliga avtal eller annars uppträda som privaträttsligt subjekt. Legalitetskravet kan även vara uppfyllt genom ett förvaltningsbeslut, exempelvis om åtgärden har stöd i myndighetens regleringsbrev. Bestämmelsen innebär inte att varje enskild åtgärd som en myndighet vidtar måste ha uttryckligt stöd i en viss lagbestämmelse eller i andra föreskrifter som har meddelats i enlighet med 8 kap. regeringsformen (prop. 2016/17:180 s. 289). Beträffande överlämnande av förvaltningsuppgift åt enskild krävs dessutom stöd i lag om uppgiften innefattar myndighetsutövning.[15]

Det material som finns: En grundlig genomgång har gjorts av Förvaltningslagsutredningen i betänkandet en ny förvaltningslag (SOU 2010:29 s. 142 ff.). Där har poängterats att myndigheternas verksamhet enligt legalitetsprincipen styrs av de regler om arbetsuppgifterna som lagstiftaren eller annan normgivare beslutat och att några nyskapelser i form av särskilda samarbetsorgan, som oberoende av fastlagda normer tillåter sig att fatta beslut som svårligen kan härledas till den ena eller andra av de samverkande myndigheterna, inte får förekomma. Se även regeringens proposition 2016/17:180 en modern och rättssäker förvaltning – ny förvaltningslag, där det anförts att myndigheterna inte alltid i tillräcklig utsträckning tar reda på om att de har stöd i rättsordningen för sina åtgärder. Utvecklingen från en mer klassisk förvaltning mot en förvaltning med ökade inslag av informationsuppgifter och mera kundrelaterade aktiviteter, till exempel i form av olika digitala självbetjäningstjänster, har inneburit ökade risker i detta avseende (s. 58). Regeringen har förklarat att vad som bör krävas är någon form av normmässig förankring för all typ av verksamhet som myndigheten bedriver men att det inte bör ställas krav på att varje enskild åtgärd som en myndighet vidtar kan kopplas till ett specifikt bemyndigande. Kravet på legalitet bör inte heller uppfattas så att en myndighets åtgärd måste ha uttryckligt stöd i en viss lagbestämmelse eller i andra föreskrifter som har meddelats i enlighet med 8 kap. regeringsformen (a. prop. s. 59 och 289). eSam har också tagit upp dessa frågor i juridiska vägledningen för verksamhetsutveckling inom e-förvaltning (s. 18, s. 40 och s. 60). Se även eSams checklista för jurister, avsnitt 2.1, särskilt om utvecklingsinsatsen innebär samverkan med annan – myndighet eller enskild.

[15] Se 12 kap. 4 § regeringsformen och exempelvis den särreglering som ges i 2 kap. 4 § tullagen (2000:1281).

Gör så här: Läs igenom de lagar och förordningar som är tillämpliga för myndigheten, särskilt myndighetens instruktion, samt myndighetens regleringsbrev och de särskilda beslut som regeringen fattat där myndigheten ges i uppdrag att utföra något som rör den digitala förvaltningen. Leta efter sådant som ger myndigheten i uppdrag att göra något inom berört område. Den snabba utvecklingen och de generella utvecklingsuppdrag som lämnats rörande den digitala förvaltningen ger skäl till uppmärksamhet på att utvecklingsinsatser som resulterat i permanent verksamhet också bör ges ett rättsligt stöd i exempelvis myndighetens instruktion. Uppmärksamma också att om samverkan ska ske med annan myndighet eller enskild behöver denna samverkan vara förenlig med myndighetens kompetens.[16]

Följden av att legalitetskravet inte uppfylls är att myndigheten agerar utan rättsligt stöd, med det ansvar det kan föra med sig för myndighetens ledning.

2.3 E-underskrifter (Att göra 3)

> Att göra 3: När det finns krav på att en viss typ av underskrift ska användas, exempelvis avancerade e-underskrifter, ska myndigheten använda angiven typ. I de fall det finns krav på underskrift utan att en viss typ anges, behöver myndigheten välja en teknisk lösning som ger en lämplig skyddsnivå. Även när regler om krav på underskrift inte finns behöver myndigheten överväga att välja en lämplig skyddsnivå.

Myndigheten måste bedöma vilken skyddsnivå som ska krävas för underskrifter och stämplar när myndigheter planerar en papperslös tjänst för att ställa ut och ge in e-handlingar som ska skrivas under, eller en funktion för att själv upprätta och expediera e-underskrivna handlingar. Frågan berör olika regelverk. Myndigheten måste också överväga vilken skyddsnivå som bör krävas vid e-legitimering och automatiserade behörighetskontroller. Beträffande dessa frågor hänvisas till eSams Juridiska vägledning för införande av e-legitimering och e-underskrifter.

Allmänt om kraven: Det är verksamhetens behov och kraven på skydd för bland annat rättssäkerheten (avsnitt 2.4) och informationssäkerheten som blir avgörande för vilka kontroller av äkthet och vilka skydd mot manipulationer av utställare och innehåll som ska införas genom underskrifter och stämplar, jämför avsnitt 4.1. Det är i första hand myndigheten som behöver kunna lita på att

[16] I sammanhanget bör nämnas att myndigheten också kan vara bunden av avtal eller andra överenskommelser som behöver följas.

mottagna handlingar är äkta och svara för att erforderliga krav på äkthetskontroll uppfylls vid en digitalisering, men parter och andra måste också kunna vara trygga med att myndigheten inte grundar beslut på falska handlingar.[17] För myndigheter som ska driva in fordringar i andra länder, exempelvis CSN, är det också betydelsefullt om e-handlingarna får åberopas som bevis och kan betraktas som tillförlitliga i domstol.

Redan när en digital tjänst tas fram bör myndigheten ta tillvara möjligheten att utforma det tekniska förfarandet och funktionerna i ett eget utrymme efter verksamhetens behov.

Finns det krav på att en viss typ av underskrift ska användas, exempelvis avancerade e-underskrifter, måste myndigheten använda angiven typ. När det inom aktuellt område inte finns några krav i författning på underskrift eller när det krävs underskrift utan att någon viss typ anges behöver myndigheten välja en skyddsnivå som är anpassad till de behov av rättssäkerhet och skydd för det allmännas intressen som tas upp i avsnitt 2.4. Närmare krav på vissa typer av underskrifter följer av regler i eIDAS-förordningen eller nationella krav i författning.

Det är normalt sett möjligt att tillgodose samma skydd som en underskrift kan ge utan underskrift, så länge myndigheten beaktar kraven på äkthet, informationssäkerhet och rättssäkra förfaranden på annat lämpligt sett. På så vis är en underskrift inte alltid nödvändig för att tillgodose de skyddsbehov som finns. Valet av skyddsnivå kan göras utifrån verksamhetensbehov men också med beaktande av tillgänglig teknik och användarvänlighet. Myndigheten ska kunna lita på mottagna handlingar och svara för att kraven på rättssäkerhet tillgodoses i myndighetens ärendehandläggning. För bland annat straffskyddet och tilliten vid en rättslig prövning blir det dock av betydelse att e-underskrifter eller e-stämplar används med en säkerhetsnivå som ger e-handlingar urkundskvalitet. Enskildas rättssäkerhet, det allmännas intressen och övriga berörda skyddsintressen måste beaktas.

De digitala tjänsterna och användargränssnitten samt myndigheternas verksamhetssystem behöver vara utformade så att var och en förstår när en handling blir ”slutlig”, vad den innehåller, när den granskas och skrivs under och när den skickas till eller från en myndighet. Annars kan den person som framstår som utställare invända att han eller hon aldrig har upprättat eller aldrig gett ut

[17] Riksarkivets publikation Elektroniskt underskrivna handlingar (s. 32).

(skickat) handlingen. E-underskrifter som är avancerade eller kvalificerade har inte heller någon för en människa uppfattbar form utöver ett mönster av digitala signaler. När förekomsten av sådana underskrifter presenteras på till exempel bildskärm och det ser ut som en underskrift på papper är det alltså inte är själva underskriften som presenteras utan en slags bild som visar att det finns en e-underskrift. Dessa användargränssnitt behöver göras begripliga för undertecknare och förlitande aktörer.

Numera ska även EU-medborgare under vissa förutsättningar få logga in i myndigheters e-tjänster med utländska e-legitimationer som uppfyller vissa krav. Vanligtvis kan de emellertid inte, efter att användaren identifierats av myndigheten och släppts in, användas för att bruka själva e-tjänsten. En rapport har därför lämnats till regeringen om en nationell funktion som kan kompensera att utländska e-legitimationer inte innehåller svenskt personnummer. Genomförs förslaget kommer utländska e-legitimationer att kunna brukas även i svenska e-tjänster.

Det material som finns: Av eIDAS-förordningen och tillämpningsföreskrifter följer vissa krav på underskrifter och anknytande infrastruktur. Olika lagtekniska konstruktioner har använts. I något enstaka fall har begreppet undertecknande ansetts innefatta e-underskrifter – i andra inte. Krav på e-underskrifter har i andra fall angetts så att det ska vara ett ”elektroniskt dokument”[18] eller en avancerad e-underskrift enligt eIDAS-förordningen. I några lagmotiv förs resonemang kring val av nivå, bland annat i prop. 2017/18:126 om domstolsavgöranden och strafföreläggande. I eSams Juridiska vägledning för införande av e-legitimering och e-underskrifter, E delegationens vägledning för elektroniska original, kopior och avskrifter och bilaga 1 till Riksarkivets rapport Elektroniskt underskrivna handlingar beskrivs dessa förutsättningar. Se även eSams checklista för jurister, avsnitt 3.1.2 och 5.1.2 och hänvisningar där.

Gör så här: När det finns ett krav i författning på underskrift eller liknande inom det aktuella förvaltningsområdet, utan att någon viss typ av underskrift föreskrivs (exempelvis att e-underskrifter ska vara avancerade) väljer myndigheten utifrån berörda skyddsintressen en lämplig skyddsnivå. Föreskrivs viss typ av underskrift behöver myndigheten också se till att angiven typ används.

[18] Begreppet ”elektroniskt dokument” förekommer i ett antal författningar, se bland annat 19 kap. 10 § jordabalken, där det definieras som en upptagning som har gjorts med hjälp av automatiserad behandling och vars innehåll och utställare kan verifieras genom ett visst tekniskt förfarande, enligt vad som föreskrivs av regeringen eller den myndighet som regeringen bestämmer. – Normalt krävs en avancerad elektronisk underskrift när detta begrepp brukas.

Även när föreskrifter om form inte finns behöver myndigheten välja en tillräcklig skyddsnivå och uppnå den. I de allra flesta fall är en avancerad e-underskrift tillräcklig.

Tänk på att den automatiserade hanteringen i vissa digitala tjänster inte generellt kan anses vara förenad med någon större risk och att vissa ärenden kan vara granskade av handläggare som ser när något inte verkar stämma. En lägre nivå av skydd för underskrifter än en avancerad e-underskrift kan i så fall räcka. Dessutom kan automatiserade kontroller ha införts där tekniska skydd kompenserar en brist på traditionell mänsklig kontroll. När det gäller undertecknande eller slutförandet på annat sätt av en befattningshavare vid en myndighet kan ett alternativ till avancerade e-underskrifter vara att myndighetens personal identifieras på ett säkert sätt i myndighetens skyddade miljö, men att de handlingar som personalen färdigställer förses med myndighetens e-stämpel. Hanteringen blir därmed enklare att administrera i den skyddade digitala miljö som finns inom myndigheten. Handlingar kan i så fall också expedieras med en tydlig koppling till myndigheten och med ett starkt skydd mot att innehåll eller utställarangivelse har manipulerats (jämför de olika skyddsnivåer som i allmänna ordalag har beskrivits i prop. 2017/18:126).

Följden av att en tillräcklig skyddsnivå inte upprätthålls kan vara att individer utför rättshandlingar under sken av att vara någon annan, att rättsförluster uppkommer till följd av att beslut fattas oriktigt, exempelvis att ett företag försätts i konkurs på ”egen ansökan” trots att någon ansökan aldrig gjorts av angiven person, eller att någon oriktigt förnekar sin underskrift eller rättshandling så att det drabbar annan.

2.4 Rättssäkerhet (Att göra 4)

> Att göra 4: När en myndighet inför en e-tjänst där e-handlingar ges in, eller när myndigheten dokumenterar beslut eller andra viktiga uttalanden i digital form behöver myndigheten analysera och bedöma de risker som mera allmänt kan uppkomma från rättssäkerhetssynpunkt. Myndigheten behöver kompensera dessa risker med balanserade skydd, så att ingripanden av olika slag kan ske både i enskilda fall och genom generella åtgärder.

Frågan om vilka risker som mera allmänt kan finnas från rättssäkerhetssynpunkt eller för det allmännas intressen vid införandet av en sådan tjänst

behöver genomlysas. En risk behöver kompenseras så att ingripanden kan ske både i enskilda fall och genom generella åtgärder.

Allmänt om kraven: En myndighet, som för handläggningen av ett ärende använder sig av information i digital form, måste tillföra uppgifterna till handlingarna i målet eller ärendet i läsbar form (i praktiken skriva ut dem på papper). Detta gäller dock inte om det inte finns särskilda skäl, se 4 kap. 3 § Offentlighets- och sekretesslagen (2009:400; OSL). Som ett särskilt skäl räknas att upptagningen finns lätt tillgänglig, till exempel via bildskärm, vilket blir fallet efter skanning där de pappersbaserade förlagorna gallras och ersätts med en digital avbild (så kallad ersättningsskanning). Gallring får endast ske om det finns ett i laga ordning fattat gallringsbeslut eller om det följer av till exempel en registerförfattning att vissa uppgifter ska gallras.[19] I övrigt finns inte generella regler om dokumentation. Speciella regler finns emellertid i författningar som rör förfarandet hos myndigheter. I 27 § FL föreskrivs att en myndighet som får uppgifter på något annat sätt än genom en handling snarast ska dokumentera dem, om de kan ha betydelse för ett beslut i ärendet. Av lagmotiv framgår att det i förvaltningslagens krav på dokumentation ligger att denna ska ske på sätt som är bestående för framtiden (se prop. 2016/17:180 s. 320). Uppgifter får således bevaras digitalt.

En mottagande myndighet får enligt 21 § FL begära att en avsändare ska bekräfta att en viss handling kommer från honom eller henne. Myndigheten avgör alltså själv, dels generellt vilka skydd som bör byggas in i digitala tjänster och eget utrymme, dels om myndigheten i det enskilda fallet ska begära bekräftelse och på vilket sätt en bekräftelse ska lämnas.[20] Skulle en ansökan vara förfalskad eller ha undertecknats av någon som inte är behörig att utföra berörd rättshandling kan detta visserligen rättas till inom ramen för myndighetens ärendehandläggning. Har beslut redan fattats och vunnit laga kraft behöver det emellertid undanröjas genom ett särskilt rättsmedel såsom en ansökan om resning. Sådana händelser är ovanliga, men har exempelvis en falsk egen ansökan om konkurs lett till att ett företag försatts i konkurs eller en uppgift om firmatecknare obehörigen ändrats i ett publikt register kan förluster dock uppkomma för enskilda och det allmänna.

Här måste en bredare analys göras än den riskbedömning som krävs när myndigheten ska välja vilka nivåer av skydd som ska införas för e-legitimering,

[19] Om Riksarkivet har föreskrivit att viss gallring ska ske eller om det följer av en registerförfattning fattar myndigheten som förvarar handlingarna vanligtvis ett tillämpningsbeslut om löpande gallring.
[20] Se bland annat prop. 2016/17:180 s. 306.

e-underskrifter, e-stämplar och automatiserade behörighetskontroller. Bland annat behöver det beaktas om riskerna för skada är fördelade på ett ändamålsenligt sätt och om den digitala hanteringen har utformats så att straffrättsligt ansvar kan utkrävas i tillräcklig omfattning, jämför avsnitt 4.1. Vid automatiserad ärendehandläggning och automatiserat beslutsfattande behöver myndigheten också uppmärksamma behovet av att en ändamålsenlig dokumentation bevaras över ärendegången och att dessa förfaranden även i övrigt ger underlag för att följa upp och få insyn i ärenden, jämför avsnitt 4.9.

Det material som finns: Myndigheter har sedan lång tid erfarenheter från pappersmiljö av att bedöma juridiska risker för missbruk av den service som myndigheten tillhandahåller och för manipulationer av förvaltningsärenden. När denna hantering istället ska ske digitalt blir förutsättningarna emellertid delvis komplexa och svårtillgängliga för myndighetsföreträdare och andra som har att svara för att ett tillräckligt skydd införs. I praktiken brukar för den digitala miljön hänvisas till ett systematiskt arbete enligt standardiserade förfaranden för ledningssystem för informationssäkerhet (LIS). Detta ger dock bara begränsad vägledning för de rättsligt relaterade frågor som uppkommer. Förvaltningslagens kärna utgörs av grundläggande rättssäkerhetsgarantier som måste upprätthållas (se SOU 2010: 29 s. 121 och 131). Här blir begripligheten för användare en central fråga vid utformningen av digitala tjänster, jämför E-nämndens vägledning för användargränssnitt som uppfyller legala krav.

Gör så här: Överväg på motsvarande sätt som när hanteringen sker på papper vilka risker som mera allmänt uppkommer. Vidta lämpliga åtgärder för att ge skydd från informationssäkerhetssynpunkt genom bland annat e-legitimering och automatiserade behörighetskontroller. Utforma användargränssnitten så att de inte missförstås. Säkerställ att handlingar kommer fram så som det varit tänkt, utan att fel eller brister i digitala tjänster eller verksamhetssystem hindrar detta. Utför kontroller automatiserat av behörigheter och lämnade uppgifter när det behövs.

Följden av att en tillräcklig skyddsnivå inte upprätthålls kan exempelvis vara att individer utför rättshandlingar under sken av att vara någon annan, oriktigt förnekar sin underskrift eller får olovlig åtkomst till data. Rättsförluster kan också uppkomma till följd av att beslut fattas på grundval av felaktig information.

2.5 Vad ingår i en e-handling och vad ska bevaras (Att göra 5)

> Att göra 5: När en myndighet upprättar e-handlingar eller inför en digital tjänst där e-handlingar ges in behöver myndigheten utforma hanteringen så att det inte uppstår tvekan om vad som ingår i själva handlingen, vilka metadata (utanför handlingen) som blir till hos myndigheten och vad som måste bevaras för att bibehålla möjligheterna att söka, sammanställa och äkthetskontrollera handlingar.

När en myndighet planerar att hantera uppgifter digitalt krävs inte bara ändamålsenliga val av handlingsslag (exempelvis av e-original eller e-bestyrkta kopior) och val av skyddsnivåer för e-underskrifter och e-stämplar (exempelvis avancerade eller kvalificerade). Myndigheten måste också kunna skilja de komponenter som är en del av själva handlingen – t.ex. de uppgifter som ingår i en e-urkund – från data som utan att ingå i e-handlingen ger stöd för att använda den (till exempel vid sökning och sammanställning och vid prövning av om en handling är förfalskad eller annars manipulerad).

Allmänt om kraven: Frågan besvaras olika beroende på i vilket juridiskt sammanhang den väcks (exempelvis om en viss e-handling uppfyller ett formkrav eller om den kan vara en urkund eller ha avsedd bevisverkan i sig utan att stödjande material behöver åberopas). Även när frågor om offentlighetsinsyn och bevarande och gallring ska bedömas blir det av betydelse vad som ingår i en handling, respektive vad som ses som stödjande material utom handlingen. Här blir det också av betydelse om det är fråga om register eller färdiga handlingar i tryckfrihetsförordningens mening. Verksamhetens behov är avgörande för vilka handlingar som behöver upprättas (såsom föreläggganden eller beslut) eller samlas in av myndighet (såsom identitetsintyg och annat kontrollmaterial). Informationssystemens och infrastrukturers uppbyggnad bygger i allt högre grad på att vidhängande uppgifter upprättas om handlingar (s.k. metadata). Införs e-underskrifter och e-stämplar tillkommer vanligtvis kontrollmaterial i digital form eftersom äkthetskontroll alltid görs i it-miljö medan pappersurkunder sällan eller aldrig blir föremål för motsvarande kontroller.[21]

[21] Det kontrollmaterial som därvid uppkommer hos en myndighet har visat sig sällan bli använt. Bland annat har stora mängder data rörande underskrifter bevarats trots att de i praktiken aldrig används och knappast är av betydelse eftersom äktheten redan kontrollerats och dokumenterats.

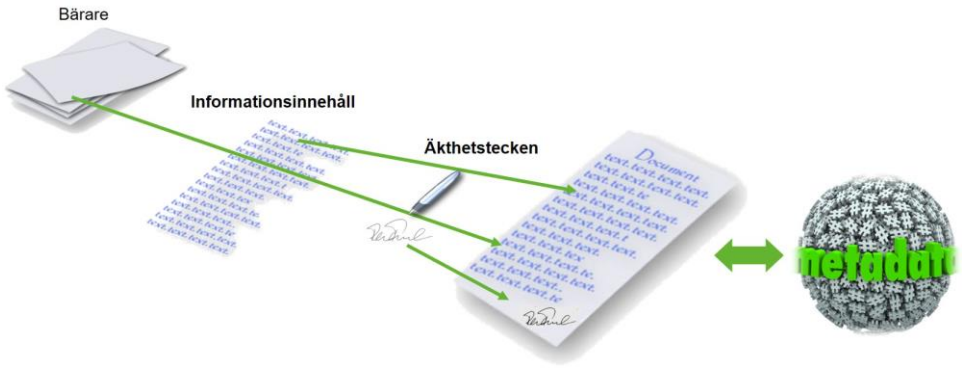
När myndigheten utformar en e-tjänst bör en lämplig säkerhetsnivå skapas redan genom utformningen av eget utrymme och det tekniska förfarandet. Handlingar som kommer in till myndighet måste enligt arkivförfattningarna bevaras i ursprungligt skick. Detta innefattar i vart fall två utmaningar. För att en otillåten gallring inte ska ske måste ett bevarande ske över tid av, dels de sök- och sammanställningsmöjligheter som finns, dels de tekniska möjligheter som skapats för att kontrollera en handlings äkthet.[22] De handlingar som myndigheten upprättar måste bevaras på motsvarande sätt. Utan att ett beslut om gallring har fattats i behörig ordning får alltså inga handlingar raderas, om de har blivit allmänna i tryckfrihetsförordningens mening och därmed arkiv-handlingar. Även en förfalskad handling ska således bevaras i ursprungligt skick om det inte finns ett gallringsbeslut.

Statliga myndigheter får normalt inte gallra utan att först ha fattat tillämpnings-beslut om gallring med stöd av antingen gallringsföreskrifter från Riksarkivet eller regler om gallring i registerförfattningar (se vidare avsnitt 4.3). Till Riks-arkivets gallringsföreskrifter hör föreskrifterna om gallring av allmänna handlingar av tillfällig eller ringa betydelse.

En beskrivning som underlättar förståelsen av vad som normalt är en del av själva handlingen finns i följande figur. Texten, tillhörande bilder eller liknande informationsinnehåll kan ses som en komponent (förklaringsinnehållet). En underskrift, en stämpel eller något annat äkthetstecken kan ses som en annan komponent. Dessutom finns en tredje komponent i form av en bärare där informationsinnehåll och äkthetstecken finns lagrade. Bäraren mister delvis sin betydelse i digital miljö. Detta beskrivs närmare i E-delegationens vägledning för elektroniska original, kopior och avskrifter.

[22] Här är det möjligheten som ska bevaras. Metadata kan i princip omvandlas till en annan typ av index i ett annat format, men handlingen som sådan ska bevaras i ursprungligt skick.

Figur 3: En beskrivning av vad som normalt är en del av själva handlingen



En handlings kontrollerbarhet, sökbarhet eller användbarhet brukar också stödjas av information som inte anses ingå i själva handlingen, exempelvis av uppgifter i diarier eller andra slag av metadata[23] med tillhörande strukturer, som kan bidra till besked bland annat om en handlings innehåll och utställare och ge underlag för kontroller av äkthet och en utställares juridiska behörighet eller annars för att automatisera ärendegång och beslutsfattande. Teoretiskt skulle den som skriver under en handling kunna ta del också av metadata och hantera metadata som en del av den information som han eller hon skriver under. Vanligtvis vet undertecknaren dock inte om att metadata har skapats och ser dem inte. Undertecknaren kan därmed knappast betraktas som utställare av dem.[24] Ett exempel på detta är hur de som undertecknar en årsredovisning och den som därefter skriver under ett fastställelseintyg i Bolagsverkets tjänst för årsredovisning normalt varken ser eller känner till att metadata skapats enligt en särskild syntax så att uppgifterna i senare led kan återanvändas helt automatiserat. Ansvaret för metadata bör klarläggas i de fall där en automatiserad process använder digitala metadata som undertecknaren av berörd handling varken ser eller förstår. Ett straff- eller skadeståndsrättsligt ansvar för undertecknaren kommer under sådana omständigheter knappast i fråga.

Vilket informationsinnehåll, vilka äkthetstecken och vilka metadata som från juridisk utgångspunkt anses ingå i själva e-handlingen och vilka metadata som ska tillföras utanför handlingen behöver således bedömas när en digital tjänst tas fram. Juristen ser naturligtvis texten och e-underskriften som nödvändiga delar av den handling som har skrivits under med till exempel en avancerad e-underskrift. Den som utgår från den tekniska hanteringen ser sannolikt även metadata i form av exempelvis tidsstämplar och den elektroniska underskriften

[23] Metadata brukar delas in i kategorierna beskrivande, administrativa, strukturella och användargenererade.
[24] Detta gäller även när e-underskriften omfattar vissa metadata.

(som ersätter pappersarkens funktion att hålla samman och avgränsa vad som är en handling) som en del av själva e-handlingen. Undertecknare vet knappast om att dessa tekniska data finns. Ett annat exempel är hur data som representerar själva underskriften tekniskt kan finnas antingen sammanslagen med data som representerar texten i ett särskilt filformat eller som en separat fil vidhängande den undertecknade handlingen. Oavsett teknisk lösning uppfattar juristen underskriften som en komponent i själva e-urkunden. Det behöver härvid ofta avgöras om det som är en del av själva handlingen respektive metadata bör arkiveras tillsammans eller delas upp mellan exempelvis ärendehanteringssystem respektive ett dokumentarkiv.

Olika bedömningar om vad som ingår i själva e-handlingen och vad som anses vara stödjande data utanför ramen för själva e-handlingen kan också göras beroende på vilket rättsområde som berörs. En ändring av metadata, för att byta tekniskt format i metadatahanteringen kan knappast utgöra en urkundsförfalskning när undertecknaren inte kunnat se dem vid granskningen inför underskrift. Däremot skulle en radering av metadata som hör till en handling kunna utgöra gallring av den, oberoende av om utställaren av handlingen känt till att dessa data tillförts.

Det finns bara ett begränsat material där beskrivna frågor tas upp på detaljnivå. Beträffande kraven på god offentlighetsstruktur, se eSams checklista för jurister, avsnitt 3, och SOU 2018:25. Se även avsnitt 4.3 med hänvisningar.

Gör så här: Se avsnitt 4.3 med hänvisningar, jämför avsnitt 4.1.

Följderna av att det inte klarlagts vad som ingår i en handling kan vara många, t.ex. att arkivförfattningarna inte följs, att det från offentligrättsliga eller straffrättsliga utgångspunkter inte står klart vem som ställt ut eller annars svarar för en uppgift eller att rättsförluster uppkommer för den som återanvänder och litar på en uppgift.

2.6 Eget utrymme och återanvändning (Att göra 6)

Att göra 6: En myndighet som inför eget utrymme behöver ge god service och skydda eget utrymme mot missbruk. Myndigheten bör också införa funktioner för att i eget utrymme återanvända uppgifter och handlingar från andra aktörer.

Med eget utrymme menas enligt en definition av E-delegationen ett skyddat förvar som tillhandahålls elektroniskt endast som led i teknisk bearbetning eller teknisk lagring för annans räkning. Ett sådant utrymme föreligger bara när handlingar som förvaras där är undantagna från handlingsoffentlighet enligt 2 kap. 13 § första stycket tryckfrihetsförordningen (TF). En första fråga vid införande av e-tjänster är ofta om de ska innehålla eget utrymme. Införs det ska myndigheten utforma eget utrymme så att endast användaren tar del av uppgifter i eget utrymme och att utrymmet inte missbrukas.

Behöver en myndighet ha styrkande handlingar från en annan myndighet, exempelvis ett registerutdrag, för att kunna handlägga ett ärende uppkommer frågan om användaren ska behöva vända sig till den andra myndigheten och begära ut en sådan handling för att sedan ge in den till den första myndigheten eller om denna hantering kan underlättas genom funktioner för återanvändning i eget utrymme. Samtidigt uppkommer frågan om användaren ska behöva fylla i alla uppgifter själv eller om kvalitetssäkrade uppgifter kan hämtas automatiserat till eget utrymme från den bästa källan för sådan information, se avsnitt 4.7.

Allmänt om kraven: När eget utrymme tillhandahålls ska handlingar i utrymmet behandlas endast som led i teknisk bearbetning och teknisk lagring för annans räkning och så att de inte anses ha kommit in till myndigheten enligt förvaltningslagen. I utrymmet kan myndigheten tillhandahålla stöd för att upprätta (förifylla) handlingar och för att kontrollera en handling innan den skickas till myndighetens mottagningsfunktion. Rättsläget har förtydligats i två lagstiftningsärenden år 2017 när det gäller hur eget utrymme förhåller sig till reglerna om handlingsoffentlighet och offentlighets- och sekretesslagens regler om tystnadsplikt. Där framgår att en myndighet kan tillhandahålla såväl en servicetjänst som en presentationstjänst där användares handlingar hanteras bara tekniskt i enlighet med 2 kap. 13 § första stycket TF. Regeringen har dock noterat att det saknas vägledande avgöranden som ger tydligt besked om vilka tjänster som uppfyller kraven för eget utrymme. E-sam har därför i en juridisk vägledning redovisat de krav som behöver uppfyllas.

Eget utrymme förenklar för användare genom den återanvändning av uppgifter som kan ske där. Ett informationsutbyte mellan myndigheter får inte äga rum i strid mot EU:s dataskyddsförordning, registerförfattningar eller offentlighets- och sekretesslagen. Ett utbyte bör inte heller äga rum om sådan åtkomst leder till att en myndighets handlingar blir allmänna hos en annan myndighet endast till följd av teknisk åtkomstmöjlighet (direktåtkomst). En möjlighet för en

användare att från eget utrymme begära en handling, från en annan myndighet än den som tillhandahåller utrymmet, bör därför utformas så att utlämnande sker på medium för automatiserad behandling (inte med direktåtkomst). På samma sätt behöver återanvändning i eget utrymme av grundläggande uppgifter (exempelvis fullständigt namn, folkbokföringsadress och vissa uppgifter om företag), hos andra myndigheter än den som tillhandahåller utrymmet, utformas i enlighet med reglerna om dataskydd och sekretess.

Det material som finns: Krav på eget utrymme: Regeringen har använt sig av begreppet eget utrymme i ett lagstiftningsärende genom vilket ett utökat sekretesskydd införts (se prop. 2016/17:198 s. 7) och förklarat att det finns stöd i rättspraxis för att myndigheter tillhandahåller digitala tjänster som uppfyller kraven i 2 kap. 10 § (numera 13 §) första stycket TF (a.prop. s. 16).[25] Samtidigt har regeringen noterat att det inte finns vägledande avgöranden som ger tydligt besked, i fråga om vilka av de egna utrymmen som myndigheter tillhandahåller, som uppfyller kraven enligt 2 kap. 13 § första stycket TF. Regeringen har även i motiven till den nya förvaltningslagen gjort uttalanden som ger stöd för en tolkning av 2 kap. 13 § TF anpassad till eget utrymme (se prop. 2016/17:180 s. 141 f., se även s. 7 eSams promemoria den 22 november 2017 Eget utrymme är numera accepterat i lagmotiv – men vilka juridiska krav ställs på eget utrymme?). Högsta förvaltningsdomstolen har därefter i HFD 2018 ref. 48 förklarat att rekvisitet ”endast” (förvaras som led i teknisk bearbetning eller teknisk lagring för annans räkning) för med sig att det bör krävas att myndigheten såväl administrativt som tekniskt har begränsat den egna personalens tillgång till uppgifterna så att dessa inte är tillgängliga i läsbart skick. Myndighetens personal ska enbart kunna ta del av den drifts- och säkerhetsrelaterade informationen.

I juridisk vägledning för verksamhetsutveckling inom e-förvaltning har eSam redovisat de krav som bör ställas på sådant utrymme (s. 12 ff.). eSam har också tagit upp huruvida kontroller kan utföras i eget utrymme som en service utan att det anses att handlingar som kontrolleras är inkomna till myndighet eller annars föremål för ärendehandläggning, se publikationerna Eget utrymme hos myndighet en vägledning (s. 14 och s. 23), juridisk vägledning för verksamhetsutveckling (s. 18, s. 36 och s. 54) samt ovan nämnd promemoria den 22 november 2017 om eget utrymme (s. 14).

[25] Regeringen fann vidare E-delegationens förslag mera ändamålsenligt än andra alternativ som framförts i remissvar över utredningsförslaget (a.prop. s 15 f. och s. 19).

Återanvändning av uppgifter: Dessa frågor och hur de bör lösas tas upp av eSam i Elektroniskt informationsutbyte – en vägledning för utlämnande i elektronisk form, Juridisk vägledning för verksamhetsutveckling inom e-förvaltning, Eget utrymme hos myndighet – en vägledning, och ett rättsligt uttalande den 22 november 2017 Eget utrymme hos myndighet, med tillhörande promemoria. Frågorna tas också upp i en juridisk vägledning av Bolagsverket, Skatteverket och Statistiska Centralbyrån för anslutning till infrastrukturen för vidareförmedling av grundläggande uppgifter om företag. Till detta kommer regelverk och dokumentation på Bolagsverkets webbplats beträffande den sammansatta bastjänsten för grundläggande uppgifter om företag (SSBTGU).[26] Ett intensivt utvecklingsarbete bedrivs för att ytterligare uppgifter ska kunna återanvändas. En fördel för den som tillhandahåller sådan återanvändning är att kvalitetssäkrade uppgifter tillförs eget utrymme som därefter ges in till myndighet.

Gör så här: Gå igenom de krav som behöver ställas på eget utrymme och se till att de uppfylls, bland annat att de skyddas mot att myndighetens handläggare bereder sig tillgång till eget utrymme eller att det missbrukas. Se till att föreskrifter och avtal är utformade så att myndigheten har rätt att omedelbart gallra nyttoinformation som oavsiktligt blivit allmän handling. Undersök om de tjänster som redan finns för att återanvända grundläggande uppgifter kan brukas också i en planerad ny tjänst och om de funktioner som redan införts av andra myndigheter för s.k. egen hämtning av intyg och liknande kan tas tillvara även i den nya digitala tjänsten.[27]

Följden om eget utrymme utformas felaktigt kan bli att enskildas information anses vara allmänna och offentliga handlingar, att utrymmesinnehavares privatliv kränks och att sekretessreglerade uppgifter blir tillgängliga för utomstående.

[26] Se http://bolagsverket.se/om/oss/samverkan/sammansatt-bastjanst/dokumentation-sammansatt-bastjanst-1.15560.
[27] Se Juridisk vägledningen för verksamhetsutveckling inom e-förvaltning, där egen hämtning beskrivs närmare.

3. Att ge in e-handlingar – bygg mottagning rätt

Tänk på att:

En funktion för digital mottagning, en så kallad mottagningsfunktion, gör det möjligt för enskilda att inleda ärenden digitalt, att kommunicera med myndigheten digitalt och att överklaga digitalt.

Det andra övergripande ledet i hanteringen av uppgifter för att etablera en helt digital förvaltning (se figur 1 i avsnitt 1.4) omfattar de funktioner som myndigheter tillhandahåller för att enskilda – ändamålsenligt och rättsenligt – ska kunna ge in handlingar i digital form. Frågan är hur en ansökan, en anmälan eller en annan framställning lämnas, hur ankomstdagen bestäms och hur anknytande kontroller och skydd för informationshanteringen säkerställs. Här ska myndigheten ge enskilda skydd mot missbruk och fel i hanteringen, i praktiken genom fungerande funktioner för mottagning.

Handlingar kan ges in till en digital mottagningsfunktion som kan, men inte behöver, vara knuten till en viss digital tjänst eller ett eget utrymme. Vanligtvis inleds ärenden genom en ansökan, en anmälan eller en framställan (19 § FL). En mottagningsfunktion kan också användas i ett ärende, efter ett föreläggande att avhjälpa en brist (20 § FL) eller att bekräfta vem som har avsänt en handling (21 § FL), eller för att ta emot yttranden från annan myndighet eller enskild (26 § FL) eller överklaganden (43 § FL).

3.1 Endast digital mottagning (Att göra 7)

Att göra 7: En myndighet bör klargöra om det är möjligt att för berörda ärendeslag utforma hanteringen så att handlingar endast tas emot digitalt och bara via kanaler som uppfyller tillräckliga krav på insynsskydd och integritetsskydd.

När en myndighet inför e-tjänster och andra funktioner där uppgifter ska kunna ges in uppkommer frågan om det är möjligt att begränsa kontaktvägarna för berörda ärendeslag till att myndigheten tar emot information digitalt och muntligt. Det bör vidare övervägas om myndigheten får sluta att använda digitala kommunikationskanaler som inte uppfyller tillräckliga krav på insynsskydd och

integritetsskydd, exempelvis att sluta motta meddelanden via telefax och e-post.[28]

Allmänt om kraven: Såväl verksamhetens behov av att hantera all information i digital form som användarnas befogade krav på att kunna kommunicera enkelt med myndigheten behöver beaktas när en funktion för att ta emot uppgifter och handlingar övervägs. Målet bör vara en obligatorisk digital hantering, men vissa alternativa vägar kan behövas så att alla medborgare och företag har möjlighet att smidigt kommunicera med myndigheten.[29] I vissa fall är hanteringen redan nu utformad så att det är obligatoriskt att använda digitala kanaler (till exempel i ärenden hos Skatteverket om ROT och RUT eller hos Bolagsverket om registrering av verkliga huvudmän). Användningen av en viss digital kanal kan emellertid också vara frivillig så att alternativ finns för dem som är förhindrade att kommunicera digitalt eller av olika skäl inte vill godta det utpekade förfaringssättet. eSam har av effektivitetsskäl rekommenderat en obligatorisk användning av digitala tjänster, men samtidigt erinrat om att en proportionalitetsbedömning behöver göras där myndigheten tar hänsyn till andra faktorer. Detta leder många gånger till att även sådana rutiner som telefonsamtal och personliga besök behöver erbjudas som kontaktväg.

Vid dessa val måste myndigheten följa den särreglering som gäller för berört område, såsom registerförfattningar och särskilda föreskrifter om förfarandet. Det finns emellertid också generella regler i 5 § FL om proportionalitet och i 8 kap. 2 § första stycket 2 regeringsformen om att så kallade betungande föreskrifter ska meddelas genom lag. Kravet på proportionalitet kan behöva tillämpas så att de digitala rutinerna kompletteras med kompenserande åtgärder för grupper som behöver särskild service, exempelvis via servicekontor eller telefon.

Beträffande de krav som finns i regeringsformen på att reglera vissa frågor på lagnivå har eSam däremot gjort den bedömningen att själva skyldigheten för den enskilde eller ingreppet ska meddelas i form av lag medan sättet att utföra det (exempelvis i digital form) normalt inte blir att anse som betungande i regeringsformens mening. Möjligen har regeringen gjort samma bedömning när den i förordning har beslutat att göra elektronisk ansökan obligatorisk för vissa fall. Av 1 kap. 9 § regeringsformen följer vidare att en myndighet i sin verksamhet ska agera sakligt och opartiskt. Det innebär bland annat att digitalt anhängiggjorda ansökningar inte får gynnas i förhållande till de som gets in på

[28] Lägg märke till behovet av att från alla brevmallar och liknande ta bort en adress som utmönstrats.
[29] eSams vägledning Rättsliga förutsättningar för digitalt i första hand (s. 13).

papper, bara för att stimulera att en digital kanal används. Det strider dock inte mot saklighetskravet att digitalt anhängiggjorda ansökningar ofta kan handläggas och avslutas snabbare.

Genom förvaltningslagen (2017:900) har regler i den gamla förvaltningslagen om att myndigheter måste kunna ta emot e-post och telefaxmeddelanden utmönstrats. Det föreskrivs numera (se 7 §) bara att en myndighet ska vara tillgänglig för kontakter med enskilda och informera allmänheten om hur och när sådana kan tas, samt att myndigheten ska vidta de åtgärder i fråga om tillgänglighet som behövs för att den ska kunna uppfylla sina skyldigheter gentemot allmänheten enligt 2 kap. tryckfrihetsförordningen om rätten att ta del av allmänna handlingar.

Vissa domstolar har därför redan utmönstrat telefax som kommunikationsväg och det har diskuterats om en myndighet bör avstå från e-post som saknar skydd mot olovlig insyn och istället erbjuda andra liknande men säkrare kontaktvägar.

Det material som finns: Stöd finns för att bedöma dessa frågor i en vägledning av eSam, Rättsliga förutsättningar för digitalt i första hand. eSam har också i Svenskt ramverk för digital samverkan (avsnitt 3.3.1) rekommenderat, dels att offentliga organisationer som huvudalternativ ska erbjuda tjänster till privatpersoner och företag via digitala kanaler, dels att det digitala alternativet ska vara det enda alternativet där en sådan hantering inte skapar utanförskap inom målgrupperna för tjänsten.

Gör så här: När det inte finns hinder i särreglering som gäller för berört område, såsom registerförfattningar och särskilda föreskrifter om förfarandet, bör myndigheten överväga vilka kategorier av användare som kan förväntas använda tjänsten (medborgare eller företag, unga eller gamla, grupper med särskilda behov etcetera), vilka risker som kan finns för rättsförluster vid digital respektive traditionell mottagning och vilka alternativa vägar som framstår som ändamålsenliga. Även när föreskrifter om visst förfarande eller visst skydd saknas behöver ett tillräckligt utrymme finnas för att i de undantagssituationer som uppkommer kunna förfara så att rättsförluster inte uppkommer för enskilda. – Sträva efter att utmönstra telefax och osäker e-post. Av Svenskt ramverk för digital samverkan (avsnitt 3.3.1) framgår bland annat att offentliga organisationer behöver utreda om det finns behov av ett möte med aktuell målgrupp eller om digitaliseringens möjligheter gör att arbetet kan ske på annat sätt. Av ramverket följer vidare att offentliga organisationer bör utgå från att

ett digitalt alternativ är huvudregeln för möten med privatpersoner och företag och att digitalt ska vara enda alternativet där det inte skapar utanförskap.

Följderna av att en myndighet felaktigt begränsar sin analoga tillgänglighet kan bli att enskilda berövas den rätt att kommunicera med myndighet som följer av förvaltningsrätten och att rättsförluster uppkommer till följd av att handlingar inte anses ha nått myndigheten inom en angiven frist.

3.2 Finns en ändamålsenlig funktion för mottagning (Att göra 8)?

> Att göra 8: En myndighet behöver ta reda på om den redan har en mottagningsfunktion som ger ändamålsenligt stöd för att adressera och skicka handlingar till myndigheten.

Myndigheter har vanligtvis redan funktioner för digital mottagning av meddelanden och på ett övergripande plan tas meddelanden emot och registreras på samma sätt. Det kan dock finnas tekniska skillnader mellan dem. Skillnaderna har i många fall sin grund i att olika format och säkerhetslösningar används och att vissa funktioner lämnar kvittens. Myndigheten behöver ta reda på om det redan finns ändamålsenliga funktioner för att adressera meddelanden i eget utrymme och att ta emot de meddelanden som ges in digitalt.

Allmänt om kraven: De krav som behöver ställas på en mottagningsfunktion följer dels av hur e-handlingar färdigställs och adresseras och av hur eget utrymme fungerar (se kap. 2), dels av de kontroller och registreringar som behövs när en handling kommer in (se kap. 4). Ansökningsförfaranden kan ofta ses som dialoger mellan enskilda och automatiserade funktioner hos myndigheter. Efter en säker inloggning startar flöden där information presenteras, frågor ställs och kontroller sker automatiserat i takt med att enskilda fyller i, väljer bland olika alternativ eller får information förifylld. Därefter skickas uppgifter och landar exempelvis i olika tabeller i en databas. Från juridiska utgångspunkter anses en e-handling komma in till en mottagningsfunktion. All information från den dialog som skett exempelvis i eget utrymme ges dock inte in och bevaras.

Det material som finns: Frågan om ändamålsenliga funktioner redan finns har inte uttryckligen berörts i eSams vägledningar.

Gör så här: Undersök om det finns ändamålsenliga funktioner för att adressera meddelanden och om befintliga mottagningsfunktioner uppfyller de krav som redovisas i eSams vägledningar, se nästa avsnitt. Sträva efter att återanvända, samordna och skapa enhetliga former för adressering och mottagning (jämför kap. 5).

Följderna av en bristande samordning kan bli att en flora av olika kostnadsdrivande förfaranden breder ut sig samtidigt som variationer i förfarandet leder till en rättslig osäkerhet för myndigheter och enskilda.

3.3 Mottagningsfunktionen ska vara rätt utformad (Att göra 9)

> Att göra 9: En myndighet behöver utforma sin mottagningsfunktion så att de risker och tolkningssvårigheter som eSam har beskrivit rörande inkommande handlingar minimeras. Om funktionen utkontrakteras måste den göras förenlig med bland annat reglerna om sekretess och dataskydd.

Det behöver bedömas från juridiska utgångspunkter när en handling har kommit in till en myndighet, och vem som står risken under överföringen till myndighetens mottagningsfunktion. Om funktionen utkontrakteras måste det säkerställas att uppgifter som är sekretessbelagda inte röjs för utomstående.

Allmänt om kraven: Gällande rätt innebär normalt att en e-handling har kommit in till myndighet den dag som den når den funktion där myndigheten tar emot sådana handlingar. Avsändaren står risken för att en försändelse inte når fram till mottagningsfunktionen. De regler som införts genom förvaltningslagen (2017:900; FL) medför dock vissa tolkningssvårigheter. eSam har beskrivit dem och hur de kan minimeras.

Stöd finns för att bedöma dessa frågor: I en vägledning från år 2005 för hantering av inkommande elektroniska handlingar gjorde Nämnden för elektronisk förvaltning (E-nämnden) tolkningar av 10 § i den gamla förvaltningslagen (1986:223). Myndigheterna har i allt väsentligt anpassat sina tekniska system för att följa vägledningen från är 2005. De tolkningsfrågor som paragrafen om ankomstdag i 22 § förvaltningslagen (2017:900) har fört med sig har tagits upp av eSam i en juridiska vägledningen för verksamhetsutveckling inom e-förvaltningen (se där s. 9 fotnot 9, s. 11 och s. 20) och närmare utvecklats av eSam i ett rättsligt uttalande den 26 oktober 2017 om ankomstdag för e-handlingar

och en bakomliggande promemoria om när en handling har kommit in till myndighet. E-nämndens och eSams tolkningar har stärkts genom lagförslag av Förvaltningslagsutredningen (SOU 2010:29). De har emellertid inte lett till lagstiftning. Därefter har Digitaliseringsrättsutredningen på nytt i princip lagt fram samma lagförslag som Förvaltningslagsutredningen (SOU 2018:25 s. 36). Se även eSams checklista för jurister, avsnitt 5.1.2 och hänvisningar där.

Frågor om sekretess och utkontraktering har berörts av eSam i Outsourcing – en vägledning om sekretess och persondataskydd och i rättsliga uttalanden den 17 december 2015 om röjandebegreppet enligt offentlighets- och sekretesslagen och den 23 oktober 2018 om röjande och molntjänster.

Gör såhär: Se till att de funktioner som införs är tillräckligt säkra och skapar sådana registreringar av inkommandetidpunkten att varken enskilda eller det allmänna riskerar att drabbas av rättsförluster. Anpassa tjänsten till E-nämndens och eSams rekommendationer i vägledningar, se ovan. Beakta att enskilda måste ges ett tillräckligt skydd när tekniska eller administrativa fel uppstår.

Följderna av en felaktigt utformad mottagningsfunktion kan bli en rättslig osäkerhet för såväl myndigheten som enskilda och i värsta fall rättsförluster för dem.

3.4 Automatiserade kontroller (Att göra 10)

> Att göra 10: En myndighet bör förlägga automatiserade kontroller och annat stöd till eget utrymme, så att dessa kan användas för att kontrollera materialet innan det skickas från eget utrymme. Myndigheten behöver även se till att funktionerna för att ta emot handlingar är driftsäkra och felsäkra, så att enskilda inte drabbas av rättsförluster till följd av att handlingar inte kan mottas av myndigheten.

Om e-handlingar felaktigt fastnar i filter mot skräppost och skadlig kod eller i funktioner för att kontrollera att rätt tekniska format används kan rättsförlust uppkomma för avsändare eller mottagare. Frågan är hur dessa risker kan undgås.

Allmänt om kraven: Gällande rätt innebär att eget utrymme kan utformas så att kraven i 2 kap. 13 § (tidigare 10 §) första stycket TF uppfylls (prop. 2016/17:198 s. 16). Genom att förlägga dessa kontroller till utrymmet, erbjuda dem som en helt automatiserad service åt innehavaren och bara utföra

kontroller på material som inte har skickats därifrån (det vill säga inte har lämnat utrymmet och kommit in till myndighet enligt förvaltningslagen eller tryckfrihetsförordningen) uppstår inte allmänna handlingar. Uppgifter som hanteras i utrymmet anses inte heller vara inkomna enligt förvaltningslagen, se närmare avsnitt 2.6 och HFD 2018 ref. 48. När en handling har skickats och kontroller utförs därefter men innan handlingen nått mottagningsfunktionen är rättsläget mera osäkert. Risken för att en försändelse inte kommer fram stannar dock normalt på avsändaren till dess försändelsen når mottagningsfunktionen.

Det material som finns: Se avsnitt 2.6 ovan.[30]

Gör så här: Förlägg automatiserade kontroller och annat stöd till eget utrymme, det vill säga till material som inte har skickats därifrån. Se till att funktionerna för att ta emot handlingar är driftsäkra och felsäkra[31] så att enskilda inte drabbas av rättsförluster till följd av att handlingar som skickats fastnar i kontroller eller annars inte kan mottas av myndigheten i mottagningsfunktionen.

Följderna av att automatiserade kontroller införs efter det att en handling skickats från eget utrymme men innan den nått mottagningsfunktionen kan bli att handlingen anses inkommen redan innan den nått mottagningsfunktionen, om kontrollerna ges en utformning som kan ses som ett normalt led i en ärendehandläggning.

3.5 Olika exemplar av handlingar hos olika innehavare (Att göra 11)

Att göra 11: En myndighet bör utforma uppgiftshanteringen så att det tydligt går att skilja mellan exemplar av en e-handling som finns i eget utrymme respektive i en mottagningsfunktion eller i ett verksamhetssystem hos myndigheten. Säkerställ att det som finns i eget utrymme inte blir tillgängligt för myndighetens personal eller på annat sätt allmän handling. Utrymmet ska vara privat.

[30] E-nämnden har tidigare berört dessa frågor i sin vägledning från år 2005 för hantering av inkommande elektroniska handlingar.
[31] Med felsäker menas här att när ett fel inträffar försätts funktionen i ett felsäkert läge så att rättsförlust inte behöver uppkomma.

Det uppstår olika digitala exemplar av en e-handling när den upprättas, skickas, mottas och hanteras i verksamhetssystem. Frågan är hur detta ska hanteras.

Allmänt om kraven: I eSams juridiska vägledning för verksamhetsutveckling inom e-förvaltning redovisas hur ett och samma informationsinnehåll i form av en e-handling kan finnas både i eget utrymme (utan att vara allmän handling där), och i myndighetens verksamhetssystem (som allmän handling där), efter att ett exemplar av handlingen har skickats till myndighetens mottagningsfunktion. Myndigheten behöver kunna skilja mellan olika exemplar av handlingar för att hantera dem korrekt.

Det material som finns: E-delegationen har i ett av sina betänkanden anfört att en handlings status hos en myndighet ska kunna växla över tid och att detta föranlett ett nytt andra stycke i 2 kap. 13 § TF så att en handling inte är att anse som allmän när den förvaras endast i syfte att kunna återskapa information som har gått förlorad i en myndighets ordinarie system för automatiserad behandling (se vidare SOU 2014:39 s. 49 ff.).[32] På samma sätt ska ett exemplar av en handling kunna särskiljas från ett annat exemplar, med samma eller annat innehåll, som myndigheten förvarar i en annan teknisk och administrativ kontext, till exempel ett exemplar av en handling i eget utrymme respektive ett exemplar som har överförts till myndighetens elektroniska mottagningsställe och vidare till myndighetens verksamhetssystem; jämför att en sökande kan ge in en ansökan på papper till en myndighet men ha kvar en kopia hos sig. De olika handlingarna ska från offentlighetssynpunkt bedömas var för sig.

Gör så här: Utforma hanteringen så att det tydligt går att skilja mellan exemplar av en e-handling som finns i eget utrymme respektive det som finns i en mottagningsfunktion eller i ett verksamhetssystem hos myndigheten. Säkerställ att eget utrymme har utformats så att de exemplar som finns där inte blir allmän handling och att utrymmet rensas när handlingarna inte längre behöver finnas där. Utforma tydliga regler för egna utrymmen så att rensning inte kan leda till att myndigheten anses utföra olovliga åtgärder med enskildas nyttoinformation.

Följderna om myndigheten inte kan skilja mellan dessa olika exemplar kan bli att privata handlingar hanteras som allmänna, att allmänna handlingar undan-

[32] Bakgrunden var den att Uppgiftslämnarutredningen hävdat att det inte skulle finns legalt utrymme för att ”isolera” ett tekniskt delmoment under den tid en handling förvaras hos en myndighet och betrakta detta separat – undantaget i 2 kap. 13 § TF skulle ta sikte på hela den tid som myndigheten förvarar en handling (SOU 2013:80 s. 150 ff.). Regeringen har emellertid i lagmotiv funnit att eget utrymme kan utformas så att kraven i 2 kap. 13 § (tidigare 10 §) första stycket TF uppfylls (prop. 2016/17:198 s. 16).

hålls offentligheten trots att de inte är sekretessreglerade eller att befattningshavare tar del av handlingar som de inte får läsa eller använda samt att regler om arkiv inte följs.

3.6 Skanning och gallring (Att göra 12)

> Att göra 12: En myndighet som skannar pappershandlingar behöver klargöra om förlagan som skannats in får gallras (efter gallringsbeslut) eller om såväl de digitala exemplaren som de på papper samt alla kontrolldata måste bevaras viss tid. Om skanningsfunktionen utkontrakteras krävs det att den görs förenlig med reglerna om sekretess och dataskydd.

Hur ska en myndighet kunna digitalisera hela sitt informationsflöde när handlingar kommer in även på papper? Får s.k. ersättningsskanning ske – det vill säga att pappersoriginalen gallras efter att de skannats – eller måste myndigheten bevara såväl de digitala exemplaren som de på papper och alla data från kontrollerna när skanning skett?

Allmänt om kraven: När myndigheter inför digitala tjänster eller väljer att digitalisera sin dokumenthantering kan det visa sig att även pappershandlingar hos myndigheten behöver digitaliseras om det ska föras helt digitala akter (e-akter). Så länge grundläggande krav enligt EU:s dataskyddsförordning, registerförfattningar och arkivförfattningarna uppfylls finns det normalt inte hinder mot att skanna pappershandlingar för att myndighetens personal smidigt ska kunna ta del av dem via bildskärm. Får det pappersbaserade materialet inte gallras blir det emellertid inte möjligt att införa enbart digitala arkiv (e-arkiv) och därmed en papperslös myndighet.

Enligt arkivförfattningarna ska de allmänna handlingar som upprättas eller ges in bevaras i ursprungligt skick. De får inte raderas utan gallringsbeslut.[33] Detta innefattar två utmaningar. För att gallring inte ska anses ha skett utan erforderligt gallringsbeslut måste bevarande ske över tid även av de tekniska sök- och sammanställningsmöjligheter som myndigheten har och de tekniska möjligheter som myndigheten har att bedöma om handlingarna har ställts ut av angiven utställare.[34] På ett tidigt stadium behöver myndigheten klargöra om handlingen får gallras enligt befintligt regelverk (får myndigheten besluta om

[33] Även en falsk handling ska bevaras i ursprungligt skick om det inte finns ett gallringsbeslut.
[34] Samtidigt bör myndigheten uppmärksamma om gallring kan ske av underskrivna pappershandlingar efter att de har skannats utan att detta leder till ett alltför svagt material vid en tvist där myndigheten behöver åberopa skriftligt bevis.

gallring på grund av att berörda handlingar anses vara av tillfällig eller ringa betydelse eller krävs en framställning till Riksarkivet om att få gallra, jämför avsnitt 2.5, 4.3 och 4.4).

Skanning utförs ofta av en tjänsteleverantör som myndigheten har anlitat. Frågor om sekretess och utkontraktering har berörts av eSam i Outsourcing – en vägledning om sekretess och persondataskydd och i rättsliga uttalanden den 17 december 2015 om röjandebegreppet enligt offentlighets- och sekretesslagen och den 23 oktober 2018 om röjande och molntjänster.

Det material som finns: Frågan om ersättningsskanning har inte uttryckligen tagits upp i eSams vägledningar. Den verkar inte heller ha blivit närmare genomlyst i annat sammanhang med sikte på att kunna undanröja hinder mot papperslösa myndigheter.

Gör såhär: När myndigheten skannar pappershandlingar behöver det klargöras om förlagan får gallras (efter gallringsbeslut) eller om såväl de digitala exemplaren som pappersexemplaren och alla kontrolldata måste bevaras. Om skanningsfunktionen utkontrakteras måste hanteringen göras förenlig med reglerna om sekretess.

Följderna om gallringsfrågan inte tas på allvar blir antingen ett kostsamt, onödigt bevarande eller att handlingar förstörs i strid mot arkivförfattningarna. Blir sekretessfrågan felaktigt hanterad kan det resultera i ett otillåtet, kanske straffbart, röjande.

4. Att handlägga ärenden – bygg verksamhetssystem rätt

Tänk på att:

Funktioner i verksamhetssystem gör det möjligt att i digital form handlägga ärenden och i övrigt hantera information som har kommit in eller upprättats.

Det tredje övergripande ledet (se figur 1 i avsnitt 1.4) i hanteringen av uppgifter för att etablera en helt digital förvaltning omfattar de funktioner som myndigheter inför för sin interna hantering av digital information. Myndighetens verksamhetssystem används vid ärendehandläggning, för att bereda ärenden och fatta beslut i dem. Digital information kan också hanteras i verksamhetssystem vid så kallat faktiskt handlande.

Ofta utgör digital information i ett verksamhetssystem handlingar som har färdigställts i eget utrymme, getts in via en digital mottagningsfunktion eller expedierats digitalt. Verksamhetssystem innehåller också handlingar som myndigheten själv har hämtat in eller upprättat inom ramen för ett ärende. Informationshantering omfattar således e-handlingar som inlett ärende (19 § FL), som myndigheten upprättat själv eller som producerats som led i kommunikation med part i ärende eller till följd av kommunikation med annan myndighet eller annan enskild (exempelvis dokumentation, förelägganden, remisser och svar som inkommit). Myndighetens beslut kan också förvaras i verksamhetssystem (se vidare 20, 21, 23–26 och 28 §§ FL). Olika krav på granskning och kontroll av handlingar aktualiseras när e-handlingar har kommit in till myndighet respektive har upprättats av myndigheten.

4.1 Äkthetskontroll och stämpling (Att göra 13)

Att göra 13: En myndighet behöver äkthetskontrollera inkomna e-handlingar i enlighet med den skyddsnivå som myndigheten har bestämt samt bevara dem i ursprungligt skick enligt arkivförfattningarna, skyddade med exempelvis en e-stämpel.

När e-handlingar som har skrivits under eller annars kan kontrolleras kommer in till en myndighet genomförs en äkthetskontroll genast. Detta skiljer sig från pappersmiljö där en närmare granskning för att upptäcka manipulerade

handlingar enbart sker om en handlings äkthet har ifrågasatts. Myndigheten måste också göra identitetskontroller, när endast e-legitimering sker vid uppgiftslämnande, och behörighetskontroller, när digitala rollintyg eller annan automatiserad behörighetskontroll äger rum. Beträffande dessa frågor hänvisas till eSams Juridiska vägledning för införande av e-legitimering och e-underskrifter.

Allmänt om kraven: En myndighet som har digitaliserat varje led i informationsflödet har redan valt och infört en lämplig skyddsnivå, se avsnitt 2.3 (Att göra 3). Om myndigheten har skäl att göra ytterligare kontroller kan en begäran enligt 21 § FL riktas till den som har angetts som utställare om att bekräfta huruvida handlingen kommer från honom eller henne. Myndigheten behöver också beakta de risker som mera allmänt finns från rättssäkerhetssynpunkt och vidta nödvändiga åtgärder för att hindra eller motverka rättsförluster för enskilda och det allmänna, jämför avsnitt 2.4 (Att göra 4). Hit hör att säkerställa att e-handlingarna bevaras oförändrade – i ursprungligt skick, jämför avsnitt 2.5 (Att göra 5). Myndigheten behöver dessutom bedöma vad som ska bevaras och vad som får gallras samt avskilja och ta bort det som från tid till annan ska gallras (jämför avsnitt 3.6 och 4.3).

Lägg märke till att leverantörer av underskriftstjänst vanligen också gör en kontroll av vem som har legitimerat sig för att skriva under en handling och levererar ett intyg där kontrollresultatet framgår. Reglerna om arkiv gäller först när en handling kommit in till eller upprättats av myndighet, det vill säga inte i eget utrymme eftersom sådant utrymme ska vara utformat så att de handlingar som finns där är privata.

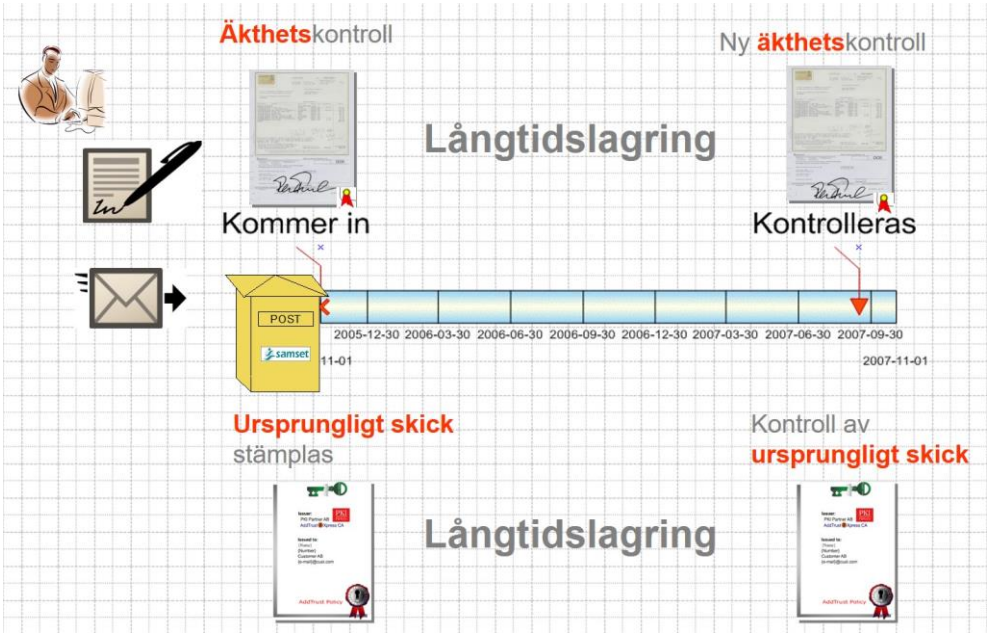
Det material som finns: Frågor om äkthetskontroll och stämpling behandlas i eSams juridiska vägledning för införande av e-legitimering och e-underskrifter (se bland annat avsnitt 3.3 och kap. 5). För området finns regler i eIDAS-förordningen.[35] Se även Riksarkivets beskrivning i sin rapport från år 2005, Elektroniskt underskrivna handlingar, av de olika kontrollmöjligheter som ges beroende på vad som bevaras, samt eSams checklista för jurister, avsnitt 3.1.2, 4.2.1 och 5.1.2.

Gör så här: Undersök vilka äkthetskontroller som en leverantör av underskriftstjänst gör åt myndigheten, vad som över tid bevaras[36] och av vem, så att

[35] Kap. 5 i E-nämndens vägledning från år 2005 för hantering av inkommande elektroniska handlingar kan också vara av intresse.
[36] Här kan bland annat utfärdarcertifikat behöva bevaras för att myndigheten ska kunna äkthetskontrollera underskriften utan leverantörens inblandning.

nödvändiga kontroller kan göras av en handlings äkthet. Utarbeta instruktioner och beskrivningar så att myndighetens handläggare kan förstå vilka kontrollmöjligheter som finns och hur de i praktiken brukas. Överdriv inte kontrollerna. I pappersmiljö utförs inget av detta på förhand.[37] Det finns få exempel på att e-underskrivna eller e-stämplade handlingars äkthet har ifrågasatts. När en myndighet väljer hur den ska lösa dessa frågor är det lämpligt att utgå från följande två alternativ (se figuren nedan). Utgångspunkten är att en e-underskriven handling nått myndighetens mottagningsfunktion och äkthetskontrollerats, normalt med stöd av en leverantör av identitetsintyg som redan gjort en äkthetskontroll. Ska myndigheten bygga sin långtidslagring av handlingen på att göra en ny äkthetskontroll när detta efterfrågas (se det övre alternativet i figuren) eller ska handlingen vid mottagandet, efter gjorda kontroller, förses med en e-stämpel (se det nedre alternativet i figuren)? Genom att lita på en e-stämpel, där det intygas att en äkthetskontroll redan har gjorts och genom vilken informationsinnehållets ursprungliga skick säkerställs, behövs ingen ny äkthetskontroll baserad på det ursprungliga kontrollmaterialet. Det räcker att kontrollera e-stämpeln när en ny kontroll efterfrågas.

Figur 4: Ska underskriften eller en stämpel utgöra kontrollunderlag på sikt



[37] Riskerna i de digitala miljöerna ser dock annorlunda ut. Att obehöriga smyger in obemärkta och manipulerar handlingar i myndigheters arkiv är långsökt. I den elektroniska miljön är ett obemärkt intrång inte lika osannolikt. När kontroller kan utföras automatiserat kompenserar det för den förändrade hotbilden jämfört med en pappersbaserad hantering.

När detta val övervägs aktualiseras också övriga frågor om hur en handlings äkthet ska kunna bevisas, exempelvis i en rättegång, och hur omfattande material myndigheten bör bevara. Se till att myndighetens avtal med leverantör av underskriftstjänst och leverantörer av identitetskontroll är utformade så att myndigheten kan få tillgång över tid till de uppgifter som behövs för en äkthetsprövning. Se samtidigt till att leverantörer inte lämnar onödigt material till myndigheten eller gör material som inte behövs tillgängligt via tekniska gränssnitt eftersom det då blir allmän handling hos myndigheten och i så fall måste bevaras eller – om behörig myndighet beslutat om det – gallras (se vidare avsnitt 4.3). Vid denna bedömning av vilket material som behövs är det lämpligt att granska om berörda ärendeslag eller typer av handlingar varit föremål för någon tvist rörande äkthet eller om äkthetskontroller annars efterfrågats över tid.

Följder av brister i kontrollförfarandet eller i bevarandefunktioner för e-underskrifter, e-stämplar och intyg över utförda kontroller kan vara att en handlings äkthet på sikt inte kan styrkas. Tvister om handlingars äkthet är dock ovanliga hos myndigheter och om omfattande loggar och liknande material bevaras över tid kan detta visa sig strida mot EU:s dataskyddsförordning eller reglerna i 2 kap. 6 § andra stycket regeringsformen om förbud mot övervakning eller kartläggning av enskildas personliga förhållanden.

4.2 Registrering och god offentlighetsstruktur (Att göra 14)

> Att göra 14: En myndighet behöver anpassa både sin beskrivning av handlingar och sitt system för att registrera och söka fram handlingar till en digital hantering från ax till limpa där föreskrivna krav på arkiv och handlingsoffentlighet beaktas och upprätthålls.

Myndigheten är skyldig att upprätta en beskrivning av sina allmänna handlingar och normalt även att registrera dem och vidta andra åtgärder för att göra det enkelt att söka fram och använda handlingar.

Allmänt om kraven: Inkommande handlingar ska enligt en huvudregel i 5 kap. 1 § offentlighets- och sekretesslagen (2009:400; OSL) registreras så snart de har kommit in till en myndighet (första stycket). Handlingar som inte omfattas av sekretess behöver emellertid enligt samma paragraf inte registreras om de hålls ordnade så att det utan svårighet kan fastställas om en handling har kommit in

(tredje stycket). Till detta kommer en särskild regel för handlingar av ringa betydelse för myndighetens verksamhet. De behöver varken registreras eller hållas ordnade (fjärde stycket). Det som en handläggare direkt kan ta fram och läsa i ett verksamhetssystem får normalt antas vara handlingar som är relevanta för ärende.[38] När e-underskrifter och e-stämplar används skapas dock också digitala data som är till endast för äkthetskontroll. Sådan data får till övervägande del antas ha ett sådant innehåll att en granskning normalt sker av experter. Dessa handlingar torde inte diarieföras sedda för sig. Det återstår sannolikt arbete för att kunna skapa en god offentlighetsstruktur bland dessa data.

Även i arkivlagstiftningen finns regler som ska tillämpas vid registrering. Enligt 5 § arkivlagen (1990:782) ska myndigheterna vid registreringen av allmänna handlingar ta vederbörlig hänsyn till handlingens betydelse för en ändamålsenlig arkivvård och vid framställningen av handlingar använda materiel och metoder som är lämpliga med hänsyn till behovet av arkivbeständighet. I 6 § samma lag finns vidare regler om arkivvård och arkivförteckning. Dessa regler och de i OSL överlappar varandra. Som exempel kan nämnas hur en myndighet kan ha att föra (a) en arkivbeskrivning, (b) en registerförteckning (som ska omfatta såväl personuppgiftsbehandlingar enligt EU:s dataskyddsförordning som system med elektroniska allmänna handlingar) samt (c) en arkivförteckning (som mer detaljerat redovisar uppgifter om handlingsslag, enligt en så kallad klassificeringsstruktur). Myndigheten kan dessutom ha att (d) uppfylla långtgående krav på systemdokumentation i RA-FS 2009:1 om handlingarna ska bevaras för lång tid.

Bestämmelserna ger en viss frihet att ordna registreringen efter vad som är lämpligast för den enskilda myndigheten. Något krav på central registrering finns inte i OSL. Det står myndigheterna fritt att föra speciella register, till exempel för viss del av verksamheten eller för vissa typer av handlingar; jämför att det för pappersmiljö många gånger kan vara fullt tillräckligt att nödvändiga anteckningar om handlingarna görs t.ex. på omslaget till den akt där handlingarna förvaras, på ett dagboksblad eller i en liknande innehållsförteckning till akten (jämför JO 1991/92 s. 124). Liknande förenklingar kan tänkas för exempelvis kontrolldata. Den metod som tillämpas bör emellertid användas konsekvent (JO 1995/96 s. 485).

[38] I 5 kap. 2 § OSL ges detaljerade regler om vad som ska framgå beträffande varje handling; nämligen inkommandedatum, diarienummer eller annan beteckning vid registreringen, uppgifter om handlingens avsändare och i korthet vad handlingen rör. Där föreskrivs emellertid också att uppgifter om avsändare och vad handlingen rör ska utelämnas eller särskiljas om det behövs för att registret i övriga delar ska kunna hållas tillgängligt för allmänheten.

Det material som finns: SOU 2018:25 s. 54 ff., s. 99, s. 141 och s. 184 ff., eSams checklista för jurister och de hänvisningar som ges där.

Gör så här: När varje led i informationsflödet hos en myndighet digitaliseras behöver myndigheten uppdatera arkivredovisningen och systemdokumentationen samt sina registreringsrutiner till den nya miljön. För nya digitala handlingar bestående av metadata och liknande, som skapats med anledning av de kontroller som utförs av e-underskrifter och e-stämplar, bör ett pragmatiskt synsätt kunna godtas för att denna närmast tekniska hantering ska bli ändamålsenlig, särskilt när de rör brukad säkerhetsteknik och sällan används av andra än experter.

Följderna av brister i registrering och anknytande hantering är att handlingar inte kan återfinnas och därmed varken kan brukas av myndigheten eller ge den överblick som behövs för att få vetskap om vilka allmänna handlingar som finns.

4.3 Bevarande och gallring av handlingar (Att göra 15)

> Att göra 15: En myndighet måste klargöra vilka e-handlingar som uppkommer, vad som ingår i dem, vad som utgör metadata utanför en e-handling och vilka sök-, sammanställnings- och äkthetskontrollmöjligheter som myndigheten har. Myndigheten behöver också bedöma om det redan finns stöd för gallring eller om en framställning behöver göras till Riksarkivet. För kommuner och landsting finns särskilda regler.

Som berörts i avsnitt 2.5 (Att göra 5) räcker det inte att en myndighet bevarar upprättade och inkomna handlingar i ursprungligt skick. Myndigheten måste också vidmakthålla existerande möjligheter att söka- och sammanställa uppgifter och handlingar och att bedöma handlingars autenticitet, så länge gallring inte får ske. Detta gäller för såväl verksamhetssystem, e-arkiv och pappersarkiv som de mera tekniska funktioner som används för att skriva under, stämpla eller kontrollera handlingar.

Allmänt om kraven: Grundläggande bestämmelser om bevarande och gallring av allmänna handlingar hos myndigheter finns i arkivlagen (1990:782). Enligt 3 § tredje stycket ska myndigheternas arkiv bevaras (i ursprungligt skick), hållas

ordnade och vårdas så att de tillgodoser (1) rätten att ta del av allmänna handlingar, (2) behovet av information för rättsskipningen och förvaltningen och (3) forskningens behov. Vad som menas med gallring framgår av Riksarkivets föreskrifter. Där anges att gallring föreligger när allmänna handlingar eller uppgifter i allmänna handlingar förstörs eller andra åtgärder vidtas med handlingarna som medför

- förlust av betydelsebärande data,
- förlust av möjliga sammanställningar,
- förlust av sökmöjligheter, eller
- förlust av möjligheter att bedöma handlingarnas autenticitet.

Förstörs exempelvis data som används för äkthetskontroll utgör det alltså gallring. För att förstå dessa frågor kan vissa begrepp behöva klargöras.

Det finns en skillnad mellan skydd för sanningshalt respektive skydd för äkthet. I det första fallet handlar skyddet om att innehållet inte får vara osant. Ett skydd för äkthet handlar istället om att säkerställa att uppgifterna verkligen härrör från angiven utställare. Informationsinnehållets sanningshalt säkerställs inte genom underskrifter. En handlings autenticitet kan ha manipulerats på olika sätt. Texten kan ha ändrats av en obehörig (innehållsförfalskning). Någon kan också ha skrivit annans namn (underskriftsförfalskning). Dessa skillnader är av betydelse för den digitala förvaltningens informationsflöde. Enligt arkivförfattningarna måste en inkommen eller upprättad handling – falsk eller äkta – bevaras i ursprungligt skick; dvs. med det innehåll (inklusive underskrift) som handlingen hade när den kom in till myndigheten eller upprättades där. Detta får inte blandas samman med frågan om handlingen är äkta, dvs. om den i alla delar härrör från den som framstår som utställare, eller om den är osann. Enligt arkivförfattningarna ska även handlingar som är falska (oäkta) eller osanna bevaras i ursprungligt skick.[39]

I den digitala miljön görs som framgått äkthetskontroller av varje e-underskriven handling som kommer in till en myndighet. Dessutom säkerställs handlingarnas ursprungliga skick efter mottagande och kontroll, ofta genom myndighetens elektroniska stämpel och anknytande kontrollmaterial (jämför avsnitt 4.1). Riksarkivets definition av gallring ger skydd för existerande (inkomna eller upprättade) handlingars äkthet. Definitionen syftar dock inte till att

[39] I arkivsammanhang möter man ibland också begreppen ”tillförlitlighet” och ”autenticitet” – med en något annan betydelse än vad man vanligen ger dessa ord. Tillförlitlighet överlappar till stor del både äkthet och sanningshalt, medan autenticitet inte sällan motsvarar ursprungligt skick. *Tillförlitlighet* syftar på handlingarnas trovärdighet som bevis för de aktiviteter/transaktioner som de utgjort en del av, medan *autenticitet* i detta sammanhang betyder att handlingarna inte har manipulerats eller på annat sätt ändrats efter det att de har inkommit eller upprättats.

införa nya krav exempelvis på att vissa kontroller ska införas för att granska e-underskrivna handlingars äkthet. I arkivförfattningarna ställs inte heller krav på användning av e-underskrifter eller e-stämplar och det finns inte heller bestämmelser om att det bästa bevismaterialet, till exempel ett original, inte en kopia, måste användas. Detta regleras istället i processuella regler.

I praktiken ges ofta ovidimerade fotokopior och vanlig oskyddad e-post in utan att handlingarnas äkthet blir ifrågasatt. Det är verksamhetens behov och straff- och näringsrättsliga skyddsregler som läggs till grund för eventuella krav på underskrifter. Verksamhetens behov avgör också vilka rutiner för kontroll av äkthet som ska införas för myndigheternas handläggning av ärenden och för deras informationssäkerhet.[40] Här finns dessutom risker för felaktiga slutsatser, om skyddet för ett fysiskt originalexemplar blandas samman med det kryptografiska skyddet i it-miljö för originalinnehåll och ursprungligt skick. När gallring övervägs med avseende på äkthet och rättsskipningens och förvaltningens behov behöver underskriftens funktion för olika kategori av handlingar eller ärenden beaktas. Uppstår det en förlust som är av endast ringa betydelse finns ofta förutsättningar för att besluta om gallring. Det blir av betydelse om det finns ett reellt behov av äkthetsbevis eller om någon av de andra funktioner, exempelvis avslutningsfunktionen, som en underskrift kan fylla utgör huvudskälet bakom att underskrift har krävts eller annars använts.

Av 10 § första stycket arkivlagen framgår att allmänna handlingar får gallras. Vid gallring ska enligt andra stycket alltid beaktas att arkiven utgör en del av kulturarvet och att det arkivmaterial som återstår ska kunna tillgodose de ändamål som angetts ovan (se 3 § tredje stycket).

Gallring får dessutom ske bara om det är särskilt föreskrivet eller beslutat av behörigt organ.[41] Inom statlig och kommunal förvaltning ska det finnas arkivmyndigheter. Kommunstyrelsen är arkivmyndighet i en kommun och landstingsstyrelsen i ett landsting, om inte kommunfullmäktige eller landstingsfullmäktige har utsett någon annan nämnd eller styrelse till arkivmyndighet (8 § arkivlagen).

Riksarkivet är enligt 8 § arkivförordningen (1991:446) statlig arkivmyndighet. En statlig myndighet får inte på egen hand avgöra vilka allmänna handlingar som ska gallras. Gallringen får endast ske i enlighet med föreskrifter eller beslut

[40] Riksarkivets rapport 2006:1, Elektroniskt underskrivna handlingar, s. 32.
[41] För vissa behandlingar gäller dock registerförfattningar där det förekommer föreskrifter om att gallring *ska* ske respektive *får* ske.

av Riksarkivet, om inte särskilda gallringsföreskrifter finns i lag eller förordning (14 § arkivförordningen). På det kommunala området gäller motsvarande begränsning (15 § arkivlagen). Beslut om gallring meddelas av kommunfullmäktige respektive landstingsfullmäktige som då, liksom Riksarkivet, har att följa de yttre ramar för gallring som anges i 10 § arkivlagen. Fullmäktige kan dock föreskriva att en annan nämnd ska besluta om gallring, till exempel en arkivnämnd. Detta framgår i så fall av ett arkivreglemente. Inte heller på det kommunala området får alltså arkivbildande myndighet avgöra vad som ska gallras eller inte.

Det material som finns: Se t.ex. Riksarkivets rapport 1999:1 Om gallring - från utredning till beslut samt eSams checklista för jurister, avsnitt 3, och de hänvisningar som ges där. När frågor om äkthet har tagits upp i arkivsammanhang har slutsatsen varit att det krävs närmare analyser. Se dock om underskriftens olika funktioner, punkten 5.5 eSams juridiska vägledning för införande av e-legitimering och e-underskrifter.

Gör så här: Analysera vilka handlingar som kommer in och upprättas. Bedöm vad som ska bevaras och vad som får gallras enligt gallringsbeslut av Riksarkivet. Ta reda på om material som myndigheten inte behöver för sin verksamhet är av sådan tillfällig eller ringa betydelse att myndigheten själv får besluta om gallring.[42] När nödvändiga tillämpningsbeslut om gallring har fattats behöver rutiner och systemstöd för gallring införas så att löpande gallring kan verkställas. Arkivförfattningarna kan inte åberopas för att kräva insamling av äkthetsbevis. Tänk på att det delvis gäller särskilda regler för kommuner och landsting.

Följderna av brister i arkivhanteringen är inte bara att handlingar felaktigt kan ha raderats eller inte kan återfinnas. Det kan exempelvis visa sig att ärendegången inte kan klarläggas eller att rättsförluster uppkommer till följd av att det inte går att kontrollera vad som anförts eller om en handling är äkta.

[42] Riksarkivet har meddelat föreskrifter om gallring av handlingar som är av tillfällig eller ringa betydelse. Vid tillämpning av dessa föreskrifter tar den arkivbildande myndigheten själv ställning till vilka handlingar som har sådan begränsad betydelse. Föreskriften gäller emellertid inte för gallring av skannade förlagor.

4.4 Hantering av skannade pappershandlingar (Att göra 16)

> Att göra 16: En myndighet som skannar handlingar behöver överväga om det är lämpligt och finns rättsligt stöd för att gallra pappersexemplaren.

När handlingar ges in på papper till en myndighet som ska införa digitala funktioner från ax till limpa behöver pappershandlingarna skannas. Även beslut och annat som myndigheten dokumenterar på papper behöver skannas för att kunna kommuniceras digitalt och läsas via bildskärm. Frågan blir – efter att skanning skett – om de avbildade pappershandlingarna (som ofta har originalkvalitet) också måste bevaras. I praktiken används de knappast efter att ha skannats (jämför avsnitt 2.5, 3.5 och 3.6).

Allmänt om kraven: Som framgått föreskrivs att handlingar som tagits emot eller upprättats hos myndighet ska bevaras i ursprungligt skick. Det innebär att alla åtgärder som medför informationsförlust utgör gallring eftersom handlingens ursprungliga skick därmed har gått förlorat. Exempel på sådana åtgärder är överföring av handlingar till ett annat medium genom skanning av pappershandlingar. Visserligen kräver arkivförfattningarna inte att kontroller ska utföras av inkomna handlingars äkthet men däremot ställs krav på kontroller och dokumentation av hur resultatet blivit efter skanning, särskilt om gallring ska övervägas beträffande förlagor.[43]

Det material som finns: Se eSams checklista för jurister, avsnitt 3, och de hänvisningar som ges där. När frågor om äkthet tagits upp i arkivsammanhang har slutsatsen varit att det krävs närmare analyser. Se dock om underskriftens olika funktioner, punkten 5.5 eSams juridiska vägledning för införande av e-legitimering och e-underskrifter.

Gör så här: Analysera vilka handlingar som bör skannas och överväg vilka risker som kan bli följden av att endast skannade bilder och tolkade data bevaras. Undersök hur ofta myndigheten beträffande det aktuella handlingsslaget har låtit utföra handstilsanalyser eller andra kontroller av experter för att fastställa om en handling är äkta. Överväg vilka risker som kan tillkomma från rättssäkerhetssynpunkt eller för det allmänna om underlaget för äkthetskontroll delvis gallras och om kompenserande åtgärder kan uppväga dessa risker.

[43] Riksarkivets rapport 2006:1, Elektroniskt underskrivna handlingar, s. 32.

Undersök om förlagorna får gallras enligt beslut av Riksarkivet. Utgå från att det kan ta avsevärd tid innan ett beslut föreligger.

Följden av att förlagor gallrats kan bli att en äkthetskontroll försvåras. Sådana kontroller av experter där originalexemplaren behöver finnas kvar är dock ovanliga.

4.5 Hantering av format och normgivning (Att göra 17)

> Att göra 17: En myndighet bör undersöka om den tilldelats normgivningskompetens så att myndigheten kan föreskriva att handlingar ska ges in viss väg eller i visst format och om myndighetens tekniska system klarar förekommande format.

Det är av praktisk betydelse, för en myndighet som inför e-tjänster och anknytande funktioner, om det är möjligt att begränsa kontaktvägarna för berörda ärendeslag, så att myndigheten inte tar emot exempelvis telefax och e-post, jämför avsnitt 3.1 (Att göra 7). System som myndigheter inför saknar ibland stöd för att hantera alla de format i vilka e-handlingar skickas till myndigheten eller format med vilka e-underskrifter eller e-stämplar har skapats och äkthetskontrolleras, jämför avsnitt 3.4 (Att göra 10). Vissa myndigheter har meddelat föreskrifter om tillåtna format och kontaktväg.

Allmänt om kraven: Reglerna i den gamla förvaltningslagen om att myndigheter måste kunna ta emot e-post och telefaxmeddelanden har utmönstrats. Nu föreskrivs endast att en myndighet ska vara tillgänglig för kontakter med enskilda och informera allmänheten om hur och när sådana kan tas, samt att myndigheten ska vidta de åtgärder i fråga om tillgänglighet som behövs för att den ska kunna uppfylla sina skyldigheter gentemot allmänheten enligt 2 kap. tryckfrihetsförordningen om rätten att ta del av allmänna handlingar, se 7 § FL. I sammanhanget berörs också de generella reglerna i förvaltningslagen om proportionalitet (5 § FL) och i regeringsformen om så kallade betungande föreskrifter (8 kap. 2 § första stycket 2 regeringsformen).

Regeringen har delegerat till ett antal myndigheter en rätt att föreskriva om elektronisk överföring av handlingar, se bland annat 4 kap. 2 b § aktiebolagsförordningen (2005:559) och 5 § Bolagsverkets föreskrifter (BOLFS 2008:1, ändrad genom BOLFS 2009:3) om elektroniska ansökan och anmälan för vissa

företag med mera. Där föreskrivs att handlingar får ges in elektroniskt endast genom vissa elektroniska tjänster som anges på vissa webbplatser, endast till verkets elektroniska mottagningstjänster för handlingar som ges in enligt angivna författningar och i sådant format och med sådana rutiner att verket kan ta emot, läsa och bevara handlingarna och samtidigt ge skydd mot skadlig kod och andra hot mot informationssäkerheten. När krav ställs på format som inkommande handlingar ska ha är myndigheten skyldig att följa de krav som arkivmyndigheten föreskriver, se Riksarkivets föreskrifter och allmänna råd om tekniska krav för elektroniska handlingar (RA-FS 2009:2).

Det material som finns: Frågan om normgivningskompetens tas upp i avsnitt 3.2.2 eSams vägledning om rättsliga förutsättningar för digitalt i första hand och har behandlats av E-nämnden 2005 i en vägledning för myndighetsföreskrifter vid införande av e-tjänster (05:03).

Gör så här: Undersök om normgivningskompetens delegerats till din myndighet så att en viss digital kanal och vissa format får föreskrivas. Styr dessa val så att hanteringen kan ske säkert och effektivt, exempelvis genom att föreskriva hur en handling får lämnas, att en viss e-tjänst (som har stöd för att upprätta e-handlingen) eller en viss e-blankett (med eller utan anknytning till viss e-tjänst) ska användas eller att endast vissa säkerhetslösningar för att digitalt skriva under eller legitimera sig för att lämna uppgifter är tillåtna. Ett annat alternativ, när användare väljer digitala kanaler, är att utforma dem (till exempel eget utrymme) så att de bara kan användas när ändamålsenligt format brukas och tillräckligt skydd finns för informationssäkerheten. Följ de förvaltningsgemensamma specifikationer som tagits fram för att definiera hur information ska beskrivas och struktureras i samband med överföringar för att generellt underlätta och standardisera den överföring som behövs mellan informationssystem.[44]

Följderna när olämpliga kanaler eller format får användas kan bli ytterligare risker för manipulationer och missbruk. Detta kan drabba såväl enskilda som myndigheter och föra med sig betydande merarbete och en fördröjd beslutsgång. Används olämpliga format kan informationshanteringen dessutom kompliceras och fördyras.

[44] Se https://riksarkivet.se/Media/pdf-filer/doi-t/Introduktion_till_Forvaltningsgemensamma_specifikationer_RAFGS2D20161001_.pdf

4.6 Olika exemplar av handlingar (Att göra 18)

> Att göra 18: En myndighet behöver utforma sina digitala funktioner så att myndigheten tydligt kan skilja mellan olika förvar av handlingar, och så att det enkelt kan bestämmas vilka exemplar som ska finnas kvar och vilka som bör gallras. Myndigheten måste kunna skilja de allmänna handlingarna från myndighetsinternt arbetsmaterial.

Det förekommer som framgått att en myndighet lagrar samma informationsinnehåll i form av olika exemplar. Viss text kan exempelvis förvaras i olika format och med olika äkthetstecken eller andra skydd, dels i verksamhetssystem för att hanteras av myndighetens personal, dels i e-arkiv eller på papper för att arkivförfattningarnas krav ska tillgodoses. Vissa av dessa handlingar används sällan (jämför avsnitt 1.3, 3.5 och 3.6). En myndighet bör utforma denna hantering så att det tydligt går att skilja mellan de exemplar av e-handlingar som finns i eget utrymme respektive de som finns i en mottagningsfunktion eller i ett verksamhetssystem hos myndigheten.

Beträffande kraven, det material som finns, hur myndigheten bör göra och vilka konsekvenserna kan bli, se avsnitt 3.5.

4.7 Återanvändning av uppgifter (Att göra 19)

> Att göra 19: En myndighet behöver undersöka om en planerad digital tjänst kan göras enklare för användaren, antingen genom att myndigheten begär uppgifter och handlingar direkt från annan myndighet (i stället för att enskilda ska ge in handlingarna) eller att myndigheten i eget utrymme inför en funktion där användaren kan begära uppgifter automatiserat från annan till sitt utrymme och återanvända uppgifterna där.

Det är tekniskt möjligt att koppla ihop myndigheters tekniska system för att automatiserat hämta uppgifter från en myndighet till en annan. Numera brukas bastjänster (eller med en synonym applikationsprogrammeringsgränssnitt, API) för helt automatiserat informationsutbyte maskin till maskin. Exempelvis kan en användare av en viss e-tjänst, istället för att logga in i en annan e-tjänst, i den första e-tjänsten fråga efter viss information (som också kunnat nås via den andra e-tjänsten) och få den visad i den första e-tjänsten. En bastjänst skapar och överför begäran om uppgifter helt automatiserat. Svar ges så att uppgifter kan fogas in i sitt rätta sammanhang utan manuella moment,

exempelvis så att uppgifter blir förifyllda i ett eget utrymme i den första e-tjänsten. En myndighet kan också begära uppgifter och handlingar direkt från annan myndighet (i stället för att enskilda ska ge in handlingarna från eget utrymme). Vanligtvis sätts flera bastjänster samman så att information kan flöda mellan flera myndigheter helt automatiserat. Som exempel på detta kan nämnas Vidareförmedlingstjänsten för ekonomiska uppgifter (SSBTEK) och Vidareförmedlingstjänsten för grundläggande uppgifter om företag (SSBTGU).

Allmänt om kraven: För att enskilda ska kunna återanvända uppgifter behövs ett eget utrymme. Återanvändning av uppgifter direkt mellan myndigheter kräver emellertid ingen sådan omväg. Den beskrivna hanteringen är möjlig bara när regler om sekretess eller persondataskydd inte lägger hinder i vägen. En förmedlare av uppgifter agerar i egenskap av underleverantör åt de tillhandahållare av e-tjänst som infört funktioner för återanvändning direkt mellan myndigheter eller indirekt via eget utrymme. Förmedlaren hanterar återanvända uppgifter endast tekniskt. Den som tillhandahåller en e-tjänst kan erbjuda funktioner för återanvändning till sina innehavare av eget utrymme. De som producerar (lämnar ut) uppgifter agerar i eget namn i sin it-miljö där de mottar en begäran, prövar den och lämnar ut uppgifter.

För att undgå juridiska problem bör indirekt återanvändning inte ske genom direktåtkomst mellan myndigheter. Information som hämtas från flera myndigheter bör endast momentant göras tillgänglig hos en och samma myndighet. Även i övrigt bör uppgifterna hanteras på ett ändamålsenligt sätt så att 2 kap. 13 § första stycket eller 14 § första stycket 1 tryckfrihetsförordningen blir tillämpligt. Det finns också föreskrifter i förordningen (2018:1264) om digitalt inhämtande av uppgifter från företag som syftar till att förenkla för företag att starta, driva och avveckla sin verksamhet genom att underlätta deras kontakter med och uppgiftslämnande till myndigheter. Enligt 4 § ska en myndighet så långt det är möjligt använda sådana uppgifter om företag som finns tillgängliga inom statsförvaltningen så att företag inte behöver lämna samma uppgifter flera gånger.[45]

Det material som finns: Hur återanvändningen går till och vilka rättsfrågor som uppkommer beskrivs i eSams juridiska vägledningen för verksamhetsutveckling

[45] I 6 § förordningen föreskrivs vidare: När en myndighet utvecklar ett system för inhämtande av uppgifter från företag, ska det utformas så att företags uppgiftslämnande och därmed sammanhängande kommunikation med företag som huvudregel sker digitalt. Ett sådant system ska vara säkert och bygga på vanligt förekommande tekniska lösningar. När det är lämpligt ska öppna standarder användas. Systemet ska också stödja ett samordnat inhämtande av strukturerade uppgifter i statsförvaltningen. Vid utvecklandet ska myndigheten ta hänsyn till företags förutsättningar och behov.

inom e-förvaltning (avsnitt 6.1.5 och 6.5). Det finns också en vägledning för SSBTGU.

Gör såhär: Undersök om uppgifter kan återanvändas automatiserat genom att begäras från annan myndighet innan den som tillhandahåller en e-tjänst begär att uppgifterna ska lämnas av enskilda. Se till att uppgifter vid återanvändning hanteras så att mottagande myndighet kan veta om de är kvalitetssäkrade.

Följderna av en felaktigt utformad funktion för återanvändning kan bli att myndigheten bryter mot exempelvis offentlighets- och sekretesslagen eller EU:s dataskyddsförordning.

4.8 Kommunikation i ärenden (Att göra 20)

> Att göra 20: En myndighet behöver säkerställa att ett planerat verksamhetssystem kan uppfylla de krav på kommunikation med parter och andra som följer av författning.

Myndigheter behöver kunna kommunicera digitalt med parter i ärenden och med andra som ska få information eller ges tillfälle att yttra sig. Det är emellertid sådana skillnader mellan olika kategorier av ärenden att frågan i denna vägledning endast tas upp från ett övergripande perspektiv.

Allmänt om kraven: Av 25 § FL följer att en myndighet, innan den fattar ett beslut i ett ärende ska, om det inte är uppenbart obehövligt, underrätta den som är part om allt material av betydelse för beslutet och ge parten tillfälle att inom en bestämd tid yttra sig över materialet. Under vissa förutsättningar får myndigheten dock avstå från sådan kommunikation. Myndigheten bestämmer hur underrättelse ska ske.

Det material som finns: Här hänvisas till lagmotiv, rättspraxis och doktrin inom området då allmänna förvaltningsrättsliga regler gäller, oberoende av om hanteringen sker på papper eller med tekniska metoder. Beträffande underrättelse, se kap. 5.

Gör så här: Undersök om planerade tekniska och administrativa lösningar uppfyller de juridiska kraven rörande kommunikation med parter och andra i ärenden.

Bristande kommunikation kan anses vara ett så allvarligt fel att ett ärende måste tas om, det vill säga tas upp till ny prövning av samma myndighet.

4.9 Automatiserade beslut (Att göra 21)

> Att göra 21: En myndighet som inför en helt papperslös hantering bör undersöka vilka beslut som kan och bör fattas helt eller delvis automatiserat och se till att system som införs för sådana beslut utformas på ett rättsenligt och ändamålsenligt sätt. För kommuner finns hinder.

Det har blivit allt vanligare att myndigheter fattar förvaltningsbeslut helt automatiserat. Myndigheterna kan i praktiken inte bortse från denna utveckling, där det också förekommer maskinella beslut som handläggare har en viss kontroll över.

Allmänt om kraven: En osäkerhet finns om en myndighet har rätt att utan särskild tillåtande författningsreglering fatta beslut helt automatiserat. E-delegationen fann dock i sitt betänkande (SOU 2014:75) Automatiserade beslut – färre regler ger tydligare reglering, att det förvaltningsrättsligt inte krävs uttryckligt stöd i författning. Delegationen föreslog därför att ett antal bestämmelser i lag och förordning där det anges att myndighet får fatta automatiserade beslut skulle utmönstras. Skälet för förslaget var att dessa särregler felaktigt hade tolkats motsatsvis så att bara beslut som omfattas av en särbestämmelse kunde få fattas automatiserat. Genom den nya förvaltningslagen infördes en föreskrift i 28 § FL om att beslut kan fattas automatiserat. E-delegationens förslag att utmönstra särreglering har inte lett till lagstiftning. Genom att det i lagen slås fast att beslut kan fattas automatiserat tydliggörs dock, enligt regeringens uttalande i lagmotiven, att det inte behövs en reglering i en specialförfattning för att en myndighet ska kunna använda den automatiserade beslutsformen.

Enligt artikel 22.1 i EU:s dataskyddsförordning ska en registrerad ha rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripen profilering, vilket har rättsliga följder för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne. Undantag från rättigheten att inte bli föremål för automatiserat individuellt beslutsfattande gäller för beslut som tillåts enligt nationell rätt (som den personuppgiftsansvarige omfattas av) och som fastställer lämpliga åtgärder till skydd för den registrerades rättigheter, friheter och berättigade intressen. eSam har anfört att de generellt tillämpliga bestämmelserna i den nya förvaltningslagen får anses

innefatta sådana lämpliga skyddsåtgärder för den registrerade att automatiserade beslut får fattas när de faller inom ramen för förvaltningslagens tillämpningsområde och är överklagbara. Regeringen har gjort samma bedömning i prop. 2017/18:95, Anpassningar av vissa författningar inom skatt, tull och exekution till EU:s dataskyddsförordning, s. 100, och prop. 2017/18:254, Anpassning av utlänningsdatalagen till EU:s dataskyddsförordning, s. 55.

Det material som finns: Frågan har tagits upp av E-delegationen i betänkandet Automatiserade beslut – färre regler ger tydliga reglering (SOU 2014:75) och av eSam i ett rättsligt uttalande den 19 mars 2018 om automatiserade beslut. Vidare har SKL utarbetat en promemoria om automatiserat beslutsfattande i den kommunala förvaltningen, där vissa hinder mot automatiserat beslutsfattande inom kommuner och landsting har beskrivits. Beträffande bland annat kraven på god offentlighetsstruktur och rättssäkerhet, se eSams checklista för jurister avsnitt 5.1 och SOU 2018:25, se även ovan avsnitt 4.2 och 4.3 och Svenskt ramverk för digital samverkan (avsnitt 3.4.2).

Gör så här: Undersök vilka beslut myndigheten fattar som är av sådant slag att de skulle kunna automatiseras. Bedöm om det finns juridiska, tekniska eller administrativa hinder mot en automatisering. Se till att beslut om införande fattas behörigen, på rätt beslutsnivå, och dokumenteras av myndigheten innan funktionen tas i drift. eSam har i Svenskt ramverk för digital samverkan (avsnitt 3.4.2) rekommenderat att offentliga organisationer ska automatisera offentliga digitala tjänster så långt som möjligt. Även mer komplexa flöden såväl inom organisationerna och flöden som sker i samverkan med andra organisationer behöver enligt ramverket automatiseras.

Följderna av att ta en felaktig funktion i drift kan bli att fattade beslut undanröjs till följd av fel i förfarandet.

5. Att expediera e-handlingar – bygg rätt för att skicka

Tänk på att:

Funktioner för att expediera e-handlingar gör det möjligt att bereda ärenden och kommunicera med parter och andra berörda i ärenden samt att delge handlingar.

Det fjärde övergripande ledet (se figur 1 i avsnitt 1.4) omfattar de funktioner som myndigheter använder för att expediera handlingar, till exempel inom ramen för en myndighets ärendehandläggning, och de rättsfrågor som denna hantering väcker när den offentliga förvaltningen digitaliseras.

Expediering sker för att kontakta enskilda eller andra myndigheter, exempelvis för att inhämta kompletteringar (20 § FL), för att begära att en enskild bekräftar en handling (21 § FL) eller förtydligar en framställan (23 § FL), för att kommunicera material av betydelse för ärendets utgång (25 § FL), för att skicka remisser till en annan myndighet eller en enskild (26 § FL) och för att delge handlingar, exempelvis beslut (33 § FL). Även om det finns funktioner hos en myndighet för att expediera handlingar digitalt kan en lämplighetsbedömning ge vid handen att en handling istället bör sändas på papper. Valet beror på eventuella formkrav och vad som anses vara lämpligt utifrån bland annat förvaltningsrättsliga, dataskyddsrättsliga och informationssäkerhetsrättsliga utgångspunkter. Handlingarna måste överföras på ett tillräckligt säkert sätt. I praktiken kan detta ske genom Mina meddelanden eller inloggning i någon annan tjänst där kommunikationen skyddas och annars sker på ett säkert sätt så att risken för obehörig åtkomst minimeras. För enklare meddelanden som inte behöver ett sådan skydd kan expediering emellertid ske även via exempelvis oskyddad e-post.

5.1 Uppgifter om e-adress (Att göra 22)

Att göra 22: En myndighet behöver få veta till vilken adress en digital försändelse bör skickas. Adresserna bör kunna göras tillgängliga för myndigheten utan att denna hantering leder till att enskilda drabbas av skräppost till följd av att adresser sprids.

Att försändelser behöver adresseras har berörts i avsnitt 3.2. För kommunikation på papper finns uppgifter om folkbokföringsadress och annat stöd där myndigheter får veta till vilken adress de ska skicka försändelser. Motsvarande stöd saknas i digital miljö. Det blir därför ofta en utmaning för avsändande myndighet att finna en ändamålsenlig e-adress. Önskemål om att skapa register över e-adresser har varit svåra att tillgodose eftersom handlingsoffentligheten leder till att sådana register hos en myndighet kan missbrukas av de som vill skicka oönskade försändelser (skräppost). Här kan myndighetens Mina Sidor och en anslutning till Mina Meddelanden underlätta.

Allmänt om kraven: I 25 § folkbokföringslagen (1991:481) föreskrivs en skyldighet att inom en vecka anmäla flyttning till Skatteverket. Anmälningsskyldigheten är straffsanktionerad (42 §). Dessutom har enskilda möjlighet att begära eftersändning eller på annat sätt säkerställa att de kan nås med traditionell papperspost.[46] Någon sådan ordning finns emellertid inte för digitala adresser, med undantag för en skyldighet som kan följa av avtal att meddela adress. Regeringen har också i ett lagstiftningsärende anfört att en nackdel med att skicka handlingar på digital väg kan vara att det ibland kan föreligga osäkerhet i fråga om ett telefaxnummer eller en e-postadress tillhör mottagaren. Till skillnad från vad som gäller vid översändande med traditionell post saknas det, i varje fall för närvarande, ofta möjlighet att på något tillförlitligt sätt kontrollera att till exempel en e-postadress är korrekt. Vissa e-postadresser kan inte heller med någon säkerhet knytas till en viss användare eller ett visst abonnemang (prop. 2009/10:237 s. 121).

Det material som finns: Frågan verkar inte ha utretts närmare med sikte på den digitala förvaltningens behov.

Gör så här: Använd förmedlingsadressregistret i tjänsten Mina meddelanden. När det inte är möjligt bör myndigheten inhämta tillförlitliga uppgifter om digital adress, helst från berörd person. Från rättssäkerhetssynpunkt är det viktigt att mottagaren verkligen bereds möjlighet att ta del av meddelandet.

Följderna av felaktig adressering kan bli att mottagares rättssäkerhet inte tillgodoses eller att ett förvaltningsförfarande försenas i onödan.

[46] Det har mot den bakgrunden ansetts rimligt att en part själv får stå risken vid så kallad förenklad delgivning vid underlåtenhet att meddela rätt adress till myndigheten.

5.2 Insynsskydd (Att göra 23)

> Att göra 23: En myndighet behöver skydda e-handlingar som expedieras mot obehörig insyn. Myndigheten bör därför ta fram underlag och rutiner för att skicka meddelanden krypterat. E-post och liknande bör dock kunna användas när innehållet är sådant att det inte finns hinder från lämplighetssynpunkt mot att kommunicera utan skydd.

I pappersmiljö godtas att sekretessreglerade uppgifter sänds i förslutna kuvert som delas ut i brevlådor vid vägkanten.[47] En bedömning måste dock göras för att myndigheten ska finna en lämplig skyddsnivå för digitala försändelser. Många adressater har inte någon brevlåda för säkra digitala försändelser, men använder digitala tjänster där inloggning sker med e-legitimation. Sådana tjänster kan kombineras med funktioner för användare där de på ett säkert sätt kan ta emot meddelanden, läsa dem och lämna svar. Försändelser kan dessutom ha ett innehåll som är av sådan art att de kan skickas via till exempel e-post eller SMS. Myndigheten behöver expediera försändelser digitalt på ett tillräckligt säkert sätt och införa de arkitekturer som krävs för denna hantering.

Allmänt om kraven: Krav på insynsskydd följer av Offentlighets- och sekretesslagen (2009:400; OSL) och av EU:s dataskyddsförordning. Enligt dessa regler får sekretessreglerade uppgifter inte röjas och personuppgifter inte behandlas i strid mot reglerna om dataskydd. Här finns inte utrymme för en närmare genomgång. I ett lagstiftningsärende har regeringen förklarat att det är särskilt angeläget att handlingar som skickas elektroniskt hamnar rätt eftersom det, till skillnad från vid användande av post- och budtjänster där handlingen läggs i ett kuvert, saknas möjligheter att hemlighålla innehållet för den som felaktigt råkar få handlingen skickad till sig (prop. 2009/10:237 s. 121).

Det material som finns: Området har behandlats av E-offentlighetskommittén (SOU 2010:4) och i prop. 2009/10:237 Ny delgivningslag samt av eSam i Outsourcing – en vägledning om sekretess och persondataskydd och i rättsliga uttalanden den 17 december 2015 om röjandebegreppet enligt offentlighets- och sekretesslagen och den 23 oktober 2018 om röjande och molntjänster.

[47] Var och en som passerar kan plocka upp försändelsen ur lådan, bryta den och ta del av innehållet. I elektronisk miljö används ofta ännu osäkrare kanaler såsom e-post där den som har brutit igenom skyddet för kommunikationen kan ta del av uppgifterna på distans. För båda dessa former av missbruk finns bestämmelser om straff i brottsbalken. Kraven på skydd för fysiska personers integritet och företagens intressen av närmast ekonomiskt slag har dock fört med sig att nya system för säkra försändelser såsom Mina meddelanden börjat användas. Där krävs e-legitimation för tillgång till uppgifterna och innehållet skyddas av stark kryptering under överföringen mellan parterna.

Gör så här: Undersök om meddelandets innehåll är känsligt eller annars kräver insynsskydd till följd av reglerna i OSL eller EU:s dataskyddsförordning. Eftersom det ofta blir fråga om en masshantering eller återkommande kommunikation av liknande slag bör myndigheten ta fram rutiner för att skicka meddelanden krypterat och sätta sig in i vilka led i överföringen och lagringen samt vilka delar av ett meddelande som insynsskyddet omfattar. E-post och liknande oskyddade försändelser bör emellertid kunna användas när innehållet är sådant att det inte finns hinder enligt författning eller från lämplighetssynpunkt mot att kommunicera på det sättet.

Följderna av att skyddet mot obehörig insyn inte upprätthålls kan bli ett både otillåtet och straffbart röjande eller ett agerande i strid mot EU:s dataskyddsförordning vilket kan leda till bland annat sanktionsavgifter.

5.3 E-delgivning (Att göra 24)

> Att göra 24: En myndighet bör undersöka om och i så fall hur myndigheten kan delge handlingar i digital form. Myndigheten bör utarbeta underlag och rutiner för att skicka dels via säkra kanaler såsom Mina meddelanden, dels via e-post eller SMS när detta får ske och är ändamålsenligt.

Syftet med delgivning är att säkerställa att en person har fått del av en viss handling. De formkrav som finns på området behöver därför upprätthållas. Det allmänna lägger ned betydande kostnader för att delge via traditionella kanaler, men i många fall kan även digitala kanaler användas. Dessa möjligheter har underskattats i den praktiska hanteringen och det finns sannolikt en besparingspotential om det klargörs när och hur delgivning kan ske på digital väg.

Allmänt om kraven: De regler som gäller för delgivning framgår av delgivningslagen (2010:1932; DelgL) och delgivningsförordningen (2011:154; DelgF). Enligt 16 § DelgL sker vanlig delgivning genom att handlingen skickas eller lämnas till delgivningsmottagaren. Bestämmelsen är teknikneutral och hindrar inte att handlingen skickas eller lämnas exempelvis digitalt.[48] Enligt lagmotiven bör de möjligheter som digital kommunikation ger kunna tas tillvara i högre grad än vad som tidigare skett (prop. 2009/10:237 s. 92). En situation då det kan finnas anledning för myndigheten att avstå från att skicka handlingen digitalt eller att vidta särskilda säkerhetsåtgärder, är när innehållet i handlingen

[48] Endast myndighet får emellertid vid vanlig delgivning skicka handlingen på elektronisk väg (17 §).

är särskilt känsligt. Ett sätt att delge sådana handlingar digitalt kan enligt regeringen vara att skicka ett meddelande om att handlingen finns tillgänglig på exempelvis en domstols webbplats och att delgivningsmottagaren, efter identitetskontroll med e-legitimation, kan ta del av handlingens innehåll och därigenom också bekräfta mottagandet (prop. 2009/10:237 s. 121 f.). Mina meddelanden bör kunna användas på motsvarande sätt.

Myndigheter kan enligt motiven till delgivningslagen i många fall skicka handlingar på elektronisk väg om delgivningsmottagaren har anvisat en sådan överföringsmetod i det enskilda delgivningsärendet. I tveksamma fall kan det vara lämpligt att kontakta delgivningsmottagaren innan handlingen skickas. Vid en prövning av om det är olämpligt att skicka en handling på digital väg är det en grundläggande förutsättning att myndigheten med tillräcklig grad av säkerhet vet att delgivningsmottagaren nås på exempelvis en viss e-postadress. Myndigheten måste vid bedömningen också beakta risken för att andra än delgivningsmottagaren kan ta del av handlingens innehåll. Det kan därför finnas anledning att undvika att skicka handlingar till en adress som anvisats av annan än delgivningsmottagaren (prop. 2009/10:237 s. 238 f.).

Vid vanlig delgivning ska delgivningsmottagaren bekräfta mottagandet (6 § DelgF) och det är viktigt att myndigheten får bevis om detta. Det finns emellertid inget formkrav. Ofta bekräftar mottagaren genom att på papper underteckna ett mottagningsbevis eller delgivningskvitto och skicka tillbaka det. Mottagandet kan dock bevisas även på annat sätt, exempelvis elektroniskt. För att en bekräftelse per e-post ska kunna godtas bör i regel krävas att meddelandet avsänts från en adress som är känd eller som det finns en möjlighet att kontrollera innehavaren av i efterhand. Ett annat sätt att bekräfta mottagandet av en handling kan vara att delgivningsmottagaren genom användande av sin e-legitimation bekräftar mottagandet på myndighetens webbplats (prop. 2009/10:237 s. 239).

Det material som finns: Dessa frågor verkar inte ha utretts närmare med sikte på den digitala förvaltningens behov (se dock avsnitt 5.1 ovan, SOU 1996:40 s. 31 och 75 ff., Ds 2003:29 s. 69, Ds 2016:10 s. 57 ff. och prop. 2016/17:123 samt den nämnda prop. 2009/10:237 och Kronofogdemyndighetens delgivningshandbok).

Gör så här: Undersök om en enklare väg kan väljas för att delge, exempelvis via myndighetens webbplats eller Mina meddelanden.

Följderna av en felaktig hantering kan bli att mottagares rättssäkerhet eller persondataskyddet inte tillgodoses. Samhället drabbas dock av betydande kostnader till följd av delgivningssvårigheter, där möjligheter att använda digitala tjänster och försändelser bör kunna tas tillvara på ett ändamålsenligt sätt.

6. Annan användning

6.1 Digitalisering utanför ärendeprocessen

Vägledningen kan vara till nytta för att digitalisera även annat än den i avsnitt 1.4 beskrivna ärendeprocessen. Det kan till exempel handla om att utbyta information, att förmedla kunskap, att sammanställa och tillgängliggöra statistik, att lagra och annars hantera information åt andra för it-drift och e-arkiv eller att tillhandahålla tjänster för identitets- och behörighetskontroller.

Sådan informationshantering tar inte sin utgångspunkt i de led som beskrivits för ärendeprocessen utan ger vanligtvis stöd i form av en digital funktion för att t.ex. skicka eller ta emot uppgifter, sortera eller sammanställa uppgifter, lagra och skydda uppgifter eller annars underlätta en ändamålsenlig och säker informationshantering för myndigheter eller enskilda.

6.2 Plocka russinen ur kakan

Den som använder vägledningen kan utgå från redovisade att göra-punkter även när digitaliseringen inte avser en ärendeprocess. Användaren får emellertid själv leta fram relevanta avsnitt. Detta sker lämpligen genom att gå igenom att göra-punkterna tillsammans med den översiktliga redovisningen i respektive ruta för att på så sätt finna vägledning för det konkreta fallet, se följande sammanställning av det första ledet där handlingar färdigställs.

Figur 5: Hur relevanta avsnitt kan letas fram

Här innehåller vägledningen alltså inte någon färdig metod som kan ta användaren steg för steg genom relevanta processer. Är det fråga om exempelvis ett automatiserat informationsutbyte mellan myndigheter kan användaren emellertid direkt i sammanställningen ovan se att det kan finnas underlag av intresse i avsnitten för att göra 2, 4 och 5. När användaren går vidare till de följande leden kan på motsvarande sätt t.ex. att göra-punkterna om mottagningsfunktion återanvändning och automatiserade beslut ge en fingervisning om var stöd finns för att juridiskt bedöma en funktion för att utbyta uppgifter.

6.3 Omfattande datasamlingar och nya regelverk

Allt större mängder data samlas in och bevaras i takt med att verksamheter digitaliseras. Denna information kan vara intressant för olika aktörer att ta del av och nyttja, särskilt när data har strukturerats eller kan sökas och sammanställas automatiserat i nya, kanske oväntade uppgiftskonstellationer. Samlingar av data och automatiserade möjligheter att hantera dem betraktas därmed som

en tillgång i sig. En snabb utveckling sker också inom området för robotar och artificiell intelligens.

Parallellt med denna utveckling har ny författningsreglering tillkommit för att stödja återanvändning av uppgifter, se lagen (2010:566) om vidareutnyttjande av handlingar från den offentliga förvaltningen. Samtidigt ha nya risker framträtt, exempelvis för ett utlämnande i strid mot offentlighets- och sekretesslagen och för behandling av uppgifter i strid mot EU:s dataskyddsförordning eller reglerna i 2 kap. 6 § andra stycket regeringsformen om förbud mot övervakning eller kartläggning av enskildas personliga förhållanden. Dessutom har ny författningsreglering införts för att möta ökade risker för informationssäkerheten, se till exempel säkerhetsskyddslagen (2018:585) och lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen).

Det har inte varit möjligt att ta upp dessa komplexa frågor inom ramen för denna vägledning.

eSam