

Utredning om de rättsliga förutsättningarna för AI på länsstyrelserna

Genomförd i projektet "Utforska AI inom länsstyrelserna"

Version 1

17 oktober 2025

Ansvariga för utredningen

Sofia Fridén

Therese Ortner

Catrine Nylén

Hilda Wall Gullstrand

Länsjurist, Länsstyrelsen Västra Götaland

Länsassessor, Länsstyrelsen Skåne

IT-säkerhetsjurist, Länsstyrelsen Västra Götaland

Jurist Safir, Länsstyrelsen Stockholm



Länsstyrelserna

Innehållsförteckning

Förkortningslista	4
1. Sammanfattning	5
2. Inledning	5
2.1 Uppdraget	6
2.2 Förutsättningar.....	6
3. Juridiska perspektiv.....	7
3.1 Grundläggande rättsliga principer och den statliga värdegrunden.....	7
3.1.1. Transparens och förklarbarhet	7
3.1.2. Objektivitet, legalitet och proportionalitet	7
3.1.3. Effektivitet	8
3.1.4. Etik och respekt för människors lika värde	8
3.1.5. Praktisk tillämpning.....	9
3.2 Offentlighet och sekretess.....	10
3.2.1 Allmänna handlingar	10
3.2.2. Sekretess.....	10
3.2.3. Diarieföring.....	10
3.2.4 Bevarande och gallring	11
3.2.5 Praktisk tillämpning	11
3.3 Dataskydd.....	12
3.3.1 Att behandla personuppgifter	12
3.3.2 Personuppgiftsansvar och personuppgiftsbiträden	13
3.3.3 Den registrerades rättigheter.....	13
3.3.4. Konsekvensbedömning	13
3.3.5. Praktisk tillämpning	14
3.4 AI-förordningen	15
3.4.1. Kompetensinsatser	15
3.4.2. Risknivåer	16
3.4.3. Praktisk tillämpning	17
3.5 Immaterialrätt	18
3.5.1 Upphovsrätt.....	18
3.5.2. Varumärkesrätt	18

3.5.3. Licensvillkor	18
3.5.4. Praktisk tillämpning	19
3.6 Upphandlings- och avtalsrätt	20
3.6.1. Praktisk tillämpning	21
3.7 Informationssäkerhet	21
3.7.1. IT-säkerhet och cybersäkerhet	22
3.7.2. Öppna data	22
3.7.3. Praktisk tillämpning	22
3.8 Skadeståndsrätt	23
3.8.1. Praktisk tillämpning	24
3.9 Straffrätt	24
3.9.1 Tystnadsplikt	24
3.9.2 Dataintrång	24
3.9.3 Tjänstefel	25
3.9.4 Praktisk tillämpning	25
3.10 Arbetsrätt och arbetsmiljö	26
3.10.1 Praktisk tillämpning	26
3.11 Automatiserat beslutsfattande och automatiserat beslutsstöd	27
3.11.1 Praktisk tillämpning	27
4. Slutsatser	27
Bilagor	28
Checklista vid användning av AI-chattbotar	29
Checklista för personuppgiftsbehandling vid innovation	30
Checklista arbetsrättslig analys	32
Ansvarsfull AI på Länsstyrelsen	33

Förkortningslista

AI-förordningen	Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens
BrB	Brottsbalken
Dataskyddsförordningen	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter
DIGG	Myndigheten för digital förvaltning
EDBP	Europeiska dataskyddsstyrelsen (European Data Protection Board)
eSam	eSamverkansprogrammet – ett medlemsdrivet program för samverkan mellan 41 myndigheter
FL	Förvaltningslagen (2017:900)
IMY	Integritetsskyddsmyndigheten
LOD	Lagen om den offentliga sektorns tillgängliggörande av data (2022:818)
LOU	Lag (2016:1145) om offentlig upphandling
Länsstyrelseinstruktionen	Förordning (2017:868) med länsstyrelseinstruktion
MSB	Myndigheten för samhällsskydd och beredskap
NIS2-direktivet	Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen
OSL	Lagen om offentlighet och sekretess (2009:400)
PRV	Patent- och registreringsverket
RF	Regeringsformen (1974:152)
Safir	Den länsstyrelsegemensamma funktionen för informationssäkerhet och dataskydd
TF	Tryckfrihetsförordningen (1949:105)

1. Sammanfattning

Länsstyrelserna har ett nationellt projekt som syftar till att utforska möjligheterna att använda AI på länsstyrelserna. De juridiska förutsättningarna sätter ramarna för användningen. AI-förordningen reglerar vad som gäller för olika former av AI-system utifrån ett riskperspektiv. Därutöver gäller samma lagar och regler när vi använder AI-system, som för allt annat vi gör när vi utför vårt uppdrag som statlig myndighet. Det innebär bland annat att regleringar kring handlingsoffentlighet, dataskydd och informationssäkerhet är centrala. De grundläggande rättsliga principerna och de grundläggande värden som uttrycks i den statliga värdegrunden blir också aktuella. Det innebär bland annat att länsstyrelserna behöver vara effektiva och proportionerliga samtidigt som vi är transparanta och kan förklara vad vi gör och hur vi kommit fram till våra slutsatser. Därutöver kan de rättsliga förutsättningarna variera beroende på vilken typ av AI som ska användas och för vilka uppgiftsmängder. Då flera rättsområden aktualiseras behöver ett flertal bedömningar göras innan AI-tjänster kan anskaffas, utvecklas och användas i myndighetens verksamhet.

Länsstyrelserna behöver göra egna bedömningar av vilka systemstöd som är lämpliga för vår breda och komplexa verksamhet. Ett AI-system som ger stor nyttohemtagning för en myndighet med homogen verksamhet kanske inte ger samma effekt i vår. Samtidigt kanske länsstyrelserna kan se unika fördelar med AI-stöd där just komplexiteten är anledning till att verksamhetsområdet behöver utvecklas och ges utökat systemstöd.

Denna promemoria syftar till att skapa en grundförståelse för vilka utmaningar och möjligheter länsstyrelserna har. De faktiska ramarna för ett AI-initiativ behöver dock bedömas i varje enskilt fall. Rättsutredningen avslutas med bilagor som innehåller checklistor som kan användas som stöd i bedömning av AI-system.

2. Inledning

Inom ramen för det länsstyrelsegemensamma projektet Utforska AI ska länsstyrelserna öka kunskapen om AI inom länsstyrelsekollektivet på en strategisk och taktisk nivå genom:

- Kunskapshöjande insatser
- Konkreta verksamhetsområden för lärande
- Beslutsunderlag med en rekommendation för fortsatt AI-arbete

Det första projekt målet handlar om att öka förståelsen för bland annat rättsliga förutsättningar för AI-utveckling. Det finns många juridiska aspekter att ta hänsyn till inför implementering av AI-system hos länsstyrelserna. Dessa redogörs för i avsnitt 3 nedan. Avsnittet ger en översiktlig genomgång av gällande rätt, men en djupare detaljerad utredning kommer fortsatt behöva göras inför varje införande av ett specifikt AI-verktyg. Slutsatserna redovisas i avsnitt 4.

2.1 Uppdraget

Denna promemoria syftar till att utgöra ”en juridisk möjlighetsorienterad utredning som granskar tillämpningen av AI utifrån lagar och regler som gäller för länsstyrelserna. Utredningen ska identifiera juridiska risker och möjligheter samt kommuniceras brett inom länsstyrelserna för att säkerställa medvetenhet och regelefterlevnad. Identifierade hinder bör i de fall där det är relevant lyftas vidare till beslutsfattare.” Utredningen utgör delmål 1 i projektplanen för det länsstyrelsegemensamma projektet ”Utforska AI”.

Utredningen görs utifrån den kunskap och lagstiftning som finns idag. Innan det kommit vägledande praxis från domstolarna är det mycket som kommer vara oklart. På grund av den snabba utvecklingen inom AI kommer det finnas behov av att löpande se över och uppdatera detta dokument.

I arbetet med denna promemoria har underlag hämtats från flera olika svenska myndigheter, däribland IMY, DIGG, PRV samt eSam¹. Vi har också löpande omvärldsbevakat olika svenska myndigheters arbeten med AI och deras AI-policys. Alla myndigheter har olika förutsättningar och uppdrag och hanterar olika informationsmängder. Det förklarar varför vissa myndigheter i större utsträckning tillåter olika tjänster, medan andra har en mer restriktiv hållning.

2.2 Förutsättningar

Länsstyrelsernas uppdrag är brett. Av länsstyrelseinstruktionen² framgår att länsstyrelsen ”ansvarar för den statliga förvaltningen i länet, i den utsträckning inte någon annan myndighet har ansvaret för särskilda förvaltningsuppgifter”. Det innebär att länsstyrelserna i många fall har de uppdrag som inte har någon naturlig hemvist hos någon annan förvaltningsmyndighet. En del av uppdragen anges i länsstyrelseinstruktionen, medan andra framgår av annan författning eller lämnas direkt i regleringsbrev eller genom riktade regeringsuppdrag.

Länsstyrelserna har en överenskommelse om gemensam IT-drift.³ Detta innebär att länsstyrelsernas IT-avdelning har sin hemvist hos Länsstyrelsen i Västra Götaland, men tillhandahåller IT-tjänster för samtliga 21 länsstyrelser. Enligt överenskommelsen har IT-avdelningen genom värmlänsstyrelsen ett totalansvar för länsstyrelsernas IT- och teleteknikförsörjning. Värmlänsstyrelsen ansvarar för länsstyrelsernas IT-säkerhet samt för att IT-miljön ges en ändamålsenlig, effektiv och enhetlig utformning. Uppdraget i IT-överenskommelsen fråntar inte länen deras ansvar avseende bland annat allmänna handlingar, behandling av personuppgifter och informationssäkerhet. Däremot innebär IT-överenskommelsen att enskilda län inte kan anskaffa eller nyttja IT-tjänster som kan äventyra IT-säkerheten i den gemensamma IT-miljön.

¹ Se förkortningslista ovan

² Förordning (2017:868) med länsstyrelseinstruktion

³ Dnr 115-25010-2019 Länsstyrelsen Västra Götaland

3. Juridiska perspektiv

För utveckling och användning av AI-system gäller ett stort antal regelverk. Det mest specifika är AI-förordningen, men även andra regelverk blir tillämpliga i varierande grad. I detta avsnitt har vi samlat gällande lagstiftning som kan aktualiseras vid användning eller utveckling av AI.

3.1 Grundläggande rättsliga principer och den statliga värdegrunden

AI inom offentlig sektor måste användas och utvecklas på ett ansvarsfullt sätt. Samma regelverk som normalt sett gäller för all verksamhet som bedrivs inom offentlig sektor gäller även vid val av tekniska verktyg och vid digitalisering av myndighetens verksamhet. Detta innebär att myndigheten behöver ha välutvecklade processer för att säkerställa efterlevnaden av regelverken samt på ett systematiskt sätt dokumentera hur ett tänkt AI-system förhåller sig till regelverken och de rättsliga grundprinciperna.

3.1.1. Transparens och förklarbarhet

En av anledningarna till det höga förtroende som finns för offentlig sektor i Sverige idag är att den är transparent. Var och en har med stöd av offentlighetsprincipen rätt att begära ut allmänna handlingar. För att göra det enkelt att nyttja den rätten har en myndighet också en skyldighet att dokumentera, hålla sina handlingar ordnade och på begäran lämna ut allmänna handlingar skyndsamt.

En svensk myndighet ska även vara transparent i sitt beslutsfattande.

Förvaltningslagen ställer krav på att en myndighet ska motivera sina beslut och förklara den avvägning som gjorts för att nå den aktuella slutsatsen. För att använda AI-system vid beslutsfattande krävs alltså att myndigheten kan förklara AI-systemets inre funktioner på ett sätt som de som påverkas av beslutet kan förstå. Det ligger dock i AI-systemens natur att agera självständigt och dra egna slutsatser utifrån den träningsdata som systemet tränats på och de värden som systemen försetts med. Det är ofta svårt, till och med för den som utvecklat systemet, att förklara exakt hur systemet har nått en viss slutsats.

3.1.2. Objektivitet, legalitet och proportionalitet

En svensk myndighet ska i all sin verksamhet förhålla sig sakligt och opartiskt. En myndighet ska beakta allas likhet inför lagen och var och ens rätt till skydd från betydande intrång i den personliga integriteten. Legalitetsprincipen är en demokratisk grundprincip som innebär att en myndighet bara får vidta åtgärder som har stöd i rättsordningen. Därutöver ska de åtgärder som en myndighet vidtar inte vara mer långtgående än att de står i rimlig proportion till vad som kan förväntas vinnas med åtgärden.⁴

Vid utveckling eller användning av AI ska dessa grundläggande principer vara utgångsläget. Innan en myndighet använder eller utvecklar ett AI-system är det därför viktigt att klargöra vilket rättsligt stöd som finns för det aktuella AI-systemet samt att bedöma vad syftet är med att använda eller skapa systemet och vad de

⁴ 1 kap. 1 och 9 §§, 2 kap. 6 och 21 §§ regeringsformen (1974:152), RF, och 5 § förvaltningslagen (2017:900), FL.

tänkta vinsterna förväntas bli. Dessa vinster ska sedan ställas i förhållande till de risker som systemet kan medföra för att avgöra om användning eller utveckling av AI i det enskilda fallet är proportionerligt. En sådan bedömning bör alltid dokumenteras.

Vid anskaffning eller utveckling av AI-system behöver myndigheten säkerställa att systemets funktionalitet ryms inom ramen för vad som är myndighetens uppdrag och inte har en vidare funktionalitet eller hanterar fler uppgifter än vad myndigheten är behörig att hantera. All AI-utveckling behöver ske i syfte att främja myndighetens kärnverksamheter och uppdrag.

3.1.3. Effektivitet

Myndigheter ska på ett effektivt sätt ge medborgarna service. Det framgår av den statliga värdegrunden.⁵ Effektivitet handlar om att hushålla med statens medel, men även om att handlägga ärenden snabbt, enkelt och med tillräcklig kvalitet. Myndigheternas strävan mot att vara effektiva måste vägas mot skyldigheten att samtidigt uppfylla andra krav i den statliga värdegrunden.

Utvecklingen av AI bedöms av AI-kommissionen innebära stora effektivitetsvinster och kostnadsbesparingar för offentlig sektor och förväntas leda till samhällsvinster.⁶ Att inte använda AI kan innebära risker utifrån ett effektivitetsperspektiv.

3.1.4. Etik och respekt för människors lika värde

Den offentliga makten ska utövas med respekt för alla människors lika värde och för den enskilda människans frihet och värdighet.⁷ Det innebär bland annat att myndigheter behöver säkerställa att de grundläggande fri- och rättigheterna efterlevs och att ingen blir diskriminerad i myndighetens verksamhet.

AI-modeller är ofta till sin natur icke-transparenta. En stor del av AI:s funktionalitet bygger på maskininlärning, och den metod inom maskininlärning som kallas djupinlärning. Metoden är effektiv och kan hantera stora mängder data, däremot går det inte i detalj att härleda hur resultaten tagits fram.⁸ Det uppstår en så kallad black-boxproblematik. Användaren av AI-modellen eller systemet kan se indata och ta del av den utdata som genereras, men saknar helt insyn i vad som händer inuti AI-modellen när den producerar utdata. Användaren förlorar på så vis kontrollen över hur informationen hanteras och sammansätts.

Riskerna för kränkning av var och ens fri- och rättigheter kan variera, men uppstår framförallt till följd av att AI-modeller kan ha inbyggda fördomar (bias) baserat på den data som modellen har tränats på. Till exempel kan en demografisk grupp som är

⁵ [Den statliga värdegrunden](#) (Statskontorets webbplats 2025-03-18)

⁶ [AI-kommissionens Färdplan för Sverige](#) (Regeringens webbplats 2025-06-16)

⁷ 1 kap. 2 § första stycket RF

⁸ [Analys: AI-system som är svarta lådor kan utgöra ett hinder för att uppfylla informationskraven enligt GDPR | techlaw.se](#) (Techlaw webbplats, 2025-06-16)

underrepresenterad alternativt överrepresenterad i referensdatamängder bli föremål för felaktiga bedömningar eller fördomar.⁹

3.1.5. Praktisk tillämpning

Som statlig verksamhet och som statliga tjänstepersoner har vi en skyldighet att i allt vi gör utgå från de grundläggande rättsliga principer som den statliga värdegrunden bygger på och att förhålla oss till de lagar och regler som gäller för vår verksamhet. En myndighet som vill använda AI behöver säkerställa en uppfyllelse av principerna i den statliga värdegrunden samt dokumentera, följa upp och utvärdera arbetet. Som myndighet behöver vi vara medvetna om riskerna kring AI och hantera dem strategiskt för att avgöra om och i så fall på vilket sätt AI kan vara ett verktyg för att på bättre sätt genomföra vårt uppdrag.¹⁰ I vissa sammanhang kan det vara utmanande att efterleva de grundläggande rättsliga principerna vid användning av AI inom offentlig sektor.

Att myndigheten ska förhålla sig sakligt och opartiskt innebär vid användning av AI bland annat att myndigheten behöver säkerställa att det inte förekommer diskriminering eller fördomar i den utdata som myndigheten använder i sin verksamhet. Detta kan ske bland annat genom att använda AI-system där risken för hallucinationer¹¹ är minimal, exempelvis system som är särskilt anpassade för ändamålet, tränat på en specifik datamängd och testat på ett tillförlitligt sätt. Därutöver behöver varje enskild medarbetare som använder AI ta ansvar för att vara tydlig i sin instruktion till AI-modellen, sin prompt (instruktion/indata), för att på så vis ge förutsättningar för korrekt utdata som är tillämplig i de aktuella fall där den är tänkt att nyttjas. Var och en behöver också ta ansvar för hur innehållet i den data som genereras av AI-system används och då särskilt säkerställa att den aktuella datamängden inte speglar fördomar eller innehåller andra felaktigheter.

Vid användande av AI inom offentlig sektor är det därför viktigt att ha god kunskap och förståelse för att inbyggda fördomar förekommer och att kritiskt granska den utdata som genereras. De som använder AI i sin tjänsteutövning är fullt ut ansvariga för, och ska ha full kontroll över sitt arbete. Det går inte att lägga över ansvaret på AI-systemet om något blir fel.

Det yttersta ansvaret för verksamhetens AI-användning ligger hos respektive länsstyrelses landshövding. Beslut som rör användning av AI-system behöver följa ordinarie beslutsprocesser och förhålla sig till myndighetens arbets- och delegationsordning.

⁹ [Gender shades: intersectional phenotypic and demographic evaluation of face datasets and gender classifiers](#) (Massachusetts Institute of Technology (MIT) webbplats 2025-06-16)

¹⁰ [Myndigheterna och AI - En studie om möjligheter och risker med att använda AI i statsförvaltningen](#) (Statskontorets webbplats 2025-06-16)

¹¹ Begreppet innebär att en AI-modell skapar information som är felaktig, påhittad eller orelevant.

3.2 Offentlighet och sekretess

Var och en har rätt att ta del av allmänna handlingar om inte handlingarna omfattas av sekretess.¹² Det följer av offentlighetsprincipen.

För att kunna säkerställa att offentlighetsprincipen efterlevs behöver alla myndigheter bedöma vad som utgör allmänna handlingar och vad som omfattas av sekretess enligt offentlighets- och sekretesslagen, OSL.

3.2.1 Allmänna handlingar

Handlingar som förvaras hos en myndighet, och är att anse som inkomna till eller upprättade hos myndigheten, utgör allmänna handlingar. Att en handling har upprättats innebär att den har färdigställts eller på annat sätt nått sin slutliga form.¹³ Huvudregeln är att allmänna handlingar är offentliga, om det inte finns tillämpliga bestämmelser om sekretess.

Offentlighetsprincipen omfattar inte enbart färdiga allmänna handlingar utan även så kallade potentiella allmänna handlingar. Det är sammanställningar som kan göras med olika sökningar och som myndigheten har en skyldighet att göra om det kan ske med rutinbetonade åtgärder.¹⁴

3.2.2. Sekretess

Sekretess innebär både handlingssekretess och tystnadsplikt. Det gäller inte bara för uppgifter i allmänna handlingar, utan även för uppgifter som finns hos en myndighet i sådana handlingar som inte är allmänna. Sekretess gäller som huvudregel inte bara i förhållande till enskilda utan också mellan myndigheter.¹⁵ Även internt på en myndighet är det viktigt att inte sprida sekretessbelagda uppgifter mer än vad som är nödvändigt för att utföra uppgiften. En uppgift som skyddas av sekretess får inte heller utnyttjas utanför den verksamhet för vilken den är sekretessreglerad.¹⁶

Med röjande av uppgift menas att uppgiften lämnas ut i strid mot tystnadsplikten.¹⁷ Förbudet mot att röja en uppgift gäller oavsett om det görs muntligen, genom utlämnande av allmän handling eller på något annat sätt. Otillåtet röjande av en sekretessbelagd uppgift är straffsanktionerat som brott mot tystnadsplikten. Detta ansvar har den enskilde medarbetaren som röjer uppgiften och inte arbetsgivaren. Se vidare under avsnitt 3.9 om straffrätt.

3.2.3. Diarieföring

Myndigheter har en skyldighet att upprätta register över sina allmänna handlingar.¹⁸ Registrering av allmänna handlingar bidrar även till att hålla ordning på myndighetens dokumentation.

¹² 2 kap. 1 och 2 §§ tryckfrihetsförordningen, TF.

¹³ 2 kap. 4 § TF

¹⁴ 2 kap. 6 § 2 st TF

¹⁵ 8 kap. 1 och 2 §§ OSL

¹⁶ 7 kap. 1 § OSL

¹⁷ 3 kap. 1 § OSL

¹⁸ 5 kap. 1 och 2 §§ OSL

Ett register ska innehålla uppgift om:

1. datum då handlingen kom in eller upprättades,
2. diarienummer eller annan beteckning handlingen fått vid registreringen,
3. i förekommande fall uppgifter om handlingens avsändare eller mottagare, och
4. i korthet vad handlingen rör.

3.2.4 Bevarande och gallring

Ett arkiv bildas av myndighetens allmänna handlingar, samt de minnesanteckningar eller beslutskoncept som myndigheten beslutar ska tas om hand för arkivering.¹⁹

Myndigheterna kan inte bevara alla allmänna handlingar för evigt. Allmänna handlingar får därför gallras. Gallring innebär att uppgifterna förstörs och inte kan återskapas.²⁰ För att gallring ska få ske måste det finnas ett gallringsbeslut som kan tillämpas på den aktuella handlingstypen. Statliga myndigheter får endast gallra allmänna handlingar i enlighet med föreskrifter eller beslut av Riksarkivet, om inte särskilda gallringsföreskrifter finns i lag eller förordning.

3.2.5 Praktisk tillämpning

Användning och utveckling av AI-system kräver att länsstyrelsen säkerställer att offentlighetsprincipen och sekretessreglerna följs. Myndigheten behöver därför i förväg analysera om det uppstår handlingar vid användning av AI och om dessa i så fall är allmänna. Allmänna handlingar ska hållas ordnade och diarieföring och gallring ska ske när så krävs. Allmänna handlingar som inte omfattas av sekretess ska lämnas ut på begäran. Detta gäller även sådana potentiella handlingar som inte finns vid begäran, men som myndigheten enkelt kan sammanställa. Med hjälp av AI-funktionalitet finns det sannolikt möjlighet att sammanställa fler uppgifter med så kallade ”rutinbetonade åtgärder”, vilket innebär att handlingsoffentligheten kan öka. Det kan i sin tur leda till mer omfattande sekretessbedömningar.

Enligt vissa AI-tjänsters användarvillkor sparas promptar och responsen (svar/utdata) på företagets servrar under en viss period för säkerhetsgranskning och support. Dessa sparas också i användarens chatthistorik om en inställning om automatisk radering inte gjorts. Observera att myndighetens egna säkerhetskopior som utgångspunkt inte anses utgöra allmänna handlingar.²¹

Allmän handling skulle kunna uppstå av de promptar som matas in i AI-systemet samt den respons som verktyget genererar, åtminstone om de används och expedieras. Om en begäran om utlämnande görs, och dessa uppgifter anses vara förvarade hos myndigheten, kan uppgifterna därför komma att lämnas ut. En självständig bedömning måste alltid göras vid varje begäran om utlämnande.

En prompt skulle även kunna betraktas som en slags ”mellanprodukt”, det vill säga att den inte anses vara färdigställd och inte heller tagits omhand för arkivering och därför inte omfattas av begreppet allmän handling i tryckfrihetsförordningens mening. Responsen skulle dock möjligen kunna anses vara upprättad och färdigställd,

¹⁹ 3 § arkivlagen (1990:782)

²⁰ 10 § arkivlagen och 2 kap. 1 § RA-FS 1991:1

²¹ 2 kap 13 § OSL

och därmed utgöra en allmän handling. Eftersom frågan inte prövats av domstol ännu, behöver vi ha med i beräkningen att det skulle kunna uppstå allmänna handlingar i AI-systemen. Det behöver i så fall finnas gallringsbestämmelser som reglerar när radering får ske.

När vi kommunicerar med ett externt AI-system, exempelvis en chattbott, innebär det att vi lämnar ut information. Vi vet inte hur den information som vi förser verktuget med används och sprids vidare, även om inställningen gjorts att den inte får användas som träningsdata. Länsstyrelserna ansvarar alltid för att säkerställa att den information som lämnas ut till ett AI-system hanteras på rätt sätt. Att sekretess anses röjd även vid muntlig delning av uppgifter behöver särskilt uppmärksammas när generativa AI-system som är avsedda att fånga upp ljud och samtal för exempelvis transkribering används.

Kommunikation med ett externt AI-system kan innebära ett utlämnande av uppgifter. Detta innebär att det som skrivs eller laddas upp i ett sådant AI-system som huvudregel inte får omfattas av sekretess.²² Om det är fråga om ett AI-system som länsstyrelsen själv byggt och driver i egen regi har vi kontroll över informationen och det blir i det fallet inte fråga om ett utlämnande. Det innebär att länsstyrelserna i större utsträckning kan hantera sekretessbelagd information i egenutvecklade IT-system.

Vid utveckling av egna IT-system uppkommer andra frågor kopplade till handlingsoffentligheten. Då kommer länsstyrelserna behöva ta ställning till om, och i så fall i vilken utsträckning, träningsdata, metadata och loggar av olika slag utgör allmänna handlingar.

3.3 Dataskydd

Om AI-användningen innebär att personuppgifter behandlas, aktualiseras bestämmelserna i dataskyddsförordningen²³. Därutöver kan ytterligare bestämmelser vara tillämpliga, beroende på vilken typ av personuppgifter som ska behandlas, exempelvis brottsdatalagen (2018:1177) och dataskyddslagen (2018:218) med tillhörande förordning.

3.3.1 Att behandla personuppgifter

För att en personuppgiftsbehandling ska vara laglig krävs att det finns en rättslig grund som behandlingen kan stödjas på.²⁴ Enligt dataskyddsförordningen måste det även finnas ett tydligt, specifikt och berättigat ändamål för behandling av personuppgifter. Av ändamålet framgår syftet med behandlingen och det behöver vara bestämt redan innan behandlingen påbörjas. Därutöver ska inte större mängd personuppgifter behandlas än vad som är nödvändigt för att uppfylla syftet, tillgången till personuppgifterna ska begränsas och skyddas och uppgifternas

²² 10 kap 2a § OSL innebär en sekretessbrytande bestämmelse som kan tillämpas i vissa fall när uppgifter enbart används för teknisk bearbetning och lagring.

²³ Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter

²⁴ [Rättslig grund för behandling av personuppgifter | IMY](#) (webbplats 2025-06-16).

riktighet behöver säkerställas löpande. Personuppgifter ska inte heller lagras längre än vad som krävs. Genom att uppfylla dessa krav kan myndigheten säkerställa skyddet för enskilda personers grundläggande fri- och rättigheter enligt dataskyddsförordningen och minska risken för att personuppgiftsincidenter inträffar.

3.3.2 Personuppgiftsansvar och personuppgiftsbiträden

Den som bestämmer mål och medel med en personuppgiftsbehandling är personuppgiftsansvarig. Om en annan part behandlar personuppgifter för den personuppgiftsansvariges räkning blir denne ett personuppgiftsbiträde, exempelvis en leverantör av ett AI-system som behandlar personuppgifter för verksamhetens räkning. I sådana fall krävs ett personuppgiftsbiträdesavtal mellan den ansvarige och biträdet. Syftet med ett personuppgiftsbiträdesavtal är att säkerställa att båda parter följer dataskyddsförordningen, är medvetna om sina skyldigheter och åtaganden och skyddar de personuppgifter de kommer i kontakt med. I avtalet ska den personuppgiftsansvarige bland annat lämna skriftliga instruktioner till personuppgiftsbiträdet som sätter ramarna för vad biträdet får göra med personuppgifterna.

3.3.3 Den registrerades rättigheter

Länsstyrelsen behöver säkerställa de registrerades rättigheter, såsom information till den registrerade, rättelse och radering. Information till den registrerade innebär att länsstyrelsen som personuppgiftsansvarig ska lämna information både när uppgifterna samlas in och om den registrerade begär det. Det ställer höga krav på att myndigheten vet hur personuppgifterna hanteras och att de inte används för andra syften än vad länsstyrelsen samlade in uppgifterna för samt informerat den registrerade om. Det finns även krav på dokumentation för att möjliggöra transparens. Utöver den grundläggande information som alltid ska lämnas till den registrerade när personuppgifter behandlas uppställs särskilda krav på information till den registrerade när en myndighet tillämpar automatiserat beslutsfattande eller profilering. Artikel 29-gruppen²⁵ har tagit fram riktlinjer, som ratificerats av Europeiska dataskyddsstyrelsen (EDPB²⁶), om automatiserat individuellt beslutsfattande och profilering där ytterligare vägledning ges om hur bland annat öppenhet bör tillämpas i fråga om profilering. Enligt riktlinjerna behöver den registrerade kunna få tillräckligt mycket information hur beslut fattats och kunna förstå skälen till beslutet.

3.3.4. Konsekvensbedömning

Om AI-systemet kommer behandla känsliga personuppgifter, en omfattande mängd personuppgifter, automatiska beslut eller någon av de andra kriterier som IMY

²⁵ Arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter var en rådgivande och oberoende arbetsgrupp inom EU som ansvarade för att ta fram riktlinjer för tillämpningen av dataskyddsdirektivet.

²⁶ European Data Protection Board

konkretiserat utifrån EDPB:s riktlinjer²⁷ ska en konsekvensbedömning göras. Om en behandling av personuppgifter sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska det före behandlingen av personuppgifter, alltså innan AI-systemet används, göras en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. Det innebär också att en konsekvensbedömning behöver göras om redan pågående behandlingar ändras så att den övergår till en sådan ”typ av behandling” som sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Det kan exempelvis bli aktuellt om fler uppgifter samlas in än som ursprungligen var planerat eller om nya tekniska lösningar införs.

3.3.5. Praktisk tillämpning

Personuppgifter kan förekomma i många olika sammanhang när en myndighet använder AI. Personuppgifter kan finnas i allt från träningsdata, indata och utdata till metadata. Det är myndighetens skyldighet som personuppgiftsansvarig att upprätthålla skyddet för den registrerades rättigheter. Detta innebär att myndigheten som personuppgiftsansvarig ska lämna information om vilka personuppgifter myndigheten behandlar. För att kunna göra detta krävs att myndigheten identifierar när behandlingar av personuppgifter sker vid användande av AI. När personuppgifter används i externa AI-system är det därför av stor vikt att noggrant granska tjänstens användarvillkor för att se när personuppgifter kan komma att användas och utifrån vilka ändamål. Länsstyrelsen är som utgångspunkt alltid ansvarig för den behandling av personuppgifter som sker när myndigheten använder AI, även när personuppgifter behandlas på ett till synes oförutsebart sätt och även när behandlingen sker av en leverantör som länsstyrelsen ingått avtal med. Undantag kan gälla för funktioner som länsstyrelsen uttryckligen motsatt sig och där tydliga instruktioner har lämnats till leverantören om att sådana funktioner inte ska ingå i AI-systemet.

Innan länsstyrelsen implementerar eller använder AI är det därför viktigt att kontrollera om personuppgifter förekommer eller kan komma att användas. Ett sätt att uppfylla principen om uppgiftsminimering är att använda sig av syntetisk data, pseudonymiserad data²⁸ eller träningsdata som helt rensats på personuppgifter. Om verksamheten har tänkt använda personuppgifter i ett AI-system behöver verksamheten först säkerställa att det finns ett tydligt ändamål och en rättslig grund för detta. Om så är fallet ska bedömas vilken typ av personuppgifter det kan röra sig

²⁷ [När ska en konsekvensbedömning genomföras? | IMY](#) (webbplats 2025-03-07)

²⁸ Art 4.5 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (dataskyddsförordningen).

om och vem som är ansvarig för behandlingen. Om det behövs ska personuppgiftsbiträdesavtal tecknas. Därutöver behöver verksamheten säkerställa att samtliga grundläggande principer i dataskyddsförordningen efterlevs när personuppgifter hanteras, bland annat genom att säkerställa att inte fler personuppgifter används än vad som är nödvändigt och att uppgifterna skyddas på ett tillräckligt sätt. Om känsliga personuppgifter ska behandlas bör även en konsekvensbedömning göras. Innan personuppgifterna används ska verksamheten lämna information till den registrerade som på ett tydligt sätt förklarar hur och varför uppgifterna används samt vilka rättigheter den registrerade har i samband med det.

3.4 AI-förordningen

EU:s AI-förordning²⁹ började gälla i vissa delar i februari 2025 och gäller som svensk lag. Den kommer i stort sett gälla fullt ut från och med den 2 augusti 2026. Syftet med förordningen är bland annat att skapa en trygg och etiskt hållbar miljö för AI-innovation inom EU, samtidigt som den skyddar medborgarnas fri- och rättigheter. Att bryta mot förordningens regler kan medföra sanktioner.³⁰

Förordningen är i grunden en produktsäkerhetslagstiftning, vilket innebär att reglerna ska se till att AI-system och de produkter med AI-teknik som släpps ut på marknaden inom EU ska vara säkra. Den anger olika krav och skyldigheter för utvecklare, produkttillverkare, distributörer, importörer, tillhandahållare, ombud och användare av AI både inom privat och offentlig sektor. Högst krav ställs på kategorin leverantör. En leverantör är den som utvecklar ett AI-system, en tillhandahållare är den organisation som använder det färdiga systemet i sin verksamhet. Privat användning omfattas inte av AI-förordningen.

3.4.1. Kompetensinsatser

För leverantörer och tillhandahållare ställs krav på AI-kunnighet³¹, dvs att personal som arbetar med driften av och använder systemen har tillräcklig kunskap. Kravet medför inte någon skyldighet att mäta de anställdas kunskaper om AI, men en tillräcklig nivå av AI-kompetens med beaktande av de anställdas tekniska kunskap, erfarenhet och utbildning ska säkerställas. Vad som är en tillräcklig nivå är inte exakt definierat. EU-kommissionen har dock skapat en webbplats med frågor och svar kring vad det innebär i praktiken³².

För att uppfylla kravet på AI-kunnighet i AI-förordningen ska leverantörer och tillhandahållare av AI-system åtminstone säkerställa en allmän förståelse av AI inom organisationen, exempelvis vad AI är för något, hur det fungerar och vilken AI som används inom organisationen. Vidare behöver riskerna med de AI-system som

²⁹ Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens (AI-förordningen)

³⁰ Behovet av svensk anpassning till AI-förordningen har utretts i SOU 2025:101

³¹ Artikel 3.56, 4 och skäl 20 AI-förordningen

³² [AI Literacy - Frågor & Svar | Shaping Europe's digital future](#) (webbplats 2025-09-05)

används analyseras, dvs vad de anställda behöver veta när de hanterar ett särskilt AI-system, vilka risker de måste vara medvetna om och hur riskerna kan minskas.

Utifrån den analysen bör kompetensåtgärder vidtas med tanke på skillnader i teknisk kunskap, erfarenhet och utbildning samt i vilket sammanhang AI-systemen ska användas, inom vilket område och för vilket ändamål. Övervägandena omfattar både juridiska och etiska aspekter. Därför är det viktigt med en förståelse för AI-förordningen inom hela organisationen.

3.4.2. Risknivåer

AI-förordningen utgår från ett riskbaserat system. Risknivåerna delas in i fyra kategorier; minimal risk, begränsad risk, hög risk och oacceptabel risk.³³ Ju högre risk, desto högre krav ställs på systemet. Risknivån bedöms utifrån syftet och funktionen med AI-systemet.

Den riskbaserade metoden utgör grunden för en proportionell och effektiv uppsättning bindande regler i AI-förordningen. År 2019 utarbetades sju icke-bindande etiska riktlinjer för tillförlitlig AI av den oberoende AI-expertgruppen som utsetts av EU-kommissionen. De sju principerna omfattar mänskligt agentskap och mänsklig tillsyn, teknisk robusthet och säkerhet, integritet och dataförvaltning, transparens, mångfald, icke-diskriminering och rättvisa, samhällets och miljöns välbefinnande samt ansvarsskyldighet³⁴.

Oacceptabel risk

AI-system med oacceptabel risk är förbjudna och omfattar system som betraktas som ett tydligt hot mot människors grundläggande rättigheter. Exempel på detta är biometrisk kategorisering, ansiktsgenkänning i realtid på allmänna platser för brottsbekämpande ändamål eller system som kan läsa av människors känslor på en arbetsplats.

Hög risk

AI-system med hög risk är system som kan ha en betydande skadlig inverkan på hälsa, säkerhet och grundläggande rättigheter. I bilaga III till förordningen listas de AI-system som utgör hög risk, ett sådant exempel är anställningsförfarande med programvara för analys och sortering av CV. Listan kan utökas eller ändras allteftersom.

Ett AI-system med hög risk måste uppfylla de krav som AI-förordningen ställer innan det kan tas i bruk eller släppas ut på EU:s marknad. Dessa krav inkluderar bland annat riskhanteringssystem, cybersäkerhet, transparens, mänsklig tillsyn, CE-märkning, övervakning av driften, sparande av loggar och teknisk dokumentation. En tillhandahållare ska se till att AI-system med hög risk används på ett säkert sätt inom organisationen, vilket till exempel innebär att se till att AI-systemets bruksanvisning följs och att berörda arbetstagare och fackförbund informeras innan systemet börjar användas.

³³ Artikel 5-17 samt skäl 26 AI-förordningen

³⁴ Skäl 27 AI-förordningen, [Ethics-guidelines-AI_SV.pdf](#) (webbplats 2025-10-27)

Begränsad risk

För system med begränsad risk ställs krav på transparens, dvs upplysningsskyldighet, för att säkerställa att de som använder systemet informeras om att det är ett AI-system. Exempelvis den som använder en chattbott på en hemsida ska bli medveten om att man interagerar med en maskin.

Minimal eller ingen risk

För AI-system med minimal eller ingen risk finns inga särskilda regler i AI-förordningen. Här menas system som inte utgör någon påtaglig fara för användarna eller samhället. Exempel på sådana system är spamfilter och stavningskontroller, som endast utför enklare, begränsade uppgifter.

3.4.3. Praktisk tillämpning

Eftersom rättsområdet är nytt finns inte någon vägledande praxis och därmed inte svar på alla frågor om tillämpningen.

Länsstyrelsen kan omfattas av AI-förordningens regler för olika kategorier. Exakt vilka regler som gäller kan variera och beror på omständigheterna i varje enskilt fall, till exempel beroende på hur länsstyrelsen har tänkt att utveckla eller använda ett AI-system, för vilket ändamål och i vilken typ av verksamhet. Om länsstyrelsen både utvecklar och därefter använder ett AI-system behöver dels reglerna för leverantörer, dels reglerna för tillhandahållare följas. Länsstyrelsen kan alltså omfattas av reglerna för olika kategorier samtidigt.

Även om inte alla bestämmelser i AI-förordningen har trätt i kraft än är det viktigt att länsstyrelserna förbereder sig inför att hela AI-förordningen börjar gälla. En del av förberedelsen kan vara att inventera vilka AI-system som redan används i organisationen samt vilka som planeras. Utveckling och användning av AI-system bör vara förenlig med AI-förordningen redan från start för att undvika behov av att ändra i systemen eller rutinerna i efterhand, vilket skulle kunna bli både besvärligt och kostsamt.

Om länsstyrelsen avser att utveckla ett AI-system behöver en bedömning av vilken risknivå det har göras tidigt i processen. Även ett system som normalt sett inte används för högriskändamål kan betraktas som ett högrisksystem, beroende på vilket ändamål det används för. Tänk på att det som görs i tjänsten inte utgör privat användning, även om ett privat konto eller en egen enhet används, och att AI-förordningen då är tillämplig.

DIGG:s förtroendemodell³⁵ för artificiell intelligens kan användas som stöd. Modellen är ett verktyg för självutvärdering av användningen av AI inom offentlig förvaltning. Det främsta syftet med den är att leva upp till kraven på öppenhet och transparens som finns inom svensk offentlig förvaltning.

³⁵ [Förtroendemodellen - Sveriges Dataportal](#) (webbplats 2025-09-16)

DIGG har också ett beräkningsverktyg som ger ett underlag för att bedöma nyttan med olika digitala förändringsinitiativ eller investeringar.³⁶

3.5 Immaterialrätt

3.5.1 Upphovsrätt

Upphovsrätt innebär att den som exempelvis har tagit en bild, skapat ett konstverk, skrivit en bok eller komponerat ny musik har upphovsrätt och ensamrätt till sitt verk. Upphovsrättsinnehavaren bestämmer själv hur det får användas.

För att få upphovsrätt till ett verk krävs att den som skapat det är en människa som kunnat göra fria kreativa val. Därför har ingen automatisk upphovsrätt till en bild som helt är framställd av ett AI-system utifrån en prompt³⁷. Användarrätten av det genererade materialet kan även vara skyddad genom användarvillkor som godkänts innan verktyget började användas, dvs leverantören kan förbehålla sig rätten att använda materialet. Därför är det viktigt att alltid noga läsa användarvillkoren.

En arbetsgivare är inte automatiskt upphovsrättsinnehavare för verk skapade av anställda inom tjänsten, även om arbetsgivaren har en långtgående nyttjanderätt. Däremot kan arbetsgivaren avtala med en anställd om att den ekonomiska upphovsrätten ska övergå till arbetsgivaren.

Normalt sett har den som skapat en webbsida upphovsrätt till informationen på sidan. Flera AI-modeller tränas på information som inhämtats genom webbskrapning. Webbskrapning innebär automatisk insamling och sortering av information direkt från en webbplats. Företag och organisationer kan på så sätt samla stora mängder data från webben för att sedan exempelvis använda det för att träna en AI-modell. Om en AI-modell ska tränas på information som inhämtats genom webbskrapning behöver det först säkerställas att det finns rättigheter att använda det upphovsrättsliga materialet.

3.5.2. Varumärkesrätt

Om någon ansökt och fått sitt varumärke godkänt av PRV får denne en registrerad ensamrätt. Att utan tillstånd av rättighetsinnehavaren använda ett varumärke kan utgöra varumärkesintrång.

3.5.3. Licensvillkor

Licens betyder tillåtelse på latin och innebär att man har tillåtelse till något. Det kan vara att någon får nyttja någon annans immateriella rättighet, såsom ett patent, ett varumärke eller en programvara som är skyddad av upphovsrätt. Den som köper rätten att använda något som är licenserat kallas licenstagare. Nyttjanderätten gäller bara om licenstagaren följer licensvillkoren. Den som nyttjar någon annans immateriella rättighet utan licens gör sig skyldig till intrång.

Den som har rättigheterna till ett upphovsrättsskyddat verk kan ge någon annan licensrätt att använda verket genom att teckna licensavtal. En licens innebär en

³⁶ [Beräkningsverktyg för nyttor och kostnader | Digg](#) (webbplats 2025-09-16)

³⁷ [Vem har upphovsrätt på AI-genererade bilder? - PRV](#) (webbplats 2025-09-01)

rättighet att använda verket och licensavtalet reglerar hur verket får användas. För att förenkla för parterna finns olika licensstandarder. Dessa kan användas för att tydliggöra för parterna vilken typ av licensvillkor som ska gälla i varje enskilt fall av användande av upphovsrättsskyddat material. En sådan standard är de så kallade creative commons licenserna.³⁸

Vid användning eller utveckling av AI-tjänster kan AI-licenser användas för att säkerställa att användningen är laglig. Om licensvillkoren är tydliga vet samtliga aktörer vad de har att förhålla sig till. Detta minskar riskerna för att immateriella rättigheter används på fel sätt och medför att skapare av det skyddade verket får erkännande för sitt arbete och blir kompenserad på ett korrekt sätt. Att bryta mot licensavtal kan medföra både skadeståndsskyldighet, förlorat anseende och bristande förtroende.

Det finns olika typer av AI-licenser. Vilken licens som är lämpligast att använda beror på vilken typ av teknologi som ska utvecklas och i vilket sammanhang som tjänsten ska användas. En vanlig licenstyp vid utveckling av AI-system är den så kallade open-source-licensen. Open-source, eller öppen källa, tillåter en användare att se källkoden samt att återanvända och ändra den för att på så vis utveckla egna system där koden kan användas och utvecklas för egna ändamål. Utöver open-source-licenser kan även nämnas kommersiella licenser och akademiska licenser. Varje licenstyp är förknippad med egna krav och villkor.³⁹

Inom ramen för open-source finns framför allt två olika licenstyper, den tillåtande licensen (permissive license) och den ömsesidiga licensen (copyleft license).⁴⁰ Den tillåtande licensen tillåter användaren att fritt använda licensen under förutsättning att upphovsmannen namnges. Källkodens skapare lämnar inga garantier utan friskriver sig ansvar för eventuella skador som kan uppstå. Licenstagaren kan i sin tur licensera ut mjukvaran till andra under egna villkor. Skyldigheten att namnge den ursprungliga upphovsmannen följer dock med källkoden även om licenstagaren själv i sin tur licenserar ut egen mjukvara. Den ömsesidiga licensen syftar till att säkerställa att den aktuella mjukvaran förblir tillgänglig för användarna. Detta innebär att en licenstagare som vidareutvecklar eller gör ändringar i en licenserad källkod åtar sig att tillämpa samma licensvillkor som man själv tecknat för den ursprungliga mjukvaran. Om en licenstagare skapar egna verk med utgångspunkt i ursprungsmjukvaran behöver det vara tydligt vilka delar av verket som omfattas av den ursprungliga mjukvaran, ett så kallat härlett verk, och vilka delar som är självständiga.

3.5.4. Praktisk tillämpning

Att mata in dokument eller bilder i ett AI-system utan tillstånd av upphovsrättsinnehavaren kan utgöra upphovsrättsintrång. På samma sätt kan det bli fråga om varumärkesintrång om någon hanterar andras varumärken utan tillstånd. Det behöver därför säkerställas att det är lagligt att hantera det material som laddas upp.

³⁸ [Om Creative Commons licenserna - CC Sweden](#) (webbplats 2025-10-15)

³⁹ [Licenser att tänka på när AI blir större - Dagens Juridik](#) (webbplats 2025-09-08)

⁴⁰ [Introduktion till open source-licenser - Carl Gleisner](#) (webbplats 2025-09-08)

Detta gäller oavsett om det är öppen information som finns på internet eller är tillgängligt på annat sätt.

Gällande AI-genererade bilder, videor och ljudfiler är det den som använder det som genererats som ansvarar för att användningen inte inkräktar på någons upphovsrätt samt att det finns tillstånd enligt användarvillkoren för AI-tjänsten att använda det. Det innebär att det är användaren och inte leverantören av AI-systemet som gör sig skyldig till upphovsrättsbrott om hanteringen är olaglig. Det går inte att lägga över ansvaret på AI-systemet.

Det kan vara svårt att avgöra i vilka fall användning av ett AI-genererat material innebär upphovsrättsintrång om det inte går att ta reda på varifrån AI-systemet hämtat sin inspiration. Eftersom vissa AI-system är tränade på material från hela internet kan resultaten ha betydande likheter med en bild eller text som redan finns. Detta skulle kunna leda till skadeståndskrav eller krav på upphovsrättsersättning.

För att undvika att länsstyrelsen eller medarbetarna gör sig skyldiga till upphovsrättsintrång behöver användaren noga granska det genererade materialet innan det används och sprids. Ett sätt att ta reda på om det finns ett liknande verk är att göra en text- eller bildsökning på webben. Detta är dock ingen garanti för att det är fritt fram att använda och sprida det AI-genererade materialet.

Eftersom den som skrivit prompten till ett helt och hållet AI-genererat material som huvudregel inte har upphovsrätt till det genererade materialet, kan det vara otillåtet att ange att man har upphovsrätt när sådan inte föreligger⁴¹.

Vid användning eller utveckling av egna AI-system är det viktigt att noggrant gå igenom användarvillkoren för att se vilka licensvillkor som källkoden är förknippad med. Verksamheten behöver ha en god kännedom om vilken mjukvara som utvecklats av tredje part som används och hur dessa får inkluderas i det egna vidareutvecklingsarbetet. Om exempelvis källkoden begärs ut som allmän handling är det viktigt att känna till om licensvillkoren kan medföra att viss del av källkoden skulle kunna omfattas av villkor, exempelvis om den ursprungliga upphovsmannen behöver anges eller om vissa licensvillkor behöver säkras upp genom licensavtal.

Länsstyrelsernas webbplatser innehåller texter, kartor, bilder, ljud och illustrationer som är upphovsrättskyddade och får inte användas utan tillstånd. Detsamma gäller våra logotyper. Om någon utan tillstånd genomför webbskrapning skulle det kunna innebära immaterialrättsligt intrång. Länsstyrelsen behöver avgöra i varje enskilt fall om sådant tillstånd kan lämnas.⁴²

3.6 Upphandlings- och avtalsrätt

När länsstyrelsen ingår avtal och gör inköp måste vissa bestämmelser följas för att på bästa sätt ta tillvara konkurrensen på marknaden och hushålla med skattemedlen. Detta framgår av reglerna för offentlig upphandling. Upphandlingsregelverket bygger på fem grundläggande principer:

⁴¹ [Vem har upphovsrätt på AI-genererade bilder? - PRV](#) (webbplats 2025-09-01)

⁴² [Rekommendation om öppna licenser och immaterialrätt | Digg](#) (webbplats 2025-09-01)

- icke-diskriminering
- likabehandling
- proportionalitet
- öppenhet
- ömsesidigt erkännande⁴³

Om upphandlingens värde understiger vissa tröskelvärden kan tjänsten direktupphandlas.⁴⁴ Oavsett upphandlingsform ingår myndigheten ett avtal med leverantören för den upphandlade tjänsten. Av länsstyrelsernas respektive arbetsordningar följer vilka som får teckna avtal och attestera betalningar för myndighetens räkning. Enskilda medarbetaren har oftast inte rätt att ingå avtal för en länsstyrelse. Det kan även gälla möjligheten att förbinda myndigheten vid avtalsvillkor genom att nyttja gratistjänster. Innan en AI-tjänst upphandlas eller avropande behöver en noga kravställning göras.

3.6.1. Praktisk tillämpning

Vid anskaffning av AI-funktionalitet i form av programvara, licenser eller tjänst kan bedömningar behöva göras om det är aktuellt att inleda en offentlig upphandling eller göra ett avrop från Kammarkollegiets ramavtal. Viss AI-funktionalitet ingår i tjänster som länsstyrelserna redan har upphandlat eller avropat. Då behövs som utgångspunkt ingen ytterligare konkurrensutsättning göras. I vissa fall kan dock kompletterande bedömningar behöva göras för att säkerställa att även funktionalitet som tillkommer inom ramen för ett befintligt avtal uppfyller krav på informations-säkerhet etc. Även när det finns möjlighet enligt upphandlingsregelverken att göra en direktupphandling kan det finnas riktlinjer på respektive länsstyrelse som styr formerna för anskaffningen. IT-överenskommelsen reglerar också i vilken mån enskilda länsstyrelser får köpa egna IT-tjänster. IT-säkerheten i den gemensamma IT-miljön får inte äventyras.

Det är viktigt att ha kunskap om AI-tekniken för att kunna genomföra en korrekt kravställning vid upphandling och för att relevanta frågor ska kunna ställas till leverantören. Innan avtal tecknas bör testkörning av systemet göras med syntetisk data för att säkerställa att den har önskad funktionalitet. Kvalitetsuppföljning bör göras löpande. Uppsägningsvillkor och eventuellt vite behöver regleras på förhand om det visar sig att systemet brister i något hänseende. Att avtalsvillkoren kan upplevas som svårlästa eller att rätten att ingå avtal för myndigheten uppfattas som byråkratisk är inte anledning att kringgå beslutsordningen genom att nyttja privata konton i tjänsten. Det rör sig fortfarande om en behandling av myndighetens information.

3.7 Informationssäkerhet

Informationssäkerhet handlar om ansvar, riskmedvetenhet och helhetssyn. Länsstyrelserna behöver arbeta för att förhindra att information läcker ut, förvanskas och förstörs, samt att rätt information finns tillgänglig för rätt personer i

⁴³ 4 kap. 1 § lag (2016:1145) om offentlig upphandling (LOU)

⁴⁴ 19a kap. lag (2016:1145) LOU

rätt tid. Att myndigheter ska jobba med informationssäkerhet framgår av Myndigheten för samhällsskydd och beredskaps (MSB) föreskrift 2020:6. Av föreskriften framgår bland annat att myndigheten ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av utpekade standarder. Det framgår vidare att informationssäkerhetsarbetet ska utformas utifrån de risker och behov som myndigheten identifierar. Det ska omfatta all behandling av information som myndigheten ansvarar för och integreras med myndighetens befintliga sätt att leda och styra sin organisation.⁴⁵ Föreskriften riktar sig mot respektive myndighetsledning, men det är viktigt att minnas att länsstyrelserna har gemensam IT, en gemensam förvaltning av gemensamma komponenter och processer. Av MSB:s föreskrift kan utläsas att informationssäkerheten ska omfatta all behandling av information som myndigheten ansvarar för.

3.7.1. IT-säkerhet och cybersäkerhet

IT-säkerhet handlar om förmågan att förebygga, förhindra, upptäcka, begränsa och åtgärda konsekvenser av obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid databehandling samt dator- och telekommunikation. IT-säkerhet är en central del av informationssäkerheten. Kraven på att en myndighet ska införa ändamålsenliga och proportionerliga säkerhetsåtgärder följer av MSB:s föreskrifter.⁴⁶

Genom införandet av NIS2-direktivet⁴⁷ i svensk rätt (cybersäkerhetslagen) följer nya krav på IT-säkerhet. NIS2-direktivet syftar till att uppnå en hög gemensam cybersäkerhetsnivå inom EU. Därigenom tillkommer krav på riskanalyser och olika former av säkerhetsåtgärder. Kraven förenas med möjlighet att utdela sanktionsavgifter. Länsstyrelserna föreslås bli tillsynsmyndighet, vilket ställer särskilda krav på egen regelefterlevnad.

3.7.2. Öppna data

Lagen om den offentliga sektorns tillgängliggörande av data⁴⁸ kallas i dagligt tal för öppnadata lagen. Den stiftades som ett led i genomförandet av Europaparlamentets och rådets direktiv om öppna data och vidareutnyttjande av information från den offentliga sektorn. Det övergripande syftet är att främja den offentliga sektorns tillgängliggörande av data för vidareutnyttjande, särskilt i form av öppna data. Tillgängliggörandet förutsätter att krav på informationssäkerhet och skydd av personuppgifter kan upprätthållas och att det inte innebär ett röjande av uppgifter som skyddas av sekretess eller risker för Sveriges säkerhet.

3.7.3. Praktisk tillämpning

Inför användning av AI ska en bedömning utifrån ett informationssäkerhetsperspektiv göras. Övergripande frågor är; vem har rätt till vilken information, hur får

⁴⁵ 5 § MSBFS 2020:6

⁴⁶ 6 § MSBFS 2020:6

⁴⁷ Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, proposition (2025/26:28) Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag

⁴⁸ Lag (2022:818) om den offentliga sektorns tillgängliggörande av data, LOD

informationen användas internt, får informationen delas externt och i så fall med vem? För att få hela perspektivet krävs att en informationssäkerhetsanalys genomförs och att den information som ska hanteras (datamängden) är informationsklassad⁴⁹. Länsstyrelserna har en gemensam klassningsmodell och ett metodstöd som förvaltas av den gemensamma funktionen för informationssäkerhet och dataskydd, Safir.⁵⁰ Safir förvaltar även de länsstyrelsegemensamma användarriktlinjerna för informationssäkerhet⁵¹ som kan aktualiseras vid användning av AI.

Datamängden behöver vara rensad på information som är olämplig för det syfte som AI-systemet avser uppfylla. Genom att riskbedöma informationsmängden och klassificera innehåll som ska användas klarläggs vilka skydds nivåer som informationen bör omfattas av. Tekniska, organisatoriska och administrativa säkerhetsåtgärder kan behöva vidtas. En informationsklassning ger en fingervisning av hur informationsmängden får hanteras, spridas, bevaras och delas. Notera att även information som inte omfattas av sekretess kan vara olämplig att använda om den är verksamhetskritisk.

Informationssäkerhet och IT-säkerhet är aspekter som normalt fångas upp i ordinarie utvecklings- och förvaltningsprocesser. Det är därför viktigt att följa beslutade ordinarie processer.

Bra AI-funktionalitet kräver hög kvalitet på data. Det kan handla om hur data är strukturerad, ordnad och metadatasatt. Att arbeta med datakvalitet kan även underlätta tillgängliggörande av data i större utsträckning, exempelvis genom tillhandahållande av öppna data. Samtidigt ger stora mängder strukturerad data nya risker genom möjlighet till kartläggning och analys av samband.

Vid en informationsklassning är det därför viktigt att bedöma om den aktuella informationsmängden som kommer att behandlas i ett AI-system möjliggör sammanställningar av en stor mängd aggregerade data. Verksamheten behöver i sådana situationer ta ställning till om modellen kan identifiera sårbarheter i myndighetens organisation, kartlägga funktionalitet och brister eller skapa risk- och sårbarhetsanalyser, och klassa systemet därefter.

3.8 Skadeståndsrätt

Arbetsgivare har principalansvar för sina arbetstagare. Som huvudregel ansvarar arbetsgivaren för eventuella skador som en medarbetare orsakar.

Skadeståndsansvar kan bli aktuellt bland annat vid person-, sak-, eller förmögenhetsskador som orsakats genom fel eller försummelse i

⁴⁹ En informationsklassning innebär en värdering av informationsmängderna med utgångspunkt i aspekterna konfidentialitet, riktighet och tillgänglighet. Länsstyrelserna har ett gemensamt metodstöd som består av mallar, utbildningsmaterial, presentationer med mera. Metodstödet finns på den länsstyrelsegemensamma samarbetsytan för informationssäkerhetsanalyser, [Informationssäkerhetsanalyser - Start](#) (2025-03-06).

⁵⁰ [Länsstyrelsernas gemensamma modell för informationsklassning](#)

⁵¹ [Användarriktlinjer för informationssäkerhet](#)

myndighetsutövning. I vissa fall kan en myndighet även bli skadeståndsskyldig när felaktiga upplysningar eller råd lämnats.

Bristen på transparens i AI-system innebär att det kan vara svårt att bevisa ett orsakssamband mellan systemets funktion och en uppkommen skada. EU-kommissionen hade därför lagt fram ett förslag till ett AI-ansvarsdirektiv som innehöll en bevislättning för den som lidit en skada. Syftet med direktivet var att göra det lättare att driva utomobligatoriska skadeståndsanspråk för skador orsakade av AI. Förslaget har dock dragits tillbaka efter att politisk överenskommelse inte kunnat nås. I avsaknad av EU-gemensam lagstiftning gäller nationell skadeståndsrätt tillsvidare.

3.8.1. Praktisk tillämpning

Länsstyrelsen behöver beakta risken för skadeståndsanspråk för eventuella skador som kan uppstå på grund av de AI-system som används. För att minimera riskerna för skador behöver en noggrann bedömning av potentiella risker och konsekvenser göras på förhand. Vidare är det viktigt att säkerställa en mänsklig kontroll (s.k. ”human in the loop”) av AI-genererad utdata för att säkerställa att det inte förekommer uppenbara felaktigheter som, beroende på användning, skulle kunna leda till att skadeståndsanspråk riktas mot myndigheten.

3.9 Straffrätt

Straffrättsliga perspektiv kan aktualiseras vid användande av AI. Framför allt rör det bestämmelser i brottsbalken (BrB) som gäller för tjänstepersoner, såsom brott mot tystnadsplikt och tjänstefel. Även dataintrång kan bli aktuellt i detta sammanhang. Om en myndighet använder AI-system i tekniska produkter såsom exempelvis drönare eller självkörande fordon, kan även andra brott aktualiseras såsom exempelvis vållande till kroppsskada.

3.9.1 Tystnadsplikt

Otillåtet röjande av en sekretessbelagd uppgift är straffsanktionerat som brott mot tystnadsplikt.⁵² Tystnadsplikten enligt OSL gäller för myndigheter och de som deltar i myndighetens verksamhet.⁵³

3.9.2 Dataintrång

Dataintrång regleras i brottsbalken.⁵⁴ Den som olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling, eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift, kan dömas för dataintrång. Dataintrång kan aktualiseras vid användning av AI-system exempelvis vid olovlig åtkomst till data för att träna algoritmer. Brottet omfattar också situationer av behörighetsöverskridande, dvs. när någon har faktisk tillgång till uppgifter i ett register, men använder detta på ett olovligt sätt.

⁵² 20 kap. 3 § BrB

⁵³ 2 kap. 1 § OSL

⁵⁴ 4 kap. 9c § BrB

Det är bara tillåtet att göra sökningar och ta del av uppgifter som är nödvändiga för att utföra sina arbetsuppgifter, även om man tekniskt sett har tillgång även till annan information. Det är därför viktigt att säkerställa att åtkomst till automatiserade system är begränsad till behöriga användare. Om ett AI-system används för att automatisera åtkomst till olika system kan ansvarsfrågan bli mer komplex, särskilt om AI-systemet agerar autonomt. Rättsliga bedömningar av AI-system måste därför ta hänsyn till både tekniska och juridiska aspekter, inklusive AI-systemets autonomi och användarens egna ansvar.⁵⁵

3.9.3 Tjänstefel

Tjänstefel enligt brottsbalken⁵⁶ innebär att en person vid myndighetsutövning uppsåtligen eller av oaktsamhet genom handling eller underlåtenhet åsidosätter vad som gäller för uppgiften.

Enligt AI-förordningen kan länsstyrelsen ha rollen som både leverantör och tillhandahållare. Oavsett om länsstyrelsen är leverantör eller tillhandahållare av AI-system finns en skyldighet enligt AI-förordningen att bedöma potentiella systemrisker utifrån utformningen, funktionen och användningen av deras tjänster, inklusive risker som kan uppstå vid felaktig användning av AI-system. Leverantörer av AI-system med hög risk måste dokumentera och förklara sina val av riskhanteringsåtgärder och inkludera rimligen förutsebar felaktig användning i sina bruksanvisningar. Leverantörer av AI-modeller med systemrisk är skyldiga att utföra avancerade modellutvärderingar och säkerställa en adekvat skyddsnivå för att minimera risker.⁵⁷

3.9.4 Praktisk tillämpning

Länsstyrelsen behöver beakta risken för att incidenter kan inträffa vid användning av AI-teknik. För att minimera riskerna för incidenter behöver en noggrann bedömning av dessa samt potentiella konsekvenser göras på förhand.

Om en anställd använder ett AI-system på ett sätt som strider mot det avsedda ändamålet eller AI-leverantörens bruksanvisning, och detta leder till skada för enskilda eller det allmänna, kan det utgöra tjänstefel eller brott mot tystnadsplikten. Ett annat exempel är om en anställd helt förlitar sig på ett AI-system för att fatta beslut utan att säkerställa att systemet är korrekt konfigurerat eller att genererad utdata är tillförlitlig.

Därutöver är det viktigt att myndighetens information inte används på ett oförutsebart sätt eller att medarbetare tar del av mer information än vad som ryms inom den egna befogenheten när AI tränas eller promptas. Att som medarbetare ta del av mer uppgifter i myndighetens system än vad som behövs för den egna tjänsteutövningen kan innebära ett dataintrång.

⁵⁵ Svensk och europeisk IT-rätt, Hajo Michael Holtz, 2024, modul 4C

⁵⁶ 20 kap. 1 § BrB

⁵⁷ Art 55 AI-förordningen

3.10 Arbetsrätt och arbetsmiljö

En arbetsgivare har arbetsledningsrätt, vilket innebär att det är arbetsgivaren som avgör om AI ska användas eller inte och i så fall på vilket sätt. En arbetsgivare behöver dock göra en del bedömningar utifrån vilken påverkan ett införande kan få på medarbetarna utifrån flera perspektiv såsom exempelvis förändrade arbetsuppgifter, arbetsmetoder och arbetsmiljö. En arbetsgivare kan också behöva upprätta en risk- och konsekvensanalys utifrån arbetsmiljölagens bestämmelser och utifrån vad som framgår däri överväga om införandet av AI-verktyg kan innebära en sådan förändring av arbetsmiljön att det tillkommer ytterligare skyldigheter för arbetsgivaren.

Enligt brottsbalken⁵⁸ kan arbetsmiljöbrott aktualiseras om en arbetsgivare uppsåtligt eller av oaktsamhet inte följer de krav som ställs i arbetsmiljölagen för att förebygga ohälsa eller olycksfall. Detta kan inkludera brister i säkerheten vid användning av AI-system som påverkar arbetsmiljön.

En arbetsgivare har rätt att besluta om och införa nya arbetsverktyg i verksamheten. Om ett AI-system används utan att nödvändiga säkerhetsåtgärder vidtas, kan detta utgöra ett åsidosättande av arbetsmiljöansvaret. Exempel på detta kan vara:

- Bristande riskbedömning av AI-systemets påverkan på arbetsmiljön
- Underlåtenhet att utbilda personal i hur AI-systemet ska användas säkert
- Felaktig implementering av AI-system som leder till olyckor eller ohälsa⁵⁹.

3.10.1 Praktisk tillämpning

En noggrann risk- och konsekvensanalys gällande vilken påverkan AI-systemet kan få på arbetstagarna kan behöva göras innan införandet. De AI-system som används bör ingå i det systematiska arbetsmiljöarbetet på myndigheten för att löpande följa upp användningen och utvärdera dess påverkan på arbetsmiljön. Det kan också vara lämpligt att tidigt involvera och informera fackliga organisationer samt att fundera över vilka krav som ställs vid rekryteringen av personal.

Länsstyrelsen är enligt AI-förordningen skyldig att säkerställa att arbetstagarna har adekvat och tillräcklig utbildning i de system som de ska använda. Skriftliga rutiner behöver tas fram som löpande uppdateras. Det är viktigt att det är tydligt hur AI-systemen får och inte får användas. Det behöver också säkerställas att kompetensen upprätthålls inom länsstyrelsen så att medarbetarna har rätt kunskaper för att kunna bedöma riktigheten i det material som AI-verktyget skapar och för att behålla den mänskliga kontrollen (human in the loop). Risken är annars att nödvändig kompetens och erfarenhet förloras.⁶⁰ Även ur ett kontinuitetsperspektiv är detta viktigt.

⁵⁸ 3 kap. 10 § BrB

⁵⁹ [Analysera hur arbetsplatsen påverkas av att införa generativ AI och förbered omställningen | Digg](#) (webbplats 2025-09-18)

⁶⁰ [Analysera hur arbetsplatsen påverkas av att införa generativ AI och förbered omställningen | Digg](#) (webbplats 2025-09-18)

3.11 Automatiserat beslutsfattande och automatiserat beslutsstöd

Myndigheter får fatta automatiska beslut.⁶¹ Det kan i speciallagstiftning finnas undantag för automatiserat beslutsfattande. Exempelvis framgår av dataskyddsförordningen att den registrerade har rätt att inte bli föremål för ett beslut som grundas på automatiserad behandling om det får rättsliga följder eller på liknande sätt påverkar honom eller henne i betydande grad⁶². För varje skriftligt beslut ska det finnas en handling som visar: dagen för beslutet, vad beslutet innehåller och vem eller vilka som har fattat beslutet. När beslutet fattats automatiserat ska detta framgå, i stället för en namngiven beslutsfattare.

Automatiserade beslut innebär beslut som fattas helt på maskinell väg utan att en människa är delaktig i beslutsfattandet. Automatiserat beslutsstöd innebär att en automatiserad bedömning av omständigheterna i ärendet görs. Denna bedömning används sedan av en människa som stöd vid dennes beslutsfattande. Eftersom själva beslutet fattas av en människa är automatiserat beslutsstöd inte detsamma som ett automatiserat beslut.

3.11.1 Praktisk tillämpning

Ett automatiserat beslutsfattande kan vara lämpligt för beslut där det finns tydliga regler för när ett tillstånd eller en ansökan ska beviljas och beslutet grundas enbart på uppgifter som den enskilde själv lämnat. Det skulle också kunna tillämpas på beslut som grundas på uppgifter som efter godkännande från den enskilde tillförts beslutsunderlaget.⁶³ Oftast har automatiserat beslutsfattande inget med AI att göra utan är helt vanliga datorprogram som beslutar enligt förutbestämda regler. När AI-teknik används för automatiserade beslut blir beslutsprocesserna ännu mer komplicerade och svåra att förstå.⁶⁴ Innan AI används vid automatiserade beslut behöver bedömningar göras kring till vilken grad det är lämpligt. Myndighetsbeslut ska alltid motiveras, vara transparenta och förutsebara.

4. Slutsatser

Utifrån ett juridiskt perspektiv finns goda förutsättningar för Länsstyrelserna att använda AI-system i sin verksamhet. AI-tekniken har potential att kunna effektivisera många arbetsuppgifter inom länsstyrelserna. Användning av AI kan samtidigt medföra vissa risker. Genom att känna till dessa risker och vidta åtgärder för att minska dem ökar förutsättningarna för att myndigheten kan använda AI på ett ansvarsfullt sätt. Innan en AI-funktionalitet införs behöver den tänkta effektivitetsvinsten sättas i förhållande till de rättsliga krav myndigheten har att förhålla sig till. När det exempelvis gäller de olika principerna i den statliga värdegrunden ska en balans mellan samtliga värden eftersträvas.

⁶¹ 28 och 31 §§ FL

⁶² Art 22 i dataskyddsförordningen

⁶³ Prop. 2016/17:180 s.192

⁶⁴ [Stora risker när algoritmerna tar besluten | Internetstiftelsen](#) (webbplats 2025-10-13)

Det finns många aspekter att ta hänsyn till inför implementering av AI-system hos länsstyrelserna. Vilka regelverk som blir tillämpliga och i vilken utsträckning beror på vad det är för AI-funktionalitet som planeras och hur ett AI-system är tänkt att användas. För att kunna ta ställning till förutsättningarna för att använda ett specifikt AI-system inom länsstyrelserna behöver en helhetsbedömning göras av såväl de rättsliga förutsättningarna som vilka risker och konsekvenser som aktualiseras i det enskilda fallet. En grundläggande fråga länsstyrelsen behöver ställa sig inför anskaffning eller användning av ett AI-system är vilken risknivå enligt AI-förordningen det omfattas av. System med oacceptabel risk är som nämnts förbjudna, medan system med hög, begränsad och låg risk kan användas om olika former av krav är uppfyllda.

AI-förordningen gäller parallellt med andra lagar och regler. Även om viss användning är tillåten enligt förordningen kan det finnas bestämmelser i annan lagstiftning som begränsar eller på annat sätt påverkar hur det aktuella AI-systemet kan användas för det tänkta ändamålet. Det är därför inte tillräckligt att bedöma AI-systemet bara utifrån förordningen.

Jurister, informationssäkerhets- och dataskyddssamordnare, IT-medarbetare och representanter från verksamheten behöver kunna arbeta tillsammans och ha en förståelse för varandras perspektiv och kunskap. För att möjliggöra en rättssäker AI-användning på länsstyrelserna behövs det jurister med digitaliseringskompetens, inklusive särskild AI-kompetens. Det finns behov av att de jurister som ska stötta länsstyrelserna i bedömningen av användning och utveckling av AI-system får adekvat utbildning. Denna kompetens behöver succesivt byggas upp. Det finns också behov av personal med kompetens att göra informationssäkerhetsanalyser på respektive län. Det är varje enskild länsstyrelse som ansvarar för att göra analyser av de AI-system som används.

Eftersom gällande regelverk för AI är både komplext och ännu inte prövat i domstol i någon större utsträckning är det mycket som fortfarande är oklart. För att hantera osäkerheterna och förhindra att AI-systemen hanteras på fel sätt rekommenderas att verksamheten gör en helhetsbedömning inför varje ny användning av AI-system samt dokumenterar dessa bedömningar. Vidare rekommenderas att ta fram tydliga rutiner för hur respektive AI-system får användas. På så vis får varje enskild medarbetare bästa möjliga förutsättningar för att använda de implementerade systemen på ett ansvarsfullt sätt. Som stöd vid bedömningar av AI-system kan bilagda checklistor och DIGG:s förtroendemodell användas.

Bilagor

Checklista vid användning av AI-chattbottar

Checklista för utveckling av AI-system

Checklista arbetsrättslig analys

Ansvarfull AI på länsstyrelserna

Checklista vid användning av AI-chattbottar⁶⁵

Innan du promptar – ställ dig själv dessa frågor:

1. Använder jag ett verktyg som har genomgått en informationssäkerhetsanalys?
2. Har jag tagit del av och förstått användarvillkoren för verktyget?
3. Har jag kännedom om AI-policyn och tillhörande rutiner
4. Har jag tillräcklig AI-kunnighet för att använda verktyget?
5. Använder jag endast öppen och offentlig information?
6. Delar jag inga sekretessbelagda uppgifter?
7. Delar jag inga personuppgifter?
8. Är all text avidentifierad och fri från metadata?
9. Kan jag visa detta för vem som helst om det begärs ut enligt offentlighetsprincipen?
10. Har jag rätt att använda den information jag matar in, dvs finns det ingen risk för upphovsrättsintrång?
11. Formulerar jag mig sakligt och vårdat?

Efter du fått resultatet – kontrollera detta:

1. Är svaret öppen och offentlig information?
2. Innehåller resultatet varken sekretesskyddade eller personuppgifter?
3. Är resultatet och dess källor korrekta och rimliga?
4. Finns det risk för fördomar eller partiskhet i resultatet?
5. Har jag rätt att använda resultatet, dvs finns det ingen risk för upphovsrättsintrång?
6. Är språket vårdat?
7. Följer resultatet den statliga värdegrunden?
8. Kan jag stå för och fullt ut ansvara för resultatet?

⁶⁵ Framtagen inom AI-projektet på Länsstyrelsen Skåne

Checklista för personuppgiftsbehandling vid innovation⁶⁶

Förslag på frågor att besvara för att skapa en bild av vilken personuppgiftsbehandling som är aktuell i er innovation.

Det är viktigt att du och din organisation tidigt i arbetet skapar en gemensam bild av vad ni vill åstadkomma med en innovation. I denna checklista finns förslag på frågor att besvara för att skapa en bild av vilken personuppgiftsbehandling som är aktuell i er innovation, digitalisering och digital verksamhetsutveckling.

Det är bra att under arbetets gång återkomma till dessa frågor för att säkerställa att ni följer dataskyddsförordningen. Kom ihåg att dokumentera svaren på frågorna tillsammans med era resonemang och ställningstaganden.

1. Har ni involverat dataskyddsombudet så tidigt som möjligt i arbetet med innovationen?
2. Behandlar ni personuppgifter genom/i innovationen?
 - Behandlar ni enbart uppgifter som är nödvändiga med hänsyn till ändamålet för behandlingen?
3. Ska ni samla in nya personuppgifter, eller ska ni behandla personuppgifter ni redan behandlar på ett nytt sätt?
4. Vad är det övergripande syftet med behandlingen och varför ska den införas?
5. Vilken aktör (avdelning, enhet, etc.) ska utföra behandlingen?
 - Är flera aktörer inblandade i behandlingen?
6. Vem är personuppgiftsansvarig för den pågående behandlingen? Kan ett gemensamt personuppgiftsansvar föreligga mellan er och någon ytterligare aktör?
7. Kan en biträdessituation föreligga i en eller flera delar av personuppgiftsbehandlingen?
8. Har ni säkerställt att eventuella personuppgiftsbiträden är tillförlitliga genom att de ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas?
9. I vilken omfattning sker personuppgiftsbehandlingen?
 - Hur många registrerade kommer att beröras av behandlingen?
 - Hur många personuppgifter om varje registrerad kommer att behandlas?

⁶⁶ [Checklista | Digg](#) (webbplats 2025-09-18)

10. Behandlas känsliga personuppgifter, uppgifter om lagöverträdelser eller person- eller samordningsnummer?
11. Har ni säkerställt att en rättslig grund finns för all aktuell personuppgiftsbehandling i dataskyddsförordningen och författningar som styr er verksamhet?
12. Hur ska behandlingen utföras?
 - Har ni haft inbyggt dataskydd och dataskydd som standard som utgångspunkter i framtagandet av innovationen?
 - Vilket system ska användas för behandlingen?
 - Vilka behandlingar av personuppgifter utförs, är det till exempel insamling, hämtning, lagring och gallring?
 - Har ni kartlagt alla delar av flödet av personuppgifter i innovationen (vilka komponenter som ingår, vilka behandlingar och eventuella lagringar som sker av personuppgifterna i dessa komponenter)?
 - Hur samlas personuppgifterna in? Varifrån kommer de?
 - Med vem delas personuppgifterna, till exempel andra aktörer, leverantörer, personuppgiftsbiträden, osv.?
 - Förekommer tredjelandsoverföring i någon del? Har ni i så fall säkerställt att ni har stöd för överföringen?
13. Har ni informerat de registrerade om personuppgiftsbehandlingen
14. Kan ni ta omhand begäran från registrerade om att utöva rättigheter?
15. Har ni med särskild hänsyn tagen till de risker som behandling medför vidtagit lämpliga säkerhetsåtgärder för att skydda personuppgifterna?
16. Har ni en process för att dokumentera, rapportera och hantera säkerhetsincidenter?
17. Har ni dokumenterat personuppgiftsbehandlingen som helhet, inbegripet de ändamål för vilka personuppgifter behandlas, säkerhetsåtgärder, rättslig grund etc.?

Checklista arbetsrättslig analys⁶⁷

Arbetsmiljö

- Hur stora förändringar innebär det för medarbetarna om en AI-lösning införs?
- Hur förändras arbetsmiljön för medarbetarna?
- Behövs några särskilda åtgärder ur ett arbetsmiljöperspektiv?
- Ryms eventuella förändringar inom arbetsledningsrätten?
- Behöver en risk- och konsekvensbedömning genomföras?

Information och kommunikation

- Finns en skyldighet att samråda med skyddsombud eller arbetsgivarorganisationer?
- Finns en informationsskyldighet?

Utbildning och användning

- På vilka sätt får AI-lösningen användas?
- På vilka sätt får AI-lösningen inte användas?
- Hur ska medarbetarna instrueras och utbildas i hur AI-lösningen får användas?
- Hur lång inlärningsperiod behöver medarbetarna?
- På vilket sätt säkerställer ni att användningen är i linje med verksamhetens instruktioner även över tid?

⁶⁷ [Analysera hur arbetsplatsen påverkas av att införa generativ AI och förbered omställningen | Digg](#) (webbplats 2025-10-16)

Ansvarsfull AI på Länsstyrelsen⁶⁸

VAD vill vi göra?

- Initiativ från verksamheten utifrån ett verkligt behov.
- Fokus på ändamålet – vad vill vi uppnå?
- Är AI den bästa lösningen?
- Ryms det i vårt uppdrag och budget?
- Vem ska nyttja resultatet och vem påverkas av det? En eller flera funktioner och/eller länsstyrelser, allmänheten?

VILKEN data?

- Vilken information kan behöva användas och hur?
- Förekommer personuppgifter?
- Förekommer sekretesskyddad information?
- Är informationen klassad?
- Vilka säkerhetskrav ställs på hanteringen av informationen?

HUR vill vi göra?

- Befintligt system, egen utveckling eller upphandling (LOU)?
- Vilken typ av system och risknivå enligt AI-förordningen?
- Informationssäker träningsdata?
- Dialog om tekniska förutsättningar och åtgärder för riskminimering.
- Licenser och annan upphovsrätt?
- Implementera, utvärdera, testa?
- Drift, underhåll och förvaltning?

Juridiska RAMAR

- Förhållande till statlig värdegrund och förvaltningslag?
- Uppstår allmänna handlingar? Vad ska diarieföras?
- Ansvar, krav och AI-kunskap utifrån risknivå?
- Finns begränsningar i avtalsvillkor?
- Risker utifrån skadestånd och straffrätt?

⁶⁸ Framtagen inom det nationella projektet ”Utforska AI inom länsstyrelserna”

- Krävs arbetsrättsliga åtgärder?
- Finns tydliga förhållningsregler för användaren?