



DATAOMBUDSMANNENS BYRÅ

GÖR UPP EN DATASKYDDSBESKRIVNING!

Uppdaterad 27.07.2010

www.tietosuoja.fi

Exempel på nättjänster och liknande funktioner där lagenligheten bör provas enligt personuppgiftslagen och där en dataskyddsbeskrivning bör införas:

- 1) Insamling av information över internet, t.ex.
 - Kundförfrågningar på internet
 - Arbetsplatsansökningar på nätet
 - Anmälningssblanketter på internet
 - Näthandel
 - Insamling av besökarrespons
- 2) Diskussionsforum som förutsätter registrering
- 3) Annan registrering i nättjänsten.

VILKEN INFORMATION SKALL DATASKYDDSBESKRIVNINGEN INNEHÅLLA?

Till en registrerads rättigheter hör enligt 24 § i personuppgiftslagen att kunna få information om den framtida behandlingen av uppgifterna som han eller hon lämnar. Enligt 24 § 1 mom. i personuppgiftslagen skall åtminstone följande uppgifter lämnas vid insamling av personuppgifter:

- uppgifter om den registeransvariga och vid behov om dennes företrädare
- ändamålet med behandlingen av personuppgifterna
- uppgifter om regelbunden utlämning av uppgifter
- de uppgifter som behövs för att utöva den registrerades rättigheter vid behandlingen av personuppgifter (bland annat rätten till insyn i 26 §, rätten till rättelse av en uppgift i 29 § och rätten att förbjuda insamling av uppgifter för direktmarknadsföring och liknande i 30 §).

Därutöver skall det organ som tillhandahåller nättjänsten, dvs. den registeransvariga, göra upp en registerbeskrivning över det personregister som uppstår och hålla beskrivningen allmänt tillgänglig (10 §). Enligt förarbetena till lagen skall också registerbeskrivningen läggas ut på internet, om själva registret finns på nätet (RP 96/1998, s. 43). Registerbeskrivningen eller den information som den skall innehålla skall således fogas till nättjänsten som en del av dataskyddsbeskrivningen. Informationen som skall ingå i registerbeskrivningen sammanfaller i stor utsträckning med innehållet i den ovan relaterade upplysningsplikten enligt 24 § i personuppgiftslagen, men den omfattar även ett viktigt tillägg då den kräver en beskrivning av principerna för skyddet av registret.

Dataombudsmannens byrå har gjort upp en anvisning och modellblankett för registerbeskrivningen. Den finns på byråns webbsidor (www.tietosuojafi.fi). En mer omfattande broschyr som beskriver innehållet i upplysningsplikten i 24 § och som kompletterar denna anvisning (Allmän upplysningsplikt enligt personuppgiftslagen) finns likaså på dataombudsmannens byrås webbsidor. Båda broschyrerna kan även beställas per post.

PLANERING OCH UTFORMNING AV DATASKYDDSBESKRIVNINGEN

Dataskyddsbeskrivningen är ett begrepp som utformats för att förena upplysningsplikten i 24 § i personuppgiftslagen och skyldigheten att hålla en registerbeskrivning allmänt tillgänglig i 10 §. Genom att sköta om beskrivningen säkras man att nättjänster som samlar in personuppgifter är lagenliga. *Dataskyddsbeskrivningen kan göras upp i helt fri form, om den bara innehåller den information som 10 och 24 § i personuppgiftslagen föreskriver.*

Utöver att man gör upp en dataskyddsbeskrivning skall man dock alltid vid behandling av personuppgifter även iakttä övriga stadganden i personuppgiftslagen.

Bestämmelser i personuppgiftslagen som också skall beaktas i samband med en nättjänst

- Planeringskravet, dvs. definieringen av ändamålet med behandlingen (6 §), och planeringen av övriga behandlingsfaser och säkerställning av lagenligheten (6 §, 5 §), bland annat:
 - definiering av de personuppgifter som samlas in och utvärdering av informationskällor och –innehåll (9 §)
 - klarläggning av rättigheterna och skyldigheterna för överlåtelse (8 § och specialbestämmelser i fråga), uppbevaring (34 §) samt förstöring (34 §, 32 §, 5 §) av uppgifter
 - planering och säkerställande av att de registrerades rättigheter förverkligas (26–30 §)
- Aktsamhetsplikten som gäller hela verksamheten (5 §)
- Beaktande av relevans- och felfrihetskravet i alla faser av behandlingen (9 §)
- Förpliktelsen att skydda uppgifterna (32 §)
- Tystnadsplikten (33 § eller specialbestämmelsen i fråga).

EXEMPEL

För att konkretisera saken tar vi i denna anvisning upp ett exempel på en dataskyddsbeskrivning för registreringsblanketter på webbsidor med hänsyn till de innehållsliga och planeringsmässiga aspekter som bör beaktas.

Utförandet av en elektronisk tjänst på internet behöver på förhand planeras och prövas ur personuppgiftslagens allmänna bestämmelsers synvinkel (se info lådan på föregående sida).

Till de tjänster på internet som förutsätter registrering hör t. ex. blanketter för deltagande i tävlingar på nätet, registrering av användare, registrering av arbetssökande eller nätformulär för medlemsansökningar – det finns ett otal möjliga tjänster som samlar in personuppgifter. I alla dessa fall där man begär personuppgifter måste man lämna den information som lagen föreskri-

ver i samband med tjänsten. Ifall det inte är nödvändigt att ge uppgifterna för att använda tjänsten, skall information lämnas även om detta.

En dataskyddsbeskrivning som placeras i anknytning till en nättjänst (till exempel genom en egen länk) kunde med iakttagande av de krav lagen uppställer till exempel innehålla följande (märk att informationsinnehållet i sista hand dock bestäms från fall till fall):

Exempel: personregister som uppstår genom registrering av prenumeranter för en tidning på nätet

Dataskyddsbeskrivning

- **Registeransvarig för registret** är företag X (*adress*). Kontaktperson är X (utförliga kontaktuppgifter) [och för det tekniska utförandet svarar X].
- De personuppgifter som samlas in används till att upprätthålla och sköta kundrelationerna till vår nättidnings abonnenter samt till att möjliggöra servicekontakter.
- Registret upptar följande uppgifter: ...
(du kan också använda registerbeskrivningen som stöd).
- Uppgifterna sparas för den tid som kundförhållandet varar (*uppbevaringstid och förstöring skall fastslås enligt 34 § i personuppgiftslagen*).
- Lämnade uppgifter skyddas på nätet med: ... (*nämn till exempel om den elektroniska förbindelsen är SSL-skyddad = Secure Sockets Layer*).
- Registret som de lämnade uppgifterna bildar skyddas ...
(Även här kan du hänvisa till registerbeskrivningen)
- De kontaktuppgifter ni lämnar kan överlåtas för följande direktmarknadsföring: ..., såvida ni inte har förbjudit överlåtelse.
Möjligheten till förbud skall antecknas på registreringsblanketten.
- Abonnenter har rätt att kontrollera den information som gäller dem själva, rätt att yrka på rättelse av en felaktig uppgift, rätt att förbjuda den registeransvariga att använda uppgifter som gäller dem själva för direktreklam eller liknande ändamål samt rätt att även i övrigt tillgripa de rättigheter som personuppgiftslagen ger dem. Begäran i saken riktas till XX.
- En **registerbeskrivning** enligt 10 § i personuppgiftslagen finns även till påseende på nätet =länk X/annanstans (*var*).

I samband med utformningen av feedbackblanketter måste de ansvariga fastslå om responsten tas emot *med eller utan personens (sändarens) identifikationsuppgifter*. Personuppgifter bör aldrig samlas in utan påkallat behov.

Den som ger feedback behöver informeras om önskat sätt för insändande (anonymt, med personuppgifter).

När feedback tas emot med personuppgifter, skall de registeransvariga på förhand planera och bedöma om responsten bildar ett register som faller inom ramen för personregisterlagens tillämpningsområde och vilket ändamålet med insamlingen och behandlingen av feedback är (2.2 §, 3 § 1 punkten och 6 §). Meddelanden som sänds in med en feedbackblankett (t.ex. via

e-post) och som innehåller personuppgifter kan bilda ett personregister, om uppgifterna sammanförs till ett enhetligt, manuellt personregister enligt 3.1 § 3 punkten i personuppgiftslagen eller om ett sådant uppstår då feedback behandlas genom automatisk databehandling.

Om feedbacken bildar ett personregister skall en dataskyddsbeskrivning göras upp. *Även i det fallet att feedback ges anonymt behöver man informera om till exempel i vilken utsträckning uppgifterna är skyddade för det fall att någon ändå vill sända in sina personuppgifter.*

Exempel: dataskyddsbeskrivning som ansluts till en blankett för feedback på internet

Dataskyddsbeskrivning

Dataskyddsbeskrivning

- Uppgifter som samlas in genom responssystemet för företag/myndighet XX är endast avsedda för insamling av responsen för ändamålet X (vid behov att göra det möjligt att ta kontakt för ändamål X).
- Man kan även ge feedback anonymt och det är därför inte nödvändigt att uppge namn och kontaktuppgifter.
- Om man ändå vill uppge namn och kontaktuppgifter, bildar de lämnade uppgifterna ett personregister med namnet X.
- Registeransvarig för registret är företag/samfund X (*till exempel kommunstyrelsen i X kommun, adress X*). Kontaktperson är X (*utförliga kontaktuppgifter*).
- Registret består av uppgifter i feedback som sänts in på elektronisk väg/andra specificerade uppgifter/vad? (Du kan använda registerbeskrivningen som stöd).
- Responsen sparas tills ärendet är slutbehandlat (*uppbevaringstiden skall fastslås enligt 34 § i personuppgiftslagen*).
- Då information lämnas genom feedback skyddas uppgifterna på nätet/vid överföringen på följande sätt: ... (*nämn t. ex. om den elektroniska förbindelsen är SSL-skyddad = Secure Sockets Layer*).
- Uppgifterna i responsen överläts inte till någon annan part.
- Den som gett feedback har rätt att få kontrollera de uppgifter han eller hon lämnat om sig själv och rätt att yrka på rättelse av felaktig information. Begäran i saken riktas till XX.
- En **registerbeskrivning** enligt 10 § i personuppgiftslagen finns även till påseende på nätet (länk X)/annanstans (*var*).

När det gäller **nättjänster som tillhandahålls av myndigheter** är det bra att nämna om den information som lämnas till myndigheten i responsen eller på annat sätt är offentlig. Offentligheten fastslås enligt lagen om offentlighet i myndigheternas verksamhet (621/1999) eller enligt en eventuell speciallag.

Det är bra att informera dem som lämnar uppgifter om att de inte har anledning att lämna känsliga uppgifter i nättjänsten (ifall inget skydd för uppgifterna har ordnats). Annan information som

är nödvändig för användarna av en nättjänst skall ges från fall till fall, efter verksamhetens behov och med beaktande av de allmänna bestämmelserna i personuppgiftslagen.

Om det i ett fall med en internetjänst är fråga om till exempel affärsverksamhet på nätet, såsom näthandel med konsumenter som målgrupp, skall de ansvariga inte bara beakta bestämmelserna i personuppgiftslagen, utan även de *åligganden som andra lager påför verksamheten*. Till dessa hör, i samband med den nämnda **näthandeln**, särskilt lagen om tillhandahållande av informationssamhällets tjänster (458/2002), vilken Kommunikationsverket övervakar och ger anvisningar för, samt 6 kapitlet i konsumentskyddslagen (1072/2000), som faller inom Konsumentverkets och Konsumentombudsmannens verksamhetsområde. Konsumentverket har utarbetat en broschyr i ämnet, vilken kan läsas på verkets webbsidor.

Det är viktigt att lägga märke till att *man skall göra upp separata registerbeskrivningar om man samlar in uppgifterna för olika ändamål*. Uppgifterna i varje *registerbeskrivning* kan på det ovan beskrivna sättet inkluderas i en vederbörlig dataskyddsbeskrivning. Ur tjänsteanvändarnas synpunkt och för att lagens skyldigheter skall uppfyllas är det väsentligt att informationen ges i förståelig form och på ett sätt som är ändamålsenligt för alla som använder tjänsten. Dataskyddsbeskrivningen bör således – t.ex. genom en länk – ges som en fast anknytning till tjänsten.

INFORMATION OM KAKOR

Enligt 7 § i lagen om dataskydd vid elektronisk kommunikation (516/2004), som trädde i kraft den 1 september 2004, skall man i anslutning till en nättjänst även lämna information om eventuell användning av kakor (cookies).

Detta kan lätt genomföras genom att foga ett särskilt avsnitt om användningen av kakor till dataskyddsbeskrivningen. Lagen innehåller dock också ett undantag från upplysningsplikten: i det fall att det enda syftet med kakorna är att tekniskt underlätta användningen av tjänsten eller användaren uttryckligen har begärt en tjänst som bygger på användning av kakor behöver man inte informera om kakorna.

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. Kakor är nödvändiga för att t.ex. nätbanker och näthandel skall fungera.

Exempel: information om kakor som uppfyller lagens villkor

"På våra webbsidor använder vi oss av så kallade kakor, dvs. cookies. En kaka är en liten textfil som sänds till en användares dator och sparas där för att den som underhåller webbsidorna skall kunna känna igen dem som ofta besöker sidorna, underlätta inloggning för besökarna och sammanställa information om besökarna. Med hjälp av den här informationen kan vi kontinuerligt förbättra innehållet på våra sidor. Kakor skadar inte en användares dator eller filer. Vi använder dem för att kunna erbjuda våra kunder information och tjänster som motsvarar varje kunds individuella behov.

Ifall den som besöker våra webbsidor inte vill att vi får den ovan nämnda informationen med hjälp av kakor kan han eller hon i de flesta webbläsare koppla från kakfunktionen. Detta går till exempel i webbläsaren Internet Explorer till så, att man går till menyn "Verktyg", väljer "Inter-

net-alternativ” och fliken ”Säkerhet”.

Det är dock bra att lägga märke till att kakor kan behövas för att vissa av våra webbsidor och nättjänster skall fungera på vederbörligt sätt”.

Vem har ansvaret för att en dataskyddsbeskrivning görs upp?

Med *registeransvarig* avses enligt definitionen i personuppgiftslagen ”en eller flera personer, sammanslutningar, inrättningar eller stiftelser för vilkas bruk ett personregister inrättas och vilka har rätt att förfoga över registret eller vilka enligt lag ålagts skyldighet att föra register” (3 § 4 punkten). Den som tillhandahåller en nättjänst eller för vilkens räkning personuppgifter samlas in har i egenskap av registeransvarig ansvaret för att en dataskyddsbeskrivning görs upp, dvs. att upplysningsplikten samt skyldigheten att göra upp en registerbeskrivning och hålla den allmänt tillgänglig iakttas. Denna part skall se till att lagens förpliktelser följs och ge anvisningar för det tekniska genomförandet.

Underlåtelse att iaktta förpliktelsen är enligt 48.2 § 1 punkten i personuppgiftslagen en straffbar handling. Dataombudsmannen övervakar att personuppgiftslagen följs och kan vid behov anmäla ett ärende för åtal.

Informeringen om kakor övervakas av Kommunikationsverket enligt 31 § i lagen om dataskydd vid elektronisk kommunikation. *Försummelse att informera om kakor är straffbar enligt 42.2 § 2 punkten i lagen om dataskydd vid elektronisk kommunikation.*

Vid planering och tillhandahållande av nättjänster är det värt att notera att välskött datasekretess ökar öppenheten och förtroendet samt förbättrar användarvänligheten i tjänsterna. Att framföra de uppgifter som lagen föreskriver i samband med tillhandahållandet av tjänsten garanterar att webbsidorna i fråga får en så säker användning som möjligt och främjar därmed de egentliga, funktionella målsättningarna. Att skydda registrerades integritet och deras intressen och rättigheter bör inte ses som en separat förpliktelse, utan den utgör en väsentlig del av god datahanteringssed och kundbetjäning.

Personuppgiftslagen och övriga lagar och paragrafer som nämns i denna broschyr finns i sin helhet i Statens författningsdatabas på adressen www.finlex.fi. Allmän information om dataskydd och personuppgiftslagen finns på webbsidorna för datombudsmannens byrå på adressen www.tietosuoja.fi. Information om lagen om dataskydd vid elektronisk kommunikation och om kakor finns på Kommunikationsverkets webbsidor på adressen www.ficora.fi. Konsumentverket har producerat en broschyr om näthandel, ”Kauppapaikka Internetissä – Verkkokauppiain ohje”, som kan läsas på Konsumentverkets webbsidor på adressen www.kuluttajavirasto.fi.