Datainspektionen

Datainspektionens tillsyn av länsstyrelsernas elektroniska förvaltning

Datainspektionen granskade under år 2010 Länsstyrelsen i Västra Götalands hantering av personuppgifter i den elektroniska förvaltningen. Mot bakgrund av de uppgifter som framkom förelades Länsstyrelsen i Västra Götaland att åtgärda de brister i behandlingen av personuppgifter som Datainspektionen fann vid inspektionen. Datainspektionens beslut överklagades till Förvaltningsrätten i Stockholm som avslog överklagandet. Domen har vunnit laga kraft.

Datainspektionen har med anledning av sitt beslut och Förvaltningsrättens dom under hösten 2012 genomfört en enkättillsyn gentemot landets länsstyrelser. Tillsynen har inte omfattat Länsstyrelsen i Västra Götaland. Syftet med enkättillsynen har varit att undersöka hur personuppgifter hanteras i den elektroniska förvaltningen hos länsstyrelserna.

I det följande lämnas en sammanfattning över de yttranden som länsstyrelserna har lämnat. Sammanfattningen innehåller även Datainspektionens synpunkter och information vad gäller behandlingen av personuppgifter i elektroniska förvaltningen. Var och en av de länsstyrelser som har varit föremål för Datainspektionens granskning erhåller därutöver ett beslut utifrån de uppgifter som respektive länsstyrelse har lämnat. I besluten kommer hänvisningar att göras till denna sammanfattning.

Sammanfattningen följer i huvudsak dispositionen i enkäten.

Behandling av personuppgifter i handläggningsplattformen Platina

I vilken mån behandlar länsstyrelserna personuppgifter i elektroniska ärendehanteringssystem? På vilket sätt begränsas tillgången till personuppgifter i sådana system och finns det rutiner för tilldelningen av behörigheter?

Samtliga av de 20 stycken länsstyrelser som omfattas av Datainspektionens enkättillsyn uppger att de behandlar personuppgifter i

Postadress: Box 8114, 104 20 Stockholm
Besöksadress: Drottninggatan 29, plan 5
Webbplats: www.datainspektionen.se
E-post: datainspektionen@datainspektionen.se
Telefon: 08-657 61 00
Telefax: 08-652 86 52

handläggningsplattformen Platina. Ett antal länsstyrelser uppger att vissa enheter även använder andra elektroniska ärendehanteringssystem, till exempel i landsbygdsrelaterade ärenden. Datainspektionens tillsyn omfattar enbart personuppgiftsbehandling i handläggningsplattformen Platina. I sammanhanget vill dock Datainspektionen understryka att de regler och principer som redogörs för hur personuppgifter ska behandlas även gäller när länsstyrelserna behandlar personuppgifter i andra ärendehanteringssystem.

Länsstyrelserna har vad gäller behörigheter i Platina i huvudsak uppgett att anställda vid en viss länsstyrelse har behörighet till den egna länsstyrelsens ärenden. De anställda har dock inte behörighet till information som är belagd med sekretess eller till särskilt verksamhetsspecifika delar av handläggningsplattformen.

Datainspektionens sammantagna uppfattning är att anställda på en länsstyrelse åtminstone har läsbehörighet till samtliga ärenden som finns registrerade på den länsstyrelsen där den anställde arbetar. Vid vissa länsstyrelser ska enligt den enskilda länsstyrelsens egen rutin tilldelas behörighet efter beslut av den anställdes chef och genom IT-enhetens/den IT-säkerthetsansvariges försorg. Ett antal länsstyrelser har dock uppgett att behörigheter beställs från den gemensamma IT-enheten vid länsstyrelsen i Västra Götaland efter anmälan av den anställdes chef.

Datainspektionen vill mot bakgrund av detta lämna följande synpunkter och vägledning.

En grundläggande princip i personuppgiftslagen (1998:204) är att anställda enbart bör ha tillgång till den information som de behöver för att kunna utföra sina arbetsuppgifter. Tillgången till personuppgifter ska således vara behovsstyrd och inte obegränsad (9 § personuppgiftslagen). Med hänsyn till att Platina innehåller stora mängder personrelaterad information, varav vissa uppgifter kan vara av känslig eller integritetskänslig karaktär, är det viktigt att behörigheten begränsas till vad den anställde behöver utifrån verksamhetsområde och arbetsuppgifter. Datainspektionen anser därför att det inte är förenligt med personuppgiftslagen att tilldela samtliga anställda inom en och samma länsstyrelse behörighet till alla personuppgifter som hänför sig till den egna länsstyrelsens ärenden. I sammanhanget vill Datainspektionen understryka att det inte är tillräckligt ur integritetsskyddshänseende att enbart begränsa tillgången till personuppgifter utifrån om uppgifterna är belagda med sekretess eller inte. När personrelaterad information tillgängliggörs i handläggningsplattformen måste såväl offentlighets- och sekretesslagen (2009:400) som personuppgiftslagens bestämmelser beaktas.

Som har beskrivits ovan ska behörigheten i Platina bedömas utifrån vad den anställde behöver för sitt arbete. Det kan således variera utifrån vilket verksamhetsområde den anställde arbetar inom och vilka arbetsuppgifter den anställde har. Begränsningen av behörigheter bör lämpligen föregås av en analys över vilket behov av tillgång till personuppgifter som finns vid respektive länsstyrelse. Vid behörighetstilldelningen bör visst spelrum finnas. Det måste till exempel finnas möjlighet att arbeta som vikarie för en kollega exempelvis vid sjukdom eller annan kortare frånvaro. Det är dock viktigt att det finns utarbetade rutiner för tillgången till uppgifter i handläggningsplattformen och för hur behörighetstilldelningen ska utföras.

Vilken information ges till de anställda om behandling av personuppgifter i handläggningsplattformen? Finns det rutiner för åtkomstkontroll (till exempel genom logguppföljning)?
Det stora flertalet av alla länsstyrelser har uppgett att alla nyanställda genomgår en interaktiv webbaserad utbildning i Platina. Sådan utbildning har även genomförts för samtlig personal då Platina togs i drift. Ett antal länsstyrelser uppger att nyanställd personal genomgår en förvaltningsrättslig utbildning varvid information om allmänna principer för tillgång till personuppgifter i Platina och sökning efter sekretessbelagd information ges.

Datainspektionens sammantagna uppfattning är att länsstyrelserna inte ger de anställda någon allmän information vad gäller behandling av personuppgifter enligt personuppgiftslagen. Det saknas även skriftlig information för de anställda avseende vad som gäller angående personuppgiftsbehandlingen i Platina. I den mån länsstyrelserna informerar de anställda om personuppgiftslagen är informationen specifikt anknuten till en avgränsad del av behandlingen av personuppgifter, till exempel hur den anställda kan, eller får, söka efter information.

I princip samtliga länsstyrelser har angett att det i dagsläget inte genomförs några åtkomstkontroller och att det saknas rutiner för sådana åtgärder. Ett antal länsstyrelser svarar att de tekniska möjligheter till åtkomstkontroll som finns i Platina är svåra att arbeta med. Länsstyrelserna har vidare uppgett att någon åtkomstkontroll inte genomförs på grund av att sekretesskyddade uppgifter inte är tillgängliga för andra än de anställda som arbetar med den specifika uppgiften.

Datainspektionen vill mot bakgrund av detta lämna följande information. Eftersom det är den anställde själv som tillgängliggör uppgifter i Platina är det en viktig att denne känner till vilka uppgifter som får offentliggöras i handläggningsplattformen. Att enbart informera om vad som gäller för

behandling av sekretessbelagd information är enligt Datainspektionen inte tillräckligt. Det är viktigt att den anställde har en klar uppfattning av vad som är tillåtet enligt såväl personuppgiftslagens som offentlighets- och sekretesslagens bestämmelser. Länsstyrelserna ska därför se till att de anställda får relevant utbildning om vilka regler som gäller vid behandling av personuppgifter och vilken information som får behandlas i Platina. Det är därtill viktigt att de anställda vet vilka konsekvenserna blir om man bryter mot instruktionerna och andra relevanta bestämmelser.

Länsstyrelserna måste se till att minska risken för otillåten åtkomst till de personuppgifter som behandlas i systemet. Det kan åstadkommas genom systematiskt och återkommande åtkomstkontroll varigenom obehörig åtkomst kan upptäckas och beivras. Åtkomstkontroller är viktiga genom att de kan ha en avhållande verkan på anställda som kan frestas att olovligen läsa uppgifter de inte behöver för sitt arbete. Det ska finnas rutiner för åtkomstkontrollen och de anställda måste informeras om att logguppföljning utförs kontinuerligt.

Ankomstregistret Archive Manager
Används ankomstregistret Archive Manager (eller något annat elektroniskt ankomstregister) i verksamheten? Hur begränsas åtkomsten till personuppgifter, finns rutiner för åtkomstkontroll och behörighetstilldelning? Får de anställda information om vad som gäller för behandling av personuppgifter i ankomstregistret?
Samtliga länsstyrelser, förutom Länsstyrelsen Gävleborg, använder ankomstregistret Archive Manager i sin verksamhet. Länsstyrelsen i Västerbottens län uppger att de har tillgång till ankomstregistret men inte använder det.

De länsstyrelser som har tillgång till Archive Manager har utformat sitt svar gemensamt och har uppgett följande.

Länsstyrelserna tillhandahåller det elektroniska ankomstregistret gemensamt och ett personuppgiftsbiträdesavtal har upprättats med leverantören. När uppgifter skickas via e-tjänsten lagras uppgiften i systemet. Därefter skickas uppgiften automatiskt vidare till den länsstyrelsen som avsändaren har angett som mottagare. När uppgiften inkommer till ankomstregistret registreras den i Platina och förses med ett ankomstnummer vilket är den för avsändaren kända identiteten på ärendet. Alla som har behörighet i ankomstregistret har möjlighet att söka på ärendets ankomstnummer. Detta i syfte att underlätta identifieringen av de ärenden som på grund av felaktigt angiven mottagare inkommit till en annan länsstyrelse än den som ärendet härrör till. Behörighet

till Archive Manager tilldelas efter ansökan genom IT-enheten i Västra Götalands läns försorg.

Totalt uppges 24 personer ha tillgång till Archive Manager. Hur många av dessa personer som finns hos respektive länsstyrelse anges inte, men några av länsstyrelserna har i sina svar uppgett att ett fåtal personer vid den egna länsstyrelsen har en sådan behörighet. Datainspektionen uppfattar detta som att det vid varje länsstyrelse (förutom vid Länsstyrelsen Gävleborg) finns ett antal personer med behörighet till detsamma.

Någon åtkomstkontroll eller några rutiner för åtkomstkontroll finns inte vid någon av de länsstyrelser som använder Archive Manager. Vid inloggning i systemet visas en informationsruta där det framgår vilka regler som gäller för att hantera den information som registreras i systemet. Gallring av de formulär som registreras sker tre månader efter det att ärende registrerades i Archive Manager.

Datainspektionen vill mot bakgrund av vad som har beskrivits ovan lämna följande synpunkter och vägledning.

I Archive Manager mellanlagras all den information som enskilda lämnar i den publika e-tjänsten som tillhandahålls tillsammans av nästintill samtliga av landets länsstyrelser. Detta innebär att registret kan komma att innehålla stora mängder av personrelaterad information. Eftersom länsstyrelserna inte närmare kan kontrollera vilka uppgifter som avsändaren lämnar i e-formuläret, kan ankomstregistret innehålla en mängd personuppgifter som länsstyrelserna inte förväntar sig. Bland dessa uppgifter kan till exempel sådana uppgifter som enligt 13 § personuppgiftslagen är att anse som känsliga registreras. Mot bakgrund av detta anser Datainspektionen därför att det bör ställas höga krav på säkerheten.

Länsstyrelserna är enligt 31 § personuppgiftslagen skyldig att vidta tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av:

- de tekniska möjligheter som finns
- vad det kostar att genomföra åtgärderna
- särskilda risker som finns med behandlingen, och
- hur pass känsliga de behandlade personuppgifterna är.

Nedan följer en redovisning av de tekniska och organisatoriska åtgärder som Datainspektionen anser länsstyrelserna måste vidta vid behandling av personuppgifter i Archive Manager.

- Datainspektionen förutsätter att antalet personer med åtkomst till personuppgifter i ankomstregistret är begränsat till det antal personer vid varje länsstyrelse som har ett klart motiverat behov av tillgång till uppgifterna.

- För att begränsa den elektroniska tillgången till uppgifterna måste det finnas ett system för behörighetsstyrning. Med hjälp av ett sådant system bör åtkomstmöjligheterna tekniskt begränsas så mycket som det är faktiskt och praktiskt möjligt med hänsyn till den aktuella verksamheten. Länsstyrelserna måste även se till att det finns rutiner för tilldelning och kontroll av behörigheterna.

- Det måste finnas tydliga instruktioner som anger under vilka förutsättningar de anställda får ta del av de uppgifter som har registrerats i Archive Manager. Instruktionerna bör vara skriftliga och finnas allmänt tillgängliga för berörda personer, till exempel via det egna intranätet. För att minimera risken för otillåten åtkomst måste länsstyrelserna se till att de som arbetar med Archive Manager får relevant utbildning, Den anställde ska ha en klar uppfattning om vad som är tillåtet och vilka konsekvenserna blir om man bryter mot de instruktioner och regler som gäller. Det måste också på ett tydligt sätt framgå hur efterlevnaden av instruktionerna följs upp.

- Det måste finnas väl fungerande rutiner för åtkomstkontroll, i syfte att beivra obehörig åtkomst. Länsstyrelserna måste se till att det genomförs åtkomstkontroller såväl på förekommen anledning som systematiskt och återkommande i den fortlöpande verksamheten.

Publicering av personuppgifter på Internet

Har Länsstyrelsen ett offentligt elektronsikt diarium och är detta i sådana fall tillgängligt för sökning via Internet? Om Länsstyrelsen har ett sådant diarium; vilka personuppgifter visas och vilka rutiner finns kring publiceringen av personuppgifter? Publiceras känsliga personuppgifter eller personuppgifter om lagöverträdelser i det elektroniska offentliga diariet?

Samtliga länsstyrelser uppger att de har ett offentligt elektroniskt diarium som är sökbart via Internet. Det stora flertalet av alla länsstyrelser har i huvudsak uppgett följande.

Det offentliga diariet innehåller fält för diarienummer, status, in/upp-datum, ärenderubrik, avsändare/mottagare, postort, kommun, tillkomst,

beslutsdatum och enhet. I Platina finns ett fält/en funktion (”PuL-rutan”) där det ska anges om personuppgifter ska synas i samband med att ärendet publiceras i det elektroniska offentliga diariet. Grundinställningen i Platina är att fältet ska vara ikryssat så att inga personuppgifter syns och fältet måste således aktivt avmarkeras för att uppgifterna ska synliggöras via Internet. Ett antal länsstyrelser har även uppgett att det har fattats beslut om att fältet alltid ska vara ikryssat om någon av de uppgifter som är synliga på Internet avser en privatperson. Ett fåtal länsstyrelser har uppgett att rutiner angående publicering på Internet finns eller håller på att utarbetas.

Nästintill samtliga länsstyrelser uppger att sådana uppgifter som enligt 13 § personuppgiftslagen är att betrakta som känsliga eller sådana uppgifter som rör lagöverträdelser enligt 21 § personuppgiftslagen inte publiceras i det elektroniska offentliga diariet. Ett flertal länsstyrelser anger att så kallade indirekta personuppgifter, exempelvis fastighetsbeteckning, publiceras i samband med vitesföreläggande eller överklagan av bygglovsärenden.

Datainspektionen lämnar följande synpunkter och vägledning.

Diarier kan innehålla integritetskänsliga uppgifter av olika slag och kan därför inte göras omedelbart tillgängliga på Internet. Det finns åtskilliga aspekter som länsstyrelserna måste beakta så att publiceringen inte strider mot personuppgiftslagens bestämmelser. I grunden handlar det om att utforma väl fungerande tekniska och administrativa publiceringsrutiner, så att inte personuppgifter som är sekretesskyddade eller på annat sätt känsliga i integritetshänseende når obehöriga. I vissa fall kan redan uppgiften om att en person förekommer i ett ärende hos en myndighet inom ett visst verksamhetsområde vara av så integritetskänslig natur att det finns risk för att den registrerades personliga integritet kränks genom publiceringen. Så kan till exempel vara fallet i fråga om ärenden som på något sätt rör en persons brottslighet.

Som huvudregel får personuppgifter bara behandlas med samtycke från den som uppgiften rör vilket framgår av 10 § personuppgiftslagen. För att länsstyrelserna ska ha rätt att tillgängliggöra personuppgifter i ett diarium som görs allmänt tillgängligt via Internet utan att de registrerade gett sitt samtycke därtill, krävs att behandlingen är tillåten med stöd av en intresseavvägning enligt 10 § punkten f) personuppgiftslagen. Länsstyrelsen måste således ha ett berättigat intresse för behandlingen som väger tyngre än den registrerades intresse av skydd mot kränkning av den personliga integriteten. Omständigheter som spelar in vid intresseavvägningen är till exempel ändamålet med behandlingen, vilka uppgifter som behandlas och på vilket sätt behandlingen utförs.

Att publicera direkta personuppgifter, exempelvis personnamn eller personnummer, i ett offentligt elektroniskt diarium innebär en risk för otillbörliga integritetsintrång. Det är därför svårt att se något bärande skäl till att enskilda av olika anledningar ska behöva tåla att sådana uppgifter görs allmänt tillgängliga på Internet. Uppgifter som direkt pekar ut enskilda kan således normalt inte tillgängliggöras på Internet med stöd av en intresseavvägning enligt 10 § punkten f) personuppgiftslagen.

Vissa uppgifter kan uppfattas som särskilt integritetskänsliga. Det gäller till exempel uppgifter om lagöverträdelser som innefattar brott eller att någon person är föremål för vitessanktioner. Det är inte tillåtet att publicera direkta personuppgifter i dessa typer av ärenden. I undantagsfall kan det dock med stöd av en intresseavvägning vara tillåtet att publicera indirekta personuppgifter, exempelvis ärendenummer, i sådana ärenden. Känsliga personuppgifter får dock aldrig publiceras i ett diarium som tillgängliggörs via Internet. Detta gäller såväl direkta som indirekta personuppgifter.

Datainspektionen vill i sammanhanget påpeka att länsstyrelserna inte stentrianmässigt kan publicera alla dokument som registreras som ärenden på myndigheten och som innehåller personuppgifter. En bedömning av om publiceringen är tillåten måste alltid göras i det enskilda fallet utifrån bland annat i vilket sammanhang uppgifterna förekommer, vilken spridning de riskerar att få och vad publiceringen kan få för konsekvenser för den enskilde. Det är därför viktigt att länsstyrelserna har rutiner för vad som gäller för publicering i det offentliga diariet och att de anställda har fått information kring detta. Personuppgifter som publiceras på Internet blir ofta sökbara vilket innebär en väsentligt ökad risk för omfattande spridning av uppgifterna. Länsstyrelsen ska därför se till att det material som har publicerats tas bort från webbplasten när publiceringen inte längre är nödvändig med hänsyn till det ändamålet som föranlett den, det vill säga syftet med att göra diariet tillgängligt på Internet.