Vägledning

Designprinciper och krav för eget utrymme

ES2022-04

Juni 2022

Innehållsförteckning

1 Inledning

1.1 Bakgrund

eSams medlemmar har uttalat ett behov av att konkretisera eSams juridiska vägledningarna kring eget utrymme i hur man utformar säkra lösningar med eget utrymme i digitala tjänster. Denna vägledning är baserad på Arbetsförmedlingens designprinciper och krav vid utformning av e-tjänster med eget utrymme (Dnr Af-2021/0092 7368).

1.2 Syfte

Eget utrymme saknar en tydlig legaldefinition men är trots detta ett vedertaget begrepp i offentlig förvaltning. Stöd för myndigheter att tillhandahålla servicetjänster eller presentationstjänster i form av eget utrymme finns i undantagsbestämmelsen från handlingsoffentlighet i 2 kap 13 § Tryckfrihetsförordningen och myndighetens serviceskyldighet enlighet 6 § Förvaltningslagen. Har myndigheten väl bestämt att tillhandahålla e-tjänst med eget utrymme tillkommer krav på tjänstens utformning.

Denna vägledning syftar till att stödja personer som arbetar med utformning av e-tjänster att fatta rätt beslut avseende utformningen och utveckling av eget utrymme vid utveckling av lagliga och rättssäkra e-tjänster. Kravlistan är generell och gör inte anspråk på att vara uttömmande. Det kan därför förekomma andra särskilda krav som behöver beaktas. Ett exempel på sådana är krav på tillgänglighet enligt lag (2017:1937) om tillgänglighet till digital offentlig service (DOS-lagen). Denna vägledning och checklistan för digital tillgänglighet bör därför användas parallellt vid utformning av webbgränssnitt.

1.3 Målgrupp

Denna vägledning är avsedd i första hand för personer som har en roll i organisationen som arbetar med utformning och utveckling av e-tjänster med eget utrymme, exempel på sådana roller kan vara produktägare, IT-arkitekter, service designer, Front-End/Back-End utvecklare och UX designer.

1.4 Vad är eget utrymme?

Ett eget utrymme kan beskrivas som en insynsskyddad elektronisk plats som bara användaren har åtkomst till. Ett eget utrymme tillhandahålls som en service åt användaren ofta som en servicetjänst eller presentationstjänst men även andra former

existerar. Eget utrymme kan också tillhandahållas i syfte att samla information i eget konto och att dela denna information med andra.

Egna utrymmen är oftast avsedda för att upprätta, bekräfta och skicka in handlingar till myndigheten, att ta emot och förvara handlingar från myndigheten, att ta del av sammanställd information från myndigheten, andra myndigheter och aktörer. Handlingar kan t.ex. upprättas genom att spara en delvis ifylld e-tjänst som kan göras klar och skickas in vid ett senare tillfälle.

En hel e-tjänst behöver inte utgöras av eget utrymme. Det egna utrymmet kan t.ex. vara begränsat till ett visst processteg (serviceskede). Informationen i det egna utrymmet är inte att betrakta som allmänna handlingar, väl inkommen hos myndigheten utgör ansökan en allmän handling förvarad hos myndigheten i ett verksamhetssystem.

En fördjupad beskrivning kring de juridiska aspekterna av eget utrymme återfinns i eSams vägledningar inom området[1].

[1] https://www.esamverka.se/stod-och-vagledningar.html

2 Begrepp och definitioner

Följande begrepp och definitioner är antingen juridiska begrepp med eller utan legaldefinitioner. Vissa har direkt stöd i lag medan andra är *rättsfigurer* som har vedertagen juridisk betydelse eller tillämpning. Flera av dessa begrepp förekommer som föremål för kravuppfyllnad. Därför är bra att känna till innebörden av dessa, i synnerhet vid utformning av e-tjänster med eget utrymme.

Begrepp	**Definitioner**
Allmän handling	En handling som förvaras hos en myndighet och är inkommen till eller upprättad hos en myndighet.
Anvisat mottagningsställe	Funktion för automatiserad behandling som myndigheten har anvisat för försändelser.
Bastjänst eller API	Applikationsgränssnitt för kommunikation mellan maskin och maskin
Direktåtkomst	Det finns ingen legaldefinition av begreppet direktåtkomst. Med direktåtkomst avses vanligtvis att någon har direkt tillgång till någon annans informationssamling och på egen hand kan söka efter information, dock utan att kunna påverka innehållet i informationssamlingen.
Drift- och säkerhetsrelaterad information	Upplysningar som är nödvändiga för att tillhandahålla och administrera tjänsten, upprätthålla dess funktionalitet och säkerhet.

	-Driftsrelaterad information utgörs i regel av metadata som visar på hur en användare har rört sig i tjänsten, hur denne har navigerat på sidan, klickströmmar samt hur många användare som har använt tjänsten och dess olika funktioner. -Säkerhetsrelaterad information utgörs av uppgifter som samlas in vid inloggning och identitetskontroll, exempelvis personnummer och användar-ID. - Säkerhetsloggar kan i vissa fall innehålla nyttoinformation
Egen hämtning	När en innehavare av ett eget utrymme från utrymmet begär uppgifter från annan myndighet eller aktör och får dem utlämnade direkt till sitt eget utrymme.
Egen delning	När en innehavare av eget utrymme överför uppgifter från utrymmet till någon annan, exempelvis enskild, myndigheten eller annan myndighet, och därmed gör uppgifterna åtkomliga för mottagaren.
E-legitimation	Alternativ till e-legitimationer är mobilt bank-id, bank-id på dator, Freja e-id plus, Telia e-legitimation, AB Svenska Pass

	eller en godkänd e-ID från ett annat EU-land. Läs mer om e-legitimationer på https://www.digg.se
E-tjänst	En digital tjänst som har ett användargränssnitt för kommunikation mellan människa och maskin.
Handling	En framställning i skrift eller bild samt en upptagning som endast med tekniska hjälpmedel kan läsas, avlyssnas eller på annat sätt uppfattas.
Hjälptjänst	Tjänst för att ge stöd till användare av en E-tjänst eller att förklara uppgifter som lämnas till användare i en E-tjänst.
Känsliga personuppgifter[2]	Särskilda kategorier personuppgifter som bland annat rör uppgifter om hälsa, sexualliv, sexuella läggning, ras och etnisk tillhörighet, religion, politiska åsikter eller fackföreningstillhörighet.
Mottagningsfunktion	En funktion hos myndigheten där elektroniska handlingar mottas, ankomstregistreras, diarieförs och i vissa fall kvitteras.
Nyttoinformation	Upplysningar om vilka val en användare har gjort eller det

[2] Se artikel 9.1 i EU:s dataskyddsförordning

	faktiska innehållet i de uppgifter denne själv har lämnat, t ex kontaktuppgifter, profiluppgifter, anteckningar eller innehållet i utkast, nedladdningar eller gjorda sökningar.
Personuppgift	Upplysning som avser en identifierad eller identifierbar fysisk person.
Presentationstjänst	En typ av e-tjänst där innehavaren av ett eget utrymme får handlingar visade utan att det som visas blir tillgängligt för andra.
Servicetjänst	En typ av e-tjänst där innehavaren av eget utrymme kan utforma utkast till handlingar i sitt utrymme, få uppgifter förifyllda eller annars utlämnade, antingen av den som tillhandahåller utrymmet eller annan med stöd av egen hämtning eller egen delning, sända handlingar till en mottagningsfunktion och vidta andra nödvändiga åtgärder.
Serviceskede	Ett förlopp (process) där användaren för egen räkning hanterar uppgifter utan att det är fråga om ärendehandläggning och utan insyn från utomstående.

Upptagning (för automatisk bearbetning)	Dator- eller datalagrad information som kan läsas, avlyssnas eller uppfattas på annat sätt endast med tekniska hjälpmedel.
Verksamhetssystem	Den it-miljö där myndigheten eller annan svensk myndighet utför sitt arbete.

3 Designprinciper och krav

3.1 Allmänt

Vid utformning av e-tjänster med eget utrymme aktualiseras ett antal frågeställningar av juridisk, administrativ och teknisk karaktär. Juridiken ställer i regel krav på vad som ska skyddas, hur ansvar bör fördelas och skyldigheter uppfyllas medan administrativa åtgärder och tekniska lösningar säkerställer en effektiv regelefterlevnad. Att implementera rätt administrativa och tekniska åtgärder är därför en förutsättning för att leva upp till gällande lagkrav.

I det följande kommer ett antal krav att ställas. Beakta varje krav utifrån föremålet för det som ska utvecklas och avsedd funktionalitet. Vissa krav kanske inte är tillämpliga eftersom de helt enkelt inte är relevanta. Bortse då ifrån dessa. Det kan finnas krav du anser saknas i checklistan. Beakta då dessa krav istället.

3.2 Grundfunktionalitet

Eget utrymme kan användas för olika syften och rymma olika funktioner. Vissa funktioner finns uteslutande i *servicetjänster* medan andra förekommer i så kallade *presentationstjänster*. Den grundfunktionalitet som förekommer i e-tjänster med eget utrymme bärs upp av rättsliga krav. Delningsfunktioner och kvittenser tillhör i regel grundfunktionaliteten i servicetjänster, exempelvis funktion för att skicka handlingar till en angiven mottagare. Hämtningsfunktioner är också i regel en *presentationstjänst* i vilken myndighetsinformation eller information från andra aktörer sammanställs och visas i eget utrymme.

Åtkomst till eget utrymme förutsätter att användaren har loggat in i tjänsten - på sitt konto eller e-brevlåda. För detta behövs en säker behörighetshantering med e-identifiering av innehavaren samt vid behov hantering av fullmakter för exempelvis gode män eller andra företrädare.

Kraven nedan är på intet sätt uttömmande utan utgör endast en förteckning över de vanligaste funktionerna och vilka krav som gäller för dessa.

	Checklista för grundfunktionaliteten	
1	Utforma eget utrymme i e-tjänsten så att det krävs inloggning med stark autentisering genom godkänd e-legitimation eller annan säkerhetslösning så som två-faktors autentisering	☐
2	Utforma inloggningen beroende på om det är en privatperson eller ett företag. Olika kategorier av användare kan kräva olika inloggningstekniker. Det behöver vara tydligt med vilken roll man loggar in.	☐
3	Vid *egen delning,* utforma delningsfunktionen så att information delas med avsedd mottagare först efter att användaren samtyckt till att informationen lämnas ut.	☐
4	Vid *egen delning* ska en kvittens lämnas när uppgifterna finns tillgängliga för myndigheten, även när uppgifterna delas med en annan myndighet.	☐
5	Vid *egen hämtning*, utforma funktionen så att uppgifterna inhämtas först efter en uttrycklig begäran.	☐
6	Vid *egen hämtning*, utforma funktionen så att innehavaren endast kan inhämta nödvändiga uppgifter för ändamålet.	☐

7	Vid *omedelbar hämtning*, utforma funktionen så att uppgifterna som automatiskt hämtas från annan myndighet eller aktör är nödvändiga för ändamålet och inte rör någon annan än användaren.	☐
8	Vid *egen visning*[3], utforma funktionen så att uppgifterna sammanställs och presenteras på ett korrekt sätt i eget utrymme.	☐

3.3 Användargränssnitt

E-tjänsten bör utformas så att det tydligt framgår vad som är ett eget utrymme och vilken del av tjänsten som myndigheten har tillgång till. Gränserna för det egna utrymmet och myndighetens verksamhetssystem måste vara tydligt angivna. Det får exempelvis inte råda någon tvekan om när en handling blir en inlämnad allmän handling hos myndigheten.

Användargränssnittet för eget utrymme ska tydligt visa vad som finns i utrymmet, när en handling sänds därifrån och vilka exemplar som finns kvar. För att underlätta för både användaren och myndigheten bör användargränssnittet utformas för att möjliggöra självbetjäning och självadministration.

Användargränssnittet bör utformas så att användaren ska kunna rätta och radera uppgifterna samt göra egna registerutdrag eller exportera uppgifterna till annan myndighet eller företag (dataportabilitet). För att underlätta för myndigheten att fullgöra sina skyldigheter som personuppgiftsansvarig bör användargränssnittet utformas så att insamling av ostrukturerad information undviks.

[3] Se eSams Vägledning för verksamhetsutveckling inom e-förvaltningen 3.0_2018

	Checklista för användargränssnittet	
1	Utforma användargränssnittet så att det säkerställs att det är tydligt för användaren om en handling är ett utkast eller annan handling som användaren själv disponerar över (i eget utrymme) respektive en handling som är inskickad till myndigheten.	☐
2	Utforma användargränssnittet så att det tydligt framgår att varken myndigheten eller någon annan än användaren har tillgång till informationen i eget utrymme utan dennes medgivande. Om det egna utrymmet är relaterat till företag kan åtkomst ske till behöriga företrädare utan medgivande.	☐
3	Utforma användargränssnittet så att användaren informeras om att undantag från p. 2 gäller för teknisk och administrativ personal hos myndigheten som behöver tillgång till eget utrymme för att tillhandahålla teknisk support, administrera tjänsten och beivra missbruk.	☐
4	Säkerställ att användaren loggas ut efter en förutbestämd tid av inaktivitet.	☐
5	Utforma användargränssnittet så att det tydligt framgår vilken information som finns i eget utrymme.	☐
6	Utforma användargränssnittet så att det tydligt framgår att handlingar som skickas till eller på annat sätt delas med myndigheten blir allmänna handlingar.	☐

7	Utforma användargränssnittet så att fritextfält undviks till förmån för t.ex. kryssrutor, menyer. Utformas användargränssnittet med fritextfält bör användaren särskilt informeras om att inte tillföra personuppgifter till e-tjänsten som rör andra personer än n eller ange olämpligt innehåll.	☐
8	Utforma användargränssnittet så att det ger stöd för nödvändig självbetjäning vid registerutdrag och dataportabilitet samt självadministration av personuppgifter i kontot.	☐
9	Utforma användargränssnittet så att det krävs en aktiv handling för att dela uppgifter med myndigheten eller annan aktör, exempelvis genom en knapptryckning.	☐
10	Utforma användargränssnittet så att användaren måste acceptera användarvillkoren för e-tjänsten innan den används.	☐
11	Tillförs och behandlas känsliga personuppgifter i eget utrymme bör användargränssnittet utformas så att ett samtycke inhämtas innan uppgifterna laddas upp eller tillförs tjänsten på annat sätt.	☐
12	Utforma användargränssnittet med plats för tydlig och lättillgänglig information om myndigheten personuppgiftsbehandling i e-tjänsten (integritetsmeddelande).	☐
13	Utforma gränssnittet så att det hjälper användare när det blir fel. Det måste vara tydligt för användaren var felet finns och felet behöver beskrivas med text. Välformulerade felmeddelanden ger användarna möjlighet att fylla i så felfri data som möjligt i formulären.	

3.4 It- och informationssäkerhet

En förutsättning för egna utrymmen är att de utgör en privat och insynsskyddad elektronisk ”plats” för användaren. All information som finns i eget utrymme är skyddad av sekretess. Detta innebär att myndigheten aktivt måste förhindra obehörig åtkomst till informationen genom att vidta lämpliga tekniska och administrativa säkerhetsåtgärder. Vilka åtgärder som är lämpliga måste avgöras från fall till fall utifrån uppgifternas skyddsvärde.

Innan säkerhetsåtgärder vidtas bör informationen klassificeras utifrån vikten av konfidentialitet, tillgänglighet, riktighet och spårbarhet både inom och utanför användarens eget utrymme. Därtill bör en hot- och riskbedömning göras.

	Checklista för it- och informationssäkerhet	
1	Genomför en informationskartläggning, informationsklassning och en hot- och riskbedömning samt konsekvensbeskrivning enligt GDPR.	☐
2	Välj en godkänd *E-legitimation* för inloggning till eget utrymme som motsvarar kraven på tillitsnivå i förhållande till skyddsnivå.	☐
3	Vidta åtgärder så att alla sekretessmedgivanden och samtycken för personuppgiftsbehandling (inklusive återkallelse av sådana samtycken) loggas och sparas i lämpligt verksamhetssystem.	☐

4	Behörigheter ska endast tilldelas personal som i sin befattning behöver tillgång till *drift- och säkerhetsrelaterad information* för exempelvis verksamhetsutveckling, ekonomiadministration, statistikframställning, teknisk support eller för att förhindra missbruk av tjänsten. Behörigheter till *Nyttoinformation* ska inte tilldelas personal inom myndigheten	☐
5	Tilldelning av behörigheter ska ske genom delegation. Efter genomförd behovsanalys tilldelas nödvändiga behörigheter inom en angiven behörighets- och befattningsnivå.	☐
6	I anvisningarna och manualerna för e-tjänsten bör framgå den närmare innebörden av aktuella behörighets- och befattningsnivåer, vilka faktorer som ska beaktas vid tilldelning av viss behörighet och krav på kunskap hos den som förordnas.	☐
7	Behöriga befattningshavares tillgång till eget utrymme ska tekniskt övervakas med loggar och inloggning med minst två faktorer ska eftersträvas.	☐
8	Säkerställ att nödvändiga skydd finns mot skadlig kod såsom virus, trojaner och spionprogram, genom antivirusprogram, patchning och uppdaterade operativsystem.	☐
9	Tillåt endast vissa fördefinierade och etablerade filformat som är utformade enligt krav i DOS-lagen, exempelvis MS Word, PPT, Excel, PDF eller motsvarande för uppladdning i tjänsten. EXE-filer kan innehålla skadlig kod och bör därför undvikas.	☐

10	Genomför regelbundna penetrationstester av e-tjänsten för att upptäcka sårbarheter och brister i it-miljön.	☐
11	Säkerställ att nödvändigt skydd finns mot överbelastningsattacker (DDOS), exempelvis genom att filtrera bort trafiken genom system för intrångsdetektering (IDS), brandväggar eller router.	☐
12	Säkerställ att säkerhetsrelaterade händelser loggas. En säkerhetsrelaterad händelse kan exempelvis vara en tidsstämpel när uppgiften hämtades från eget utrymme, och vem (vilket system) som hämtade uppgiften, även vilken åtgärd som gjordes (hämtade/läsning, förändrade, skriva).	☐
13	Överväg om informationen i eget utrymme bör skyddas med kryptering. Ta särskilt informationens känslighet, tjänstens funktion och genomförandekostnader i beaktande. Om kryptering utgör en lämplig skyddsåtgärd behöver rutiner för säker hantering av krypteringsnycklar utformas.	☐
14	Vidta åtgärder så att information rensas automatiskt vid en viss förutbestämd tidpunkt, aktivitet eller inaktivitet. Personuppgifter får inte sparas längre än vad som är nödvändigt för ändamålet med behandlingen och så kallade datakyrkogårdar utsätter såväl enskilda som myndigheten för stora informationsrisker.	☐

3.5 Lösningsarkitektur

Lösningsarkitekturen bör ge stöd för samtliga funktioner i e-tjänsten samt säkerhets- och lagkrav. Särskilt bör arkitekturen utformas så att information i eget utrymme inte

oavsiktligt inkommer till myndigheten och därmed blir allmänna handlingar. Men arkitekturen bör också utformas så att information som finns sparad i eget utrymme är tillgänglig och riktig när innehavaren behöver den.

Arkitekturen bör även ge rätt tekniska förutsättningar för självbetjäning och självadministration samt förhindra förekomsten av funktionsglidning och sammanblandning av uppgifter.

	Checklista för lösningsarkitekturen	
1	Utforma arkitekturen så att samtliga funktioner i e-tjänsten möjliggörs med avsedd prestanda och tillräckligt hög säkerhet i förhållande till specifikation och tilldelad skyddsnivå.	☐
2	Utforma arkitekturen så att information i eget utrymme inte oavsiktligt inkommer till myndigheten och därmed blir allmänna handlingar.	☐
3	Utforma arkitekturen så att denna ger tekniska förutsättningar för administration för registerutdrag, radering och rättelser av personuppgifter.	☐
4	Utforma arkitekturen så att information lagras på ett sätt som förhindrar obehörig åtkomst.	☐
5	Utforma arkitekturen så att endast den autentiserade användaren får åtkomst till *nyttoinformationen* i dennes utrymme.	☐
6	Utforma arkitekturen så att handlingar som skickas in från eget utrymme går till ett *anvisat mottagningsställe* där handlingen kvitteras, ankomstregistreras och diarieförs.	☐

7	Verifiera att användargränssnittet ger användaren möjlighet att få en god överblick över information som hämtats från myndighetens verksamhetssystem eller från andra aktörer.	☐
8	Utforma arkitekturen så att information som kan komma att användas för produktförbättringar, statistik mm sparas i ett verksamhetssystem och inte primärt i eget utrymme. Var uppmärksam på att information som sparas i ett verksamhetssystem hos myndigheten eller annan myndighet utgör allmän handling och ska hanteras därefter.	☐
9	Utforma arkitekturen så att användarens användning av och beteende i eget utrymme inte övervakas i större utsträckning än nödvändigt i syfte att myndigheten ska få information som grund för verksamhets- och produktutveckling, administration, teknisk support och för att framställa statistik. Inga andra uppgifter än drift- och säkerhetsrelaterad information får användas för dessa ändamål.	☐

3.6 Hjälptjänster

Hjälptjänster är en vanligt förekommande del av en e-tjänst. En typ av stöd kan vara en interaktiv instruktion, exempelvis videoklipp i hur man fyller i en blankett eller en kalkylfunktion för att räkna ut ett belopp. Hjälptjänster som förutsätter insyn i användarens eget utrymme eller som kan likställas med ärendehandläggning eller myndighetsutövning är däremot mer problematiska. Hjälptjänster bör heller inte utformas så att de ger upphov till automatiserat beslutsfattande enligt förvaltningslagens mening, hänsyn behöver även tas till bestämmelserna om automatiserat beslutsfattande enligt artikel 22 i GDPR.

Hjälptjänster bör utformas så att den hjälpsökandes eget utrymme hålls intakt och att den enskilde användaren inte utsätts för integritets- och säkerhetsrisker. Som regel ska ingen annan än användaren av eget utrymme ha tillgång till den nyttoinformation som finns där. Om myndigheten har tillgång till någon annans egna utrymme innebär detta att innehållet utgör allmänna handlingar, även om det sker under en kort session då hjälpen erbjuds. Det är särskilt viktigt att hjälptjänster utformas med lagen (2017:1937) om tillgänglighet till digital offentlig service (DOS-lagen) i åtanke.

	Checklista för hjälptjänster	
1	Utforma hjälptjänster så att det krävs en aktiv åtgärd av användaren att nyttja hjälptjänsten, särskilt om denna behöver tillgång till privata uppgifter som endast finns i eget utrymme. I förekommande fall rör det sig om så kallad *egen delning*. Man bör även kunna göra ett aktivt val att inte längre kunna nyttja hjälptjänsten.	☐
2	Utforma hjälptjänsten så att endast nödvändig information görs tillgängligt för myndighetens handläggare.	☐
3	Vidta åtgärder så att oönskat intrång i den personliga integriteten inte uppstår, exempelvis genom behörighetsstyrning, säkerhetsloggar och tekniska skyddsåtgärder.	☐
4	Utforma hjälptjänster så att kopior av innehållet i eget utrymme undviks eller att nya upptagningar skapas som kan utgöra allmänna handlingar, exempelvis konversationer. Nya samlingar av allmänna handlingar bör inte byggas upp för hjälptjänstens egen skull.	☐

5	Kopiorna som skapas hos och av myndigheten blir allmänna handlingar. Dessa bör tas bort efter avslutat ärende. För att ta bort dessa måste det finnas beslut om gallring.	☐

3.7 Avtal och användarvillkor

Användarvillkoren utgör en integrerad del av användaravtal som ingås av användaren av e-tjänsten. Att avtalsvillkoren utformas på ett korrekt och tydligt sätt är inte minst viktigt för att förhindra och beivra missbruk av e-tjänsten. Avtalet kan även tjäna som rättslig grund för myndighetens personuppgiftsbehandling.

Avtal ska inte användas i situationer som begränsar individer eller företag att fullgöra sina skyldigheter. Ta hjälp av juridisk kompetens inom organisationen för att utforma korrekta avtals- och användarvillkor för e-tjänsten.

	Checklista för avtal och användarvillkor	
1	Utforma villkoren så att det tydligt framgår att ett civilrättsligt avtal ingås mellan myndigheten och den enskilde användaren när denne accepterar villkoren.	☐
2	Utforma villkoren så att de tydligt anger e-tjänstens avsedda användningsområde.	☐
3	Utforma villkoren så att innebörden av eget utrymme förklaras, med särskild betoning på att ingen annan än användaren har tillgång till förrän dessa har skickats in till myndigheten eller delats med någon annan aktör.	☐
4	Utforma villkoren så att det tydligt framgår att endast inskickade handlingar blir föremål för myndighetens handläggning och beslut.	☐

5	Utforma villkoren så att myndighetens skyldigheter beskrivs, inte minst för att rättfärdiga nödvändig personuppgiftsbehandling (tillämpas endast om rättslig grund är fullgörande av avtal).	☐
6	Utforma villkoren så att användarens skyldigheter tydligt anges, exempelvis att inte bereda obehöriga tillgång till e-tjänsten, att inte ladda upp otillåtet innehåll eller sprida skadlig kod genom att ladda upp och dela smittat innehåll.	☐
7	Utforma villkoren så att följderna vid missbruk av tjänsten tydligt framgår, exempelvis rätten att stänga av användaren från tjänsten, radera konto och andra rättsliga åtgärder.	☐
8	Utforma villkoren så att det är tydligt för användaren att administrativ och teknisk personal hos myndigheten har rätt att använda drifts- och säkerhetsrelaterad information för att göra analyser och sammanställa statistik samt rensa information om det föreligger misstanke om missbruk av e-tjänsten.	☐
9	Utforma villkoren så att eventuella ansvarsbegränsningar (friskrivningar) avseende tjänstens funktion och prestanda framgår, t ex att vissa funktioner endast stöds av en viss typ av webbläsare eller är beroende av en fungerande internetanslutning. Friskrivningar rörande säkerhet bör inte göras om dessa riskerar att undergräva den elektroniska ”platsens” status som eget utrymme.	☐

10	Ange vem som är innehavare av immateriella rättigheter och att otillåten kopiering av källkod även utgör ett brott. Om öppen källkod används i någon del av produkten, utforma villkoren så att upphovsrätten och de särskilda licensvillkoren framgår.	☐
11	Ange i villkoren tillämplig lag och var eventuella tvister ska lösas.	☐

3.8 Information om personuppgiftsbehandling

Enligt artikel 13 och 14 i den allmänna dataskyddsförordningen (DSF) har den registrerade rätt till information som rör behandlingen av dennes personuppgifter. Det är den som är personuppgiftsansvarig som är skyldig att kommunicera denna information, som ska vara koncis, klar, tydlig, begriplig och lättillgänglig. Därmed bör varje e-tjänst innehålla ett specifikt integritetsmeddelande som anger förutsättningarna för myndighetens behandling av användarens personuppgifter. Integritetsmeddelandet bör kommuniceras tydligt innan användaren registrerar sitt konto och nyttjar en e-tjänst. Integritetsmeddelandet får inte gömmas i användarvillkoren och bör därför inte utgöra en del av avtalet. Det finns inga krav på att användaren ska intyga att denne läst integritetsmeddelandet.

Krav på godkännande av integritetsmeddelandet bör undvikas då det inte är fråga om samtycke till behandling av personuppgiftsbehandling. Denna rätt uppstår med stöd av allmänintresset eller avtal.

Ta hjälp av juridisk kompetens inom organisationen för att utforma ett korrekt integritetsmeddelande för e-tjänsten.

	Checklista för information om personuppgiftsbehandlingen	
1	Ange i integritetsmeddelandet att myndigheten är personuppgiftsansvarig för behandling av personuppgifter i e-tjänsten samt hur man kommer i kontakt med myndigheten. Ange även om det finns någon annan personuppgiftsansvarig vid sidan av myndigheten, t ex en annan myndighet med vilken uppgifterna delas.	☐
2	Ange ändamålet för personuppgiftsbehandlingen, dvs varför personuppgifter behöver samlas in och behandlas i e-tjänsten. Det kan finnas olika ändamål beroende på i vilket skede man befinner sig i. Om personuppgifterna kommer att användas vid ett senare tillfälle för ett annat ändamål bör detta anges. Likaså om ni använder personuppgifter som har samlats in för ett annat ändamål.	☐
3	Ange på vilken rättslig grund myndigheten behandlar personuppgifter i e-tjänsten. I regel görs detta med stöd av allmänintresset men även fullgörande av avtal kan i vissa fall vara lämpligt. Det senare om det saknas lagstöd för att åberopa allmänintresset som rättslig grund men ändå faller inom myndighetens uppgifter.	☐
4	Utforma texten så att det tydligt framgår om och vilken information som hämtas från andra aktörer och skäl till detta, om ni har en direktåtkomst till ett register hos en annan myndighet eller öppen data.	☐

5	Utforma texten så att det tydligt framgår om, när och med vilka andra personuppgiftsansvariga som personuppgifter delas eller överförs. Denna information bör även framgå i direkt anslutning till att användaren delar information i eget utrymme.	☐
6	Ange om personuppgifter delas eller förs över till aktörer utanför EU och EES-området och de rättsliga förutsättningarna för detta.	☐
7	Ange lagringstiden för personuppgifter i eget utrymme respektive i verksamhetssystem som används för e-tjänstens tillhandahållande.	☐
8	Ange vilka rättigheter innehavaren har i det enskilda fallet att begära registerutdrag, rättelse, radering (och i vissa fall dataportabilitet), samt tillvägagångssätt.	☐

Bilaga 1 Tillämpliga lagar

1.1

Eget utrymme vilar mot ett undantag i Tryckfrihetsförordningen om handlingsoffentlighet. Men även andra lagar och regler påverkar utformningen av e-tjänster med eget utrymme. Främst är följande lagar aktuella; Offentlighet- och sekretesslagen, Förvaltningslagen, den allmänna dataskyddsförordningen (GDPR) och den kompletterande dataskyddslagen samt registerförfattningarna. Vidare aktualiseras Myndigheten för samhällsskydd och beredskap - MSB föreskrifter på informationssäkerhetsområdet och i undantagsfall säkerhetsskyddslagen i den mån e-tjänsten bearbetar eller lagrar säkerhetsskyddsklassificerade uppgifter (vilket starkt avråds från). Avtalslagen påverkar utformningen av användarvillkoren för tjänsten och när ett avtal anses vara ingått.

För en mer utförlig genomgång av lagstiftningen hänvisas till eSams juridiska vägledningar om eget utrymme.

1.2 Tryckfrihetsförordningen (1949:105)

Tryckfrihetsförordningen (TF) är en av Sveriges grundlagar. och ger bland annat uttryck för offentlighetsprincipen. Huvudregeln är att alla och envar ska ha rätt att ta del av allmänna handlingar (2 kap 1 §) om det inte föreligger sekretess.

En allmän handling är alla slag av uppgifter som är dokumenterade antingen på papper eller elektroniskt och förvaras hos myndigheten i ett verksamhetssystem (2 kap 3 och 6 §§).

Eget utrymme stödjer sig på ett undantag från offentlighetsprincipen. En handling som förvaras hos myndigheten endast som ett led i en teknisk bearbetning eller teknisk lagring för någon annans (än myndighetens) räkning anses inte som allmän handling. Säkerhetskopior utgör heller inte allmänna handlingar. (2 kap 13 §).

1.3 Offentlighet- och sekretesslagen (2009:400)

Offentlighet- och sekretesslagen (OSL) är den allmänna lag som reglerar sekretess och tystnadsplikt hos myndigheter. Uppgifter hos en myndighet som omfattas av sekretess medför samtidigt en tystnadsplikt hos myndighetens befattningshavare. Tystnadsplikten är straffrättsligt sanktionerad i 20 kap 3 § Brottsbalken och ett otillåtet röjande kan leda till böter eller fängelse i högst ett år.

Enligt 40 kap 5 § gäller absolut sekretess för sådana uppgifter som rör enskildas personliga och ekonomiska förhållanden och som endast tekniskt bearbetas eller lagras för annans räkning, dvs i eget utrymme. Bestämmelsen kompletterar undantaget för handlingsoffentlighet i 2 kap 13 § TF.

Sekretessen kan efterges (brytas) genom att den enskilde ger sitt samtycke (10 kap 1 §). När n till eget utrymme delar uppgifter med myndigheten, annan myndighet eller enskild genom *egen delning* förutsätts att denne samtyckt till att bryta sekretessen. Motsvarande gäller om myndigheten begär tillgång till uppgifter i samband med användarstöd (hjälptjänster).

Det är därför viktigt att användargränssnittet är utformat på sådant sätt det krävs en aktiv handling och att användaren förstår innebörden av samtycket. Ett sekretessbrytande samtycke under OSL ska dock inte förväxlas med ett samtycke för behandling av personuppgifter under dataskyddsförordningen (GDPR). För att undvika förväxling används ofta begreppet ”sekretessmedgivande”.

1.4 Förvaltningslagen (2017:900)

Förvaltningslagen (FL) gäller för handläggning av ärenden hos myndigheten. Handlingar som finns i ett eget utrymme och som ännu inte är inskickade till myndigheten befinner sig i ett *serviceskede*. Ett ärende påbörjas först när handlingen har inkommit och diarieförts hos myndigheten (22 §). Det är först när handlingen är inkommen som denna är att betraktas som en allmän handling enligt 2 kap 3 § TF.

Förvaltningslagen är direkt tillämplig eget utrymme genom myndighetens skyldighet att erbjuda den enskilde sådan hjälp som kan förenkla och förbättra kontakterna med myndigheten. För denna sakens skull finns inget uttryckligt krav på att tillhandahålla eget utrymme, men om myndigheten väl gör detta sker det med stöd av serviceskyldighet enligt 6 §. Samma bestämmelse har även i vissa fall använts till att finna stöd för behandling av personuppgifter.

Handlingar som har mottagits av myndigheten ska bekräftas. Detta framgår av 22 § och utgör grund för kravet på kvittens i samband med *egen delning*.

Såväl sekretessmedgivanden (samtycken) som samtycken för personuppgiftsbehandling bör dokumenteras och sparas. Av 27 § framgår att en myndighet som får uppgifter på något annat sätt än genom en handling ska snarast dokumentera dem, om de kan ha betydelse för ett beslut i ärendet.

1.5 Dataskyddsregleringen

De allmänna bestämmelserna om behandling av personuppgifter finns i EU:s dataskyddsförordning (EU) 2016/679 (GDPR). Denna EU-rättsakt ger varje medlemsstat ett utrymme att i vissa fall komplettera med egna nationella bestämmelser.

Sverige har i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (DSL) bland annat infört bestämmelser för att reglera förhållandet till tryck- och yttrandefriheten, rättslig grund för myndigheters behandling av personuppgifter, behandling av känsliga personuppgifter, person- och samordningsnummer samt kompletterande bestämmelser avseende behandling av personuppgifter för arkiv- och statistikändamål.

eSam är ett medlemsdrivet program för samverkan mellan myndigheter och Sveriges Kommuner och Regioner (SKR) för att underlätta och påskynda digitaliseringen inom det offentliga. eSam bildades 2015 som en frivillig fortsättning på E-delegationen. En viktig uppgift för eSam är att ta fram stöd och vägledningar som ger förutsättningar för att öka den digitala samverkan inom offentlig förvaltning.

Alla stöddokument finns på esamverka.se

I eSam ingår Arbetsförmedlingen, Bolagsverket, Boverket, Centrala Studiestödsnämnden, Domstolsverket, eHälso-myndigheten, Ekonomistyrningsverket, Folkhälsomyndigheten, Försäkringskassan, Havs- och vattenmyndigheten, Inspektionen för vård och omsorg, Jordbruksverket, Kriminalvården, Kronofogdemyndigheten, Lantmäteriet, Länsstyrelserna, Migrationsverket, Naturvårdsverket, Patent- och Registreringsverket, Pensionsmyndigheten, Polisen, Riksarkivet, Rättsmedicinalverket, Sida, Skatteverket, Skolverket, Statens institutionsstyrelse, Statens servicecenter, Statens tjänstepensionsverk, Statistiska centralbyrån, Tillväxtverket, Trafikverket, Transportstyrelsen, Tullverket och Universitets- och högskolerådet (december 2021)