

Datainspektionen informerar

Nr 2/2011

Allmänna råd om personregister

Enligt 1 § landskapslagen (2007:89) om Datainspektionen skall Datainspektionen följa den allmänna utvecklingen inom sitt verksamhetsområde och ta nödvändiga initiativ. Datainspektionen skall informera om gällande regler samt ge anvisningar och råd om behandlingen av personuppgifter.

Datainspektionens allmänna råd är inte bindande. De är rekommendationer om hur de bindande kraven i landskapslagen (2007:88) om behandling av personuppgifter inom kommunal- och landskapsförvaltningen (personuppgiftslagen) kan uppnås vid behandling av personuppgifter **i samband med uppgörande av registerbeskrivningar.**

Datainspektionen

den 20 september 2011

Innehåll

1	Sammanfattning	4
2	Varför en registerbeskrivning?	4
3	Vem har ansvaret för att en registerbeskrivning upprättas?.....	5
4	Registerförare (registerbiträde).....	5
5	Vad är en personuppgift?	6
5.1	LL om behandling av personuppgifter	6
5.2	EU:s dataskyddsdirektiv	6
6	Personuppgifter i register.....	8
6.1	Grundläggande skyldigheter enligt LL om behandlingen av personuppgifter	9
6.2	Administrativ säkerhet.....	10
6.3	Användarrättigheter	11
6.4	Fysisk säkerhet	11
6.5	Grundläggande frågor gällande datasäkerheten.....	12
6.6	Säkerheten gällande utrustning och programvara.....	12
6.7	Datamediers (CD-ROM-skivor, magnetband, disketter m.m.) säkerhet.....	12
6.8	Säkerhet i datatrafiken	12

1 Sammanfattning

Inom förvaltningen förekommer olika typer av administrativa system i vilka personalen och medborgarna ingår. För att skydda egendom förekommer bland annat system för fastighetskötsel och även i viss mån kameraövervakning. Se Datainspektionens allmänna råd beträffande kameraövervakning (Datainspektionen informerar Nr 1/2011).

Grundläggande för all behandling är att de personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen och att inte fler personuppgifter behandlas än nödvändigt. En viktig aspekt är också att lämpliga säkerhetsåtgärder vidtas.

Sammanfattningsvis bör den registeransvariga tänka på följande:

- Kartlägg förekomsten av personregister
- Definiera ändamålet med behandlingen
- Användning i samklang med ändamålet
- Kartlägg en eventuell hotbild
- Skapa en fungerande organisation för säkerhet
- Skaffa den utrustning som behövs och använda den rätt
- Upprätta regler och rutiner
- Informera och utbilda kontinuerligt
- Följ upp att regler och rutiner följs och respekteras
- Instruera, utbilda och övervaka
- Testa säkerheten regelbundet
- Kvalitet
- Skydda uppgifterna
- Informera den registrerade
- Tillgänglig registerbeskrivning

2 Varför en registerbeskrivning?

Enligt 5 § landskapslagen (2007:88) om behandling av personuppgifter är registeransvarig myndighet skyldig att upprätta en registerbeskrivning över register med personuppgifter. Det föreligger således en informationsplikt till de registrerade.

3 Vem har ansvaret för att en registerbeskrivning upprättas?

En registeransvarig

Begreppet registeransvarig är fristående i den bemärkelsen att det främst bör tolkas i enlighet med gemenskapens dataskyddslagstiftning och funktionellt i den bemärkelsen att det är avsett att fördela ansvaret i förhållande till det faktiska inflytandet. Det åligger således den registeransvariga att säkerställa att personuppgifter ska behandlas på ett korrekt och lagligt sätt. Bestämmelserna om den registrerades rätt till information, tillgång, rättning, utplåning eller blockering samt rätt att göra invändningar mot behandlingen av personuppgifter har utformats på ett sätt som skapar skyldigheter för den registeransvariga. Den registeransvariga är i princip ansvarig för eventuella skador till följd av otillåten behandling vilket följer av skyldigheten att efterleva dataskyddsbestämmelserna. Begreppet registeransvarig är också avgörande för att fastställa vilken nationell lag som är tillämplig i en behandlingsåtgärd eller serie av behandlingsåtgärder.

Flera registeransvariga

Parter som agerar tillsammans har en viss flexibilitet när det gäller att fördela skyldigheter och ansvar sinsemellan, så länge de garanterar en fullständig efterlevnad. Det viktigaste är att se till att efterlevnaden av dataskyddsbestämmelserna och ansvaret för eventuella brott mot dataskyddsbestämmelserna är tydligt fördelade. Det gäller i synnerhet i komplexa behandlingsmiljöer där olika registeransvariga har del i behandlingen av personuppgifter. I dessa fall är det viktigare än någonsin att de registrerade får tydlig information som förklarar de olika steg och aktörer som ingår i behandlingen. Dessutom bör det tydligt framgå om varje registeransvarig har befogenhet att tillgodose alla rättigheter för registrerade, eller vilken registeransvarig som är behörig för vilken rättighet.

Straffbestämmelser

Underlåtelse att iakttä förpliktelsen att upprätta en registerbeskrivning är enligt 29 § 1 mom. 1) punkten och 2 mom. en straffbar handling (personregisterförseelse).

4 Registerförare (registerbiträde)

Den registeransvariga myndigheten fattar beslut om det ska finnas registerförare (registerbiträde) för myndighetens personregister. En registerförare har en viktig funktion vid tillämpningen av bestämmelserna gällande sekretess och säkerhet vid behandlingen. Registerföraren agerar för den registeransvarigas räkning. Den registeransvariga myndigheten skall följa instruktionerna från registeransvarig åtminstone i fråga om ändamålet med behandlingen av personuppgifter.

5 Vad är en personuppgift?

5.1 LL om behandling av personuppgifter

Personuppgifter är "all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet" (2 § landskapslagen om behandling av personuppgifter).

5.2 EU:s dataskyddsdirektiv

Dataskyddsdirektivet (EU-direktiv 95/46/EG) återspeglar lagstiftarens avsikt att hålla begreppet personuppgifter¹ så brett som möjligt för att omfatta all information rörande en identifierbar individ.

Varje upplysning

Begreppet "varje upplysning" i direktivet signalerar tydligt lagstiftarens vilja att utforma ett brett begrepp för personuppgifter. Artikel 29-arbetsgruppen för skydd av personuppgifter har i ett yttrande² kommit fram till att begreppet kräver en vid tolkning. Artikel 29-arbetsgruppen inrättades enligt artikel 29 i direktiv 95/46/EG. Den är ett oberoende rådgivande EU-organ i frågor som gäller dataskydd och integritet.

Som avser en

Benämningen kan anses avse en *person* när det handlar om den personen. Det kan innebära att uppgifter registreras i en persons akt på ett personalkontor och avser personens situation som anställd. Det kan också avse bilden av en person som filmas av en övervakningskamera eller uppgifter om resultatet av en patients medicinska test i patientens patientjournal.

I vissa fall gäller informationen *föremål* och inte enskilda personer. Dessa föremål tillhör vanligtvis någon, eller är utsatta för eller har ett särskilt inflytande på personer, eller har en sorts fysisk eller geografisk närhet till personer eller andra föremål. Uppgifter om värdet på ett hus är information om ett föremål. Det är klart att bestämmelserna om uppgiftsskydd inte är tillämpliga om denna information endast kommer att användas som illustration för fastighetspriserna i ett visst område. Under vissa omständigheter anser Artikel 29-gruppen att sådan information också kan betraktas som personuppgifter. Huset som sådant utgör ju en ägares tillgångar, och följaktligen kommer informationen om värdet att användas för att t.ex. avgöra ägarens skyldighet att betala skatt. Följden blir att sådan information bör betraktas som personuppgifter.

Identifierad eller identifierbar fysisk person

En person kan identifieras direkt genom ett namn eller indirekt genom ett telefonnummer, registreringsnummer, personbeteckning, passnummer eller av en kombination av väsentliga kriterier som gör att personen känns igen genom att den grupp som han tillhör ringas in (ålder, yrkesverksamhet, bostadsort etc.).

¹ "personuppgifter: varje upplysning som avser en identifierad eller identifierbar fysisk person (den registrerade). En identifierbar person är en person som kan identifieras, direkt eller indirekt, framför allt genom hänvisning till ett identifikationsnummer eller till en eller flera faktorer som är specifika för hans fysiska, fysiologiska, psykiska, ekonomiska, kulturella eller sociala identitet"

² Yttrande 4/2007 om begreppet personuppgifter

Vidare kan en person identifieras indirekt genom s.k. unika kombinationer vilket avser en eller flera faktorer som är specifika för personens fysiska, fysiologiska, psykiska, ekonomiska, kulturella eller sociala identitet. Vissa utmärkande egenskaper är så unika att en person lätt kan identifieras ("den nuvarande stadsdirektören"), men en kombination av upplysningar på kategorinivå (ålderskategori, regionalt ursprung m.m.) kan också vara tämligen avgörande under vissa omständigheter, särskilt om det finns tillgång till någon form av ytterligare information.

Det bör noteras att även om identifiering genom namnet i praktiken är vanligast så är ett namn i sig inte alltid nödvändigt för att identifiera en individ. T.ex. i datafiler för registrering av personuppgifter ges de registrerade vanligen en unik identifierare för att undvika sammanblandning mellan två personer i filen. Även på nätet ger verktygen för övervakning av Internettrafiken möjlighet att på ett enkelt sätt identifiera en dators beteende och bakom den datoranvändaren. På detta vis pusslar man ihop individens personlighet för att tillskriva individen vissa beslut. Utan att ens ta reda på en individs namn och adress är det möjligt att kategorisera personen på grundval av socioekonomiska, psykologiska, filosofiska och andra kriterier och tillskriva honom eller henne vissa beslut. Individens kontaktpunkt (en dator) kräver nödvändigtvis inte längre att individens identitet i snäv bemärkelse avslöjas. Således kan en individ identifieras utan att hans eller hennes namn är känt.

I själva verket är den registeransvariges syfte med databehandlingen en relevant faktor för att bedöma vilka hjälpmedel som kan komma att användas för att identifiera personer. I de fall där syftet med databehandlingen innebär identifiering av individer kan man förutsätta att den registeransvarige eller någon annan delaktig person har eller kommer att ha hjälpmedel som rimligen kan komma att användas för att identifiera den registrerade. Att hävda att enskilda individer inte är identifierbara när syftet med databehandlingen just är att identifiera individer, vore oerhört motsägelsefullt. Därför bör informationen anses avse identifierbara individer och behandlingen omfattas av uppgiftsskyddsbestämmelserna. IP-adresser har ansetts vara uppgifter som avser en identifierbar person³.

Anonyma uppgifter kan enligt direktivet definieras som all information som avser en fysisk person som inte kan identifieras varken av den registeransvariga eller av någon annan, med beaktande av alla hjälpmedel som i syfte att identifiera vederbörande rimligen kan komma att användas antingen av den registeransvariga eller av någon annan person.

Syftet med *pseudonymisering* (en process för att dölja identiteter) är att kunna samla ytterligare uppgifter om en och samma individ utan att behöva känna till personens identitet. Pseudonymisering kan ske på ett sätt som *går att spåra* genom användning av förteckningar över identiteter och deras motsvarande pseudonymer eller genom att använda tvåvägs krypteringsalgoritmer för pseudonymisering. Att dölja identiteter kan också ske på ett sätt så att *återidentifiering inte är möjlig*, t.ex. genom envägs kryptering, som i allmänhet skapar anonymiserade uppgifter. Pseudonymer bör vara slumpmässiga och omöjliga att förutsäga. Spårbara pseudonymiserade uppgifter kan anses som information om individer som är indirekt identifierbara.

³ Enligt Artikel 29-arbetsgruppen för skydd av personuppgifter kan nätleverantörer och förvaltare av lokala nätverk (LAN) med rimliga medel identifiera de Internet-användare som de har tilldelat IP-adresser eftersom de i allmänhet i en fil bokför datum, tidpunkt, varaktighet och den dynamiska IP-adress som Internet-användaren har fått. Samma sak gäller för Internet-leverantörer som för en loggbok på http-servern.

Kodade uppgifter är ett klassiskt exempel på pseudonymisering. Informationen avser individer som har betecknats med en kod, medan nyckeln för att koppla samman koden och de vanliga identifierarna (namn, födelsedatum och adress) för individerna sparas för sig. Om de koder som används är *unika för varje enskild person* uppstår en risk för identifiering vid varje tillfälle som det är möjligt att få tillgång till den nyckel som används för krypteringen. Om däremot koderna *inte är unika*, utan samma koder används för att beteckna individer i olika kommuner och för uppgifter från olika år kan den registeransvariga eller en tredje part endast identifiera en viss individ om de vet vilket år och vilken kommun som uppgifterna avser. Om denna tilläggsinformation har försvunnit, och den rimligen inte kommer att återfinnas, kan det anses att informationen inte avser identifierbara individer och därför inte omfattas av uppgiftsskyddsbestämmelserna.

Fysisk person

Personuppgifter avser därför i princip identifierade eller identifierbara levande personer. När information som är uppgifter om en avliden person samtidigt kan anses avse en levande person är de följaktligen personuppgifter enligt direktivet.

6 Personuppgifter i register

Med personregister avses varje strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden.

Behandling av personuppgifter avser varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte. Exempel på sådan behandling är insamling, registrering, organisering, lagring, bearbetning eller sammanställning.

Redan vid planeringen av och i samband med att bland annat nättjänster ställs till förfogande bidrar skyddet av den personliga integriteten i regel till en ökning av användningen av digitala nättjänster. Enligt 7 § lagen om dataskydd vid elektronisk kommunikation (FFS 516/2004) föreligger en plikt att informera om kakor⁴ (Cookies). Tillsynsmyndighet är Kommunikationsverket.

IT-system har som syfte att förbättra effektiviteten inom organisationen. För i stort sett all behandling av personuppgifter gäller landskapslagen om behandling av personuppgifter⁵. Följande omständigheter bör beaktas i samband med att personuppgifter behandlas på ett systematiskt sätt:

⁴ Kakfiler innehåller uppgifter som beskriver användningen av en internetjänst och sparas t.ex. på användarens dator. Informationen kan användas till att styra kontakten mellan en webbläsare och en server på nätet. En kaka kan spara information om t.ex. de webbsidor en användare besökt för att en sida senare skall kunna "komma ihåg" en användare nästa gång han eller hon kommer till samma sida.

⁵ Undantagna är staten, Ålands polismyndighet, privata sektorn samt till den del en åländsk myndighet utför uppgifter och därmed hanterar personuppgifter som enligt 27 § Självstyrelselagen hör till rikets lagstiftningsbehörighet tillämpas rikslagen.

6.1 Grundläggande skyldigheter enligt LL om behandlingen av personuppgifter

Var finns personuppgifterna?

Inventera systemen med flera strukturerade samlingar av personuppgifter och fastställ ändamålen med behandlingen av personuppgifter. Exempel på personregister kan vara kund- och personalregister, fastighetsskötsel såsom dörrlås och fysisk säkerhet, schema, betyg m.m. Även insamling av information över Internet såsom kundförfrågningar, arbetsplatsansökningar, anmälningssblanketter och insamling av besökarrespons är exempel på nättjänster och liknande funktioner där lagligheten bör prövas utgående från landskapslagen om behandling av personuppgifter och där en registerbeskrivning bör upprättas.

Hur länge får uppgifterna bevaras?

Analysera och ta ställning till behovet av bevarande och gallring. Personuppgifterna skall i regel inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen.

Arkivlagen ger vägledning i frågor som gäller bevarande och gallring. Skriftliga riktlinjer och rutiner för bevarande och gallring av personuppgifter bör tas fram i syfte att radera uppgifter när de inte längre behövs.

Informera

Informera genom att upprätta en *registerbeskrivning* över register med personuppgifter (se bifogad blankett). Registerbeskrivningen skall innehålla bl.a. uppgifter om

- Vilken myndighet som är registeransvarig
- vem som är registerförare (registerbiträde)
- för vilket ändamål uppgifterna hanteras
- rätten till registerutdrag
- rätten till rättelse

Var och en har i regel rätt att på ansökan få information om personuppgifter som rör honom eller henne behandlas i ett register eller inte.

Avtal med systemleverantörer

Om myndigheten anlitar en extern systemleverantör som även sköter driften och lagrar myndigheternas personuppgifter i sina datorer, krävs det att myndigheten ingår ett avtal med leverantören. I avtalet skall regleras hur personuppgifterna får hanteras och hur ansvaret och förpliktelserna i samband med registreringen hanteras. Till exempel får leverantören behandla personuppgifterna bara i enlighet med instruktioner från myndigheten och leverantören är skyldig att vidta åtgärder för att upprätthålla god IT-säkerhet.

Avtal om köptjänster

I avtal om köptjänster definieras vilka rättigheter och skyldigheter myndigheten och den privata serviceproducenten har. När avtal om köptjänster ingås är det skäl att i avtalen ta in bestämmelser om hur handlingarna skall förvaltas, hur de skall göras upp, uppbevaras, utplånas eller arkiveras. Det är dessutom skäl att i avtalen anteckna hur upplysningar om handlingarna skall ges till den registrerade eller till en person i partsställning eller till någon annan utomstående.

6.2 Administrativ säkerhet

Uppgifter i frånvarorapporteringen

Känsliga uppgifter⁶ kräver i regel samtycke. "Sjuk", "förkyld" m.m. är känsliga personuppgifter. Utan samtycke får arbetsgivaren eller skolan bara registrera att arbetstagaren eller eleven haft frånvaro. Det gäller dock inte för journalföring inom skolhälsovården där hälsouppgifter får registreras utan samtycke.

Personuppgifter i IT-system

Rutiner och riktlinjer till personalen gällande fria textfält (d.v.s. där det är fritt att skriva vad man vill). Det måste finnas tydliga instruktioner till användarna om vilken information som får skrivas i fritextfältet. Instruktionerna bör exempelvis ange hur värderande omdömen om personal eller elever ska formuleras och att kränkande uttalanden inte är tillåtna.

När krävs samtycke?

Personuppgifter får bland annat behandlas bara om den registrerade har lämnat sitt otvetydiga samtycke till behandlingen eller om behandlingen är nödvändig för att ett avtal med den registrerade skall kunna fullföljas, den registeransvarige skall kunna fullfölja en rättslig skyldighet när behandlingen regleras i lag, vitala intressen för den registrerade skall kunna skyddas eller för att utföra en arbetsuppgift då den registrerade på grund av ett kund- eller tjänstgöringsförhållande, ett medlemskap eller annan därmed saklig anknytning till den registeransvarigas verksamhet.

Undantaget från förbudet att behandla känsliga uppgifter får bl.a. göras om behandlingen sker med uttryckligt samtycke från den som uppgifterna avser, behandlingen är reglerad i lag, behandlingen gäller medlemskap i fackförbund och behandlingen är nödvändig för att den registeransvariga skall kunna fullgöra sina skyldigheter eller utöva sina rättigheter inom arbetsrätten, behandlingen är nödvändig för att den registrerades eller någon annans vitala intressen skall kunna skyddas, om den registrerade är förhindrad att lämna sitt samtycke eller behandlingen är nödvändig för förebyggande hälso- och sjukvård, medicinska diagnoser, vård eller behandling eller administration av hälso- och sjukvård eller uppgifterna behandlas av en person som är yrkesverksam inom hälso- och sjukvården och har tystnadsplikt.

Uppgifter om personbeteckning får behandlas om den registrerade lämnat sitt samtycke eller när behandlingen är reglerad i lag. Personbeteckning får dessutom behandlas om det är nödvändigt för att göra en säker identifiering av den registrerade för att utföra en i lag angiven uppgift, för att uppfylla den registrerades eller registeransvarigas rättigheter eller skyldigheter eller för historisk eller vetenskaplig forskning eller statistikföring.

⁶ Känsliga personuppgifter är bland annat etnisk tillhörighet, politiska åsikter, religiös eller filosofisk övertygelse, brottslig gärning eller ett straff, medlemskap i fackförening eller uppgifter som rör hälsa eller sexualliv eller någons behov av socialvård.

Känsliga personuppgifter

Det är enligt landskapslagen om behandling av personuppgifter i princip förbjudet att behandla känsliga uppgifter. I lagen definieras vissa slag av uppgifter som känsliga.

Det är uppgifter som avslöjar

- Ras eller etniskt ursprung
- Politiska åsikter
- Religiös eller filosofisk övertygelse
- Medlemskap i fackförbund
- brottsuppgifter⁷

Och uppgifter som rör

- Hälsa
- Sexualliv

Förbudet gäller inte bara behandling som direkt avslöjar eller rör något av de angivna förhållandena utan även behandling som innebär att sådana förhållanden indirekt kan utläsas.

Hemliga personuppgifter

I vissa fall förekommer skyddade personuppgifter såsom namn och adress. I sådana fall skall åtkomsten begränsas och spridning av uppgifterna begränsas. Personalen skall informeras genom att rutinerna regelbundet följs upp.

6.3 Användarrättigheter

Begränsa personalens behörighet

För att hindra obehöriga från att få tillgång till personuppgifter bör det finnas rutiner för behörighetskontroll. Det bör gå att identifiera användare och bekräfta användarens identitet, exempelvis genom personliga lösenord. Behovet ska styra behörigheten.

Straffbestämmelser

Den som vid behandling av personuppgifter yppar vad han eller hon har fått kännedom om enskild persons egenskaper, personliga förhållanden eller ekonomiska ställning kan göra sig skyldig till brott mot tystnadsplikt.

6.4 Fysisk säkerhet

Förebygg att obehöriga har tillgång till utrymmen där personuppgifter behandlas. Det bör finnas rutiner för tillträdeskontroll för att säkerställa att enbart behörig personal får tillträde till utrymmen där det finns IT-utrustning. Behovet av att kunna göra en viss arbetsuppgift kan göras till utgångspunkt för hur en tillträdeskontroll utformas.

⁷ Med brott avses inte bara att någon är dömd i ett brottmål utan även en misstanke om brott omfattas av förbudet

6.5 Grundläggande frågor gällande datasäkerheten

IT-säkerhetsåtgärder

Den registeransvariga myndigheten skall vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna skall åstadkomma en säkerhetsnivå som är lämplig med beaktande av

- A) De tekniska möjligheter som finns,
- B) Vad det skulle kosta att genomföra åtgärderna,
- C) De särskilda risker som finns med behandlingen av personuppgifterna, och hur pass känsliga de behandlade personuppgifterna är.

När den registeransvariga myndigheten anlitar ett registerbiträde, skall den registeransvariga förvissa sig om att registerbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att registerbiträdet verkligen vidtar åtgärderna.

6.6 Säkerheten gällande utrustning och programvara

Syftet bör vara att kontrollera att det inte är möjligt att komma åt systemet utan att vara behörig. Det skall inte vara möjligt att uppgifter tillförs, överförs, ändras eller avlägsnas utan tillräckliga befogenheter. Det skall vara möjligt att i efterskott granska och verifiera vilka uppgifter som lagts till eller avlägsnats samt när det skett och av vem.

6.7 Datamediers (CD-ROM-skivor, magnetband, disketter m.m.) säkerhet

Kontrollera att datamedier som innehåller personuppgifter inte kan läsas, kopieras, ändras, bortföras eller på annat sätt hamna i orätta händer.

6.8 Säkerhet i datatrafiken

Kontrollera att systemet inte kan användas utan befogenhet via dataöverföringsutrustning eller nätförbindelser.

Google och andra sökmotorer

Är Google registeransvarig för information?

Nej. Det är den webbplats där informationen ursprungligen publicerades som är registeransvarig. En sökmotor har ett väldigt begränsat ansvar och är i stort sett bara ansvarig för sådan information som sparas trots att den ursprungliga webbplatsen raderats t.ex. vid cachning.

Tillvägagångssättet för att få bort information från sökmotorn är att ta bort informationen från webbplatsen och se till att webbsidan eller delar av den inte indexeras.

Personuppgifter i sociala media

Användningen av Facebook, Twitter, bloggar och andra typer av sociala medier kan innebära att personuppgifter behandlas. Det innebär i så fall att landskapslagen om behandling av personuppgifter är tillämplig.

Det är viktigt att komma ihåg att ansvaret för personuppgifter som publiceras via ett socialt media är beroende av utformningen av den sociala medietjänst som används och att de sociala medierna är under ständig förändring och utveckling.

Vad beträffar Facebook och bloggar så är myndigheten ansvarig för personuppgifter som publiceras på myndighetens Facebook-sida och/eller blogg. Ansvaret omfattar både personuppgifter som myndigheten själv publicerar och personuppgifter som publiceras av andra i till exempel en kommentar på sidan. Även den besökare som skrivit en kommentar kan ha ett ansvar för vad den själv skrivit. Vad beträffar Twitter så ansvarar myndigheten endast för personuppgifter som myndigheten själv publicerar, inte personuppgifter som andra twittrade lämnat. Orsaken till det begränsade ansvaret är att myndigheten inte kan påverka andras twitter-inlägg.

Myndigheten har ett ansvar för att personuppgifter på dess Facebook-sida, blogg, Twitterkonto och liknande inte behandlas på ett sådant sätt att de kränker enskildas personliga integritet. Det innebär att myndigheten även ska hålla uppsikt över besökarens kommentarer för att upptäcka kränkande personuppgifter. Kränkande personuppgifter ska avlägnas. Myndigheten kan bli skadeståndsskyldig för kränkande personuppgifter.

För att minska risken för kränkningar av enskildas personliga integritet och för att minska risken för skadeståndsansvar bör myndigheten vidta åtgärder i förebyggande syfte. Dessa åtgärden kan bland annat vara att informera om syftet med Facebook-sidan, bloggen eller liknande samt för vilket ändamål kommentarsfunktionen är tänkt att användas, vilka typer av kommentarer som inte får förekomma och vad som kan hända om enskilda inte följer anvisningarna. Vidare kan besökare ombes att rapportera kränkande innehåll. Myndigheten bör ha rutiner för att hantera klagomål. Det är viktigt att utforma sidan så att det tydligt framgår att det är en myndighet som står bakom den.