Datainspektionen

Vägledning för kommuner:

Personuppgifter och e-förvaltning

Innehåll

1. Inledning **3**

2. Personuppgiftslagen **4**

2.1 Allmänt 4

2.2 Hanteringsreglerna 4

2.3 Missbruksregeln 5

2.4 Personuppgiftslagen och kommunerna 5

2.5 Några grundläggande begrepp 6

3. Allmänt om e-förvaltning kommunerna **7**

3.1 Tendenser 7

3.2 Intressebalanser 7

3.3 Säkerhetspolicy och sårbarhetsanalys 8

4. Elektroniska dokument- och ärendehanteringssystem **9**

4.1 Allmänt 9

4.2 Elektroniska diarier 9

4.3 Elektronisk dokumenthantering 12

4.4 Gallring och arkivering 15

4.5 Säkerhet 15

4.6 Sammanfattning – checklista 18

5. Elektroniska tjänster **21**

5.1 Allmänt 21

5.2 Exempel på kommunala e-tjänster 21

5.3 Information i samband med tillhandahållande av e-tjänster 22

5.4 Säkerhet för personuppgifter 24

5.5 Publicering av diarier och protokoll på Internet 29

5.6 Övrig publicering av information på kommunens webbplats 30

5.7 Sammanfattning – checklista 33

6. Geografiska informationssystem **37**
6.1 Allmänt 37
6.2 Behandling av personuppgifter i GIS 37
6.3 Säkerhet 41
6.4 Sammanfattning – checklista 42
7. Mellankommunalt samarbete **45**
7.1 Allmänt 45
7.2 Personuppgiftsansvar 45
7.3 Integritetsskyddsaspekter 46
7.4 Gemensamt kommuninvånarregister och fastighetsregister 47
7.5 Säkerhet 48
7.6 Sammanfattning – checklista 50
8. Andra publikationer **51**

Omslagsbild: Stockbyte

1. Inledning

Det har alltsedan slutet av 90-talet varit ett prioriterat område för regeringen att utnyttja informationsteknikens möjligheter och skapa en väl utvecklad e-förvaltning. Datainspektionen har i regleringsbreven för 2006 och 2007 fått i uppdrag att bidra till utvecklingen av en effektiv och rättssäker elektronisk förvaltning genom att särskilt bevaka enskildas personliga integritet.

För att underlätta e-förvaltningens utveckling har det tillkommit lagändringar och specialregleringar som möjliggör dels en automatiserad hantering av personuppgifter och dels ett utökat informationsutbyte inom och mellan myndigheter. Det finns t.ex. särskild registerlagstiftning för de flesta av de stora statliga myndigheterna. Kommunernas utveckling mot e-förvaltning och alltmer IT-baserade verksamhetssystem har dock, bortsett från en specialreglering av socialtjänstens verksamhet, fått ske enbart med stöd av personuppgiftslagen (PuL).

I den kommunala verksamheten finns en medvetenhet om att dokumenthanteringen styrs av flera olika lagar, bl.a. tryckfrihetsförordningen, sekretesslagen, förvaltningslagen och arkivlagen. Däremot saknas till viss del kunskaper om personuppgiftslagens bestämmelser. Datainspektionen har mot bakgrund av sitt uppdrag, och med hänsyn till det stora förändringsarbete som för närvarande pågår inom många kommuner, sett ett behov av att ge vägledning från inspektionen för att IT-system och tjänster ska implementeras i överensstämmelse med personuppgiftslagen.

Denna vägledning omfattar behandling av personuppgifter inom den kommunala verksamheten, bortsett från socialnämndernas verksamhet som styrs av särskild registerlagstiftning. Vägledningen riktar sig främst till kommunala personuppgiftsombud, kommunjurister, förvaltningschefer och övriga medarbetare som deltar i olika e-förvaltningsprojekt. Tanken är att vägledningen ska kunna användas både vid undervisning och i det löpande arbetet. Vägledningen kan dessutom i de mer allmänna delarna tjäna som riktlinjer för behandling av personuppgifter av andra personuppgiftsansvariga än kommuner. Framför allt är förhoppningen att vägledningen ska leda till en ökad insikt om när och hur personuppgiftslagen är tillämplig.

Datainspektionen har i vägledningen försökt vara så tydlig som möjligt, bl.a. genom att ta fram olika exempel. I slutet av varje kapitel finns en kombinerad sammanfattning och checklista. Dessa checklistor bör inte betraktas som uttömmande. Eftersom många frågeställningar ännu inte är rättsligt prövade, bör det framhållas att vägledningen i många avseenden ger uttryck för Datainspektionens egna ställningstaganden.

Vid arbetet med denna vägledning har Datainspektionen tagit emot värdefulla synpunkter från VERVA (Verket för förvaltningsutveckling) och Sveriges Kommuner och Landsting.

2. Personuppgiftslagen

2.1 Allmänt

Personuppgiftslagens (1998:204) syfte är att skydda enskilda personer mot att deras integritet kränks genom behandling av personuppgifter. Lagen är huvudsakligen tillämplig på behandling av personuppgifter som helt eller delvis utförs med hjälp av datorer.

Sedan den 1 januari 2007 finns två separata regelverk i personuppgiftslagen. Utöver de s.k. hanteringsreglerna, som anger under vilka förutsättningar behandling av personuppgifter i strukturerat material är tillåten, har det kommit till en missbruksregel, enligt vilken behandling av personuppgifter i ostrukturerat material är tillåten under förutsättning att den inte kränker den enskilde.

2.2 Hanteringsreglerna

I lagen finns vissa grundläggande krav på den som behandlar personuppgifter, till exempel att personuppgifter bara får samlas in för särskilda, uttryckligt angivna och berättigade ändamål (9 §). I personuppgiftslagen anges också när behandling av personuppgifter överhuvudtaget är tillåten. Utgångspunkten är att personuppgifter bara får behandlas om den registrerade har lämnat sitt samtycke till behandlingen (10 §). Utan samtycke får uppgifterna bara behandlas när behandlingen är nödvändig i vissa situationer som anges i lagen. Det är t.ex. tillåtet att behandla personuppgifter om det är nödvändigt för att den personuppgiftsansvarige ska kunna fullgöra en rättslig skyldighet eller kunna utföra en arbetsuppgift i samband med myndighetsutövning. Det kan också vara tillåtet att behandla personuppgifter med stöd av en intresseavvägning.

För känsliga personuppgifter gäller särskilda restriktioner (13–19 §§). Med känsliga personuppgifter menas till exempel sådana personuppgifter som rör hälsa eller sexualliv. Huvudregeln är att det är förbjudet att behandla känsliga personuppgifter om den registrerade inte har lämnat sitt uttryckliga samtycke till behandlingen.

Personuppgiftslagen innehåller även regler om information till de registrerade (23–27 §§) Om den registrerades samtycke krävs för att behandlingen av hans eller hennes personuppgifter ska vara tillåten, måste samtycket alltid föregås av information. Den registrerade har också rätt att gratis en gång per kalenderår, efter skriftligt undertecknad ansökan, få besked om vilka personuppgifter om honom eller henne som behandlas och hur uppgifterna behandlas (registerutdrag).

Den registrerade har rätt att på begäran få rättelse om personuppgifterna inte har behandlats i enlighet med bestämmelserna i personuppgiftslagen, det vill säga om uppgifterna är felaktiga eller om personuppgiftsbehandlingen på något annat sätt strider mot lagen (28 §).

I personuppgiftslagen finns även regler om säkerhet vid behandlingen av personuppgifter (30–32 §§). Den personuppgiftsansvarige är skyldig att vidta tekniska och organisatoriska åtgärder för att skydda personuppgifterna och därmed åstadkomma en lämplig säkerhetsnivå. Om den ansvarige anlitar ett personuppgiftsbiträde för att utföra behandling av personuppgifter, ska det finnas ett avtal som särskilt reglerar säkerhetsfrågorna (personuppgiftsbiträdesavtal).

En myndighet som behandlar personuppgifter kan bli skadeståndsskyldig gentemot den registrerade (48 §). En del regler i lagen är också straffsanktionerade (49 §).

2.3 Missbruksregeln

Personuppgiftslagen har ändrats för att underlätta vardaglig behandling av personuppgifter som typiskt sett inte medför några större risker för kränkningar av de registrerades personliga integritet.

Enligt 5 a § personuppgiftslagen behöver hanteringsreglerna inte tillämpas på behandling av personuppgifter som inte ingår i eller är avsedda att ingå i en samling av personuppgifter som har strukturerats för att påtagligt underlätta sökning efter eller sammanställning av personuppgifter. Den som behandlar personuppgifter i ostrukturerat material, t.ex. löpande text på Internet eller sedvanliga filsystem och e-postprogram, behöver således inte längre följa personuppgiftslagens detaljerade hanteringsregler. Avsikten är att hanteringsreglerna inte ska behöva tillämpas på sådant som inte framstår som något regelrätt personregister eller någon annan form av system av uppgifter. Sådan behandling är tillåten utan andra restriktioner än att den registrerades personliga integritet inte får kränkas.

2.4 Personuppgiftslagen och kommunerna

Hanteringsreglerna i personuppgiftslagen ska tillämpas vid sådan behandling av personuppgifter som ingår i eller är avsedd att ingå i en samling av personuppgifter som har strukturerats för att *påtagligt* underlätta sökning efter eller sammanställning av personuppgifter. Det krävs således att det finns en personuppgiftsanknuten strukturering av materialet som är av viss kvalitet för att hanteringsreglerna ska bli tillämpliga. Ett exempel på en sådan struktur är ett ärendehanteringssystem.

Frågan om en behandling är undantagen från personuppgiftslagens hanteringsregler ska bedömas utifrån det behandlade materialets helhet. Om materialet som sådant, dvs. hela samlingen av uppgifter, har strukturerats så att hanteringsreglerna är tillämpliga, t.ex. i ett ärendehanteringssystem, ska hanteringsreglerna tillämpas på samtliga personuppgifter som finns i materialet oavsett om vissa personuppgifter inte har strukturerats. Hanteringsreglerna ska även tillämpas på ostrukturerade dokument som ännu inte ingår i systemet men som är avsedda att infogas i systemet senare. Ett elektroniskt diarium över allmänna handlingar och de handlingar som är elektroniskt åtkomliga via själva diariet omfattas t.ex. fortfarande av hanteringsreglerna.

De flesta kommuner använder sig redan av sammanhållande ärendehanteringssystem eller har för avsikt att implementera sådana system inom en överskådlig tidsperiod. I den här vägledningen utgår därför Datainspektionen från att hanteringsreglerna huvudsakligen är tillämpliga på behandling av personuppgifter hos kommunerna.

2.5 Några grundläggande begrepp

Personuppgifter – all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.

Behandling av personuppgifter – varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte, t.ex. insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring.

Personuppgiftsansvarig – den som ensam eller tillsammans med andra bestämmer ändamålen, dvs. syftet med och medlen för behandlingen av personuppgifter. Personuppgiftsansvaret i en kommun ligger normalt hos de kommunala nämnder som är så självständiga att de kan anses utgöra förvaltningsmyndigheter. En kommunal nämnd som är förvaltningsmyndighet är således personuppgiftsansvarig för de behandlingar av personuppgifter som nämnden har att utföra.

Personuppgiftsbiträde – den som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Den registrerade – den som en personuppgift avser.

Samtycke – varje slag av frivillig, särskild och otvetydig viljeyttring genom vilken den registrerade, efter att ha fått information, godtar behandling av personuppgifter som rör honom eller henne.

3. Allmänt om e-förvaltning i kommunerna

3.1 Tendenser

Den offentliga förvaltningen har för närvarande som mål att öka öppenheten mot medborgarna genom att bland annat bredda tillgången till existerande handlingar, förbättra insynen i ärendehanteringen och skapa en delaktighet i planeringsarbetet. Dessutom förväntas myndigheterna ta fram och tillhandahålla ny information om t.ex. prioriteringar, beslutsgrunder, kvalitet och tillgänglighet.

Ärendehanteringen kan rationaliseras genom elektroniska funktioner för att ta emot och bereda inkomna ärenden. Standardiserade informationstjänster kan tillhandahållas genom automatiserade självbetjäningssystem. Många av dessa tjänster förutsätter en säker identifiering av motparten, antingen för att bindande avtal ska kunna träffas eller för att konfidentiell information ska bli tillgänglig.

Inom den statliga sektorn är verksamhetssystemen som regel myndighets-specifika, medan det inom den kommunala sektorn ofta finns likartade behov hos alla kommuner. Därmed finns det ett betydande utrymme för förenkling och effektivisering genom samarbete med att utveckla ändamålsenliga system.

3.2 Intressebalanser

Den nya tekniken skapar möjligheter att göra sammanställningar av uppgifter och göra information tillgänglig på ett annat sätt än tidigare. Numera överförs personuppgifter mellan olika myndigheter i ett tempo som för några år sedan knappast var möjligt, och informationsflödet skapar i sig nya möjligheter. Idén om en elektronisk förvaltning har under senare år dominerat utvecklingen, och på många offentliga arbetsplatser är ambitionerna på området höga. Det är dock viktigt att den nya tekniken används på ett sätt som inte äventyrar skyddet för enskilda människors integritet.

En utökad e-förvaltning syftar bland annat till att öka tillgängligheten till information inom och mellan myndigheter. Genom digitalisering av dokument och nya sökfunktioner som möjliggör sammanställningar av information finns personuppgifter att tillgå på ett helt nytt sätt. Frågor om tillgänglighet och säkerhet utgör därför kärnfrågor inom e-förvaltningen.

Enligt personuppgiftslagen får personuppgifter behandlas enbart för berättigade ändamål. Det innebär att personuppgifter inte får beskådas eller användas enbart

av det skälet att de finns tillgängliga. Det är till exempel inte tillåtet att utan urskiljning publicera alla offentliga handlingar på en myndighets webbplats. En publicering av en handling måste vara tillåten enligt personuppgiftslagen, även om handlingen inte omfattas av sekretess.

3.3 Säkerhetspolicy och sårbarhetsanalys

En verksamhet bör ha en säkerhetspolicy – i vart fall om man hanterar känsliga personuppgifter eller behandlar personuppgifter i stor skala. I en sådan policy redovisas organisationens säkerhetsstrategi, ansvarsfördelning och övergripande mål för säkerheten. Policyn ska vara tydlig, lätt att förstå och enkel att tillämpa i praktiken. Den bör också vara skriftlig och allmänt tillgänglig inom organisationen. Den bör även omprövas fortlöpande och anpassas till det aktuella behovet av skydd.

Som en utgångspunkt för arbetet med informationssäkerhet är det lämpligt att dessutom göra risk- och sårbarhetsanalyser för att klarlägga vilken säkerhetsnivå som ska gälla för skyddet av organisationens information och informationssystem. Som underlag för hur säkerhetsåtgärderna ska utformas bör man bedöma hur sannolikt det är att olika typer av störningar ska inträffa och vilka konsekvenser det i så fall skulle få.

Kommunen bör därför göra klart för sig vilken hotbild som finns, dvs. vilka händelser som skulle kunna drabba den egna IT-miljön, hur stor risken är för att ett hot blir verklighet, vilka konsekvenserna kan bli om ett hot blir verklighet samt vilka resurser en obehörig behöver för att realisera ett hot, dvs. vilken kunskap, utrustning eller omständighet som krävs för att hotet ska kunna genomföras. En viktig bedömningsgrund är uppfattningen om informationens ”värde” med utgångspunkt från aspekter på konfidentialitet och sekretess, krav på riktighet och tillgänglighet, liksom krav på spårbarhet och oavvislighet[1].

1 En princip inom informationssäkerhet som går ett steg längre än spårbarhet och som innebär att en utförd handling inte ska kunna förnekas av den som utfört den. För att uppnå detta används olika former av elektroniska signaturer.

4. Elektroniska dokument- och ärendehanteringssystem

4.1 Allmänt

I många kommuner införs dokument- och ärendehanteringssystem som ett medel för att möta de växande kraven på effektivitet och organisationsförändringar. Systemen medför en omfattande automatiserad behandling av personuppgifter, eftersom de ofta kombinerar bl.a. diarium, ärende- och dokumenthantering, gruppstöd och projektstöd och i förlängningen kopplas ihop med gränssnitt gentemot medborgarna.

Integritetsaspekterna blir fler och fler i takt med att volymen personlig information som är teoretiskt tillgänglig för många ökar. En stor organisation medför en omfattande ärendehantering som berör många människor. För att de nya IT-verktygen inte ska hamna i konflikt med personuppgiftslagen, måste det finnas tillräckliga garantier för att obehöriga inte får tillgång till sekretesskyddad information eller integritetskänsliga uppgifter. När nya lösningar utformas, måste man därför särskilt ta hänsyn till frågorna om att upprätthålla integritetsskydd och säkerhet.

4.2 Elektroniska diarier

4.2.1 Diarium enligt sekretesslagen

Alla myndigheter ska enligt 15 kap. sekretesslagen föra ett diarium över allmänna handlingar. Av diariet ska framgå det datum då handlingen kom in eller upprättades, diarienummer, från vem handlingen kommit eller till vem den har expedierats och i korthet vad handlingen rör. Uppgift om vem handlingen har kommit ifrån eller till vem den har expedierats samt uppgift om vad handlingen rör får dock utelämnas eller särskiljas, om det behövs för att registret i övriga delar ska kunna lämnas ut till allmänheten.

När de generella reglerna om diarieföring infördes i sekretesslagen 1981, motiverades de med att diareföring är en nödvändig förutsättning för att offentlighetsprincipen ska fungera i praktiken. Det framhölls att reglerna borde syfta till att garantera allmänhetens rätt att få tillgång till allmänna handlingar.[2]

Varje myndighet är således skyldig enligt sekretesslagen att tillhandahålla allmänheten ett diarium som inte innehåller uppgifter som är sekretessbelagda.

2 Prop. 1979/80:2 Del A.

Om myndigheten väljer att tillhandahålla diariet elektroniskt, t.ex. i en särskild dator som finns tillgänglig för allmänheten på kommunkontoret, måste även bestämmelser enligt personuppgiftslagen tillämpas på innehållet i diariet. Särskilda regler gäller om kommunen publicerar diarier på Internet (se avsnitt 5.5).

Vilka personuppgifter ett offentligt elektroniskt diarium får innehålla måste bedömas utifrån det angivna ändamålet. Enligt 9 § personuppgiftslagen ska inte fler personuppgifter behandlas än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Ifråga om det diarium som förs med stöd av sekretesslagens bestämmelser är ändamålet att utgöra ett stöd för allmänheten när det gäller att få tillgång till allmänna handlingar. Ett sådant diarium får således innehålla de uppgifter som krävs för att det ska vara möjligt att identifiera allmänna handlingar. Vilka uppgifter som ansetts nödvändiga för ändamålet framgår i huvudsak av sekretesslagens bestämmelser. Som huvudregel gäller därför att ett offentligt elektroniskt diarium inte bör omfatta fler personuppgifter än diarienummer och – om uppgifterna inte är sekretessbelagda – uppgift om vem handlingen kommit från eller till vem den har expedierats samt uppgift om vad handlingen rör.

När det gäller att ange vad handlingen rör, behöver diariet inte utvisa innehållet i varje enskild handling i ett ärende. Det är tillräckligt att det finns en ärendemening som anger vad ärendet handlar om. De enskilda handlingarna kan sedan anges med enbart t.ex. ”ansökan”.[3]

En ärendemening i diariet bör inte innehålla känsliga personuppgifter enligt 13 § personuppgiftslagen. Hos en kommun kan sådana uppgifter t.ex. avse att ett visst barn har ansökt om särskoleplats, vilket kan vara en uppgift om hälsa. Även personuppgifter som inte är känsliga i personuppgiftslagens mening men som ändå kan uppfattas som kränkande eller integritetskänsliga, t.ex. olika personalärenden, bör också föra med sig krav på att ärendemeningen redigeras. Personuppgifter om lagöverträdelser, t.ex. uppgift om miljöbrott, djurplågeri, svartbyggen etc. ska inte registreras i ett offentligt diarium.

Ett offentligt elektroniskt diarium som tillhandahålls med stöd av sekretesslagen bör inte innehålla fler direkta personuppgifter än eventuella namn. Personnummer bör således undvikas i sådana diarier. Inte heller uppgifter om adresser och telefonnummer bör registreras i ett offentligt diarium.

I princip kan sägas att samma regler som gäller enligt 12 § personuppgiftsförordningen för publicering av diarier på Internet även är vägledande för ett offentligt elektroniskt diarium (se avsnitt 6.5).[4]

---

3 Jfr prop. 1979/80:2 Del A s. 358.

4 En utförlig redovisning av de rättsliga förutsättningarna för publicering av personuppgifter i diarier på Internet finns i Statskontorets rapport 2003:1 ”Diarier på Internet – vägledning för myndigheter”, tillgänglig på www.verva.se.

4.2.2 ”Internt diarium”

Det förekommer att myndigheter tillämpar begreppet diarium även på register som används internt som arbetsredskap inom myndigheten. Ett sådant register har inte som ändamål att bereda allmänheten tillgång till allmänna handlingar utan används ofta snarare som en innehållsförteckning för dokument- och ärendehanteringssystemet eller som en katalog över tidigare och pågående ärenden. Även om det diarium som förs med stöd av sekretesslagens bestämmelser och det ”diarium” som används internt rent tekniskt inte utgör två separata register, kan man för att underlätta en bedömning enligt personuppgiftslagen se de olika diarierna som två separata diarier med var sitt ändamål.

Ändamålet att använda det ”interna diariet” som ett arbetsredskap – att kunna sortera bland ärenden och berörda enskilda – ger ett något större utrymme att registrera olika personuppgifter. Den kommunala nämnden kan ha behov av att behandla kompletterande uppgifter som personnummer, adresser, telefonnummer och uppgifter om ärendet utöver den information som lämnas i ärenderubriken. Det kan även finnas behov av att registrera information om olika ärenden som har anknytning till varandra.

Det är dock inte tillåtet att registrera personuppgifter i det ”interna diariet” enbart på grund av att de finns tillgängliga. Behovet av att registrera uppgifterna måste kunna motiveras utifrån ändamålet. Det kan t.ex. vara nödvändigt att låta en ärendemening i det ”interna diariet” innehålla känsliga personuppgifter i ett ärende som rör ansökan om särskola, men det är tveksamt om ett fritextfält i ett sådant ärende bör innehålla kompletterande fakta.

4.2.3 Kommungemensamt diarium

När en kommunal nämnd gör personuppgifter tillgängliga för övriga nämnder inom kommunen genom ett s.k. ”delat diarium”, krävs det en särskild bedömning enligt personuppgiftslagen. Detta gäller oavsett vilken sekretess som gäller mellan nämnderna. Eftersom personuppgiftsansvaret i en kommun ofta är uppdelat på så sätt att varje nämnd är ansvarig för sin egen verksamhet, innebär ett s.k. delat diarium att personuppgifter lämnas ut till övriga nämnder.

Kriterierna för bedömningen av vilka personuppgifter ett delat diarium kan innehålla är desamma som för bedömningen av vilka uppgifter som får finnas i ett diarium som förs med stöd av sekretesslagen. Att övriga nämnder ges åtkomst till olika personuppgifter får till exempel inte vara oförenligt med det ändamål för vilket uppgifterna samlades in. Mot bakgrund av nämndernas självständighet bör utgångspunkten vara att en kommunal nämnd inte får registrera fler uppgifter i ett diarium som är avsett för övriga nämnder än vad som får registreras i ett elektroniskt diarium avsett för allmänheten.

En sådan regel kan dock inte tillämpas generellt. Vissa nämnder samarbetar mycket nära med varandra och kan med hänsyn till detta ha ett påtagligt behov av att ha tillgång till varandras ”interna diarier”. Exempelvis kan en grundskolenämnd och en gymnasienämnd i vissa fall ha ett delat ansvarsområde. I så fall är det inte oförenligt med det ändamål för vilket uppgifterna samlades in att mer omfattande lämna ut personuppgifter.

4.3 Elektronisk dokumenthantering

4.3.1 Personuppgiftsbehandling vid elektronisk dokumenthantering

Kommuner har många ansvarsområden och en bred ärendeflora. De kommunala nämnderna tar dagligen emot handlingar av allehanda slag. En del kommuner har infört rutiner som innebär att dokument skannas in i dokument- och ärendehanteringssystemet. Målsättningen är ofta att alla handlingar ska hanteras och förvaras elektroniskt – allt från inkomna handlingar till de handlingar nämnden har upprättat. En sådan omfattande behandling av personuppgifter i ett dokument- och ärendehanteringssystem kan innebära risker för otillbörligt intrång i människors personliga integritet. Framför allt medför inskanningen av dokument en avsevärd skillnad i fråga om tillgängligheten till uppgifter. Det är betydligt lättare att ta fram information ur en elektronisk databas med stora sökmöjligheter, jämfört med den tidigare pappersbaserade hanteringen.

Eftersom kommunen inte har möjlighet att påverka innehållet i inkommande handlingar, kan det förekomma personuppgifter av känslig karaktär även i skrivelser som normalt sett inte kan förväntas innehålla den sortens uppgifter. Det förekommer även att personer som inte berörs av ett ärende namnges i vissa skrivelser. När nämnden sedan upprättar egna handlingar i ärendet kan det vara nödvändigt att i t.ex. skälen för ett beslut återge anförda uppgifter. Av 8 § personuppgiftsförordningen framgår att känsliga personuppgifter får behandlas i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av det. I de allra flesta fall är det således tillåtet att behandla känsliga personuppgifter med anledning av ärendehantering.

Frågan om vilka sökmöjligheter som ska få finnas i ett personregister är av stor betydelse utifrån integritetsskyddet. Genom att göra sammanställningar baserade på t.ex. person eller företeelse är det möjligt att snabbt sammanföra och överblicka stora informationsmängder. Även förhållandevis harmlösa uppgifter kan, om de ställs samman med andra sådana uppgifter, skapa en totalbild av människors enskilda förhållanden som i sin tur kan innebära ett otillbörligt intrång i individens personliga integritet. Ingår känsliga uppgifter i en sådan sammanställning

kan denna upplevas som mycket kränkande. I de flesta registerlagstiftningar har därför införts begränsningar av sökbegreppen i syfte att förhindra kartläggningar av enskilda på sätt som inte är motiverade av ändamålen och som enskilda kan uppfatta som intrång i den personliga integriteten.

Eftersom kommuner (bortsett från socialnämnderna) inte styrs av några registerlagar, är personuppgiftslagen tillämplig vid sökning och sammanställning av personuppgifter. Det innebär bland annat att när anställda gör olika sökningar i kommunens dokument- och ärendehanteringssystem, måste detta göras för berättigade ändamål som har sin grund i verksamheten. Det är inte tillåtet att som anställd söka efter uppgifter i systemen av privata skäl. Den som olovligen söker efter uppgifter i systemen kan dessutom göra sig skyldig till dataintrång enligt 4 kap. 9 c § brottsbalken.

Med begreppet allmän handling avses inte bara färdiga elektroniska handlingar utan även s.k. potentiella handlingar, d.v.s. varje sammanställning av handlingar som en myndighet kan göra med hjälp av tillgängliga program. Allmänheten kan således begära ut olika sammanställningar av personuppgifter som allmänna handlingar. Detta gäller under förutsättning att uppgifterna kan ställas samman med en enkel arbetsinsats och utan nämnvärda kostnader eller andra komplikationer. Principen gäller oavsett om en sammanställning av informationen har gjorts av kommunen själv innan handlingen begärs ut och oberoende av om informationen behövs för kommunens verksamhet. Personuppgiftslagen hindrar inte att uppgifter ställs samman på grund av en begäran om allmän handling.

För att förhindra att integritetskänsliga sammanställningar av information framställs, är det lämpligt att kommunen överväger om det utifrån de ändamål för vilka personuppgifter behandlas i dokument- och ärendehanteringssystemet finns skäl att införa olika tekniska sökbegränsningar.

4.3.2 Brottsuppgifter

En kommunal nämnd är en myndighet och hindras därför inte av det principiella förbudet i 21 § personuppgiftslagen att behandla brottsuppgifter. För att en nämnd ska få behandla sådana uppgifter, måste behandlingen dock vara tillåten enligt övriga bestämmelser i personuppgiftslagen. Det måste t.ex. alltid finnas ett berättigat ändamål för behandlingen, och den får inte inkludera fler personuppgifter än vad som är nödvändigt. Personuppgiftsbehandlingen måste även vara tillåten enligt 10 § personuppgiftslagen, t.ex. för att nämnden ska kunna fullgöra en rättslig skyldighet eller kunna utföra en arbetsuppgift i samband med myndighetsutövning. Exempel på tillåten behandling kan vara när en miljönämnds ärendehantering omfattar uppgifter om miljöbrott eller djurplågeri.

Datainspektionen har däremot ansett att det inte är tillåtet att i dokument- och ärendehanteringssystemet registrera värderande omdömen som utgör personuppgifter om brott. Exempelvis får en miljönämnd, som vill göra riskbedömningar av tillsynsobjekt för att kunna planera sina inspektioner, inte registrera uppgifter om att en enskild person uppträtt hotfullt, givit sig in i handgemäng eller allmänt verkar våldsam. Sådana uppgifter får inte finnas i ett sökbart dokument- och ärendehanteringssystem för de ändamål som ett sådant system brukar vara avsett för. Om det finns ett väl motiverat behov av att registrera den här typen av uppgifter, t.ex. av säkerhetsskäl, kan det dock vara tillåtet att göra det i ett separat register som har till ändamål att tillgodose det avsedda behovet. Det är då lämpligt att förvara registret, som t.ex. sparats i form av en excelfil, med särskilt åtkomstskydd.[5]

4.3.3 Tillgången till dokument- och ärendehanteringssystemet

Ett dokument- och ärendehanteringssystem innehåller stora mängder information, varav en stor del är relaterad till enskilda personer. I synnerhet när inkommande handlingar skannas in i systemet, kommer innehållet att omfatta en mängd uppgifter som av olika skäl kan upplevas som känsliga.

En grundläggande princip är att anställda i en kommunal förvaltning endast bör ha tillgång till information som de behöver för sitt arbete. Beroende på hur omfattande nämndens verksamhetsområde är och beroende på anställningsuppdraget kan detta innebära olika mycket information. Det måste finnas möjligheter att arbeta som backup för en kollega, och det är inte meningen att behörighetsbegränsningar i systemet ska göra det omöjligt att någon hoppar in som vikarie. Det är dock viktigt att den personuppgiftsansvarige ser till att personrelaterad information inte flödar fritt, utan att det finns rutiner för tillgången till uppgifter i systemet.

De nya dokument- och ärendehanteringssystemen gör det även möjligt med ett större utbyte av information mellan olika kommunala nämnder. Det talas om horisontella flöden till skillnad från tidigare system som har ansetts alltför ”stuprörsformade”. Vid implementeringen av dessa nya system är det emellertid viktigt att inte enbart styras av de tekniska möjligheterna utan även ta hänsyn till integritetsriskerna.

Eftersom kommunens olika nämnder normalt sett är personuppgiftsansvariga för sina egna verksamheter, innebär en överföring av personuppgifter mellan dem att uppgifter lämnas ut. En sådan personuppgiftsbehandling måste precis

5 Datainspektionen har i ett samrådsyttrande, dnr 370-2006, behandlat en fråga rörande en miljöförvaltning som ville registrera riskbedömningar av tillsynsobjekt i sitt ärendehanteringssystem.

som all övrig behandling ha stöd i personuppgiftslagen. Bland annat får utlämnandet inte strida mot det ursprungliga ändamålet med insamlingen av uppgifterna.

I vissa fall kan flera förvaltningar behöva tillgång till samma information. Om två nämnder arbetar integrerat, t.ex. en grundskole- och en gymnasienämnd, kan det finnas skäl att lämna ut uppgifter till varandra. Tillgången måste dock alltid vara behovsstyrd och får inte vara obegränsad.

4.4 Gallring och arkivering

Enligt huvudregeln ska alla personuppgifter gallras när de inte längre behövs för verksamheten. De grundläggande kraven i 9 § personuppgiftslagen innebär att personuppgifter inte får bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Men en myndighet får enligt 8 § andra stycket personuppgiftslagen trots bestämmelserna i lagen arkivera och bevara allmänna handlingar. Bestämmelser om myndigheternas bevarande av allmänna handlingar finns bl.a. i arkivlagen (1990:782).

Att allmänna handlingar registreras och bevaras i ursprungligt skick hos myndigheterna är en förutsättning för att allmänheten ska kunna utnyttja rätten att ta del av allmänna handlingar. Även om en kommunal nämnd mot bakgrund av detta har rätt att arkivera olika handlingar, bör tillgången till handlingarna begränsas. Det är t.ex. inte lämpligt att dokument- och ärendehanteringssystemet gör det möjligt med obegränsade sökningar bland alla inskannade handlingar som någonsin kommit in till myndigheten.

Arkivering av handlingar bör åtminstone innebära att handlingarna avskiljs från det diarium och dokument- och ärendehanteringssystem som används i den dagliga verksamheten.[6] Om arkiveringsfunktionen ingår i samma system, bör systemet ändå innehålla tekniska avgränsningar. Samma tanke som hittills har präglat arkivering – att det innebär att sortera och avskilja för förvaring – bör finnas med även när arkiveringen blivit elektronisk. Med hänsyn till att en anställd inte bör ha behörighet att behandla fler personuppgifter än vad som behövs för arbetet, bör den anställde inte heller ha obegränsad behörighet till personuppgifter i ett elektroniskt arkiv.

6 Se t.ex. Datainspektionens beslut den 3 juli 2006 med diarienummer 191-2006.

4.5 Säkerhet

Enligt 31 § personuppgiftslagen ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med hänsyn tagen till de tekniska möjligheter som finns, kostnaden för åtgärderna, särskilda risker med behandlingen och hur pass känsliga uppgifterna är.

Det är viktigt att personuppgiftslagen inte uppfattas som ett hinder i verksamheten utan att den istället utgör ett verktyg i säkerhetsarbetet. För att tänkesättet enligt personuppgiftslagen ska bli en naturlig del i arbetet bör det i alla organisationer upprättas rutiner och instruktioner som beaktar lagens bestämmelser.

Av 30 § personuppgiftslagen framgår att ett personuppgiftsbiträde och den eller de personer som arbetar under biträdets eller den personuppgiftsansvariges ledning bara får behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvarige.

Hos varje kommunal nämnd bör det finnas instruktioner om vem som ska göra de bedömningar som krävs enligt personuppgiftslagen när personuppgifter registreras i ett diarium. Om registreringen innebär att uppgifter utan vidare bedömning görs tillgängliga offentligt, är det inte lämpligt att varje enskild handläggare för in uppgifter om egna ärenden i det elektroniska diariet. Detta bör istället göras centralt av personer med kunskaper om personuppgiftslagen, exempelvis registratorer.

För att förhindra obehörig användning av eller åtkomst till dokument- och ärendehanteringssystemet bör ett system för behörighetskontroll upprättas inom kommunen och inom varje nämnd. Ett sådant system bör omfatta möjligheter att identifiera användare och bekräfta användarens identitet, exempelvis genom att personliga lösenord används. Det är inte lämpligt att använda s.k. grupplösenord, eftersom dessa inte identifierar en särskild användare. Systemet bör kunna kontrollera användningen, så att endast de som behöver uppgifterna för sitt arbete får tillgång till åtkomstskyddade personuppgifter. Det bör finnas rutiner för tilldelning och kontroll av behörigheter. För att åtkomsten ska kunna kontrolleras bör det dessutom finnas en behandlingshistorik, som sparas en viss tid och följs upp.

Det bör även finnas instruktioner för hantering av känsliga personuppgifter och uppgifter om lagöverträdelser i dokument- och ärendehanteringssystemet samt för gallring.

Det är viktigt att den kommunala nämnden informerar de anställda om vad som är tillåtet, vilka konsekvenserna blir om man bryter mot en regel och hur efterlevnaden av reglerna följs upp.

Om anställda har tillgång till diarium och dokument- och ärendehanteringssystem hemifrån, dvs. via öppna nät, krävs det särskilda säkerhetsåtgärder. För att förhindra att personuppgifter förstörs, ändras eller kommer i orätta händer vid överföring via nät och för att skydda anslutna tjänster mot obehörig åtkomst bör den personuppgiftsansvarige vidta lämpliga åtgärder för att åstadkomma en tillfredsställande säkerhet. När utrustningen ansluts till Internet eller något annat öppet nät, måste anslutningen naturligtvis skyddas så att obehörig trafik förhindras. I samma syfte bör åtkomst förhindras från det öppna nätet till annan utrustning eller lokala nät hos den personuppgiftsansvarige. Om uppgifterna endast får lämnas ut till identifierade användare ska mottagarens identitet säkerställas.

Känsliga uppgifter enligt 13 § personuppgiftslagen får endast lämnas ut via öppna nät till identifierade användare, vars identitet är säkerställd med en teknisk funktion som kryptering, engångslösenord eller motsvarande. Personuppgifter ska dessutom, beroende på känsligheten hos uppgifterna, förses med krypteringsskydd vid överföring via öppet nät, till exempel Internet.

För att förhindra förlust av personuppgifter ska det finnas rutiner för säkerhetskopiering. För att säkerhetskopieringen ska fungera, bör man ta säkerhetskopior tillräckligt ofta, prova regelbundet att det går att återskapa säkerhetskopian och förvara kopian skyddad.

För ytterligare information om personuppgiftslagens krav på säkerhet vid behandling av personuppgifter hänvisas till Datainspektionens allmänna råd och informationsblad om informationssäkerhet.

4.6 Sammanfattning – checklista

4.6.1 Diarium

- **Det finns ett mycket begränsat utrymme för registrering av personuppgifter i ett diarium som används för det traditionella ändamålet att ge allmänheten tillgång till allmänna handlingar.**

  Varken personnummer, känsliga personuppgifter, brottsuppgifter eller andra personuppgifter som kan uppfattas som kränkande bör registreras i ett diarium som vem som helst kan ta del av.

- **Ett ”internt diarium” får innehålla sådana personuppgifter som är berättigade utifrån ändamålet med ett sådant register.**

  Det förekommer att myndigheter tillämpar begreppet diarium även på register som används internt som arbetsredskap inom myndigheten. Sådana ”interna diarier” kan innehålla personuppgifter i en större omfattning, t.ex. personnummer, adresser och telefonnummer. Även för registrering i ett sådant diarium krävs dock en bedömning enligt personuppgiftslagen.

- **Tänk på att nämnden måste göra en särskild bedömning enligt personuppgiftslagen när olika kommunala förvaltningar har möjlighet att ta del av varandras diarier.**

  Eftersom personuppgiftsansvaret i en kommun i allmänhet är uppdelat på så sätt att varje nämnd är ansvarig för sin egen verksamhet, innebär ett s.k. delat diarium att personuppgifter lämnas ut till övriga nämnder. Som huvudregel gäller att en kommunal nämnd inte bör registrera fler uppgifter i ett diarium som är avsett för övriga nämnder än vad som får registreras i ett elektroniskt diarium avsett för allmänheten. Undantag från huvudregeln kan dock göras beroende på hur integrerat olika nämnder arbetar.

4.6.2 Elektronisk dokumenthantering

- **Observera att personuppgiftslagen är tillämplig även när anställda söker efter uppgifter eller gör sammanställningar av information i dokument- och ärendehanteringssystemet.**

  Varje sökning måste göras för ett berättigat ändamål som har sin grund i verksamheten. Det är inte tillåtet att som anställd söka efter uppgifter i systemen av privata skäl. Den som olovligen söker efter uppgifter i systemen kan dessutom göra sig skyldig till dataintrång enligt 4 kap. 9 c § brottsbalken.

- **Sökmöjligheterna i dokument- och ärendehanteringssystemet avgör vad som är allmän handling.**

  Med begreppet allmän handling avses inte bara pappersdokument utan varje sammanställning av upprättade handlingar som en myndighet kan göra med en enkel arbetsinsats och utan nämnvärda kostnader eller andra komplikationer. Den kommunala nämnden bör överväga om det mot bakgrund av detta finns anledning att vidta särskilda åtgärder.

- **Brottsuppgifter får behandlas under förutsättning att kraven i 9 och 10 §§ personuppgiftslagen är uppfyllda.**

  Exempel på tillåten behandling kan vara när en miljönämnds ärendehantering omfattar uppgifter om miljöbrott eller djurplågeri.

4.6.3 Tillgången till dokument- och ärendehanteringssystemet

- **Anställda i en kommunal förvaltning bör endast ha behörighet att behandla personuppgifter som de behöver för sitt arbete.**

  Beroende på hur omfattande nämndens verksamhetsområde är och hur anställningsuppdraget ser ut kan den anställdes behov av tillgång till olika personuppgifter variera.

- **Observera att en överföring av personuppgifter mellan olika nämnder innebär att uppgifter lämnas ut.**

  Varje utlämnande av personuppgifter måste precis som all övrig behandling ha stöd i personuppgiftslagen. Det är inte tillåtet att generellt ge alla kommunala förvaltningar obegränsad tillgång till all information inom kommunen.

4.6.4 Arkivering

- **Arkiverade handlingar bör separeras från hanteringen av handlingar i den dagliga verksamheten.**

  Även om en kommunal nämnd har rätt att arkivera olika handlingar, bör tillgången till handlingarna i viss mån begränsas. Det är inte lämpligt att dokument- och ärendehanteringssystemet gör det möjligt med obegränsade sökningar bland alla inskannade handlingar som någonsin kommit in till myndigheten.

4.6.5 Säkerhet

- **För att tänkesättet enligt personuppgiftslagen ska bli en naturlig del i arbetet bör det i alla organisationer upprättas rutiner som tar hänsyn till lagens bestämmelser.**

  Rutiner ska finnas för registrering av personuppgifter i diarium, för behörighetskontroll avseende dokument- och ärendehanteringssystemet, för hantering av känsliga personuppgifter och brottsuppgifter samt för gallring. Det är viktigt att göra klart för de anställda vad som är tillåtet, vilka konsekvenserna blir om man bryter mot en regel och hur efterlevnaden av reglerna följs upp.

- **Om anställda har tillgång till diarium och dokument- och ärende-hanteringssystem hemifrån, krävs särskilda säkerhetsåtgärder.**

  Personuppgifter som överförs via nät bör, beroende på hur känsliga de är, skyddas t.ex. genom kryptering. Om uppgifterna endast får lämnas ut till identifierade användare ska mottagarens identitet säkerställas.

5. Elektroniska tjänster

5.1 Allmänt

Denna vägledning behandlar i huvudsak sådana e-tjänster som kommunerna erbjuder allmänheten på webben. Vägledningen behandlar inte, annat än i något undantagsfall, sådana tjänster som förmedlas genom andra kanaler, t.ex. automatiska telefontjänster, e-posttjänster och videokonferenser.

När information publiceras på Internet och kommuner erbjuder tjänster på webben gäller personuppgiftslagen. Kommunens intresse av att göra information tillgänglig måste därför vägas mot den enskildes intresse av integritetsskydd. Det innebär bl.a. att allmänhetens tillgång till information via Internet i viss mån måste begränsas. Det handlar framför allt om att skapa en tillfredsställande teknisk och administrativ säkerhet för personuppgifter, så att obehöriga inte får tillgång till sekretesskyddade uppgifter om enskilda eller uppgifter som på annat sätt är integritetskänsliga. En annan viktig del i integritetsskyddet är att den enskilde informeras om den personuppgiftsbehandling som sker i samband med att e-tjänster tillhandahålls.

5.2 Exempel på kommunala e-tjänster

Medborgarnas och företagens förväntningar på e-förvaltning och utlovade nya e-tjänster är bl.a. förenklade rutiner, snabbare beslut, bättre tillgänglighet och ökad insyn. I nuläget arbetar kommunerna med att utveckla sina e-tjänster, och det finns en vision om en väl utvecklad webbplats, där allmänheten efter inloggning kan ta del av ett varierat utbud av e-tjänster. Många kommuner använder dock fortfarande sina webbplatser huvudsakligen som informationskanal och inte som verktyg för tvåvägskommunikation mellan medborgare och förvaltning. Det rör sig framför allt om att tillhandahålla olika slags samhällsinformation på webben. Ett flertal kommuner erbjuder också möjligheten att fylla i enklare formulär och att ladda hem blanketter för utskrift. Det är också vanligt att kommuner låter allmänheten ta del av nämndernas diarier och protokoll på webben.

En del kommuner erbjuder även mer avancerade e-tjänster som kan fordra metoder för säker identifiering av användaren. Det rör sig t.ex. om möjligheten att följa sitt eget ärende via kommunens webbplats och att få tillgång till virtuella bibliotek där man kan låna böcker eller musik i traditionell och ibland även i elektronisk form. Även möjligheten att ansöka om barnomsorg och välja skola på webben, att boka lediga lokaler, att söka bygglov, att teckna elnätsavtal, lämna elmätarställning eller boka färdtjänst utgör exempel på mer avancerade e-tjänster.

Vissa kommuner erbjuder också demokratifrämjande tjänster i form av t.ex. medborgardialoger, möjlighet att lämna synpunkter eller klagomål till kommunens anställda eller förtroendevalda på webben, diskussionsforum och möjlighet för gymnasieelever att rösta i val till ungdomsfullmäktige på webben.

5.3 Information i samband med tillhandahållande av e-tjänster

När kommunen tillhandahåller e-tjänster är det i många fall fråga om en datoriserad behandling av personuppgifter. Detta innebär att personuppgiftslagens bestämmelser om information till de registrerade gäller.

Den personuppgiftsansvarige, som för kommunernas vidkommande i regel är den kommunala nämnd som ansvarar för en viss behandling, är som huvudregel skyldig att självmant lämna information till den registrerade i samband med att personuppgifterna samlas in. Informationen måste lämnas oavsett om uppgifterna samlas in med eller utan den registrerades samtycke.

Om personuppgifterna samlas in från personen själv, t.ex. då personen i fråga lämnar synpunkter i ett webbformulär och i samband med detta själv matar in sina personuppgifter, ska informationen lämnas i samband med detta. Personuppgifter bör hanteras som om de var insamlade från den registrerade själv även när de lämnas av en legal ställföreträdare, t.ex. när en vårdnadshavare lämnar uppgifter om sitt underåriga barn.

Det finns betydelsefulla undantag från informationsskyldigheten. Information behöver t.ex. inte lämnas om sådant som den registrerade redan känner till. Om en enskild person exempelvis lämnar in en ansökan om barnomsorg på webben, är nämnden inte skyldig att lämna information så länge uppgifterna bara behandlas för de ändamål som personen ifråga kan anses förutse, dvs. för handläggning av ansökan om barnomsorg.

Har personuppgifterna samlats in från någon annan källa än den registrerade, behöver information inte heller lämnas om det finns bestämmelser om registrerandet eller utlämnandet i annan lag eller författning, t.ex. sådana bestämmelser som finns i sekretesslagen om registrering av uppgifter i ett diarium.

Har personuppgifterna samlats in från någon annan källa än den registrerade, behöver kommunerna inte heller informera om det visar sig vara omöjligt eller om det skulle innebära en oproportionerligt stor arbetsinsats, förutsatt att uppgifterna inte ska användas för att vidta åtgärder som rör den registrerade.

För att avgöra om det skulle innebära en oproportionerligt stor arbetsinsats att lämna information måste en helhetsbedömning göras av samtliga relevanta omständigheter. Vid denna bedömning kan kommunerna bl.a. ta hänsyn till antalet registrerade individer, tillgången till adress- eller kontaktuppgifter för att möjliggöra information, arten av personuppgifter som behandlas och de kompensatoriska åtgärder som kan vidtas, t.ex. information om behandlingen på den personuppgiftsansvariga nämndens webbplats. Andra omständigheter som kan vägas in är behandlingens ändamål, riskerna för integritetsintrång och det intresse de registrerade kan antas ha av att bli informerade om behandlingen.

Det kan vara svårt att i enskilda fall bedöma om den som tänker använda en e-tjänst kan anses känna till behandlingen eller att avgöra om det skulle innebära en oproportionerligt stor arbetsinsats att informera om behandlingen. Datainspektionen rekommenderar därför att kommunerna i samband med att de tillhandahåller e-tjänster på webben rutinmässigt informerar användarna om sådan behandling av personuppgifter som följer av tjänsten. Förutom att ett sådant förhållningssätt är att föredra i integritetshänseende, innebär det att kommunen slipper en genomgripande och många gånger krävande översyn av när information måste lämnas för att uppfylla informationsplikten enligt personuppgiftslagen.

Den information som den personuppgiftsansvarige är skyldig att lämna självmant ska innehålla:

(a) uppgift om den personuppgiftsansvariges identitet,
(b) uppgift om ändamålen med behandlingen och
(c) all övrig information som behövs för att den registrerade ska kunna ta tillvara sina rättigheter i samband med behandlingen.

Med ”all övrig information” enligt punkt c avses bl.a. information om vilka kategorier som är mottagare av uppgifterna, skyldigheten att lämna uppgifter (registerutdrag) och rätten att ansöka om information och få rättelse.

Den personuppgiftsansvariga nämnden bör inom den egna organisationen utforma tydliga rutiner för hur informationen ska lämnas. Formerna för informationslämnandet kan variera. I många fall är det lämpligt att lämna informationen i en särskild ruta eller i ett särskilt fönster på webbplatsen i anslutning till e-tjänsten.

Utöver den information som ska ges enligt personuppgiftslagen kan kommunerna behöva lämna ytterligare information som är av annan juridisk karaktär, t.ex. om upphovsrätt, sekretess och tystnadsplikt. För att underlätta för använ-

darna bör kommunerna sträva efter att lämna informationen samordnat med den information som ska lämnas enligt personuppgiftslagen.[7]

För ytterligare information om den personuppgiftsansvariges informationsskyldighet hänvisas till Datainspektionens allmänna råd ”Information till registrerade enligt personuppgiftslagen”, som finns tillgängliga på Datainspektionens webbplats: www.datainspektionen.se.

5.4 Säkerhet för personuppgifter

5.4.1 Allmänt

Det är den personuppgiftsansvarige som självständigt och på eget ansvar måste se till att behandlingen av personuppgifter följer personuppgiftslagens bestämmelser om säkerhet. Den personuppgiftsansvariga nämnden bör därför inom den egna organisationen utforma tydliga och väl genomtänkta tekniska och administrativa rutiner, så att inte personuppgifter sprids till obehöriga.

Det är inte möjligt att generellt ange vilken säkerhetsnivå som kommunerna måste upprätthålla när de tillhandahåller e-tjänster. Enligt personuppgiftslagen krävs dock att den personuppgiftsansvarige vidtar lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna måste alltid ställas i relation till de tekniska möjligheter som finns, kostnaderna för åtgärderna, de risker som finns samt de behandlade uppgifternas känslighet. Detta innebär att kommunerna i fråga om vissa typer av tjänster måste vidta tämligen genomgripande åtgärder för att skydda personuppgifter, medan andra typer av tjänster fordrar mindre långtgående åtgärder. [8]

Det är framför allt tre säkerhetsaspekter som aktualiseras då kommunerna erbjuder e-tjänster. För det första måste kommunen i vissa fall kunna fastslå identiteten hos användare av e-tjänster (autentisering). För det andra måste kommunen säkerställa att personuppgifter skyddas då de överförs via öppna nät. För det tredje måste kommunen se till att skydda de personuppgifter som samlats in i samband med att kommunen tillhandahåller tjänster.

---

7 Se E-nämndens ”Vägledning för information som enligt lag ska lämnas på webbplatser” som finns tillgänglig på Vervas webbplats: www.verva.se.

8 Bedömningen av vilka säkerhetsåtgärder som behövs i det enskilda fallet är beroende av bl.a. vilka personuppgifter som behandlas. Det är därför nödvändigt att kommunen värderar de uppgifter som ska behandlas i samband med att man tillhandahåller e-tjänster, jfr Datainspektionens allmänna råd om säkerhet, ”Säkerhet för personuppgifter”, som finns tillgängliga på Datainspektionens webbplats: www.datainspektionen.se.

5.4.2 Identifiering av användare i samband med tillhandahållande av e-tjänster (autentisering)

Kommunerna behöver kunna fastslå identiteten hos användare av e-tjänster, dels för att kunna träffa rättsligt bindande avtal, dels för att inte obehöriga ska kunna ta del av integritetskänslig information, lämna felaktiga uppgifter eller på annat sätt förvanska information.

Det finns olika autentiseringslösningar, exempelvis användarnamn kopplade till personliga lösenord, engångslösenord och e-legitimation. Valet av autentiseringslösning bör enligt Datainspektionens mening ta sin utgångspunkt i känsligheten hos de personuppgifter som behandlas och de risker som är förknippade med behandlingen. Känsligheten hos uppgifterna beror på flera faktorer och måste alltid bedömas särskilt. Kommunerna måste även ta hänsyn till mängden uppgifter som behandlas, eftersom omfattningen av uppgifter avgör hur detaljerad en bild av en enskild person kan bli.

När kommunerna bedömer hur pass känsliga personuppgifterna är, måste de särskilt beakta de bestämmelser i personuppgiftslagen som reglerar behandling av känsliga personuppgifter. Som känsliga personuppgifter enligt lagen räknas personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening och personuppgifter som rör hälsa eller sexualliv. Om e-tjänsterna medför behandling av uppgifter av detta slag, anser Datainspektionen att det inte är godtagbart från säkerhetssynpunkt att dessa görs tillgängliga för användare genom t.ex. användarnamn och pinkod. I dessa fall fordras mer avancerade metoder för identifiering, exempelvis e-legitimation. Detsamma gäller för personuppgifter som omfattas av sekretess samt för uppgifter om lagöverträdelser som innefattar brott.

Det är svårt att generellt slå fast vilka sorters e-tjänster som fordrar mer respektive mindre avancerade autentiseringsmetoder. Valet av lösning kan inte fastställas schablonartat enbart utifrån vilka personuppgifter som behandlas utan beror på fler faktorer och måste alltid bedömas särskilt. Det finns dock vissa typer av e-tjänster som normalt sett innebär större risker i integritetshänseende och som därför fordrar mer avancerade system för autentisering. Naturligtvis finns det e-tjänster där risken för integritetsintrång är liten eller obefintlig och där det är obefogat med autentisering, t.ex. då kommunen tillhandahåller olika slags samhällsinformation på webben.

Nedan följer en punktvis uppräkning av e-tjänster som normalt sett innebär större risker i integritetshänseende och där det är befogat med mer avancerade metoder för autentisering. Givetvis kan andra aspekter än skyddet för den personliga integriteten, t.ex. ekonomiska aspekter, motivera mer avancerade metoder för autentisering.

Exempel på e-tjänster som normalt sett fordrar mer avancerade metoder för autentisering och där Datainspektionen rekommenderar att autentiseringen sker med e-legitimation eller genom användarnamn och engångslösenord:

- E-tjänster av typen ”Mina sidor”, där användaren efter inloggning kommer åt ett stort antal personuppgifter som kan vara av integritetskänslig natur.
- Elevadministrativa system där elever och vårdnadshavare efter inloggning kan kommunicera med skolpersonal och lämna eller ta del av integritetskänsligt material, exempelvis uppgifter om frånvaro, betyg, omdömen eller individuella utvecklingsplaner (för en illustration av integritetsskyddsaspekter som aktualiseras då kommunen tillhandahåller elevadministrativa system, se Datainspektionens beslut den 14 januari 2007 med diarienummer 1623-2006, som finns tillgängligt på Datainspektionens webbplats: www.datainspektionen.se).
- E-tjänster där allmänheten kan följa sitt eget ärende på webben, om tjänsten innebär att användaren kan ta del sekretesskyddat material, känsliga personuppgifter eller uppgifter om lagöverträdelser som innefattar brott.
- Bokning av eller ansökan om hemtjänst på webben, om tjänsten innebär att användaren kan ta del av känsliga personuppgifter, t.ex. uppgifter om hälsa.
- Bokning av eller ansökan om färdtjänst på webben, om tjänsten innebär att användaren kan ta del av känsliga personuppgifter, t.ex. uppgifter om hälsa.
- Ansökan om barnomsorg på webben, om tjänsten innebär att användaren kan ta del av känsliga personuppgifter, exempelvis uppgifter om att ett visst barn är i behov av särskilt stöd.
- Bokning av skolskjuts på webben, om tjänsten innebär att användaren kan ta del av känsliga personuppgifter, exempelvis uppgifter om att ett visst barn är i behov av särskilt stöd.
- Möjligheter för gymnasieelever att rösta i val till ungdomsfullmäktige på webben.
- E-tjänster som gör det möjligt för kommun och användare att utväxla information sinsemellan som kan omfattas av sekretess, vara känslig enligt personuppgiftslagen eller röra uppgifter om lagöverträdelser som innefattar brott.

5.4.3 Skydd för känsliga personuppgifter som överförs i öppna nät

När kommunerna tillhandahåller allmänheten e-tjänster på webben eller via e-post, kan det inträffa att integritetskänsliga personuppgifter utväxlas på elektronisk väg mellan parterna. De kommunala nämnderna måste därför vidta lämpliga åtgärder för att åstadkomma en tillfredsställande säkerhet för personuppgifterna.[9]

Personuppgifter som är känsliga enligt 13 § personuppgiftslagen får endast kommuniceras via öppna nät, till exempel Internet, till identifierade användare vars identitet är säkerställd med en teknisk funktion som kryptering, engångslösenord eller motsvarande. Känsliga personuppgifter ska dessutom vid överföring via ett öppet nät förses med krypteringsskydd.

Uppgifter som omfattas av sekretess samt uppgifter om lagöverträdelser som innefattar brott bör när det gäller säkerhet likställas med känsliga personuppgifter. Kommunerna måste därför se till att krypteringsskydda även sådana personuppgifter när de kommuniceras över öppna nät samt vidta tekniska åtgärder för att säkerställa att endast de tänkta mottagarna kan ta del av uppgifterna.

Användare av e-tjänster måste också kunna förvissa sig om att det är kommunen som är mottagare av uppgifterna. Kommunerna ansvarar också för att kommunikationen är krypterad. För kommunernas vidkommande kan detta lösas med hjälp av ett signerat servercertifikat[10] och SSL/TLS[11]. Datainspektionen rekommenderar att kommunerna inför denna typ av skydd för samtliga e-tjänster som räknas upp i avsnitt 5.4.2.[12]

5.4.4 Rutiner för omhändertagande av information

När kommunen erbjuder e-tjänster kan den komma att ta emot uppgifter som är sekretesskyddade eller på annat sätt integritetskänsliga. Kommunen måste därför ha väl avvägda rutiner för hur dessa uppgifter ska hanteras internt inom kommunen. Det handlar om behörighetstilldelning, administrativa rutiner och tydliga riktlinjer för när det är tillåtet för personal att ta del av personuppgifter inom respektive nämnd eller förvaltning. Den personuppgiftsansvariga nämnden bör se till att alla som har tillgång till personuppgifter får relevant utbildning. Nämnden bör t.ex. se till att de anställda har en klar uppfattning om vad som är tillåtet,

9 Se Datainspektionens beslut den 12 december 2006 med diarienummer 1082-2006, som finns tillgängligt på Datainspektionens webbplats: www.datainspektionen.se.
10 Ett servercertifikat kan liknas vid en e-legitimation, fast utställd till en server istället för till en individ.
11 SSL/TLS är säkra kommunikationsprotokoll som främst används för att krypteringsskydda kommunikation på webben. De stödjer också autentisering av både server och användare genom användning av certifikat, t.ex. servercertifikat och e-legitimationer.
12 Se Datainspektionens beslut den 6 februari 2007 med diarienummer 998-2006, som finns tillgängligt på Datainspektionens webbplats: www.datainspektionen.se.

vilka konsekvenserna blir om man bryter mot en regel och hur efterlevnaden av reglerna följs upp.

En grundläggande princip i personuppgiftslagen är att en anställd aldrig ska behandla fler personuppgifter än vad han eller hon behöver för sitt arbete. Den som är ekonomihandläggare på en utbildningsnämnd behöver t.ex. inte känna till vilka barn som har ansökt om plats på särskola. Den som olovligen söker efter uppgifter i systemen kan göra sig skyldig till dataintrång enligt 4 kap 9 c § brottsbalken.

För att det ska gå att utreda felaktig eller obehörig användning av personuppgifter bör det, beroende på känsligheterna hos personuppgifterna, finnas en behandlingshistorik som sparas en viss tid. Av behandlingshistoriken bör det framgå vem som har läst, ändrat, utplånat eller kopierat personuppgifter och vid vilken tidpunkt. Behandlingshistoriken bör naturligtvis följas upp, och den måste skyddas mot otillåtna ändringar.

För att förhindra förlust av personuppgifter när kommunen tillhandahåller e-tjänster, måste kommunen se till att det finns rutiner för säkerhetskopiering. För ytterligare information om säkerhetskopiering hänvisas till Datainspektionens allmänna råd ”Säkerhet för personuppgifter”, som finns tillgängliga på Datainspektionens webbplats: www.datainspektionen.se.

Den nya informations- och kommunikationstekniken gör det möjligt för de kommunala myndigheterna och förvaltningarna att möta kommuninvånarna gemensamt. I en del kommuner sker den första kontakten genom ett s.k. ”front office”, som har till uppgift att vidarebefordra allmänhetens frågor, synpunkter eller klagomål till rätt myndighet eller förvaltning i kommunen. Det är viktigt att ha i åtanke att även om kommunen i dessa fall utåt sett uppträder som en enhet, så kvarstår de grundläggande ansvarsgränserna mellan de kommunala nämnderna. Detta gäller även i fråga om personuppgiftsansvaret enligt personuppgiftslagen.

Enligt definitionen i personuppgiftslagen är det den som bestämmer ändamålen med och medlen för behandlingen av personuppgifter som är personuppgiftsansvarig. Det kan vara komplicerat att i förhand bedöma vilken kommunal nämnd som är personuppgiftsansvarig (eller vilka nämnder som eventuellt har ett gemensamt personuppgiftsansvar) för behandlingen av personuppgifter, då kommunen använder sig av system med front office. Det viktiga ur ett integritetsperspektiv är att det finns någon som är personuppgiftsansvarig och att det tydligt framgår för allmänheten vem som bär ansvaret. Kommunerna bör ta ställning till dessa frågor i samband med att man inför system med front office.

Det ligger i sakens natur att ett front office kan komma att behandla en mängd personuppgifter av mer eller mindre integritetskänslig natur. Kommunerna måste därför se till att det finns tillräckliga garantier för att obehöriga inte får

tillgång till integritetskänsligt material om andra människor. Kommunerna måste bl.a. se till att personuppgifterna inte bevaras längre än nödvändigt. När ett front office slussat en fråga vidare till rätt förvaltning eller myndighet bör uppgifterna i regel avidentifieras eller utplånas. Men denna regel gäller inte utan undantag. Om kommunen lagt ansvaret för ett front office hos en viss nämnd, exempelvis kommunstyrelsen, får nämnden utan hinder av bestämmelserna i personuppgiftslagen arkivera och bevara allmänna handlingar. Bestämmelser om myndigheternas bevarande av allmänna handlingar finns bl.a. i arkivlagen (1990:782) och arkivförordningen (1991:446).

5.5 Publicering av diarier och protokoll på Internet

Kommuner och landsting får enligt 12 § personuppgiftsförordningen publicera diarier, protokoll och vissa andra handlingar på Internet. Att göra dessa typer av handlingar tillgängliga för allmänheten kan ses som en form av e-tjänst.

Den information som läggs ut på Internet får som huvudregel inte innehålla personuppgifter som direkt pekar ut den enskilde, t.ex. namn, personnummer eller samordningsnummer. Men det finns betydande undantag från huvudregeln. Bortsett från person- eller samordningsnummer, som aldrig får göras tillgängliga på Internet, får övriga personuppgifter, t.ex. namn, publiceras under förutsättning att övriga uppgifter som rör den registrerade inte är känsliga (13 § personuppgiftslagen) eller rör lagöverträdelser (21 § personuppgiftslagen) och att det saknas skäl att anta att det finns risk för att den registrerades personliga integritet kränks genom överföringen.

Diarier och protokoll kan innehålla integritetskänsliga uppgifter av olika slag och kan därför ofta inte göras omedelbart tillgängliga i sin helhet på Internet. Det finns åtskilliga aspekter som kommunen måste beakta i samband med publiceringen. I grunden handlar det om att utforma väl fungerande tekniska och administrativa publiceringsrutiner, så att inte uppgifter som är sekretessskyddade 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 att den registrerades personliga integritet kränks genom publiceringen. Så kan vara fallet t.ex. i fråga om ärenden som rör ekonomiskt bistånd eller ärenden som på något sätt berör en persons brottslighet. Däremot finns det normalt inga hinder i integritetshänseende när det gäller att göra namn på anställda vid myndigheten externt tillgängliga i diarier och protokoll. Men om den anställde förekommer i något annat sammanhang än som handläggande tjänsteman, t.ex. i ett personalärende eller som part i ett förvaltningsärende, gäller samma regler som för all övrig publicering av personuppgifter.

Kommunen måste även se till att ärendemeningarna i diariet utformas på ett sådant sätt att integritetskänslig information inte röjs. Kommunen bör utarbeta standardformuleringar för vanligt förekommande ärendetyper som uppfyller krav på tydlighet utan att för den skull röja integritetskänslig information.

Om kommunen väljer att länka information till och från diariet, t.ex. genom att göra handlingar i olika ärenden tillgängliga, gäller personuppgiftslagens regler. Det innebär att det inte är tillräckligt att uppgifterna inte är känsliga, inte rör brott eller i övrigt kan uppfattas som kränkande för den enskilde för att det ska vara tillåtet att publicera dem på Internet. Enligt 10 § personuppgiftslagen gäller enligt huvudregeln krav på samtycke från den enskilde för att uppgifterna ska få publiceras. Eventuellt kan personuppgifter publiceras med stöd av en intresseavvägning, men enligt Datainspektionens mening kan kommunens intresse av att göra handlingar som rör enskilda tillgängliga via webbplatsen oftast inte anses väga över den enskildes intresse av skydd för den personliga integriteten.

I anslutning till diariet, t.ex. i en särskild ruta eller ett särskilt fönster på webben, är det lämpligt att lämna information enligt 23–25 §§ personuppgiftslagen till de personer som kan förekomma i diariet (se avsnitt 5.3). Utöver den information som kommunerna är skyldiga att lämna självmant enligt personuppgiftslagen, bör diariet innehålla en allmän upplysning till dem som tar del av Internetdiariet om att personuppgiftslagen är tillämplig om de själva börjar behandla uppgifterna, exempelvis genom att lagra eller bearbeta uppgifterna.

För en utförligare redovisning av de rättsliga förutsättningarna för publicering av personuppgifter i diarier på Internet hänvisas till de riktlinjer som utarbetats av Statskontoret och Datainspektionen i rapporten ”Diarier på Internet – vägledning för myndigheter” (Statskontorets rapport 2003:1), som finns tillgänglig på www.verva.se.

5.6 Övrig publicering av information på kommunens webbplats

5.6.1 Allmänt

På kommuners webbplatser publiceras ofta en stor mängd information som innebär behandling av personuppgifter. Det kan röra sig om allt från uppgifter om politiker och personal, verksamhetsområden och fattade beslut till en hyllning av kommunens nyss fyllda 100-åring, nyhetsartiklar, kåserier och fotografier. De rättsliga förutsättningarna för webbpubliceringen varierar beroende på om det rör sig om strukturerad eller ostrukturerad personuppgiftsbehandling.

5.6.2 Strukturerad respektive ostrukturerad personuppgiftsbehandling

Den 1 januari 2007 trädde en ny 5 a § i personuppgiftslagen i kraft. Detta innebär att lagen numera innehåller två olika regelsystem. För det första innehåller lagen en rad hanteringsregler för behandling av personuppgifter i strukturerat material, såsom register, databaser och dokument- och ärendehanteringssystem. För det andra innehåller lagen i denna paragraf en förenklad reglering för behandling av personuppgifter i ostrukturerat material, såsom löpande text och ljud och bild, som i princip får utföras fritt så länge den registrerades personliga integritet inte kränks.

Om en webbpublicering är kopplad till ärendehanteringssystemet, eller på annat sätt kan anses strukturerad för att påtagligt underlätta sökning efter eller sammanställning av personuppgifter, ska de vanliga hanteringsreglerna i personuppgiftslagen tillämpas. För att publiceringen ska vara tillåten utan samtycke från de registrerade krävs därför att behandlingen är nödvändig i någon av de situationer som anges i 10 § personuppgiftslagen. Webbpubliceringen kan t.ex. vara tillåten med stöd av en intresseavvägning, om den personuppgiftsansvariga nämnden har ett berättigat intresse av webbpubliceringen och detta intresse väger tyngre än den registrerade personens intresse av skydd för sin personliga integritet. Viss nyhetsrapportering kan eventuellt omfattas av undantaget för journalistiska ändamål i 7 § personuppgiftslagen.

Under förutsättning att aktuellt text-, ljud- och bildmaterial på kommunens webbplats inte ingår som en del i ärendehanteringssystemet och inte heller i övrigt kan anses ha en personuppgiftsanknuten struktur, kan personuppgifter publiceras så länge det inte kränker den enskildes personliga integritet.

För utförligare information om strukturerad och ostrukturerad personuppgiftsbehandling, se avsnitt 2.1–2.4 i denna vägledning.

5.6.3 Information om anställda

När kommunerna publicerar uppgifter om anställda på sina webbplatser, är det normalt fråga om ostrukturerad behandling av personuppgifter. Sådana uppgifter får publiceras utan andra restriktioner än att publiceringen inte får innebära en kränkning av de registrerades personliga integritet. Vad som är en kränkning ska inte bedömas schablonartat utifrån vilka uppgifter som behandlas, utan kommunerna måste också väga in i vilket sammanhang uppgifterna förekommer, för vilket syfte de behandlas, vilken spridning de har fått eller riskerar att få samt vad behandlingen kan leda till. Kommunerna bör också ta hänsyn till att vad som kan vara en kränkning för en viss person eller i ett visst sammanhang inte behöver vara det för en annan person eller i ett annat sammanhang.

Normalt kan det inte anses kränkande att publicera arbetsrelaterade personuppgifter om de anställda, t.ex. namn, befattning, telefonnummer, e-postadress och liknande uppgifter med anknytning till arbetet. Däremot innebär det normalt en kränkning att utan samtycke publicera uppgifter om de anställdas privatliv, t.ex. uppgift om hemadress eller hemtelefonnummer, på kommunens webbsida.

Om webbpubliceringen har strukturerats så att hanteringsreglerna är tillämpliga, är det normalt tillåtet att publicera arbetsrelaterade uppgifter om de anställda med stöd av en intresseavvägning. Vill man däremot lägga ut t.ex. hemadress eller hemtelefonnummer bör samtycken inhämtas.

Möjligheten att publicera foton på de anställda får avgöras efter en bedömning i varje enskilt fall, oavsett om det rör sig om strukturerad eller ostrukturerad behandling. Utgångspunkten är att samtycke måste inhämtas för att en publicering ska vara tillåten. Men i vissa fall kan allmänheten ha ett intresse av att känna till hur de anställda ser ut, t.ex. när det ingår i den anställdes yrkesroll att besöka enskilda människor i hemmen. Sådana anställda kan vara fastighetsskötare eller hemtjänstpersonal. I dessa fall kan publiceringen vara tillåten utan samtycke.

5.6.4 Allmänna handlingar

I kommunerna finns det ambitioner att dra nytta av informationstekniken, bl.a. genom att göra offentliga handlingar tillgängliga via webbplatsen. Men när kommunerna självmant publicerar allmänna och offentliga handlingar på Internet, går de utöver sina skyldigheter enligt offentlighetsprincipen.

Datainspektionen vill understryka att personuppgifter inte får publiceras eller behandlas i övrigt enbart av det skälet att de finns tillgängliga och inte är sekretessbelagda. Möjligheten att publicera diarier, protokoll och vissa andra handlingar på Internet regleras av bestämmelserna i 12 § personuppgiftsförordningen (se avsnitt 5.5). När kommunerna publicerar andra sorters handlingar på Internet än dem som avses i 12 § personuppgiftsförordningen, måste de utöver sekretesslagens bestämmelser beakta personuppgiftslagen (jfr avsnitt 5.6.2).

5.7 Sammanfattning – checklista

5.7.1 Information i samband med tillhandahållande av e-tjänster

- **Kommunen är normalt skyldig att på eget initiativ lämna information i enlighet med personuppgiftslagen till användare av e-tjänster.**

  När kommunen tillhandahåller allmänheten e-tjänster, är det i många fall fråga om datoriserad behandling av personuppgifter. Kommunen är därmed skyldig att lämna information till användare av e-tjänster i enlighet med personuppgiftslagen. Information ska lämnas oavsett om uppgifterna samlas in med eller utan de registrerades samtycke. Observera att kommunen inte behöver informera användare av e-tjänster om sådant de redan känner till eller kan antas känna till.

- **Personuppgiftslagen innehåller en uppräkning av den information som kommunerna är skyldiga att lämna.**

  Den information som den personuppgiftsansvariga nämnden är skyldig att lämna självmant ska innehålla uppgift om den personuppgiftsansvariges identitet, ändamålen med behandlingen och all övrig information som behövs för att den registrerade ska kunna ta tillvara sina rättigheter i samband med behandlingen. Det sistnämnda innebär att information ska lämnas om vilka kategorier som är mottagare av uppgifterna, skyldigheten att lämna uppgifter (registerutdrag) och rätten att ansöka om information och få rättelse.

- **För att undvika en i varje enskilt fall genomgripande och krävande översyn av när information måste lämnas, är det lämpligt att kommunen rutinmässigt lämnar information i samband med att den tillhandahåller e-tjänster.**

  Informationen kan ofta lämnas i en särskild ruta eller i ett särskilt fönster på webbplatsen, i anslutning till e-tjänsten.

5.7.2 Säkerhet för personuppgifter

- **Det måste finnas väl fungerande metoder för autentisering.**

  Kommunens val av autentiseringsmetod bör ta sin utgångspunkt i känsligheten hos de personuppgifter som behandlas och de risker som är förknippade med behandlingen. E-tjänster där användarna kan ta del av uppgifter som är att beteckna som känsliga enligt personuppgiftslagen, uppgifter som rör lagöverträdelser som innefattar brott samt uppgifter som omfattas av sekretess fordrar normalt mer avancerade metoder för autentisering, exempelvis e-legitimation eller engångslösenord.

- **Personuppgifter som överförs via öppna nät måste skyddas särskilt.**

  Personuppgifter som är att beteckna som känsliga enligt personuppgiftslagen, uppgifter som rör lagöverträdelser som innefattar brott samt uppgifter som omfattas av sekretess ska förses med krypteringsskydd när de överförs i öppna nät, t.ex. Internet.

- **Om uppgifter endast får lämnas ut till identifierade användare ska mottagarnas identitet säkerställas.**

  Kommunen och användare av e-tjänster måste kunna förvissa sig om att det är kommunen respektive användaren som är mottagare av uppgifterna. För kommunernas vidkommande kan detta lösas med hjälp av ett signerat servercertifikat och SSL/TLS.[13]

- **Kommunerna måste ha väl avvägda rutiner för behörighetstilldelning och tydliga riktlinjer för när det är tillåtet för personal att ta del av personuppgifter inom respektive nämnd eller förvaltning.**

  För att kunna utreda felaktig eller obehörig användning av personuppgifter bör det dessutom, beroende på känsligheterna hos personuppgifterna, finnas en behandlingshistorik som sparas viss tid. Behandlingshistoriken bör naturligtvis följas upp, och den måste skyddas mot otillåtna ändringar. Det är viktigt att göra klart för de anställda vad som är tillåtet, vilka konsekvenserna blir om man bryter mot en regel och hur efterlevnaden av reglerna följs upp.

13 För en kort beskrivning av SSL/TLS, se avsnitt 5.4.3.

5.7.3 Publicering av diarier och protokoll på Internet

- **Särskilda regler gäller för publicering av diarier och protokoll på Internet.**

  Person- eller samordningsnummer får aldrig göras tillgängliga i diarier och protokoll på Internet. I övrigt får diarierna eller protokollen innehålla direkta personuppgifter, som t.ex. namn, under förutsättning att övriga uppgifter som rör de registrerade inte är känsliga eller rör lagöverträdelser som innefattar brott. En ytterligare förutsättning för att materialet ska få publiceras på Internet är att det saknas skäl att anta att det finns risk för att den registrerades personliga integritet kränks genom överföringen.

- **Uppgifter som direkt pekar ut en registrerad som är föremål för sanktioner av typen avgifter, vite m.m. får normalt inte göras tillgängliga på Internet.**

  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 t.ex. vara fallet i fråga om ärenden som på något sätt berör en persons brottslighet.

- **Kommunerna måste se till att ärendemeningarna i diarierna utformas på ett sådant sätt att integritetskänslig information inte röjs.**

  Kommunerna bör utarbeta standardformuleringar för vanligt förekommande ärendetyper som uppfyller krav på tydlighet utan att för den skull röja integritetskänslig information.

- **Observera att personuppgiftslagen gäller då kommunen gör handlingar elektroniskt åtkomliga via diariet på Internet.**

  Utgångspunkten är att det krävs samtycke från de personer som förekommer i handlingar som görs elektroniskt åtkomliga via diariet på Internet. Kommunens intresse av att göra handlingar som rör enskilda tillgängliga via webbplatsen kan normalt inte anses väga över den enskildes intresse av skydd för den personliga integriteten.

5.7.4 Övrig publicering av information på kommunens webbplats

- **Personuppgiftslagen innehåller en förenklad reglering för vardaglig personuppgiftsbehandling som typiskt sett inte medför några större risker för kränkningar av den registrerades personliga integritet.**

  Publicering av personuppgifter i löpande text samt i ljud och bild på kommunens webbplats får i princip utföras fritt så länge det inte kränker den registrerades personliga integritet. Om webbpubliceringen däremot är kopplad till ärendehanteringssystem, eller på något annat sätt kan anses strukturerad för att påtagligt underlätta sökning efter eller sammanställning av personuppgifter, ska de vanliga hanteringsreglerna i personuppgiftslagen tillämpas.

- **Observera att personuppgifter inte får publiceras på kommunens webbplats enbart av det skälet att de finns tillgängliga och inte är sekretessbelagda.**

  När kommuner självmant publicerar allmänna och offentliga handlingar på Internet, går de utöver sina skyldigheter enligt offentlighetsprincipen. När kommunen avser att publicera handlingar på Internet måste de därför beakta bestämmelserna i personuppgiftslagen.

6. Geografiska informationssystem

6.1 Allmänt

GIS (geografiska informationssystem) är presentations- och analysinstrument som används för hantering och analys av lägesbundna data. Något förenklat kan GIS sägas vara en kombination av kartor och tabellinformation som lagras och hanteras i datorn. Tekniken gör det möjligt att sammanföra stora informationsmängder från flera olika källor eller system och framställa kartor med särskilda tematiska ändamål. Informationen kan i princip nås var som helst, t.ex. via Internet.

De flesta kommuner använder i idag GIS för olika ändamål. Systemen är ibland integrerade med fastighets- och kommuninvånarregistren och används för skilda verksamheter som fysisk planering, fastighetsbildning och bygglovshantering. Andra exempel på användningsområden är planering av skola och barnomsorg, skolskjutsar, äldreboende och färdtjänst. GIS används också som hjälpverktyg för att driva och underhålla kommunens infrastruktur.

Kommunerna tillhandahåller också olika externa e-tjänster kopplade till GIS, t.ex. möjlighet för allmänheten att ta del av adresskartor, geografisk information om skolor och information om planerad bebyggelse på webben. GIS används också tillsammans med GPS-teknik för att kontrollera var anställda och firmabilar befinner sig. På detta sätt kan allmänheten t.ex. följa på webben hur arbetet med kommunens snöröjning och färdtjänst fortskrider.

6.2 Behandling av personuppgifter i GIS

6.2.1 Intern användning av GIS

Samtidigt som GIS kan leda till en bättre verksamhet finns det integritetsrisker som måste hanteras. När GIS integreras med fastighets- och kommuninvånarregistren, går det t.ex. att sammanställa och presentera befolkningsstatistik på en elektronisk karta utifrån både ålder, kön och adresser på ett sätt som kan innebära risker i integritetshänseende.

Kommunerna bör noga analysera vilka personuppgifter som hanteras i systemen. Sekretesskyddat material får naturligtvis inte nå obehöriga. Uppgifter som görs tillgängliga i GIS kan också vara integritetskänsliga, trots att de inte omfattas av sekretess. Ett exempel är geografiska kartläggningar av var t.ex. barn under fem år eller äldre människor över 70 år bor. Sådana kartor kan utnyttjas på ett otillbörligt sätt om de kommer i orätta händer. En behandling av personuppgifter som inte omfattas av sekretess är inte nödvändigtvis tillåten enligt personuppgiftslagen.

När kommunerna använder GIS för att söka, analysera och presentera fastighetsdata och kommuninvånardata, innebär detta i regel en sådan behandling av personuppgifter som omfattas av personuppgiftslagens bestämmelser. För att det ska vara tillåtet att behandla personuppgifter, krävs att de grundläggande kraven i 9 § personuppgiftslagen är uppfyllda. Behandlingen ska bland annat vara berättigad och adekvat. För att behandlingen ska vara tillåten utan samtycke från de registrerade, krävs det dessutom att behandlingen är nödvändig i någon av de situationer som anges i 10 § personuppgiftslagen. Personuppgiftsbehandling i samband med GIS-användning kan t.ex. vara tillåten vid myndighetsutövning eller med stöd av en intresseavvägning.

När kommunerna använder GIS internt i sina egna verksamheter, kan det finnas legitima intressen av att behandla såväl direkta som indirekta personuppgifter. Men behandlingen måste ha ett i förväg bestämt ändamål, som är sakligt grundat i verksamheten. Personuppgifterna får sedan inte behandlas för något ändamål som är oförenligt med det ändamål för vilket uppgifterna samlades in. Detta innebär ett skydd mot vad som brukar kallas för ”ändamålsglidningar”. I praktiken innebär det att kommunen under hela behandlingstiden på något sätt måste hålla reda på för vilket ändamål personuppgifterna har infogats i GIS. Om kommunen t.ex. har infogat personuppgifter i en GIS-applikation i syfte att använda denna för bygglovshantering, får samma applikation normalt inte användas för ett annat ändamål, exempelvis för kartläggning av var personer i olika åldrar är bosatta.

Uppgifterna i GIS måste också behandlas i enlighet med god sed. Det är inte tillåtet att använda fler personuppgifter än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Detta innebär principiellt viktiga begränsningar i kommunernas möjlighet att behandla personuppgifter i GIS. Om kommunen t.ex. har för avsikt att använda GIS som analysverktyg för att planera skolskjutsar och därför behöver veta var någonstans i kommunen barn i olika åldrar bor, kan det vara tillräckligt att uppgifterna tillhandahålls på ett sådant sätt att enskilda individer inte kan identifieras.

En kommun får enligt personuppgiftslagen behandla känsliga personuppgifter utan samtycke i vissa undantagsfall, t.ex. för att kunna fullgöra sina skyldigheter eller utöva sina rättigheter inom arbetsrätten. Känsliga personuppgifter får aldrig behandlas enbart på grund av en intresseavvägning. Ett undantag från förbudet att behandla känsliga personuppgifter har vidare gjorts i 8 § personuppgiftsförordningen, där det framgår att känsliga personuppgifter får behandlas i löpande text, om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av det. Detta undantag är normalt inte tillämpligt när det gäller behandling av personuppgifter i GIS. Möjligheterna att behandla känsliga personuppgifter i GIS utan samtycke från de registrerade är därför tämligen begränsade. Exempelvis får den nämnd som är ansvarig för skolskjuts i kommunen, och som

vill registrera uppgifter i GIS för att kunna underlätta planeringen och utförandet av skolskjutsen, inte utan samtycke registrera uppgifter i GIS om att vissa barn är i behov av särskilt stöd.

Enligt Datainspektionens mening är det normalt inte motiverat att behandla personnummer i GIS-tillämpningar. Personnummer får behandlas utan samtycke bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. Kommunerna är därför normalt förhindrade att behandla personnummer i GIS. Det kan eventuellt anses berättigat att, inom ramen för den kommunala räddningstjänsten, behandla personnummer i GIS-tillämpningar som är avsedda att användas vid katastrofer eller allvarliga krissituationer, där det är angeläget att snabbt kunna spåra enskilda individer. En GIS-tillämpning som utformats för ett sådant ändamål får inte användas för något annat, oförenligt, ändamål.

För att en kommunal nämnd ska få behandla personuppgifter om lagöverträdelser i GIS, måste behandlingen vara tillåten enligt 10 § personuppgiftslagen. Också de grundläggande kraven i 9 § personuppgiftslagen måste vara uppfyllda. Det måste t.ex. finnas ett berättigat ändamål med behandlingen. Utrymmet för kommunerna att behandla personuppgifter om lagöverträdelser i GIS-tillämpningar får sammanfattningsvis betecknas som mycket begränsat. En del kommuner vill för planeringsändamål registrera uppgifter i GIS om var olika brott har begåtts i kommunen. Det är i princip tillåtet att registrera sådana uppgifter, förutsatt att uppgifterna avidentifierats och inte kan kopplas till enskilda individer.

6.2.2 Sökbegränsningar

För att det ska vara tillåtet för anställda i de kommunala förvaltningarna att söka fram uppgifter i GIS, krävs att de grundläggande kraven i 9 och 10 §§ personuppgiftslagen är uppfyllda. Det innebär bland annat att sökningen måste vara sakligt motiverad och ingå som ett led i den anställdes arbetsuppgifter. Det är t.ex. oförenligt med bestämmelserna i personuppgiftslagen att anställda tillåts söka efter uppgifter i systemen av privata skäl. Den som olovligen söker efter uppgifter i systemen kan dessutom göra sig skyldig till dataintrång enligt 4 kap. 9 c § brottsbalken.

När kommunerna överväger vilka sökmöjligheter som ska ingå i GIS, måste de ta hänsyn till att tekniken gör det möjligt att snabbt och enkelt sammanföra och presentera stora mängder uppgifter om enskilda individer. Även om uppgifterna var för sig inte är integritetskränkande, kan de tillsammans skapa en totalbild av människors enskilda förhållanden som kan uppfattas som ett otillbörligt intrång i den enskildes personliga integritet. Eftersom de kommunala nämnderna är personuppgiftsansvariga för behandlingen av personuppgifter

i GIS är det viktigt att de ställer krav på sina leverantörer att ta fram GIS-verktyg som inte gör det möjligt med alltför långtgående sökmöjligheter.

Frågan om sökmöjligheter hänger dessutom nära samman med handlingsoffentlighetens omfattning i en digital miljö. I myndigheternas elektroniskt lagrade material finns, utöver vad som kan benämnas som färdiga elektroniska handlingar, även s.k. potentiella handlingar, dvs. sammanställningar av uppgifter som inte utgör på förhand fixerade informationsmängder. GIS-tillämpningar, som innehåller kombinationer av kartor och tabellinformation där viss information sammanställs efter önskemål i det enskilda fallet, får anses utgöra exempel på potentiella handlingar.

Allmänheten har i princip rätt att på begäran ta del av potentiella handlingar, om det är möjligt med rutinbetonade åtgärder. Personuppgiftslagen hindrar inte att en sammanställning görs på grund av en begäran om allmän handling.

För att förhindra att integritetskränkande sammanställningar av information framställs är det lämpligt att kommunen överväger om det finns skäl att införa olika tekniska sökbegränsningar utifrån de ändamål för vilka personuppgifter behandlas i GIS.

6.2.3 GIS i form av e-tjänster

GIS kopplas i allt högre utsträckning till olika sorters e-tjänster. GIS används t.ex. för att ge allmänheten tillgång till adresskartor, geografisk information om skolor och förskolor och information om planerad bebyggelse.

Möjligheterna att behandla personuppgifter är betydligt mindre i fråga om sådana GIS-tillämpningar som görs allmänt åtkomliga på webben än sådana som enbart används internt i de kommunala förvaltningarna. GIS-tillämpningar som görs tillgängliga för allmänheten, exempelvis informationskartor på kommunens hemsidor, får som regel inte innehålla direkta personuppgifter såsom namn eller personnummer. Däremot kan GIS-tillämpningarna i princip innehålla indirekta personuppgifter, exempelvis fastighetsbeteckning eller adress, förutsatt att det finns ett sakligt motiverat behov av behandlingen och att den i övrigt är förenlig med bestämmelserna i personuppgiftslagen.

GIS används också bl.a. som hjälpverktyg för att driva och underhålla kommunens infrastruktur. Tekniken används även för att administrera kommunens snöröjning och färdtjänst. Med hjälp av GPS-teknik, som gör det möjligt att lokalisera enstaka fordon, kan allmänheten följa på webben hur arbetet fortskrider. När kommunerna använder tekniken på detta sätt behandlar de i de flesta fall personuppgifter. För att det ska vara tillåtet att använda positioneringsteknik, måste kommunens behov av att använda tekniken vara tydligt kopplat till dess

verksamhet. Efter att personuppgifterna har samlats in får de inte användas för något ändamål som är oförenligt med de ändamål som bestämdes innan insamlingen påbörjades. Om kommunen t.ex. har för avsikt att använda GIS tillsammans med positioneringsteknik som verktyg för att kontrollera hur kommunens vinterväghållning fungerar får tekniken normalt inte användas för andra ändamål, t.ex. för kontroll av enskilda arbetstagare.

Det är normalt tillåtet att använda positioneringsteknik utan arbetstagarens samtycke, så länge tekniken inte används på ett onödigt närgånget eller omfattande sätt. Men kommunen måste informera de anställda om behandlingen i enlighet med bestämmelserna i personuppgiftslagen. De arbetsrättsliga reglerna för fackliga kontakter måste också följas.

För ytterligare information om vad som gäller i fråga om positioneringsteknik hänvisas till Datainspektionens informationsblad ”Positioneringsteknik i arbetslivet”, som finns tillgängligt på Datainspektionens webbplats: www.datainspektionen.se.

6.3 Säkerhet

Kommunerna är skyldiga att skapa en tillfredsställande teknisk och administrativ säkerhet för de personuppgifter som ingår i GIS, så att obehöriga inte får tillgång till sekretesskyddade uppgifter om enskilda eller uppgifter som på annat sätt är integritetskänsliga. De kommunala nämnderna måste se till att bara anställda som behöver uppgifterna i sitt arbete ges tillgång till dem.

För att förhindra obehörig åtkomst bör det finnas ett system för behörighetskontroll. Ett sådant system bör göra det möjlighet att identifiera användare och bekräfta deras identitet. Kommunernas val av behörighetslösning bör utgå från känsligheten hos de personuppgifter som behandlas och de risker som är förknippade med behandlingen. Men det är inte lämpligt att personuppgifter i GIS görs tillgängliga för användare genom grupplösenord.

För att kontrollera åtkomsten till personuppgifter i GIS-databaser kan det vara nödvändigt med en behandlingshistorik (logg) som sparas en viss tid samt rutiner för regelbunden uppföljning av loggen. Naturligtvis fordras väl genomtänkta och väl fungerande administrativa och tekniska lösningar.

6.4 Sammanfattning – checklista

6.4.1 Intern användning av GIS

- **Kommunen måste noga överväga för vilka ändamål och på vilket sätt GIS används i den kommunala verksamheten.**

  Kommunens behandling av personuppgifter i GIS måste ha ett i förväg bestämt ändamål, som är sakligt grundat i verksamheten. Personuppgifterna får inte behandlas på ett onödigt närgånget eller omfattande sätt. Dessutom får kommunen inte behandla fler personuppgifter än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Detta innebär principiellt viktiga begränsningar i kommunernas möjlighet att behandla personuppgifter i GIS.

- **Personuppgiftslagen begränsar kommunerna möjlighet att behandla känsliga personuppgifter i GIS.**

  En kommun får enligt personuppgiftslagen behandla känsliga personuppgifter utan samtycke i vissa undantagsfall, t.ex. för att kunna fullgöra sina skyldigheter eller utöva sina rättigheter inom arbetsrätten. Känsliga personuppgifter får aldrig behandlas enbart på grund av en intresseavvägning. Möjligheterna att behandla känsliga personuppgifter i GIS utan samtycke från de registrerade är därför tämligen begränsade.

- **Det är normalt inte tillåtet att behandla personnummer i GIS utan samtycke från de registrerade.**

  Personnummer får behandlas utan samtycke bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. Kommunerna är därför i regel förhindrade att behandla personnummer i GIS.

- **Utrymmet för att behandla uppgifter om lagöverträdelser i GIS är mycket begränsat.**

  För att en kommunal nämnd ska få behandla personuppgifter om lagöverträdelser måste det bl.a. finnas ett berättigat ändamål med behandlingen. Utrymmet för att behandla uppgifter om lagöverträdelser är därför mycket begränsat. Det är däremot i princip tillåtet för kommunerna att för statistik- och planeringsändamål registrera uppgifter om var olika brott begås i kommunen, förutsatt att uppgifterna avidentifieras och inte kan kopplas till enskilda individer.

6.4.2 Sökbegränsningar

- **Anställda i de kommunala förvaltningarna bör endast ha behörighet att behandla personuppgifter som de behöver för sitt arbete.**

  För att det ska vara tillåtet för anställda att söka fram uppgifter i GIS hos en kommun, krävs att kraven i 9 och 10 §§ personuppgiftslagen är uppfyllda. Sökningen efter personuppgifter i GIS måste t.ex. vara sakligt motiverad och ingå som ett led i den anställdes arbetsuppgifter. Det är oförenligt med bestämmelserna i personuppgiftslagen att anställda tillåts söka efter uppgifter i systemen av privata skäl.

- **Tänk på att sökmöjligheterna i GIS avgör vad som är allmän handling.**

  Allmänheten har i princip rätt att på begäran ta del av potentiella handlingar, om det är möjligt med rutinbetonade åtgärder. För att förhindra att integritetskänsliga sammanställningar av information framställs utan att det behövs för verksamheten men på begäran av allmänheten med stöd av offentlighetsprincipen, är det lämpligt att kommunen överväger om det finns skäl att införa olika tekniska sökbegränsningar utifrån de ändamål för vilka personuppgifter behandlas i GIS.

6.4.3 GIS i form av e-tjänster

- **Kommunen får normalt inte behandla direkta personuppgifter i GIS-tillämpningar som görs åtkomliga för allmänheten på webben.**

  GIS-tillämpningar som görs tillgängliga för allmänheten, t.ex. informationskartor på kommunens webbplats, får i regel inte innehålla direkta personuppgifter som t.ex. namn eller personnummer. Däremot kan GIS-tillämpningarna i princip innehålla indirekta personuppgifter, exempelvis fastighetsbeteckning eller adress, under förutsättning att behandlingen är sakligt motiverad och att behandlingen i övrigt är förenlig med bestämmelserna i personuppgiftslagen.

- **En kommun som använder GIS tillsammans med GPS för att kontrollera var firmabilar och anställda befinner sig behandlar i de flesta fall personuppgifter som regleras av personuppgiftslagen.**

  Det är normalt tillåtet att använda positioneringsteknik utan den anställdes samtycke, så länge tekniken inte används på ett onödigt närgånget eller omfattande sätt. Kommunen måste informera de anställda om behandlingen i enlighet med bestämmelserna i personuppgiftslagen. De arbetsrättsliga reglerna för fackliga kontakter måste också följas.

6.4.4 Säkerhet

- **Kommunerna måste ha väl avvägda rutiner för behörighetstilldelning och tydliga riktlinjer för när det är tillåtet för personal att ta del av personuppgifter inom respektive nämnd eller förvaltning.**

  För att kommunen ska kunna utreda felaktig eller obehörig användning av personuppgifter i GIS bör det, beroende på känsligheterna hos personuppgifterna, finnas en behandlingshistorik som sparas viss tid. Behandlingshistoriken bör följas upp, och den måste skyddas mot otillåtna ändringar. Det är viktigt att göra klart för de anställda vad som är tillåtet, vilka konsekvenserna blir om man bryter mot en regel och hur efterlevnaden av reglerna följs upp.

7. Mellankommunalt samarbete

7.1 Allmänt

I syfte att utnyttja eventuella stordriftsfördelar sluter sig kommuner i allt större utsträckning samman i olika grupperingar. Det handlar om mellankommunalt samarbete i form av samverkan genom avtal, gemensamma förvaltningar som kommunalförbund och gemensamma nämnder, interkommunala bolag, gemensamma tjänster, projekt och olika samrådsorgan.

När samarbetsprojekt fördjupas och inte omfattar enbart administrativa aspekter, krävs juridiska analyser. Vissa kommuner har sett fördelar med ett samarbete som även omfattar den inre verksamheten i form av bland annat ärendehantering och gemensamma personregister. Sådant samarbete kräver vissa rättsliga överväganden, bl.a. om den kommunala kompetensen. För att ett sådant långtgående samarbete ska anses förenligt med de krav som ställs på skydd för den personliga integriteten, krävs det dessutom att verksamheten utvecklas i enlighet med de principer som gäller enligt personuppgiftslagen.

7.2 Personuppgiftsansvar

Enligt 3 § personuppgiftslagen är det den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter som är personuppgiftsansvarig. Personuppgiftsansvaret i en kommun ligger normalt hos de kommunala nämnder som är så självständiga att de kan anses utgöra förvaltningsmyndigheter. En kommunal nämnd som är förvaltningsmyndighet är således personuppgiftsansvarig för de behandlingar av personuppgifter som nämnden måste utföra.

När kommunala nämnder samarbetar – både inom en kommun och mellan olika kommuner – genom att dela på ansvarsområden och ta över handläggningen av varandras ärenden och andra åligganden, kan det uppstå oklarheter om personuppgiftsansvaret. Det är i och för sig möjligt att överlåta den faktiska behandlingen av personuppgifter, men personuppgiftsansvaret kan aldrig överlåtas. Det är därför viktigt att göra klart vem som är personuppgiftsansvarig innan någon personuppgiftsbehandling äger rum, i synnerhet när behandlingen sker för gemensamma syften.

Personuppgiftsbiträde är enligt 3 § personuppgiftslagen den som behandlar personuppgifter för den personuppgiftsansvariges räkning. Om en kommunal nämnd anlitar en annan kommunal nämnd för att utföra vissa uppgifter, blir

den nämnd som utför uppdraget ett personuppgiftsbiträde som får behandla personuppgifter enligt den personuppgiftsansvariges instruktioner. Hanteringen av personuppgifterna måste regleras särskilt i avtal (se mer om detta i avsnitt 7.5 om säkerhet).

Personuppgiftsansvaret kan även delas av flera olika parter. Om flera olika nämnder gemensamt samlar in och behandlar vissa personuppgifter, kan de dela på personuppgiftsansvaret.

Om samverkande kommuner väljer att bedriva sitt arbete genom ett kommunalförbund eller genom en gemensam nämnd, blir kommunalförbundet respektive den gemensamma nämnden personuppgiftsansvarig för den behandling av personuppgifter som förbundet respektive nämnden utför.

Det är alltid den personuppgiftsansvarige som ytterst svarar för att personuppgiftslagen följs och att de registrerade behandlas korrekt. Ansvaret är straff- och skadeståndssanktionerat. En konstruktion med ett delat personuppgiftsansvar kan vara vansklig, eftersom alla nämnderna då blir solidariskt ansvariga om någon av dem skulle använda uppgifterna på ett sätt som strider mot bestämmelserna i personuppgiftslagen.

7.3 Integritetsskyddsaspekter

Förutom frågor om personuppgiftsansvar, aktualiserar ett långtgående samarbete kommuner emellan ytterligare integritetsskyddsaspekter. Bland annat väcks frågor om tillgången till information.

Att flera kommuner går samman och delar utvecklingskostnaderna för ett IT-system påverkas inte av reglerna i personuppgiftslagen. Om kommunerna därefter väljer att använda systemet gemensamt, uppstår däremot vissa förhållanden som kräver ställningstaganden från den personuppgiftsansvariges sida. Kommuner som utan förbehåll samutnyttjar exempelvis ärendehanteringssystem, biblioteksystem, PA-system, GIS och IT-servrar eller delar jour riskerar att sprida personuppgifter på ett sätt som är oförenligt med både personuppgiftslagen och sekretesslagen.

Personuppgiftslagen kräver inte att alla kommuner använder separata system, men tillgången till personuppgifter måste begränsas. Ett samutnyttjat system måste därför alltid innehålla behörighetsbegränsningar. Vad som gäller för behörighetsbegränsningar i ärendehanteringssystem framgår av kapitel 4 och vad som gäller för GIS framgår av kapitel 6. Samma principer gäller för PA-system och biblioteksystem m.m. Om alla kommuner inom ett samarbete använder sig av ett gemensamt biblioteksystem som innehåller uppgifter om alla lånekortsinnehavare inom samarbetsområdet, är det lämpligt att begränsa

åtkomsten till uppgifterna. Ett bibliotek inom en viss kommun behöver sällan tillgång till uppgifter om låntagare som inte använder den egna kommunens bibliotek.

När kommuner delar upp arbetsuppgifter mellan sig – en tar hand om alla frågor som föranleder behov av GIS, medan en annan sköter personaladministrationen – måste kommunerna ta ställning till personuppgiftsansvaret för uppgifterna. Eventuellt behöver biträdesavtal upprättas (se mer om detta under avsnittet 7.5.1 om säkerhet).

Gemensamma projekt kan medföra behandling av personuppgifter. En gemensam bygg- och planläggning kan t.ex. innebära hantering av fastighetsuppgifter. Innan sådana projekt inleds, bör personuppgiftsansvar, behörighetsrutiner och eventuella säkerhetsåtgärder ses över.

7.4 Gemensamt kommuninvånarregister och fastighetsregister

De flesta kommuner behandlar personuppgifter om kommunens invånare i ett kommuninvånarregister (KIR). Registret innehåller folkbokföringsuppgifter om kommunens invånare och kan i vissa fall omfatta uppgifter om skyddade adresser. Kommunerna använder sig även ofta av fastighetsregister, som innehåller uppgifter om fastighetsägares namn och personnummer samt övrig fastighetsdata.

I och med att olika kommuner inleder samarbete med varandra, uppstår ett behov av tillgång till uppgifter inte bara om de egna kommuninvånarna utan även om andra kommuners invånare. Behovet kan uppstå med anledning av t.ex. delad handläggning av ärenden, planering av kommunala tjänster i form av äldreomsorg och skola eller vid planritning. Genom att slå ihop flera register och skapa ett enda stort kommuninvånarregister, alternativt genom att låta andra kommuner ta del av det egna registret, kan man lösa behovet av tillgång till uppgifter.

Kommunernas behov av en effektiv hantering av invånarnas personuppgifter måste dock vägas mot de enskildas intresse av skydd för den personliga integriteten. Stora personregister är alltid förenade med stora integritetsrisker, och Datainspektionen har hittills ställt sig kritisk till uppbyggnad av alltför omfattande register. Inspektionens ståndpunkt har dock i realiteten inte grundats på registrens storlek i sig, utan på att den personuppgiftsansvarige sällan kan visa en tydlig relation till alla de registrerade. Det måste normalt sett finnas en anknytning till de registrerade för att registrets ändamål ska anses berättigat.

Om samverkande kommuner har ett omfattande och integrerat samarbete, t.ex. med nämnder som gemensamt handlägger ärenden eller ett kommunalförbund som hanterar vissa frågor, kan det finnas skäl att upprätta ett gemensamt kommuninvånarregister. Samma sak gäller för gemensamma fastighetsregister.

7.5 Säkerhet

7.5.1 Biträdesavtal

När en kommunal nämnd anlitar en annan nämnd för att utföra dess uppgifter, kan det innebära att den anlitade nämnden blir ett personuppgiftsbiträde. Den personuppgiftsansvariga nämnden ska då enligt 31 § personuppgiftslagen förvissa sig om att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att personuppgiftsbiträdet verkligen vidtar åtgärderna.

Ett personuppgiftsbiträde får enbart behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvarige och är skyldig att vidta de säkerhetsåtgärder som den personuppgiftsansvarige kräver eller instruerar om. Ett skriftligt avtal som reglerar förhållandet mellan personuppgiftsbiträdet och den personuppgiftsansvarige ska upprättas enligt 30 § personuppgiftslagen. I avtalet ska bl.a. säkerhetsåtgärderna vid behandlingen av personuppgifter regleras. Kravet på skriftlighet innebär att avtalet måste vara uttryckt i text, men texten kan finnas på papper eller i elektronisk form. Något krav på att avtalshandlingen ska vara undertecknad finns inte, men detta kan rekommenderas ur bevishänseende.

Den personuppgiftsansvariga nämnden är skadeståndsskyldig gentemot den registrerade, även för åtgärder som en medhjälpare eller ett personuppgiftsbiträde har utfört. Ett biträde kan enligt avtal eller allmänna regler bli skadeståndsskyldigt gentemot den personuppgiftsansvarige.

7.5.2 Säker kommunikation

Beroende på hur olika samarbetande nämnder arbetar, kan det finnas behov av olika tekniska säkerhetsåtgärder. För att förhindra att personuppgifter förstörs, ändras eller förvanskas vid överföring via nät och för att skydda anslutna tjänster mot obehörig åtkomst bör den personuppgiftsansvarige vidta lämpliga åtgärder för att åstadkomma en tillfredsställande säkerhet. Personuppgifter som överförs via nät bör, beroende på hur känsliga de är, skyddas genom kryptering.

När utrustningen ansluts till Internet eller något annat öppet nät, bör anslutningen skyddas för att obehörig trafik ska förhindras. I samma syfte bör åtkomst förhindras från det öppna nätet till annan utrustning eller lokala nät hos den personuppgiftsansvarige. Om uppgifterna endast får lämnas ut till identifierade användare, bör mottagarens identitet säkerställas. Mottagarens identitet kan säkerställas genom e-legitimation, engångslösenord, aktiva behörighetskort eller motsvarande.

Behovet av åtgärder och policy för att minska säkerhetsrisker vid användning av elektronisk post bör övervägas. Genom exempelvis kryptering förhindrar man att uppgifterna kan läsas eller förvanskas i samband med överföringen. För att kryptering ska ge det skydd som krävs, måste krypteringsnycklarna vara tillräckligt kraftfulla, och nycklarna måste handhas på ett säkert sätt.

7.5.3 Tillgång till befolkningsregister

Stora befolkningsregister innehåller många personuppgifter, och det är därför angeläget att endast anställda med behov av uppgifterna i sitt arbete får ta del av dessa. Grupplösenord är således inte lämpliga.

Många kommuninvånarregister innehåller s.k. skyddade personuppgifter – uppgifter som fått en markering för särskild sekretessprövning i folkbokföringsdatabasen. Det finns inga särskilda bestämmelser i personuppgiftslagen som avser behandling av skyddade personuppgifter, men i fråga om sådana uppgifter är det extra viktigt att kraven på säkerhet beaktas och att ingen obehörig får tillgång till dem.

7.6 Sammanfattning – checklista

- **Vid allt samarbete som innefattar behandling av personuppgifter måste de inblandade parterna ta ställning till vem eller vilka som är personuppgiftsansvariga och vem eller vilka som eventuellt är personuppgiftsbiträde.**

  Personuppgiftsansvaret i en kommun ligger normalt hos de kommunala nämnder som är så självständiga att de kan anses utgöra förvaltningsmyndigheter. Personuppgiftsansvaret kan även delas av flera olika nämnder eller bäras av ett kommunalförbund.

  Om en kommunal nämnd anlitar en annan kommunal nämnd för att utföra uppgifter som innefattar personuppgiftsbehandling, blir den nämnd som utför uppdraget ett personuppgiftsbiträde som får behandla personuppgifter enligt den personuppgiftsansvariges instruktioner.

- **Biträdesavtal ska upprättas om en kommunal nämnd anlitas för att utföra vissa uppgifter åt en annan nämnd.**

  En kommunal nämnd som utgör personuppgiftsbiträde får enbart behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvarige och är skyldig att vidta de säkerhetsåtgärder som den personuppgiftsansvarige kräver eller instruerar om. Ett skriftligt avtal ska upprättas som reglerar förhållandet mellan personuppgiftsbiträdet och den personuppgiftsansvarige. I avtalet ska bl.a. säkerhetsåtgärderna vid behandlingen av personuppgifter regleras.

- **Ett mellankommunalt samarbete kan kräva särskilda säkerhetsåtgärder.**

  Personuppgifter som överförs via ett öppet nät bör, beroende på hur känsliga de är, skyddas t.ex. genom kryptering. Om uppgifterna endast får lämnas ut till identifierade användare, bör mottagarens identitet säkerställas. Dessutom bör man överväga behovet av åtgärder och policy för att minska säkerhetsrisker vid användning av elektronisk post.

- **Om samverkande kommuner har ett omfattande och integrerat samarbete, kan det finnas skäl att upprätta ett gemensamt kommuninvånarregister.**

  Kommunernas behov av en effektiv hantering av invånarnas personuppgifter måste vägas mot de enskildas intresse av skydd för den personliga integriteten. Det måste normalt sett finnas en tydlig relation mellan den personuppgiftsansvarige och de registrerade för att registrets ändamål ska anses berättigat. För tillgång till ett sådant register krävs särskilda behörigheter.

8. Andra publikationer

Diarier på Internet – Vägledning för myndigheter, 2003:1, Statskontoret (finns på VERVA:s webbplats).

Vägledning för information som enligt lag ska lämnas på webbplatser, E-nämnden (finns på VERVA:s webbplats).

Vägledningen 24-timmarswebben – Effektivare och bättre service på webbplatser i offentlig sektor, 2006:5, VERVA.

Information till registrerade enligt personuppgiftslagen, Datainspektionens allmänna råd.

Säkerhet för personuppgifter, Datainspektionens allmänna råd.

Basnivå för informationssäkerhet (BITS), KBM rekommenderar 2006:1.

Ledningssystem för informationssäkerhet – Riktlinjer för styrning av informationssäkerhet (ISO/IEC 17799:2005, IDT), BITS.

Datainspektionen

Postadress: Box 8114, 104 20 Stockholm
Besöksadress: Fleminggatan 14, plan 9
Beställningar: 08-657 61 42 (telefonsvarare)
E-post: datainspektionen@datainspektionen.se
Telefon: 08-657 61 00 Fax: 08-652 86 52
Webbplats: www.datainspektionen.se

Pris: 50 kr + moms