

Kommunfullmäktige  
Kommunstyrelsen  
Kommunstyrelsens arbetsutskott

2001-10-23

6

Kf §  
Ks §  
Au § 207

Dnr 01/KK0298-005

**Förslag till gemensam policy för Siljanskommunerna avseende IT-säkerhet**

IKT-ansvarige har med skrivelse 2001-10-05 överlämnat förslag till gemensam policy för Siljanskommunerna avseende säkerhet i IT-användandet. Förslaget innebär en del smärre redaktionella justeringar jämfört med det säkerhetsdokument för enbart Orsa, som arbetsutskottet godkände 1999-12-15, § 216.

Arbetsutskottet beslutar

- att anta upprättat förslag till gemensam säkerhetspolicy för Siljanskommunerna avseende IT-användandet samt
- att uppdra till IKT-enheten att informera kommunens förvaltningar om policyn.

Justerandes sign



Utdragsbestyrkande



# **SÄKERHET MM AVSEENDE IT-ANVÄNDANDET**

## **I SILJANSKOMMUNERNA**

**Gemensam policy för Leksands, Rättviks, Mora, Orsa och Älvdalens kommuner**

## Inledning

IT-samordnarna i Siljanskommunerna har kommit överens om att ta fram ett för de fem kommunerna gemensamt dokument om säkerhet, offentlighet mm avseende IT-användningen. Dokumentet har bedömts vara nödvändigt med anledning av att kommunerna måste ha en god offentlighetsstruktur kombinerad med ett visst säkerhetstänkande.

Detta dokument fokuseras därför på dels vad Du som användare måste tänka på för att inte äventyra de system som Du har tillgång till, dels på hur Tryckfrihetsförordningens och Sekretesslagens regler påverkar oss som arbetar inom den offentlig förvaltningen.

## Generella regler för datoranvändningen

- Du är som användare själv ansvarig för din arbetsstation och allt som görs med användning av ditt användar-ID och lösenord.
- Det är inte tillåtet att försöka få tillgång till nätverksresurser du inte har behörighet till.
- Det är inte tillåtet att försöka ändra i andra mappar och dokument i servern än dina egna.
- Det är inte tillåtet att försöka göra intrång i andra användares konton, mappar och dokument.
- Vid användning av elektronisk post skall vanliga umgängesregler iakttas.
- Kommunens nätverk får inte användas för privat vinning eller andra privata syften.
- Du får inte utan samråd med IT-avdelningen installera programvara.
- Du förbinder dig som anställd att följa kommunens säkerhetsregler för IT-verksamheten.

## Etiska regler för datoranvändningen

- Kommunen tillhörigt lagringsmedium får inte användas för lagring av information i någon form, som innebär missaktning för folkgrupp eller annan sådan grupp av personer med anspelning på t ex ras, kön, hudfärg, nationellt eller etniskt ursprung, trosbekännelse eller pornografiska bilder.
- Anslutning till kommunens nät får inte användas för spridning av sådana bilder eller sådana texter som har angetts i punkten 1. Kommunens webbsidor och sidor som dessa är länkade till får inte innehålla information av sådant slag. Sådant information får inte heller plockas upp på datorskärm eller via kommunens nät överföras till annat medium, oavsett om så sker på egen eller kommunens dator eller datormedium. Den som av misstag får upp bild av angivet slag är skyldig att omedelbart koppla ned anknytningen i fråga.
- Pressetiska regler skall tillämpas i fråga om vad som får presenteras inom ramen för kommunens anslutning till nätet genom e-post, webbsidor eller på annat sätt. Anslutning till kommunens nätverk får inte användas på sådant sätt, att annan persons integritet kränks, även om det inte innebär en överträdelse av ovan angivna regler.
- Kommunens nät får inte utnyttjas för spridande av kommersiell reklam genom e-post till grupper av mottagare eller samtliga anslutna eller på annat sätt.
- Överträdelse av ovanstående förhållningsregler kan innebära att behörigheten till kommunens datasystem dras in för användaren i fråga.

### **Fel och onormala händelser**

Du är själv ansvarig för din dator och att reglerna efterföljs. Det innebär att du är skyldig att omedelbart rapportera fel och onormala händelser (t ex om någon försökt ta sig in på din dator på något sätt) till IT-ansvarig eller nätverkstekniker. Genom loggar kan det identifieras varifrån eventuella intrång skett.

### **Lösenord och användar-ID**

För att skydda dina data måste du alltid ansluta till nätverket med det användar-ID du tilldelats samt med det lösenord du själv angivet.

Du får absolut inte "låna ut" ditt användar-ID och lösenord mer än i undantagsfall. Har du gjort det måste du omedelbart därefter byta lösenord.

Du får inte heller ha de funktioner aktiverade som gör att din dator "kommer ihåg" ditt lösenord och loggar in dig automatiskt när du slår på datorn. Funktionen finns bl a i Internet Explorer och First Class.

Lösenordet skall bytas regelbundet. Du kommer automatiskt att få en påminnelse när tiden för ditt gamla lösenord gått ut. Det är tillåtet att använda samma lösenord även till t ex FirstClass konto.

Måste du skriva upp ditt lösenord får du inte förvara det i direkt anslutning till datorn.

### **Behörighet**

*Med behörighet avses en användares rättighet att utnyttja olika resurser i ett datorsystem på ett visst, reglerat sätt. För att uppnå detta krävs flera samverkande tekniska och administrativa åtgärder i syfte att överföra organisationens regler för vem som ska ha tillgång till information till en struktur som kan användas i en automatisk kontroll.*

Med behörighetskontroll avses administrativa och tekniska åtgärder för kontroll av användares identitet, styrning av användares behörighet att använda datasystemet och dess resurser samt för uppföljning av denna användning. Denna kontroll sker vanligen i ett behörighetskontrollsystem, som möjliggör identifiering av användaren och verifiering av identiteten, reglering av åtkomsträttigheter samt registrering av användarens aktiviteter i datasystemet (loggning).

För att få tillgång till ett datasystem krävs att användaren är registrerad som behörig användare i ett behörighetskontrollsystem. Endast behöriga, med de rättigheter som beslutats, ska finnas registrerade som användare i datasystemet.

För att behörighetskontrollen ska fungera måste varje användare ha en unik användaridentitet och ett lösenord som endast denne känner till och kan ändra.

Första gången en användare ges behörighet till ett datasystem är det lämpligt att använda ett initialt lösenord som endast medger en enda påloggning med möjlighet att byta till ett eget lösenord. Detta förfarande säkerställer att det endast är användaren som känner till sitt eget lösenord. Samma rutin kan med fördel tillämpas vid alla tillfällen då användaren behöver få ett förnyat lösenord, till exempel då användaren glömt sitt lösenord.

Användaren ska, vid behov, ges en behörighetsprofil som endast medger åtkomst till de resurser i datasystemet som krävs för att lösa dennes arbetsuppgifter. Detta kan till exempel innebära individuella begränsningar för användares rätt att läsa, skriva, ändra etc. För att systemägare inom myndigheter ska kunna ta ansvar för säkerhetsskyddet i datasystem som används av flera myndigheter, krävs att central systemägare säkerställer att datasystemet är så konstruerat att ovanstående kan tillgodoses.

### **Virussydd**

Datavirus är en självständig programdel eller sekvens av kommandon som har egenskaper och förmåga att kopiera sig själv till andra lagrade program eller kommandosekvenser. Utöver att kopiera sig kan viruset innehålla instruktioner för att utföra något i datorn. Effekterna av virus varierar från korta meddelanden på bildskärmen till total radering av lagrade program och data med synnerligen allvarliga konsekvenser som följd. Exempelvis kan på detta vis affärsmässigt vital information gå förlorad eller blockeras för användning. Virus överförs vanligen genom disketter eller filöverföring i nätverk (t.ex. hämta en fil via Internet) och numera också väldigt vanligt via e-post.

Tänk på vad du laddar ner! Filer med prefixet .exe skall ni vara helt säkra på vad det är innan ni plockar hem. Skicka inte heller vidare filer som du inte vet vad de innehåller.

Arbetsstationer som är anslutna till nätverket skall uppdateras regelbundet automatiskt med nytt virussydd. Fristående datorer skall förses med virussydd.

### **Offentlighet och sekretess**

Flödet av handlingar i en kommun är omfattande. Handlingar kommer i form brev från medborgare och myndigheter, internpost skickas mellan förvaltningar och handläggare, e-post skickas och tas emot till/från allmänheten, myndigheter, inom och mellan förvaltningar mm.

En viktig fråga är hur vi hanterar dessa meddelanden. Lagen ställer krav på hur handlingar skall hanteras. Det främsta skälet till dessa lagkrav är att kommunen skall upprätthålla en god offentlighetsstruktur. Majoriteten av de handlingar som vi hanterar är offentliga, vilket innebär att vem som helst har rätt att ta del av dem utan att förklara skälet för detta.

Vilka handlingar är då offentliga? Hur kan vi på bästa sätt korrekt hjälpa den som vill se en offentlig handling? Hur gör man om man inte vill lämna ut en handling? Vilka lagregler har vi att rätta oss efter? Vad är diarieföring och vad skall diarieföras? Det är några frågor som behandlas i de följande avsnitten

### **Offentlighetsprincipen**

Offentlighetsreglerna finns i Tryckfrihetsförordningen och Sekretesslagen. I korthet innebär den s k offentlighetsprincipen att allmänhet och massmedia skall ha insyn i myndigheternas verksamhet.

Alla, svenska såväl som utländska medborgare, har rätt att läsa de handlingar som finns hos myndigheterna. Som myndigheter räknas varje kommunal nämnd/styrelse och de kommunala bolagen och därmed under dem hörande förvaltningar/enheter/avdelningar.

Undantagna från offentlighetsprincipen är dels hemliga handlingar, dels utkast, minnesanteckning eller liknande som inte tas till vara när ärendet är slutbehandlat

Vidare ingår yttrandefrihet för tjänstemän m fl i offentlighetsprincipen. Denna definieras i regeringsformen som "frihet att i tal, skrift eller bild eller på annat sätt meddela upplysningar samt uttrycka tankar, åsikter och känslor".

En tredje hörnsten i offentlighetsprincipen är meddelarfriheten. Denna innebär en rätt för ex vis tjänstemän att till massmedia meddela uppgifter och underrättelser för offentliggörande.

Yttrandefriheten och meddelarfriheten kan begränsas av sekretesslagens regler.

### **Vad är en handling och vad är en allmän handling?**

Enligt Tryckfrihetsförordningen 2 kap 3 § förstås med handling "en framställning i skrift eller bild samt upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel". En handling behöver alltså inte vara en upprättad skrivelse utan kan även vara ett ADB-register, en e-postlista eller ett ljudband. Kort sagt är en handling ett föremål som innehåller information av något slag.

När blir då handlingen allmän? Handlingen blir allmän om den förvaras hos en myndighet och enligt särskilda regler anses inkommen dit eller upprättats där. Det är viktigt att alla anställda inom kommunen är medvetna om att en handling som de får eller upprättar är en allmän handling. Det är alltså inte endast ex vis skrivelser som inkommer eller upprättas i den centrala förvaltningen som är allmänna handlingar utan även handlingar som kommer direkt till en förskola, skola eller servicehus är allmänna handlingar.

Observera att s k cookiefiler och globalfiler är allmänna handlingar. Det innebär att vem som helst har rätt att kolla vilka websidor Du surfat in på. Tänk på detta och använd internet med förstånd!

Lagtips: Tryckfrihetsförordningen 2 kap, 3 §.

### **Inkommen handling**

En handling är inkommen till myndigheten när den har anlönt till myndigheten eller tagits om hand av behörig befattningshavare. Handlingen blir allmän omedelbart när den kommit in, den behöver alltså inte diarieföras för att bli en allmän handling. Handlingen anses även inkommen om den ex vis överlämnats till tjänsteman i hemmet eller på annat ställe utanför arbetsplatsen.

Lagtips: Tryckfrihetsförordningen 2 kap, §§ 4, 6 och 7.

### **Post och diarieföring**

Post är inte endast det traditionella brevet - som post räknas också ex vis e-post och fax. I kommunen skall i princip all post diarieföras om det inte är uppenbart att den är av ringa betydelse för myndighetens verksamhet. Exempel på post av ringa betydelse kan vara kursinbjudningar och reklam.

Man behöver inte diarieföra sådan post som kan hållas så ordnad att det utan svårighet kan fastställas om handling har inkommit eller upprättats. Sådan post kan t ex vara cirkulär som hålls ordnade i egna pärmar.

Det är mycket viktigt att allmänna handlingar diarieförs. Om handlingen inte diarieförs begränsas allmänhetens och massmedias möjligheter till insyn och det strider mot andan i såväl tryckfrihetsförordningen som sekretesslagen.

Av registreringen av ett ärende skall framgå

1. Datum, då handlingen inkom eller upprättades
2. Diarienummer
3. Från vem handlingen har inkommit eller till vem den har expedierats
4. Vad ärendet handlar om (ärenderubrik).

Lagtips: Sekretesslagen 15 kap §§ 1 och 2.

### **Postöppning**

Eftersom en handling skall registreras (diarieföras) utan dröjsmål kan inte post få ligga oöppnad i flera dagar, eller i värsta fall veckor, vilket kan hända i semestertider. Post måste ovillkorligen öppnas och diarieföras. Därför är det viktigt att alla förvaltningar ordnar rutiner som innebär att all post öppnas. Detta gäller även e-post som ju är likställd med "vanlig" post.

Samtidigt uppstår ett problem; post som är direktadresserad till en tjänsteman (dvs namnet står före kommunadressen) får enligt brottsbalken inte öppnas av annan (brytande av posthemlighet) om innehållet rör dennes personliga förhållanden. Eftersom vi inte vet om brevet är av privat natur eller ej förrän innehållet är känt löses detta lämpligen genom att registrator eller annan får en fullmakt att öppna postförsändelser och e-post. Ett exempel på hur en sådan fullmakt kan utformas finns som bilaga.

Om fullmakt ej lämnas måste personen i fråga själv öppna posten och se till att den blir diarieförd, vilket således skall ske även vid semestrar eller sjukdom. Att detta inte kommer att fungera är uppenbart varför fullmakt rekommenderas starkt.

### **Utlämnande av allmän handling**

Som vi nämnt ovan har vem som helst rätt att ta del av de allmänna handlingar som förvaras av myndigheten. Detta kan ske helt anonymt, vi har heller inte rätt att fråga varför någon vill få ut handlingen. Undantaget är förstås sekretessbelagda handlingar som inte får lämnas ut till vem som helst. I vilka fall sekretessbelagda får lämnas ut framgår av Sekretesslagen 14 kap.

En begäran om att få ta del av en allmän handling skall prövas skyndsamt. Utlämnandet kan få dröja om det av hänsyn till arbetets behöriga gång inte kan ske omedelbart, men huvudregeln är att det skall ske omedelbart på stället.

Den som i första hand avgör om handlingen är allmän och offentlig är den tjänsteman som har hand om handlingen. Om denne är osäker på om handlingen kan lämnas ut skall avgörande överlåtas till myndigheten, dvs nämnden eller styrelsen. För att inte behöva kalla in hela nämnden för att avgöra en sådan fråga är det lämpligt att nämnden delegerar beslutanderätten i dessa frågor till någon, ex vis ordföranden eller cheftjänsteman. Observera att delegation inte kan ges till förtroendevald och tjänsteman. Det strider mot kommunallagens regler om s k blandad delegation. Delegation ges till förtroendevald eller tjänsteman.

Om myndigheten vägrar att lämna ut en allmän handling, t ex med hänvisning till sekretess, skall den sökande upplysas om möjligheten att hos kammarrätten överklaga beslutet. Beslutet om att vägra utlämnande skall ske skriftligt.

Som nämnts skall vi snarast möjligt på stället tillhandahålla begärd handling. Detta innebär att den sökande utan avgift får skriva av handlingen, fotografera, spela in eller på annat sätt avbilda handlingen. Om handlingen inte finns på papper utan finns lagrad i en dator skall vi ställa den teknik som behövs till förfogande.

Om kopia önskas på handlingar har vi rätt att ta betalt för detta. Taxa för kopiering fastställs i samband med antagande av budget.

Lagtips: Tryckfrihetsförordningen 2 kap §§ 12 13, Sekretesslagen 15 kap §§ 4, 6 och 7

### **Hemlig handling**

Vi har gått igenom grundreglerna för utlämnande av allmänna handlingar och i viss mån att vissa allmänna handlingar kan vara sekretessbelagda. Inom kommunens verksamhet förekommer främst sekretessbelagda handlingar inom socialtjänsten och skolverksamheten.

En allmän handling som innehåller sekretessbelagda uppgifter får hemligstämplas. Det är dock i allmänhet inte nödvändigt att sätta på en stämpel för att en handling skall vara hemlig. Enligt lagtexten får ingen annan benämning än ordet hemlig användas. Uttryck som ”konfidentiell”, ”förtrolig” eller ”endast för tjänstebruk” är helt verkningslösa.

Om någon begär att få ut en hemlig handling så skall frågan om utlämnande av handlingen prövas på vanligt sätt som beskrivits ovan. Hemligstämplingen innebär alltså inte i sig att en fråga om utlämnande skall avslås blankt utan hemligstämplingen skall uppfattas som en varningssignal. Att en uppgift i handlingen är hemlig betyder inte att hela handlingen är hemlig. Om någon begär att få se en handling som delvis är hemlig är man skyldig att visa upp den del som är offentlig och på något sätt täcka över den del som är hemlig.

Lagtips: Sekretesslagen 14 kap.

### Tystnadsplikt

Under rubriken "Offenlighetsprincipen" nämndes yttrandefrihet och meddelarfrihet. Meddelarfriheten innebär inte att tjänstemän är skyldiga att lämna muntliga uppgifter till massmedia utan bara att de har möjlighet att göra det. I vissa fall tar dock tystnadsplikten över meddelarfriheten. Detta gäller bl a inom socialtjänsten och skolans elevvårdande verksamhet.

Lagtips: Sekretesslagen 7 kap

### Gallring

Under förutsättning att kommunfullmäktige antagit gallringsregler får rensning bland meddelandena i mappar och övrig e-post göras. Exempel på gallringsbara meddelanden lämnas nedan. Observera dock att om inte kommunfullmäktige antagit gallringsregler så kan gallring inte ske utifrån detta exempel.

- Ni får kasta handlingar och e-mail som inte påverkar något ärende.
- Dubbletter och kopior får ni kasta.
- Tillfälliga listor och register som ni använt i ert eget arbete får ni kasta om ni inte behöver dom, eller dom påverkar något ärende.
- Enkäter, rapporter, förfrågningar som inte rör något specifikt ärende får kastas.
- Reklam, inbjudningar får kastas.
- Handlingar som inte berör kommunens verksamhet får kastas. Även s k cookiefiler och e-mail.
- Alla loggar för e-post (personliga brevlådor etc.) och webbsidor får rensas från meddelanden och cookiefiler som inte behövs för att ta fram meddelanden med anknytning till ett ärende.
- Arbetskopior, idéskisser, ej färdiga skrivelser (sk arbetsmaterial) får kastas när dom inte längre behövs. ("Slutdokumentet" får däremot inte kastas)
- E-mail, webbsidor och annat som skrivits ut och diarieförts eller lagrats på annat sätt får kastas.
- Felaktiga och inaktuella handlingar, e-mail och webbsidor som rättats/uppdaterats får kastas.
- Ni får kasta e-mail, webbsidor etc. om ni också fått informationen på annat sätt och vice versa. Den kastade handlingen får inte innehålla någon information av vikt för ärendet som inte finns på den sparade versionen.
- Ni får radera telefonmeddelanden, röstbrevlådemeddelanden osv. om ni gjort tjänsteanteckningar på sånt som är av betydelse för ett ärende.
- Handlingar med skriv-, räkne- eller tankefel får kastas när nya rättade handlingar finns.
- Säkerhetskopior får ersättas av nya.

### Personregister och PUL (Personuppgiftslagen)

Personuppgiftslagen har ersatt den gamla datalagen. Grundprincipen är att du inte får ha register med personuppgifter på din dator eller på annat sätt, utan att anmäla det till personuppgiftsombudet. Du skall berätta vilka uppgifter som finns i registret och vad du skall ha det till. Vem som är personuppgiftsombud känner kommunens IT-samordnare till. Du måste tala om för den registrerade vad som står om denne, om han/hon frågar.

Namn och andra personuppgifter (tel nr. e-mailadress. foto osv.) får inte läggas ut på hemsida eller på annat sätt publiceras elektroniskt utan personens medgivande om det kan antas att den enskildes integritet kränks. Personuppgifter som rör en förtroendevald avseende hans eller hennes uppdrag kan alltid läggas ut.

## BILAGOR

## Bilaga 1

**Utdrag ur Sekretesslagen.**

”Bestämmelserna avser förbud att röja uppgift, vare sig det sker muntligen eller genom att allmän handling lämnas ut eller det sker på annat sätt (sekretess).”

## 1 KAP. INLEDANDE BESTÄMMELSER

”5 § Sekretess utgör inte hinder mot att uppgift lämnas ut, om det är nödvändigt för att den utlämnande myndigheten skall kunna fullgöra sin verksamhet.

6 § Förbud att röja eller utnyttja sekretessbelagd uppgift gäller för myndighet där uppgiften är sekretessbelagd samt för person som på grund av anställning eller uppdrag hos myndigheten, på grund av tjänsteplikt eller på annan liknande grund för det allmännas räkning deltar eller har deltagit i myndighetens verksamhet och därvid har fått kännedom om uppgiften.

7 § Sådana bestämmelser, som avser överföring av sekretess från en myndighet till en annan, tillämpas även när person som avses i 6 § lämnar uppgift till annan myndighet utan att han därvid företräder den myndighet till vilken han är knuten.”

14 kap. Bestämmelser om vissa begränsningar i sekretessen och om förbehåll :

”2 § Sekretess hindrar inte att uppgift i annat fall än som avses i 1 § lämnas till myndighet, om uppgiften behövs där för

- förundersökning, rättegång, ärende om disciplinansvar eller skiljande från anställning eller annat jämförbart rättsligt förfarande vid myndigheten mot någon rörande hans deltagande i verksamheten vid den myndighet där uppgiften förekommer,
- omprövning av beslut eller åtgärd av den myndighet där uppgiften förekommer, eller
- tillsyn över eller revision hos den myndighet där uppgiften förekommer.

Sekretess hindrar inte att uppgift lämnas i muntligt eller skriftligt yttrande av sakkunnig till domstol eller myndighet som bedriver förundersökning i brottmål.”

## 15 KAP. BESTÄMMELSER OM REGISTRERING OCH UTLÄMNANDE AV ALLMÄNNA HANDLINGAR M.M

”6 § Av 2 kap. 14 § andra stycket tryckfrihetsförordningen framgår att fråga om utlämnande av allmän handling till enskild prövas av den myndighet som förvarar handlingen, om det inte är föreskrivet att prövningen skall ankomma på annan myndighet.

Svarar viss befattningshavare vid myndighet enligt arbetsordning eller särskilt beslut för värden av handling, ankommer det på honom att i första hand pröva fråga om handlingens utlämnande till enskild. I tveksamma fall skall han hänskjuta frågan till myndigheten, om det kan ske utan omgång. Vägrar han att lämna ut handling eller lämnar han ut handling med förbehåll, som inskränker sökandens rätt att yppa dess innehåll eller annars förfoga över den, skall han, om sökanden begär det, hänskjuta frågan till myndigheten. Sökanden skall underrättas om att han kan begära detta och att beslut av myndigheten krävs för att ett avgörande skall kunna överklagas. Lag (1989:171).

7 § Beslut varigenom myndighet har avslagit enskilds begäran att få ta del av handling eller lämnat ut allmän handling med förbehåll, som inskränker sökandens rätt att yppa dess innehåll eller annars förfoga över den, får överklagas av sökanden. Om inte annat följer av andra-fjärde styckena, överklagas beslutet hos kammarrätten eller, såvitt gäller kammarrätts beslut i där väckt ärende, hos Regeringsrätten. Har beslutet meddelats av organ som avses i 1 kap. 8 § andra stycket eller 9 § tillämpas bestämmelserna i 23-25 §§ och 30 § första meningen förvaltningslagen (1986:223) om överklagande.”

”10 § Personuppgifter får bara behandlas bara om den registrerade har lämnat sitt samtycke till behandlingen eller om behandlingen är nödvändig för att

- a) ett avtal med den registrerade skall kunna fullgöras eller åtgärder som den registrerade begärt skall kunna vidtas innan ett avtal träffas.
- b) den personuppgiftsansvarige skall kunna fullgöra en rättslig skyldighet
- c) vitala intressen för den registrerade skall kunna skyddas
- d) en arbetsuppgift av allmänt intresse skall kunna utföras
- e) den personuppgiftsansvarige eller en tredje man till vilken personuppgifterna lämnas ut skall kunna utföra en arbetsuppgift i samband med myndighetsutövning, eller
- f) ett ändamål som rör ett berättigat intresse hos den personuppgiftsansvarige eller hos en sådan tredje man till vilken personuppgifterna lämnas ut skall kunna tillgodoses, om detta intresse väger tyngre än den registrerades intresse av skydd mot kränkning av den personliga integriteten.”

”22 § Uppgifter om personnummer får utan samtycke behandlas bara när det är klart motiverat med hänsyn till

- a) ändamålet med behandlingen.
- b) vikten av en säker identifiering, eller
- c) något annat beaktansvärt skäl.”

”Den information som skall lämnas självmant

25 § Information enligt 23 eller 24 § skall omfatta

- a) uppgift om den personuppgiftsansvariges identitet
- b) uppgiften om ändamålen med behandlingen, och
- c) all övrig information som behövs för att den registrerade skall kunna ta till vara sina rättigheter i samband med behandlingen, såsom information om mottagarna av uppgifterna, skyldighet att lämna uppgifter och rätten att ansöka om information och rättelse.

Information behöver dock inte lämnas om sådant som den registrerade redan känner till

Information skall lämnas efter ansökan.

26 § Den personuppgiftsansvarige är skyldig att till var och en som ansöker om det en gång per kalenderår gratis lämna besked om personuppgifter som röd den sökande behandlas eller ej. Behandlas sådana uppgifter skall skriftlig information lämnas också om

- a) vilka uppgifter om den sökande som behandlas,
- b) varifrån dessa uppgifter har inhämtats,
- c) ändamålen med behandlingen, och
- d) till vilka mottagare eller kategorier av mottagare som uppgifterna lämnas ut.”

## Personuppgiftslagen

## Bilaga 2

”1 § Syftet med denna lag är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter..

Avvikande bestämmelser i annan författning

2 § Om det i en annan lag eller i en förordning finns bestämmelser som avviker från denna lag, skall de bestämmelserna gälla.”

”3 § I denna lag används följande beteckningar med nedan angiven betydelse ---

Personuppgifter	All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet
Personuppgiftsansvarig	Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter
Personuppgiftsbiträde	Den som behandlar personuppgifter för den personuppgiftsansvariges räkning
Personuppgiftsombud	Den fysiska person som, efter förordnande av den personuppgiftsansvarige, självständigt skall se till att personuppgifter behandlas på ett korrekt och lagligt sätt”

”8 § Bestämmelser i denna lag tillämpas inte i den utsträckning att det skulle inskränka myndighets skyldighet enl 2 kap. tryckfrihetsförordningen att lämna ut personuppgifter.”

” 9 § Den personuppgiftsansvarige skall se till att

- a) Personuppgifter behandlas bara om det är lagligt,
- b) Personuppgifter alltid behandlas på ett korrekt sätt och i enlighet med god sed,
- c) Personuppgifter samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål.
- d) Personuppgifter inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in,
- e) De personuppgifter som behandlas är adekvata och relevanta i förhållande till ändamålen med behandlingen,
- f) Inte fler personuppgifter behandlas än som är nödvändigt med hänsyn till ändamålen med behandlingen,
- g) De personuppgifter som behandlas är riktiga och, om det är nödvändigt, aktuella
- h) Alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen och
- i) Personuppgifter inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen”

