24.11.2004

KOMMUNIKATIONSVERKETS REKOMMENDATION OM REGISTRERING AV UPPGIFTER OM BEHANDLINGEN AV IDENTIFIERINGSUPPGIFTER

Utgivare
Kommunikationsverket

PRESENTATIONSBLAD
Utgivningsdatum
24.11.2004

Författare Kommunikationsverket	Typ av publikation Rekommendation
	Uppdragsgivare Kommunikationsverket

Publikation
Kommunikationsverkets rekommendation om registrering av uppgifter om behandlingen av identifieringsuppgifter

Referat

Denna rekommendation innehåller principer om hur den förpliktelse som avses i 15 § i lagen om dataskydd vid elektronisk kommunikation (516/2004) och som gäller registrering av uppgifter om behandlingen av identifieringsuppgifter bör genomföras hos teleföretag.

Rekommendationen har utarbetats i en grupp kallad logguppgift som bildades av Kommunikationsverkets TELCOSEC-arbetsgrupp.

Nyckelord

Seriens namn
Kommunikationsverkets publikationer

Sidoantal	Språk	Pris	Sekretessgrad
6	Svenska	3,50 €	Offentlig

Distribution Kommunikationsverket	Förlag Kommunikationsverket

Postadress
PB 313
00181 HELSINGFORS
FO-nummer
0709019-2

Besöksadress
Östersjögatan 3 A
00180 HELSINGFORS

Telefon
(09) 69 661
Telefax
(09) 6966 410

E-post
info@ficora.fi
Webbplats
http://www.ficora.fi

Innehåll

1 INLEDNING

I 15 § i lagen om dataskydd vid elektronisk kommunikation (516/2004) sägs följande:

"Ett teleföretag skall registrera detaljerade uppgifter om hur behandlingen av identifieringsuppgifter skett. Av uppgifterna skall framgå tidpunkten för behandlingen, dess varaktighet samt vem som utfört behandlingen. Händelseuppgifterna skall förvaras två år från lagringen.

Kommunikationsverket kan meddela närmare föreskrifter om hur den i 1 mom. avsedda registreringen och förvaringen tekniskt skall genomföras."

I detaljmotiveringen för 15 § i regeringens proposition för lagen om dataskydd vid elektronisk kommunikation (RP 125/2003) konstateras bl.a. följande:

"[Registreringsförpliktelsen]... gäller bara sådana identifieringsuppgifter som omedelbart kan ha avgörande betydelse för att skydda konfidentiella meddelanden och integritet." [...] Registreringsförpliktelsen enligt det föreslagna 1 mom. är av behovet påkallad speciellt för att utreda eventuellt missbruk i sådana fall då personer i ett teleföretags tjänst misstänks ha behandlat identifieringsuppgifter, som ansluter sig till konfidentiell kommunikation mellan abonnenter eller användare, för annat ändamål än sådant som är acceptabelt enligt denna lag. Å andra sidan kan man med de lagrade behandlingsuppgifterna bevisa att ingen har gjort sig skyldig till misstänkt missbruk, vilket har en positiv inverkan på rättskyddet för dem som behandlar uppgifter. Man kan anse att den föreslagna bestämmelsen har stor betydelse i fråga om det allmänna förtroendet för elektroniska kommunikationstjänster."

I lagens 44 § (ikraftträdande- och övergångsbestämmelser) bestäms följande om registreringsförpliktelsen:

"Teleföretagen skall inleda i 15 § avsedd registrering av uppgifter inom sex månader från denna lags ikraftträdande."

Med anledning av ovan anförda frågor om registreringsförpliktelsen har Kommunikationsverket beslutat att utfärda detta memorandum om hur registrering och förvaring av uppgifter om behandlingen av identifieringsuppgifter skall genomföras. Under utarbetandet har teleföretagens representanter inom Telcosec-arbetsgruppen hörts.

2 UTMANINGAR SOM HÄNFÖR SIG TILL REGISTRERING AV UPPGIFTER SOM GÄLLER BEHANDLINGEN AV IDENTIFIERINGSUPPGIFTER

2.1 System som inte stöder registrering av uppgifter om behandlingen av identifieringsuppgifter och system som inte längre har tillverkarens produktstöd

Flera av teleföretagens system stöder inte registrering av uppgifter som gäller behandlingen av identifieringsuppgifter. För många system är det inte möjligt att uppbygga en sådan funktionalitet för skäliga kostnader även om tillverkaren hade nominellt produktstöd – till exempel telefoncentraler. Dessutom är många system sådana för vilka tillverkarens produktstöd har upphört och därför är nya egenskaper inte längre tillgängliga. Uppdatering av alla dessa system i nya system inom den i lagen utsatta övergångsperioden är i praktiken inte möjligt. Teleföretagen använder också en hel del sådana aktiva utrustningar (routrar, centraler, brytare osv.) som inte är avsedda för registrering av uppgifter om behandlingen av identifieringsuppgifterna, och för vilka den avsedda funktionaliteten inte står till buds. I teleföretagen kan man också överföra identifieringsuppgifter för fortsatt behandling till ett sådant off-linesystem eller distanssystem som inte stöder registrering av uppgifter om behandlingen av identifieringsuppgifterna. Sådana system är till exempel tillämpningsprogram som körs lokalt på PC och behandlar identifieringsuppgifter. Det är också möjligt att identifieringsuppgifter skrivs ut på papper för fortsatt behandling, varvid det är omöjligt att med tekniska medel registrera uppgifter om hur behandlingen av identifieringsuppgifterna har skett.

2.2 Spridda system / spridda logguppgifter / logguppgifter i realtid

På grund av telenätens komplicerade struktur registreras uppgifter om behandlingen av identifieringsuppgifter i flera spridda system i samband med behandlingsåtgärderna. För behandlingen av enskilda identifieringsuppgifter lagras då inte några händelseuppgifter i realtid utan vederbörande uppgift kan bildas senare genom att kombinera logguppgifter från flera olika system. Det är dock inte alltid möjligt att kombinera logguppgifter i efterhand.

Ibland överförs identifieringsuppgifter längs en kedja av system: från ett originalsystem, där identifieringsuppgifterna skapas, via ett förmedlingssystem till ett insamlingssystem, där den faktiska behandlingen av identifieringsuppgifterna sker. Typiskt för system som finns i början av kedjan är att de inte är avsedda för behandlingen av identifieringsuppgifter utan enbart för förmedling av uppgifterna vidare till insamlingssystemet. Det kan också förekomma situationer då identifieringsuppgifterna har fördelat sig mellan flera system så att uppgifterna i ett enskilt system inte bildar sådana identifieringsuppgifter som lagen avser. I sådana fall är tillämpningen av registreringsförpliktelsen problematiskt.

2.3 Registrering av uppgift om behandlingens varaktighet

Registrering av uppgift som beskriver behandlingens varaktighet blir en utmaning till exempel i de fall då en kundrådgivare eller faktureringsexpert behandlar identifieringsuppgifterna på skärm eller papper. När uppgifterna behandlas på skärmen är det möjligt att de står där mycket längre än den tid som den faktiska behandlingen kräver. Det kan också hända att identifieringsuppgifter överförs för fortsatt behandling till ett sådant off-linesystem (t.ex. till bärbar dator) där registrering av behandlingstiden inte är möjligt med tekniska medel.

2.4 Att logga in som administratör och användning av konsol

För upprätthållande av system skall systemen ha aktiverade identifikationer och lösenord för administratör och de skall också vara i bruk. Administratörens inloggning är inte alltid personlig och därför är det möjligt att åtgärder som utförts som administratör inte alltid med tekniska medel kan förknippas med en viss person (den som behandlar identifieringsuppgifter). Administratören kan vanligen också i efterhand modifiera eller manipulera uppgifter som beskriver behandlingen av identifieringsuppgifterna i det lokala systemet. Därför är det också möjligt för administratören att täcka spåren av sådan behandling som kanske strider mot lagen. Konsolförbindelser behövs till exempel när systemet blir trasigt eller när det är nödvändigt att göra ändringar i specifikationer som direkt gäller aktiva utrustningar. Vid användning av konsolförbindelser sker åtgärden typiskt genom administratörens inloggning direkt bredvid utrustningen, och det är inte möjligt att registrera uppgifter om behandlingen av identifieringsuppgifterna.

3 LÖSNINGS- OCH TILLÄMPNINGSANVISNINGAR

Ett teleföretag skall kartlägga processer för hanteringen av identifieringsuppgifterna i sina system och tjänster samt skapa tillräckligt detaljerade anvisningar för personalen om behandlingen av identifieringsuppgifterna för olika ändamål.

Teleföretaget skall definiera de hanteringsprocesser och system vilka innehåller uppgifter som omedelbart kan ha avgörande betydelse för konfidentialiteten av kommunikationen samt genomföra registrering av uppgifter om behandlingen av identifieringsuppgifterna (logguppgifter) i fråga om dessa. Sådana är bl.a. system i vilka identifieringsuppgifterna förvaras annat än kortvarigt, i vilka identifieringsuppgifterna behandlas av fysiska personer och i vilka händelserna i behandlingen kan riktas mot vissa kommunikationshändelser för en viss kommunikationspart. Exempel på sådana system är biljettlager, faktureringssystem samt olika system som används för analysering av kommunikationshändelsers historia. Registreringsförpliktelsen gäller inte behandling av anonymt och/eller summerat datamaterial. Av logguppgifterna skall framgå vilka identifieringsuppgifter som behandlingen gäller, tidpunkten för behandlingen, behandlingens varaktighet och vem som utfört behandlingen.

Teleföretaget skall kontrollera det lokala underhållet av nätets låg-nivå komponenter samt hanteringen av administratörens inloggning med tanke på personalens tillämplighet. Teleföretaget skall dessutom se till att de lokala systemens fysiska säkerhet kontrolleras på ändamålsenliga sätt. För distansunderhåll och distanskontroll måste teleföretaget ha processer där utrustningars operationskontroller definieras. I processerna bör man ta hänsyn till bl.a. tillförlitlig identifiering av dem som behandlar identifieringsuppgifterna. Dessutom skall teleföretaget, om möjligt, registrera de kommandon som utförs via distansförbindelser med administratörsrättigheter.

Logguppgifterna skall registreras på ett säkert sätt och det skall finnas relevanta säkerhetskopior på uppgifterna. Teleföretaget skall registrera logguppgifterna i olika system så att olika användningsfall kan kombineras vid behov. Uppgifterna skall vara tillgängliga inom skälig tid. För system där behandlingens varaktighet inte kan definieras måste teleföretaget försöka arrangera registreringen på ett sådant sätt att en uppskattad behandlingstid kan antas på grund av händelsernas tidstämplar.

Kommunikationsverket har utfärdat en föreskrift som gäller teleföretagens allmänna informationssäkerhetsförpliktelser, nämligen föreskrift 47 B/2004 M om informationssäkerhet hos teleföretag. Föreskriften innehåller bestämmelser om teleföretagens skyldigheter bl.a. i fråga om administrativ säkerhet, användarsäkerhet och datasäkerhet. Om kontroll av fysisk säkerhet bestäms i Kommunikationsverkets föreskrift 48 A/2004 M som gäller fysiskt skydd av kommunikationsnät.