



DATAOMBUDSMANNENS BYRÅ

**EN SAMMANSLUTNINGSSABONNENTS RÄTT ATT
BEHANDLA IDENTIFIERINGSUPPGIFTER I FALL
AV MISSBRUK**

Publiserad 4.06.2009

www.tietosuoja.fi

INNEHÅLL:

1. Inledning.....	1
2. Allmänt om identifieringsuppgifter.....	3
3. Sammanslutningsabonnenten som behandlare av identifieringsuppgifter.....	4
4. Identifieringsuppgifter som del av upptäckande och utredning av missbruk.....	5
4.1 Missbrukens betydelse.....	5
4.2 Ett sista medel.....	7
4.3 Särskilda begränsningar i behandlingsrätten.....	8
5. Åtgärder före behandling.....	10
5.1 Omsorgsplikten.....	10
5.2 Planerings- och samarbetsplikt.....	12
5.3 Förhandsanmälan till dataombudsmannen.....	13
6. Förfaringssätten och förutsättningarna för automatisk sökning och manuell behandling.....	15
6.1 Automatisk sökning.....	15
6.2 Manuell behandling.....	15
6.3 Särskilda förutsättningar för manuell behandling.....	16
6.4 Redogörelse för manuell behandling.....	18
7. Åtgärder efter behandlingen.....	20
7.1 Årlig utredning till arbetstagarnas representant.....	20
7.2 Årsanmälan till dataombudsmannen.....	20

1. Inledning

Förändringen (125/2009) i lagen om dataskydd vid elektronisk kommunikation (516/2004, hädanefter LDEK), som trädde i kraft 1.6.2009, specificerar en sammanslutningsabonnents rätt att behandla identifieringsuppgifter i fall av missbruk. Sammanslutningsabonnenter kan, enligt förutsättningar som regleras i lagens 13 a – 13 k §, behandla identifieringsuppgifter, då det är frågan om förebyggande och utredning av olovligt brukande av avgiftsbelagda informationssamhällstjänster, kommunikationsnät eller kommunikationstjänster eller röjande av företagshemligheter. Dessa bestämmelser efterlevnad övervakas av dataombudsmannen.

Sammanslutningsabonnenter är alla de företag och sammanslutningar, som behandlar användarnas konfidentiella uppgifter, identifieringsuppgifter i sitt kommunikationsnät. En sammanslutningsabonnent kan till exempel vara en näringsidkare, ett andelslag, ett aktiebolag, en förening, ett universitet eller ett statligt ämbetsverk. Även bostadsaktiebolags sammanslutningsarrangemang kan vara sammanslutningsabonnenter.

Identifieringsuppgifter är alla de uppgifter som kan förknippas med en abonnent eller användare och som behandlas i kommunikationsnäten för att överföra, distribuera eller tillhandahålla meddelanden. Till identifieringsuppgifter kan höra uppgifter som hänvisar till bland annat kommunikationens routning, varaktighet, tidpunkt eller mängden av de uppgifter som skall överföras, de använda protokollen, egenskaper eller läge hos avsändarens eller mottagarens terminal, nätet för avsändaren och mottagaren samt förbindelsens början, slut och varaktighet. Identifieringsuppgifter kan även gälla formen, i vilken uppgiften sänds över nätet. Det väsentliga är, att det bör vara möjligt att förknippa dessa uppgifter till abonnenten (det kan vara en naturlig eller juridisk person) eller till användaren, som har egenskapen av en naturlig person.

Identifieringsuppgifter som kan förknippas med en naturlig person är samtidigt personuppgifter. På dessa tillämpas i utfyllande mening även bestämmelser som reglerar behandlingen av personuppgifter. Sammanslutningsabonnenten är, till den del som denna har behandlat identifieringsuppgifter, skyldig att beakta de skyldigheter som upprätthållandet av ett register medför.

Med *behandling* avses, enligt lagen om dataskydd vid elektronisk kommunikation 2 § 14 mom, insamling, registrering, organisering, användning, översändande, utlämnande, lagring, ändring, samkörning, blockering, utplåning, förstöring och andra motsvarande åtgärder.

Avsikten med denna guide är att ge en allmän översikt över sammanslutningsabonnentens rätt att behandla identifieringsuppgifter i syfte att förebygga och utreda missbruk. Guidens innehåll består förutom av lagen om dataskydd vid elektronisk kommunikation, även av dess förarbeten (regeringens propositioner och utskottens betänkanden), dataombudsmannens och kommunikationsverkets ställningstaganden samt av i rättspraxis och i rättsvetenskaplig litteratur framfört material.

Guiden innehåller anvisningar riktade till organisationers ledningar samt till dem som är ansvariga för drift och datasäkerhet, då organisationen har ställning som sammanslutningsabonnent. Guidens användare förväntas känna till grundbegreppen och förfaringssätten för datasäkerhet, riskhantering och god informationshantering. I guiden

används definitioner för datasäkerhetsbegrepp, som statsförvaltningens ledningsgrupp för datasäkerhet, VAHTI¹, har fastställt.

I denna guide behandlas inte de lagstadgade rättigheterna att behandla identifieringsuppgifter, som de övriga grupperna (teleföretag eller producenter av mervärdestjänster) som deltar i förmedling av meddelandet, har. Guiden avser inte heller styra en sammanslutningsabonnent i användningen av övriga behandlingsrättigheter, som framgår ur lagen om dataskydd vid elektronisk kommunikation.² Dessa bestämmelsers efterlevnad övervakas av Kommunikationsverket.

En sammanslutningsabonnent bör känna igen och planera de situationer då identifieringsuppgifter behandlas i dess verksamhet. En enskild behandlare skall, före påbörjandet av behandlingen av identifieringsuppgifterna, kunna definiera syftet med behandlingen för att kunna veta i vilken mån uppgifterna får behandlas. Sammanslutningsabonnenten styrs till planmässighet förutom av den allmänna omsorgsplikten (LDEK 8.3 §) även av, för behandling av identifieringsuppgifter i fall av missbruk, stadgade särskilda skyldigheter som verkar i förhand.³

Till exempel gäller sammanslutningsabonnentens rätt att behandla identifieringsuppgifter, för att sörja för dataskyddet vid elektronisk kommunikation, endast sammanslutningsabonnentens *egna* kommunikationsnäts, kommunikationstjänsters eller av sammanslutningsabonnenten behandlade identifieringsuppgifters dataskydd eller situationer då användarnas kommunikationsmöjligheter *direkt* hotas. Därutöver har behandlingsrätten begränsats till endast sådana identifieringsuppgifter, som behövs för utförandet och beredningen av de i lagens 20 § stadgade nödvändiga åtgärder för sörjandet av dataskyddet.⁴

För att förebygga eller utreda gärningar eller händelser, som *indirekt* hotar den elektroniska kommunikationens dataskydd eller kommunikationsmöjligheter, kan nödvändig behandling av identifieringsuppgifter dock komma på frågan även vid förebyggande och utredning av i lagen om dataskydd vid elektronisk kommunikation 13 a – 13 k § avsedda situationer för missbruk. Om förutsättningarna för behandlingen av identifieringsuppgifter, vilken utförs för förebyggandet och utredningen av missbruk som för övrigt hotar dataskyddet, bör man handha enligt de sätt som presenteras nedan.

¹ VAHTI- publiceringar hittas på internetadressen www.vm.fi/vahti

² En sammanslutningsabonnent får, förutom i denna guide nämnda förebyggande och utredning av missbruk, dessutom/även behandla identifieringsuppgifter i överensstämmelse med de i lagen om dataskydd vid elektronisk kommunikation stadgade syftena: för att utföra och använda tjänster samt sörja för dataskyddet för dessa tjänster enligt 19-20 § (9 §), för fakturering (10 §), för teknisk utveckling av kommunikationsnäten och tjänsterna (12 §), för statistisk analys (12a §) samt för upptäckande av tekniska fel eller brister (14 §).

³ I praktiken kan man dock först vid behandlingen av identifieringsuppgifterna utreda om det är frågan om till exempel funktionsstörningar i systemet, störningar som orsakar skada till dataskyddet, om någon har använt sammanslutningsabonnentens kommunikationsnät eller tjänster fel eller om apparaten har gått sönder. Om behandlingens syfte då ändras, bör behandlaren överväga på nytt förutsättningarna för det förändrade syftet och den tillåtna omfattningen av behandlingen.

⁴ Enligt regeringspropositionen (RP 48/2008 s. 17; 9 § detaljerade motiveringar) har man uttömmande reglerat i lagens 20 § de situationer då identifieringsuppgifter kan behandlas för sörjandet för dataskyddet samt om de åtgärder som kan göras i dessa situationer. Kommunikationsverket har gett anvisningar åt teleföretag och producenter av internetkontaktjänster, om tolkningen av den tidigare lagen (10.1.2007 och 4.10.2007 daterade anvisningar nr 5/6020/2007) och likaså av de 1.6.2009 ikraftträdande bestämmelserna (Kommunikationsverkets utlåtande 20.3.2009 nr 387/64/2009) angående identifieringsuppgifternas behandling vid sörjandet för dataskyddet.

2. Allmänt om identifieringsuppgifternas behandling

Grundlagens 10 § stadgar om skydd för privatlivet. Till detta räknas skyddet för personuppgifter och skyddet för förtroliga meddelanden. Med rätt till privatliv och skydd för förtroliga meddelanden för en användare av kommunikationstjänster avses att ingen får behandla hans meddelanden eller identifieringsuppgifter, som har samband med hans kommunikation, utan hans tillstånd eller bestämmelse i lag.⁵ Inte ens den, som med avseende på kommunikationens parter fungerar som utomstående förmedlare av meddelanden och som erbjuder tjänsten, har rätt att utan samtycke av parterna eller i lag stadgad grund behandla konfidentiella uppgifter eller identifieringsuppgifter.

Kommunikationens parter kan behandla sina egna meddelanden samt till dem anknutna identifieringsuppgifter enligt egen vilja, om inte annat har stadgats i lag. Den omfattande rätt, som kommunikationens parter har, att behandla egna meddelanden samt till dem anknutna identifieringsuppgifter, begränsas bland annat av bestämmelserna om sekretess och om personuppgifters behandling samt av upphovsrättslagen och bestämmelserna om ärekränkning.

Förutom konfidentiell kommunikation finns även kommunikation som är avsedd för allmän mottagning, till exempel meddelanden på allmänna diskussionsforum på internet. Identifieringsuppgifterna för meddelanden som har avsetts för allmän mottagning är konfidentiella på så sätt att grupperna som deltar i förmedlingen av kommunikationen får behandla dessa uppgifter endast enligt syften som har stadgats om i lag eller med samtycke av kommunikationens parter.⁶

Elektronisk kommunikation mellan avsändaren och mottagaren förutsätter vanligtvis att meddelandena förmedlas via kommunikationsnät, som faller under teleföretagens och sammanslutningsabonnenternas administration. Dessa tjänsters erbjudare måste behandla meddelandenas identifieringsuppgifter för att förmedla meddelandena och samtidigt samlas det spår av förmedlade meddelanden i deras kommunikationssystem.

I lagen om elektronisk kommunikation har det stadgats om skyldigheterna för förmedlarna av elektroniska meddelanden, med vilka man tryggar förtroligheten i kommunikationen och kommunikationsnätets användares privatliv. I 9-14 § i lagen om elektronisk kommunikation stadgas om de situationer då förmedlaren av meddelanden har rätt att behandla identifieringsuppgifter som lagras då meddelandena förmedlas till näten.

Syftet med regleringen är att trygga förverkligandet av rättigheterna för användarna av elektronisk kommunikation, på ett sätt som samtidigt garanterar meddelandets förmedlare tillräckliga handlingsmöjligheter och friheten att utöva näringsverksamhet. Regleringen tillämpas omfattande på tjänster som erbjuds i allmänna kommunikationsnät samt i interna kommunikationsnät, som är anslutna till allmänna kommunikationsnät.

⁵ Detta framgår tydligt ur 4 § i lagen om elektronisk kommunikation, enligt vilken meddelanden, identifieringsuppgifter och lokaliseringsuppgifter är konfidentiella, om inte annat bestäms i denna eller i någon annan lag samt ur 8 § 2 momentet enligt vilken konfidentiella uppgifter får behandlas av endera parten i kommunikationen eller med samtycke av en part eller om det bestäms så i lag.

⁶ Om utlämnandet av identifieringsuppgifter i samband med meddelanden som har avsetts för det allmänna stadgas i lagen om yttrandefrihet i masskommunikation (460/2003)

3. Sammanslutningsabonnenten som behandlare av identifieringsuppgifter

I företag och sammanslutningar är behandlingen av identifieringsuppgifter en del av en bredare behandling av kundinformation eller behandling av, för arbetsförhållandet nödvändiga, personuppgifter. Sammanslutningsabonnenten ordnar kommunikationsmöjligheter till sina arbetstagare eller övriga användare och deltar i meddelandenas förmedling för sitt egna kommunikationsnätets del. Lagen om dataskydd vid elektronisk kommunikation möjliggör behandling av identifieringsuppgifter, i den utsträckning som en normal verksamhet förutsätter, även för sammanslutningsabonnenter.

En sammanslutningsabonnent kan även vara part i kommunikationen, det vill säga meddelandets avsändare eller den som meddelandet var avsett till. Partsställningen för en juridisk person i kommunikationen bestäms från fall till fall. Som utgångspunkt förutsätts, för en juridisk persons partsställning, en entydig koppling till verksamheten som denne utövar samt att meddelandet var avsett till denne. En juridisk person kan ha partsställning till exempel då det gäller uppgifter i dennes egna www-server. En sammanslutningsabonnent kan även vara part i kommunikationen till exempel då en av förvaltningens kunder skickar ett meddelande som entydigt har att göra med myndighetens uppgifter, till en särskilt bestämd organisatorisk e-postadress.

Rätten att behandla identifieringsuppgifter gäller endast identifieringsuppgifter om meddelanden, som har skickats eller mottagits via sammanslutningsabonnentens egna kommunikationsnät. En sammanslutningsabonnent har rätt att behandla endast sådana identifieringsuppgifter som gäller användningen av dennes egna tjänster och som samlas i ett system som administreras av eller till förmån för denne.

Behandlingsrätten gäller till exempel endast sådana kommunikationstjänster och avgiftsbelagda informationssamhällstjänster, som är kopplade till sammanslutningsabonnentens kommunikationsnät, samt sådana informationssamhällstjänster, som sammanslutningsabonnenten har betalat för och som används via sammanslutningsabonnentens kommunikationsnät. Till exempel får kommersiella e-post- eller nätbankstjänsters identifieringsuppgifter behandlas endast till den del som det samlas identifieringsuppgifter i sammanslutningsabonnentens egna system. Vid användningen av dessa tjänster samlas endast information om adressen för den använda tjänsten, brukstidpunkten och möjligtvis användningens varaktighet i sammanslutningsabonnentens system. Sammanslutningsabonnenten har inte rätt att utreda till exempel identifieringsuppgifterna för ett e-postmeddelande som har skickats genom en kommersiell e-posttjänst.

4. Identifieringsuppgifter som del av upptäckande och utredning av missbruk

Bestämmelserna i 13 a – 13 k § i lagen om dataskydd vid elektronisk kommunikation ger rätt att behandla endast identifieringsuppgifter. I fall av missbruk får man med stöd av bestämmelserna behandla identifieringsuppgifter för såväl offentligt avsedda som konfidentiella meddelanden. Behandlingsrätten gäller även de identifieringsuppgifter, som samlas vid bläddrandet i webbsidor och som är konfidentiella enligt 4 § 3 moment i lagen om dataskydd vid elektronisk kommunikation. Bestämmelserna ger inte rätt att behandla innehållet i meddelandena.⁷

I fall av missbruk är behandlingen av identifieringsuppgifter en del av de åtgärder som används för att trygga säkerheten i organisationens system. Rätten att behandla identifieringsuppgifter anknyter till tryggheten av sammanslutningsabonnentens kommunikationsnät och kommunikationstjänsters användning samt till upptäckandet och utredningen av olagligt röjande av företagshemligheter. Behandlingen av identifieringsuppgifter är en del av de sätt, med vilka en sammanslutningsabonnent kan förebygga och utreda missbruk, som sker med hjälp av elektronisk kommunikation och som riktar sig mot dennes kommunikationsnät.⁸

Bestämmelserna i 13 a – 13 k § i lagen om dataskydd vid elektronisk kommunikation berättigar till att förebygga, upptäcka och utreda fall av missbruk som har skett genom elektronisk kommunikation i sammanslutningsabonnentens egna kommunikationsnät, till dem anknutna eller genom dem använda kommunikationstjänster och kommersiella informationssamhällstjänster. Syftet med bestämmelserna är att trygga sammanslutningsabbonenternas kommunikationsnät och tjänsters användning för dem avsedda ändamål på ett sätt som respekterar rättigheterna som kommunikationens parter har. Samtidigt möjliggör bestämmelserna en vederbörlig begränsning av en eventuell, till polisen riktad, begäran om förundersökning. Förundersökningen genomförs av polisen.

4.1 Missbrukens betydelse

Bestämmelserna i 13 a – 13 k § i lagen om dataskydd vid elektronisk kommunikation reglerar en sammanslutningsabbonents rätt att behandla identifieringsuppgifter i fall av missbruk. Bestämmelserna ger sammanslutningsabbonenterna rätt att behandla identifieringsuppgifter, då det är frågan om

1. olovligt brukande av en avgiftsbelagd informationssamhällstjänst
2. olovligt brukande av ett kommunikationsnät eller en kommunikationstjänst, eller
3. förebyggande och utredning av röjande av företagshemligheter

Enligt 2 § i lagen om tillhandahållande av informationssamhällets tjänster (458/2002) avses med en informationssamhällstjänst elektroniska distanstjänster, som utförs på begäran av mottagaren och vanligtvis mot vederlag. Det kan vara frågan om *informationssamhällstjänsters olagliga brukande* till exempel då en tjänst, som har

⁷ Angående en arbetsgivares rätt att som sammanslutningsabonnent söka fram och öppna till denne tillhörande e-postmeddelanden har reglerats i kapitel 6 i lagen om integritetsskydd i arbetslivet (759/2004).

⁸ I denna guide behandlas inte rättigheten att behandla identifieringsuppgifter i fall av missbruk (LDEK 13 §) för dem som är utomstående i förhållande till de övriga parterna i kommunikationen och inte heller för dem som har deltagit i meddelandets förmedling. Efterlevnaden av bestämmelserna övervakas av Kommunikationsverket.

prissatts i enlighet med storleken på företagets personal, olovligt delas ut för bruk till utomstående. I ett sådant fall skulle företaget vara tvunget att ansvara för den överskridande delen av användningen av den anskaffade användningsrättigheten.

Olovligt brukande av ett kommunikationsnät eller en kommunikationstjänst kan, enligt 13 a § 2 momentet i lagen om dataskydd vid elektronisk kommunikation, vara att installera anordningar, program eller tjänster i sammanslutningsabonnentens kommunikationsnät, att obehörigen ge utomstående tillträde till sammanslutningsabonnentens kommunikationsnät eller kommunikationstjänster eller att på något annat jämförbart sätt använda kommunikationsnätet eller kommunikationstjänsterna. För att betecknas som olovlig bör användningen strida mot de anvisningar, som har getts i skriftlig form och som skall förebygga missbruk, samt som stadgas om i lagens 13 b § 3 moment.

I skriftliga anvisningar, som ges till användarna, kan godkända sätt för användningen av kommunikationsnäten och kommunikationstjänsterna behandlas mera omfattande, men identifieringsuppgifter får behandlas endast för förebyggandet och utredningen av sådan olovlig användning som stadgas om i lagen. Behandlingsrätten föreligger inte om sådana instruktioner, som lagen kräver, inte har uppställts. En användare av ett kommunikationsnät eller en kommunikationstjänst bör känna till hur sammanslutningsabonnentens nät får användas.

All ovan nämnda förbjudna brukande berättigar dock inte till att behandla identifieringsuppgifter. Endast sådana identifieringsuppgifter, som anknyter till förebyggandet eller utredningen av sådant olovligt brukande av avgiftsbelagda informationssahällstjänster, kommunikationsnät eller kommunikationstjänster som orsakar betydlig skada eller olägenhet, får behandlas. Enligt 13 d § 3 momentet i lagen om dataskydd vid elektronisk kommunikation förutsätts för rätten att behandla identifieringsuppgifter att händelsen eller handlingen troligtvis orsakar betydlig skada eller olägenhet till sammanslutningsabonnenten.

Betydlig skada eller olägenhet, som avses i bestämmelsen, kan enligt regeringspropositionen vara bland annat ökade kostnader eller sådan ökad användning av dataöverföringskapaciteten, hot mot dataskydd eller annan motsvarande orsak som äventyrar, försvårar eller gör långsammare kommunikationsnätets eller tjänsternas användning för de syften som brukandet var avsedd för.⁹ Identifieringsuppgifter får inte användas till förebyggandet eller utredningen av olovlig användning, som orsakar obetydlig skada.

Sammanslutningsabonnentens egna verksamhet samt anvisningar denne gett till sina användare konkretiserar olovligt brukande samt dess betydelse för sammanslutningsabonnenten. Sammanslutningsabonnenten bör i förväg kunna definiera genom riskanalyser de förfaringssätt som med tanke på den egna verksamheten orsakar informationssamhällestjänsten, kommunikationsnätet eller kommunikationstjänsten betydlig skada eller olägenhet.

⁹ RP 48/2008, s. 27-28

Med en *företagshemlighet* avses en affärs- eller yrkeshemlighet eller annan motsvarande information gällande näringsverksamhet, som näringsidkaren håller hemlig och vars röjande skulle orsaka ekonomisk skada till denne eller en annan näringsidkare, som har anförtrott denne informationen.

Rätten att behandla identifieringsuppgifter omfattar inte allt misstänkt röjande av företagshemligheter genom användning av kommunikationsnät eller kommunikationstjänster, som denna definition avser. Behandlingsrätten begränsas till förebyggandet och utredningen av olovlig utlämning av centrala företagshemligheter till utomstående.¹⁰ Identifieringsuppgifter, som är nödvändiga för förebyggandet och utredningen, får inte behandlas, om det gäller röjande av andra än centrala företagshemligheter.

Betydelsen av företagshemligheter definieras av sammanslutningsabonnentens egna verksamhet, verksamhetsområde och den praxis och de samarbetsformer som efterlevs samt av de anvisningar som användaren har givits. Centrala företagshemligheter kan till exempel vara uppgifter, som ger företaget en konkurrensfördel och som inte kan spåras i offentliga källor och som är betydelsefulla för startandet och utövandet av näringsverksamhet. Sådana kan även vara uppgifter, om vilkas behandling och skydd, sammanslutningsabonnenten som arbetsgivare, har gjort upp speciella anvisningar eller praxis med stöd av 13 b § 2 och 3 momenten i lagen om dataskydd vid elektronisk kommunikation, eller som denne annars har skilt meddelat som hemligstämplade, eftersom ett betydande ekonomiskt intresse är anknutet till uppgifterna.

4.2 Ett sista medel

Enligt 8 § 3 momentet i lagen om dataskydd vid elektronisk kommunikation är behandlingen av identifieringsuppgifter tillåten endast i den mån som ändamålet för behandlingen kräver det och skyddet för konfidentiella meddelanden eller integritetsskyddet får inte begränsas med det mer än vad som är nödvändigt. Sammanslutningsabonnenten har, med stöd av 13 a – 13 k § i lagen om dataskydd vid elektronisk kommunikation, rätt att behandla identifieringsuppgifter endast i den mån som förebyggandet och utredningen kräver.

Förebyggandet och utredningen av röjandet av och det olovliga brukandet av företagshemligheter berättigar inte till behandling av identifieringsuppgifter, om detta mål kan nås utan att ingripa i skyddet för kommunikationen. Rätten att behandla identifieringsuppgifter är ett sista medel. Behandlingen av identifieringsuppgifter kan påbörjas först efter att lämpliga dataskyddsåtgärder för skyddandet av kommunikationsnätet och kommunikationstjänsterna eller företagshemligheten har vidtagits, om det är klart att det olovliga brukandet av tjänsterna eller röjandet av företagshemligheten inte annars kan upptäckas eller utredas.

En sammanslutningsabonnent bör i första hand eftersträva att på förhand förhindra informationssamhällstjänsternas, kommunikationsnätets och kommunikationstjänsternas olovliga brukande eller företagshemligheternas olagliga

¹⁰ Ett misstänkt röjande av företagshemligheter bör enligt 13 e § 3 momentet i lagen om dataskydd vid elektronisk kommunikation rikta sig mot, för sammanslutningsabonnentens eller dennes samarbetspartners närverksamhet, centrala företagshemligheter eller teknologisk eller annan utvecklingsarbets resultat, som troligtvis är av betydelse vid startandet eller utövandet av näringsverksamhet.

röjande till utomstående. Sammanslutningsabonnenten bör, enligt omsorgsplikten i lagens 13 b §, ordna kommunikationsnätets och tjänsternas användningsbegränsningar och skyddet av sina uppgifter på ett sätt som förebygger missbruk på möjligast bästa sätt.

Vid observerandet (förebyggandet) och utredningen av missbruk bör man i första hand använda sådana informationshanteringsmetoder, som inte förutsätter behandling av identifieringsuppgifter. Sådana metoder kan till exempel vara kontroll av systemens användnings- och felloggar, granskning av de personers uppgifter som skriver in sig på ett system till vilket tillträdet har begränsats samt övrig användning av de uppgifter som har samlats vid systemens tekniska drift/underhåll.¹¹

Utredningen av misstänkt olovligt brukande av kommunikationsnät eller kommunikationstjänster eller olovligt röjande av företagshemligheter kräver ofta även behandling av identifieringsuppgifter. Behandlingen av identifieringsuppgifter kan till exempel vara nödvändig för att utreda huruvida någon har varit i kontakt med en grupp, till vilken en företagshemlighet olovligt har givits.

Användningsändamålsenligheten föranleder att en sammanslutningsabonnent inte heller får till exempel övervaka brukandet av kommunikationsnätet eller kommunikationstjänsterna för att följa med arbetstiden eller för att utreda ifall användaren har varit i kontakt med en representant för personalen, arbetsskyddsmyndigheterna eller företagshälsovården.

4.3 Särskilda begränsningar i behandlingsrätten

Enligt 13 a § 3 momentet i lagen om dataskydd vid elektronisk kommunikation gäller inte behandlingsrätten identifieringsuppgifter för telefonitjänster i det fasta eller mobila telefonnätet. En sammanslutningsabonnent får inte behandla uppgifter om telefonsamtal, textmeddelanden eller andra motsvarande meddelanden, till den del som de överförs i fasta- eller mobila telefonnät.

Enligt 13 f § 1 momentet i lagen om dataskydd vid elektronisk kommunikation får rätten att behandla identifieringsuppgifter inte användas i fall av missbruk, för att få reda på uppgifter som berörs av källskyddet. Även om en automatisk sökning i praktiken riktar sig mot användarnas alla identifieringsuppgifter, får sökningen inte riktas på ett sådant sätt att det skulle eftersträvas att få reda på uppgifter som berörs av källskyddet. Identifieringsuppgifter får inte heller behandlas manuellt med avsikt att få reda på uppgifter som berörs av källskyddet.

Enligt 13 f § 2 momentet i lagen om dataskydd vid elektronisk kommunikation är endast sammanslutningsabonnenter, som är i arbetsgivarställning, berättigade att behandla identifieringsuppgifter med avsikt att utreda röjande av företagshemligheter.¹²

¹¹ Till behandlingen av dessa uppgifter anger lagen om dataskydd vid elektronisk kommunikation inga begränsningar, till den del som de inte kan kopplas till uppgifter (identifieringsuppgifter) om kommunikationstjänstens beställare eller användare. Det kan dock vara frågan om genom tekniska metoder förverkligad övervakning, vars användning styrs av lagen om integritetsskydd i arbetslivet (759/2004), eller om personuppgifter, vilkas behandling styrs av personuppgiftslagen (523/1999).

¹² Alla sammanslutningsabonnenter, som uppfyller de förhandsskyldigheter och de förutsättningar som det stadgas om i lagen, har dock – oberoende av arbetsgivarställningen – rätt att behandla identifieringsuppgifter

Bestämmelsen begränsar dock inte objekten för behandlingen av identifieringsuppgifter endast till användarna, som är i arbetsförhållande till sammanslutningsabonnenterna. En sammanslutningsabonnent i arbetsgivarställning, kan behandla även de användares identifieringsuppgifter, som sammanslutningsabonnenten har gett eller som annars har tillgång till företagshemligheter på ett sådant sätt som sammanslutningsabonnenten har godkänt.

Om de övriga lagenliga förutsättningarna uppfylls kan en sammanslutningsabonnent ha rätt att behandla, till exempel identifieringsuppgifter för en arbetstagare, som arbetar för en organisation som erbjuder drifttjänster till sammanslutningsabonnentens datasystem, eller identifieringsuppgifter för en arbetstagare, som arbetar för en underleverantör som sysslar med produktutvecklingsverksamhet för sammanslutningsabonnenten, förutsatt att dessa har fått på ett av sammanslutningsabonnenten godkänt sätt tillträde till företagshemligheter. Behandlingen är dock möjlig endast till den del som dessa använder sammanslutningsabonnentens kommunikationstjänster.

5. Åtgärder före behandling

En sammanslutningsabonnent bör uppfylla de förhandsskyldigheter, som stadgats om för behandling av identifieringsuppgifter, innan den behandlar identifieringsuppgifter i syfte att förebygga och utreda missbruk. Förhandsskyldigheterna är

1. omsorgsplikten (LDEK 13 b §),
2. planerings- och samarbetsplikten (LDEK 13 c §),
3. förhandsanmälan till dataombudsmannen (LDEK 13 i § 1 momentet)

Skyldigheterna gäller endast de sammanslutningsabbonenter, som avser att befatta sig med behandling av identifieringsuppgifter, antingen för att förebygga eller utreda olovligt brukande av informationssamhällstjänsten, kommunikationsnätet eller kommunikationstjänsten eller röjande av företagshemligheter. Bestämmelserna gäller inte sammanslutningsabbonenter, som inte avser att ta i bruk i lagen definierad behandlingsrätt i fall av missbruk.

5.1 Omsorgsplikten

En sammanslutningsabonnent har inte rätt att påbörja behandlingen av identifieringsuppgifter, före den har använt sig av alla de av lagen erbjudna vederbörliga informationsadministrativa metoder, med vilka olovligt brukande av informationssamhällstjänster, kommunikationstjänster eller kommunikationsnät samt röjande av företagshemligheter till utomstående kan förhindras. För skyddandet av kommunikationsnäten och kommunikationstjänsterna samt tryggheten av företagshemligheternas förtroelighet används i första hand sådana metoder som inte ingriper i användarnas kommunikation. Datasäkerhetsmetoder, som är i användning, skall granskas som en helhet på basis av riskadministration.

Lagen om dataskydd vid elektronisk kommunikation räknar i 13 b § upp de åtgärder som sammanslutningsabbonenten bör vidta före behandlingen av identifieringsuppgifter. I första hand skall sammanslutningsabbonenten sörja för dataskyddet och handledningen av användarna.

Sammanslutningsabbonenten förpliktas redan av 19 § i lagen om dataskydd vid elektronisk kommunikation att sörja för dataskyddet vid behandlingen av användarnas identifieringsuppgifter. Omsorgsplikten angående/för företagshemligheter ingår i praktiken redan i definitionen om företagshemligheter i 30 kapitlet 11 § i strafflagen. En skild omsorgsplikt före behandlingen av identifieringsuppgifter understryker sammanslutningsabbonentens skyldighet att skydda sitt kommunikationsnät och sina kommunikationstjänster samt företagshemligheter bättre än vad de allmänna omsorgsplikterna förutsätter. Efterlevnaden av omsorgsplikten konkretiserar även kriteriet, som anger att skadan och olägenheten som orsakas bör vara betydande, och som är en förutsättning för behandlingen av användarnas identifieringsuppgifter.

Tillgången till sammanslutningsabbonentens kommunikationsnät och kommunikationstjänster och till deras användning samt till centrala företagshemligheter bör begränsas enligt 13 b § 1 och 2 momentets 1 punkt. Sammanslutningsabbonenten skall på förhand vidta åtgärder, med hjälp av de metoder som finns tillhanda, i syfte att förhindra utomstående från att använda kommunikationsnätet eller en tjänst som är

anknuten därtill, på ett sätt som strider mot de villkor som har upprättats. Centrala företagshemligheter skall även faktiskt skyddas från utomstående, med hänsyn till behandlingen.¹³ Tillgången kan begränsas bland annat genom användaridentifikationer och lösenord eller annars genom att administrera användarrättigheter, samt med hjälp av brandmurar eller andra applikationer som hindrar intrång. Tillträde till företagshemligheter kan även begränsas på basis av tidpunkt, medel som används vid behandlingen och kontaktadress.

Arbetsgivaren kan skydda företagshemligheter även med andra vederbörliga/lämpliga datasäkerhetsåtgärder. Sådana är till exempel avtal om sekretess, som ingås med arbetstagarna samt nuvarande eller potentiella affärskompanjoner. Enligt lagen om säkerhetsutredningar (177/2002) kan arbetsgivaren skaffa en utredning om arbetstagarens pålitlighet, då det som skall skyddas är en synnerligen värdefull affärs- eller yrkeshemlighet eller annan, därtill jämförbar, synnerligen betydelsefull privat fördel. Arbetsgivaren kan även använda sådan teknisk övervakning, som det stadgas om i lagen om skyddet för integriteten i arbetslivet.

De meddelandetyper, som får behandlas i kommunikationsnätet, skall definieras i enlighet med 13 b § 1 och 2 momentets 2 punkt i lagen om dataskydd vid elektronisk kommunikation. Även tillåtna användningssätt av kommunikationsnäten och kommunikationstjänsterna samt behandlingssätten av företagshemligheter i kommunikationsnätet, skall definieras. Dessutom skall de destinationsadresser, till vilka kommunikation inte får utövas eller till vilka företagshemligheter inte får skickas, definieras. Om sammanslutningsabonnenten till exempel vill begränsa trafiken eller förhindra trafiken helt och hållet till vissa destinationsadresser, skall dessa definieras.

Definitionerna kan göras på en tämligen allmän nivå, men vad som räknas som missbruk bör tydligt framgå. Förteckningen över destinationsadresser behöver inte vara uttömmande på det sättet att alla förbjudna adresser skulle framgå ur den. Det måste dock sörjas för att förteckningen är tillräckligt konkret för att visa vad som är tillåtet och vad som inte är det. En sammanslutningsabonnent kan till exempel förbjuda skickande av företagshemligheter till företagets direkta konkurrenter, av vilka det upprätthålls en lista på företagets interna anslagstavla.

För att förebygga missbruk skall sammanslutningsabonnenten, i enlighet med vad som stadgas i 13 b § 3 momentet i lagen om dataskydd vid elektronisk kommunikation, *ge användaren av kommunikationsnätet eller kommunikationstjänsten skriftliga instruktioner*, i vilka det finns tillräckligt noggranna instruktioner om begränsningar som har uppsatts för användningen av kommunikationsnätet. En förutsättning för behandlingen av identifieringsuppgifter är att det till användarna av sammanslutningsabonnentens kommunikationsnät eller kommunikationstjänster har informerats om hur nätet får användas och hur man skall förfara i oklara situationer. Arbetstagare, som har att göra med sådana uppgifter som skall skyddas som företagshemligheter, skall kunna uppfatta uppgifternas karaktär som företagshemlighet samt deras centrala ställning för sammanslutningsabonnentens eller dennes samarbetspartners näringsverksamhet.

¹³ Till de personer, som har tillgång till en företagshemlighet, räknas, beroende på företagshemlighetens karaktär, typiskt organisationens ledning, samt sådana sakkunniga och i utvecklingsuppgifter arbetande, till vilkas uppgifter hör behandling av företagshemligheter. Dessutom kan sådana, som arbetar med biträdande uppgifter, samt sådana, som svarar för underhåll/drift och service av datasystemen, genom sina arbetsuppgifter eller omfattande användarrättigheter få veta om företagshemligheter.

Detta framgår bland annat av den begränsade tillgången till uppgifterna, av särskilda åtgärder som har vidtagits för att skydda uppgifterna samt av de behandlingsregler som har getts.

Känn igen, definiera och beskriv sådana förfaringssätt som orsakar betydande skada och olägenhet för informationssamhällestjänsten, kommunikationsnätet eller kommunikationstjänsten och ge användarna lämpliga anvisningar.

Klassificera företagshemligheterna och ge skriftliga instruktioner om behandlingen av centrala företagshemligheter till användaren av kommunikationsnätet och kommunikationstjänsterna.

5.2 Planerings- och samarbetsplikten

Planering. Före påbörjandet av behandlingen av identifieringsuppgifter skall sammanslutningsabonnenten namnge de personer, vars uppgift det är att behandla identifieringsuppgifterna, eller definiera ifrågavarande uppgifter eller till exempel verksamhetsenheter, i enlighet med 13 c § 1 momentet i lagen om dataskydd vid elektronisk kommunikation. Enligt stadgan är rätten att behandla identifieringsuppgifterna begränsad till endast de personer, som sörjer för driften, dataskyddet och säkerheten i sammanslutningsabonnentens kommunikationsnät eller kommunikationstjänster.

Sammanslutningsabonnenten kan ge uppgiften att behandla identifieringsuppgifter till en utomstående tjänstleverantör, till exempel till företaget som underhåller/driver sammanslutningsabonnentens kommunikationssystem och som erbjuder informationstekniska tjänster. I detta fall skall sammanslutningsabonnenten definiera tjänstleverantörens uppgifter och funktioner. I enlighet med 19 § 3 momentet i lagen om dataskydd vid elektronisk kommunikation ansvarar sammanslutningsabonnenten för lagenligheten av identifieringsuppgifternas behandling och uppgifternas säkerhet även då tredje part står för behandlingen av sammanslutningsabonnentens användares identifieringsuppgifter. Sammanslutningsabonnenten bör även vid utlokalisering av sina tjänster sörja för att förutsättningarna för rätten att behandla identifieringsuppgifter i fall av missbruk uppfylls.

Samarbete. Lagen om dataskydd vid elektronisk kommunikation ålägger sammanslutningsabonnenter, som är i arbetsgivarställning, samma samarbetsplikt i behandlingen av identifieringsuppgifter, som lagen om skyddet för integritet i arbetslivet ålägger angående behandlingen av personuppgifter. Före arbetsgivaren tar i bruk de förfaranden eller deras förändringar/modifikationer, som det stadgas om i 13 a – 13 k §, bör det förhandlas, med de arbetstagares företrädare som ärendet gäller, om behandlingens grunder, praxis, mål, avsikt och inverkan. I andra än sådana offentligrättsliga sammanslutningar och företag, som omfattas av samarbetsverksamhetslagstiftningen, skall arbetstagarna eller deras företrädare ges tillfälle, att före beslutsfattandet, bli hörda i motsvarande ärenden.

Till området för samarbetsförfarandet och förfarandet då någon hör, hör även de centrala frågorna om behandling av identifieringsuppgifter vid övervakning av olovligt brukande av kommunikationsnät eller kommunikationstjänster och röjande av företagshemligheter. Sådana frågor är till exempel avsikten med behandlingen av identifieringsuppgifterna

(förebyggandet och utredningen av olovligt brukande eller röjande av företagshemligheter), instruktioner om användningen av kommunikationsnät, identifieringsuppgifternas behandlare och de uppgifter till vilka behandling anknyts, verksamhetsprinciperna för den automatiska sökningen samt förutsättningarna för identifieringsuppgifternas manuella behandling.

Till området för samarbetsförfarandet och förfarandet då någon hörs, hör även de grunder, på vilka olovligt brukande av kommunikationsnät eller kommunikationstjänst anses förorsaka arbetsgivaren betydande skada eller olägenhet. I samma förfarande skall även de grunder, på vilka arbetsgivaren anser en företagshemlighet vara av central betydelse för sin egna eller för en samarbetspartners näringsverksamhet, behandlas. Sådana är till exempel avsikten med behandlingen av identifieringsuppgifterna (förebyggningen och utredningen av olovlig förbrukning eller röjande av företagshemligheter), instruktioner om användningen av kommunikationsnät, identifieringsuppgifternas behandlaren och uppgifter, till vilka anknyts behandling, verksamhetsprinciperna för den automatiska sökningen samt förutsättningarna för identifieringsuppgifternas manuella behandling.

Efter samarbetsförfarandet och förfarandet då någon hörs skall sammanslutningsabonnenter, som är i arbetsgivarställning, informera sina arbetstagare eller deras företrädare om de ärenden och beslut som fattats i samarbetsförfarandet, i enlighet med 21 § i lag om integritetsskydd i arbetslivet.

Enligt 13 c § 4 momentet i lagen om dataskydd vid elektronisk kommunikation skall andra än sammanslutningsabonnenter, som är i arbetsgivarställning, informera sina användare om de förfaranden och den praxis som tillämpas vid behandlingen av identifieringsuppgifter. Sammanslutningsabonnenten skall informera även andra användare av dess kommunikationsnät och kommunikationstjänster än arbetstagarna, om de förfaranden och den praxis som tillämpas vid behandlingen av identifieringsuppgifter. Till exempel läroanstalter, bostadsaktiebolag eller andra organisationer, som erbjuder kommunikationstjänster för bruk till sina användare, skall informera användarna om de ovan nämnda ärendena.

5.3 Förhandsanmälan till dataombudsmannen

Enligt 13 i § 1 moment i lagen om dataskydd vid elektronisk kommunikation skall sammanslutningsabonnenten göra en förhandsanmälan till dataombudsmannen före påbörjandet av automatisk eller manuell behandling av identifieringsuppgifter i fall av missbruk. Behandlingen av identifieringsuppgifter kan påbörjas genast efter att anmälan har gjorts, förutsatt att andra förhandsskyldigheter har uppfyllts.¹⁴

När sammanslutningsabonnenten gör sin anmälan skall denne framföra en utredning om de grunder och den praxis, som tillämpas i förfarandet vid behandlingen av identifieringsuppgifterna. Avsikten med behandlingen av identifieringsuppgifterna samt behandlarna eller de uppgifter till vilka behandling anknyts skall individualiseras i utredningen. I anmälan skall det också redogöras för verksamhetsprinciperna för den

¹⁴ Det är inte frågan om ett tillståndsförfarande. På basis av anmälan om påbörjan av behandling av identifieringsuppgifter, får dataombudsmannen vetskap om de grupper som är föremål för övervakning av lagenlighet.

automatiska sökningen samt förutsättningarna för manuell behandling av identifieringsuppgifter.

Utredningen skall innehålla grunderna, på vilka det olovliga brukandet av kommunikationsnätet eller kommunikationstjänsterna anses orsaka betydande skada eller olägenhet till sammanslutningsabonnenten. I utredningen skall också framföras grunderna, på vilka sammanslutningsabonnenten anser att en företagshemlighet är central för den egna eller samarbetspartners näringsverksamhet.

Ytterligare skall det ur anmälan framgå, hur sammanslutningsabonnenten har informerat eller kommer att informera kommunikationsnätets eller kommunikationstjänsternas användare om dessa omständigheter. De skriftliga instruktioner, som har givits åt kommunikationsnätets eller kommunikationstjänsternas användare, i avsikt att förebygga missbruk, skall bifogas till anmälan.

Om det förekommer väsentliga förändringar i de omständigheter, som är föremål för utredning, skall en ny utredning, angående dessa, levereras till dataombudsmannen. En ny anmälan skall göras till exempel då 1) identifieringsuppgifter börjar behandlas på en grund, som avviker från den som anmälts i förhand, 2) då kriterierna för den automatiska behandlingen av identifieringsuppgifter ändras, 3) då de instruktioner, som har getts till användarna, ändras avsevärt eller 4) då rätten att behandla identifieringsuppgifter ges till personer som har helt andra uppgifter, än vad som har framförts i förhandsanmälan.

Modellblanketter, som dataombudsmannens byrå har utarbetat för att styra uppgörandet av anmälningar, samt de avgifter som uppbärs vid behandlingen av anmälningar, hittas på byråns hemsida på adressen, <http://www.tietosuoja.fi>. Blanketterna kan även beställas per post.

6. Förfaringssätten och förutsättningarna för automatisk sökning och manuell behandling

6.1 Automatisk sökning

I fall av missbruk får identifieringsuppgifter i första hand behandlas med hjälp av en automatisk sökningsfunktion på basis av på förhand bestämda sökningskriterier.

Med automatisk sökning avses en funktion, i vilken sökningen varken riktas fall för fall eller med hjälp av mänsklig arbetskraft, utan i vilken systemet automatiskt söker avvikelser i kommunikationsnätet på basis av vissa på förhand bestämda kriterier. I den automatiska sökningen analyseras kommunikationstrafiken som en mängd, till exempel på basis av meddelandenas storlek, trafikens mängd, typ, uppkopplingsätt eller typen på trafikens destinationsadress. Vid automatisk sökning är det frågan om att förebygga missbruk genom att finna meddelanden, som möjligtvis kan förknippas med missbruk, med stöd av på förhand bestämda kriterier.

Den automatiska behandlingen är en fortgående verksamhet, som kan tas i bruk då förhandsskyldigheterna har uppfyllts och de ovan nämnda förutsättningarna för behandlingen av identifieringsuppgifter uppfylls. När en avvikelse har funnits i den automatiska sökningen, kan en utredning för det specifika fallet med hjälp av mänsklig arbetskraft påbörjas. Med den automatiska sökningen eftersträvas att plocka ut till manuell behandling, endast sådana identifieringsuppgifter för meddelanden, som kan förknippas med missbruk.

Den automatiska sökningen får inte riktas mot en enskild användare eller till snäva användargrupper, för att analysera deras kommunikation på basis av kommunikationsnätets- eller tjänstens användares kontaktadress. Automatisk sökning får inte användas till uppföljning av enskilda parters kommunikation, utan det måste vara frågan om iakttagelser/upptäckande av avvikelser, som tyder på missbruk. I den automatiska sökningen får inte identifieringsuppgifterna för en enskild användares meddelanden avslöjas för behandlaren av identifieringsuppgifterna.

6.2 Manuell behandling

Identifieringsuppgifter får under vissa förutsättningar behandlas även manuellt. Fall för fall riktas en manuell behandling med mänsklig arbetskraft till identifieringsuppgifterna för kontaktadressen för en viss användare eller en viss användargrupp. Det är frågan om en från fall till fall utarbetad utredning av misstanke om missbruk, vilken upptäckts med hjälp av den automatiska sökfunktionen eller på annat sätt.

Före identifieringsuppgifterna tas till manuell behandling, skall en av sammanslutningsabonnenten namngiven person, som svarar för behandlingen, på nytt utvärdera ifall förutsättningarna för betydande skada eller central företagshemlighet uppfylls för de identifieringsuppgifters del, vilka skulle komma till manuell behandling. *Till manuell behandling får tas endast sådana identifieringsuppgifter, som anknyter till olovligt brukande, som sannolikt orsakar betydande skada eller olägenhet, eller till röjande av central företagshemlighet.* Ifall de identifieringsuppgifter, som har valts till manuell

behandling, inte sannolikt kan förknippas till sådant olovligt brukande av kommunikationsnät, kommunikationstjänster eller avgiftsbelagda informationssamhällestjänster, som skulle orsaka betydlig skada eller olägenhet eller röja en central företagshemlighet, skall den manuella behandlingen avslutas och uppgifterna förstöras.

En förutsättning för manuell behandling av identifieringsuppgifter är att uppgifterna är nödvändiga för att utreda missbruket eller vem som är ansvarig för det eller för att få slut på det olovliga brukandet (LDEK 13 d och 13 e § 4 moment). Denna bestämmelse, som specificerar kravet på ändamålsenlighet i lagens 8 § 3 moment, förpliktar till att göra avvägningen om nödvändighetsförutsättningar på nytt, då identifieringsuppgifter tas till manuell behandling för att utreda missbruk, på basis av en upptäckt gjord i den automatiska sökningen eller på annan grund.

Om behandlingen av identifieringsuppgifter är nödvändig för att utreda missbruk eller för att specificera en brottsanmälan eller begäran om undersökning till polisen, måste kretsen av identifieringsuppgifter, som kommer till behandling, begränsas från fall till fall med hjälp av andra uppgifter som finns till förfogande.¹⁵ Samtidigt kan sammanslutningsabonnenten fortfarande begränsa kretsen av misstänkta och försäkra fortsättningen av sin verksamhet. Enligt nödvändighetsförutsättningen kunde även då i första hand tas till behandling endast identifieringsuppgifterna för användarens avsända och inte för dennes mottagna meddelanden. Tidsmässigt kan man ta till behandling endast sådana identifieringsuppgifter, som finns till handa i det föreliggande fallet och är nödvändiga för utredningen av fallet. Identifieringsuppgifter får inte behandlas mer omfattande än detta.

6.3 Särskilda förutsättningar för manuell behandling

För att förebygga och utreda olika missbrukssituationer vid manuell behandling av identifieringsuppgifter har det ställts vissa förutsättningar.

Manuell behandling av identifieringsuppgifter, med syfte att utreda olovligt brukande av informationssamhällestjänster, kommunikationsnät eller kommunikationstjänster, förutsätter en grundad anledning att misstänka att kommunikationsnätet, kommunikationstjänsterna eller de avgiftsbelagda informationssamhällestjänsterna används i strid med de utarbetade anvisningarna. Enligt 13 d § 2 momentet i lagen om dataskydd vid elektronisk kommunikation skall misstanken om olovligt brukande dessutom grunda sig på upptäckter av följande slag:

- 1) en avvikelse i kommunikationen har upptäckts med hjälp av en automatisk sökfunktion;

Med avvikelsen avses upptäckter, som den automatiska sökningen gör på basis av på förhand bestämda kriterier om meddelandenas storlek, typ, antal, uppkopplingsätt eller destinationsadresser. En avvikelse, som upptäcks vid en korrekt definierad automatisk sökning, ger skäl att misstänka olovligt brukande.

¹⁵ I samband med uppgörandet av brottsanmälan eller begäran om undersökning har sammanslutningsabonnenten, som målsägande, rätt att överlämna identifieringsuppgifterna för behandling till polisen enligt 13 k § i lagen om dataskydd vid elektronisk kommunikation. Bestämmelsen förpliktar samtidigt polisen till att behandla dessa uppgifter.

2) kostnaderna för användningen av en avgiftsbelagd informationssamhällstjänst har blivit ovanligt höga

3) det i kommunikationsnätet upptäcks en anordning, ett program eller en tjänst som har installerats obehörigen;

En motiverad misstanke kan väckas till exempel då det i samband med den informationsadministrativa driften upptäcks en anordning eller en tjänst, som är avvikande på basis av namngivningen eller sina funktioner. I sådana fall kan man utreda hurudan trafik det har varit till och från den ifrågavarande anordningen eller tjänsten.

4) då det i ett enskilt fall, på basis av annan med 1–3 punkten jämförbar allmänt konstaterbar omständighet, går att sluta sig till att kommunikationsnätet, kommunikationstjänsten eller en avgiftsbelagd informationssamhällstjänst används i strid med de anvisningar som avses i 13 b § 3 mom.

Till exempel kan upptäckter av från kontaktadressen kommande, på basis av kommunikationstjänstens bestämmelser, avvikande trafik, ge upphov till en motiverad misstanke.

Identifieringsuppgifter får behandlas manuellt för att utreda röjandet av företagshemligheter, om det finns grundad anledning att misstänka att en företagshemlighet har givits till en utomstående, genom användning av kommunikationsnätet eller kommunikationstjänster. En förutsättning för manuell behandlingsrätt är att man med grundad anledning kan misstänka att röjandet av företagshemligheten uttryckligen har skett med hjälp av kommunikationsnätet eller kommunikationstjänsterna. Enligt 13 e § 2 moment i lagen om dataskydd vid elektronisk kommunikation skall röjandet av företagshemligheten vidare vara grundad på upptäckter av följande slag:

1) en avvikelse i kommunikationen har upptäckts med hjälp av den automatiska sökfunktionen;

Med avvikelsen avses upptäckter, som den automatiska sökningen gör på basis av på förhand bestämda kriterier om meddelandenas storlek, typ, antal uppkopplingsätt eller destinationsadresser. En avvikelse, som upptäcks vid en korrekt definierad automatisk sökning, ger skäl att misstänka olovligt brukande.

2) en företagshemlighet offentliggörs eller utnyttjas olovligen;

En grundad anledning att misstänka olagligt röjande av företagshemlighet, kan väckas till exempel då företagshemligheten har offentliggjorts utan lov eller någon annan har utvecklat en likadan produkt eller tjänst på basis av ett hemligt utvecklingsarbete.

3) då det i ett enskilt fall, på basis av annan med 1 eller 2 punkten jämförbar allmänt konstaterbar omständighet, går att sluta sig till att en företagshemlighet olovligen har röjts för en utomstående.

6.4 Redogörelse för manuell behandling

Sammanslutningsabonnenten skall utarbeta en redogörelse över den manuella behandlingen av identifieringsuppgifter, i enlighet med 13 g § i lagen om dataskydd i elektronisk kommunikation. Ur redogörelsen skall framgå en i 13 a § stadgad grund för behandling, som kan vara antingen förebyggande och utredning av olovligt brukande av en avgiftsbelagd informationssamhällstjänst, kommunikationsnät, kommunikationstjänst eller röjande av företagshemligheter. Ur redogörelsen bör även tidpunkten för behandlingen och dess varaktighet, behandlarna samt vem som har beslutat om behandlingen framgå.

Ytterligare skall det i redogörelsen presenteras en grund, som överensstämmer med lagens 13 d och 13 e § 2 moment, på vilken den manuella behandlingen av identifieringsuppgifter har påbörjats. Om behandlingen har inletts till exempel på basis av en automatisk sökning, så skall det i utredningen presenteras på basis av vilket sökkriterium i den automatiska sökningen, som identifieringsuppgifterna har blivit utvalda till en manuell behandling. Om behandling har inletts till exempel på basis av en allmänt iakttagbar omständighet, skall denna omständighet specificeras tillräckligt noggrant i redogörelsen.

En redogörelse, som har undertecknats av alla som har deltagit i behandlingen, skall förvaras i minst två år efter att behandlingen av identifieringsuppgifter har avslutats. Förvaringen/sparandet av redogörelsen är nödvändig för att skydda rättigheterna hos användarna av kommunikationsnäten eller kommunikationstjänsterna samt hos dem som har deltagit i behandlingen och som har beslutat om den, samt för att utreda möjligt missbruk av identifieringsuppgifter.

Enligt 13 g § 3 momentet i lagen om dataskydd vid elektronisk kommunikation, skall en redogörelse över manuell behandling av identifieringsuppgifter delges den användare av kommunikationsnätet eller kommunikationstjänsterna, som är föremål för behandlingen, genast då delgivningen kan ske utan att behandlingens syfte äventyras. Redogörelsen behöver delges endast de användare, vars identifieringsuppgifter har behandlats manuellt på så sätt att den, som har deltagit i behandlingen för sammanslutningsabonnentens del, har fått kännedom om uppgifterna. Redogörelsen skall delges direkt en sådan användare av kommunikationsnätet eller kommunikationstjänsterna, som har varit föremål för manuell behandling.

Utredningstekniska omständigheter, som beror på en pågående förundersökning samt andra jämförbara omständigheter, berättigar till att skjuta upp delgivningen av redogörelsen, ända tills delgivningen kan genomföras utan att äventyra undersökningen. Det har inte utställts någon tidsgräns för delgivning, men det bör ske så snabbt som möjligt efter att behandlingen av identifieringsuppgifter har avslutats.

Bestämmelserna i 8 § 3 momentet samt 13 d § och 13 e § 4 momentet i lagen om dataskydd vid elektronisk kommunikation, begränsar delgivningens uppskjutande på utredningstekniska grunder, eftersom behandlingen inte får begränsa skyddet för konfidentiella meddelanden och integritetsskyddet mer än nödvändigt, för att utreda missbruk. När missbruket har utretts tillräckligt, skall behandlingen avslutas och av den utarbetas en redogörelse till användaren.

Efter att användaren har fått veta om behandlingen av sina identifieringsuppgifter, har denne möjlighet att försäkra sig om åtgärdernas lagenlighet och vid behov vända sig till dataombudsmannen, polisen eller den egna fackorganisationen. Utan hinder av sekretess, som baserar sig på lag eller avtal, har användaren rätt att för behandlingen av ett ärende, som gäller användarens intressen och rättigheter, överlämna redogörelsen och de uppgifter användaren fått i samband med den. Enligt 13 g § 3 momentet i lagen om dataskydd vid elektronisk kommunikation kan det inte genom avtal avvikas från denna rättighet.

Av de lagrade redogörelserna bildas ett personregister, till vilket alla de bestämmelser som reglerar behandling av personuppgifter tillämpas.¹⁶ Till dataombudsmannen skall göras en årsanmälan efter att de första redogörelserna har lagrats. Till den skall bifogas en rapport över personregistret.

¹⁶ Broschyren "Personuppgiftslagen som guide" hittas på adressen <http://www.tietosuoja.fi/16100.htm>

7. Åtgärder efter behandlingen

7.1 En årlig redogörelse till arbetstagarnas företrädare

Om sammanslutningsabonnenten är arbetsgivare, skall denne årligen lämna en redogörelse för den manuella behandlingen av identifieringsuppgifterna, till arbetstagarnas företrädare, i enlighet med 13 h § i lagen om dataskydd vid elektronisk kommunikation. Av redogörelsen skall det framgå på vilka grunder och hur många gånger identifieringsuppgifterna har behandlats under ett år.

Som företrädare för arbetstagarna, som redogörelsen ges till, fungerar i första hand en, i enlighet med ett tjänstekollektivavtal eller arbetskollektivavtal, utsedd förtroendemän eller ett i 13 kapitlet 3 § i arbetsavtalslagen (55/2001) avsett förtroendeombud. Ifall en personalgrupp inte har en sådan företrädare, skall redogörelsen ges till en i samarbetslagstiftningen avsedd samarbetsföreträdare eller representant. Ifall dessa inte heller har blivit valda, skall redogörelsen delges alla arbetstagare i den ifrågavarande personalgruppen.

Företrädarna för arbetstagarna och arbetstagarna i den personalgrupp, som har fått redogörelsen, har tystnadsplikt angående de kränkningar och misstänkta kränkningar av företagshemligheter, som de fått kännedom om, i enlighet med 13 h § 3 momentet i lagen om dataskydd vid elektronisk kommunikation. Tystnadsplikten fortsätter så länge som arbetsförhållandet är i kraft, även om personen inte längre skulle ha hand om den uppgift i vilken denne fått informationen. Tystnadsplikten hindrar dock inte att uppgifter lämnas ut till dataombudsmannen.

7.2 Årsanmälan till dataombudsmannen

Sammanlutningsabonnenten skall årligen lämna dataombudsmannen en redogörelse för den manuella behandlingen av identifieringsuppgifterna, på det sätt som stadgas i 13 i § 2 momentet i lagen om dataskydd vid elektronisk kommunikation. Redogörelsen skall ges årligen till dataombudsmannen, från och med förhandsanmälan eller den föregående årsanmälan. Anmälan behöver inte göras ifall identifieringsuppgifter inte har behandlats manuellt under året.

Ur redogörelsen skall det framgå på vilka grunder och hur många gånger identifieringsuppgifterna har behandlats under ett år. För varje gång en manuell behandling har utförts skall det redogöras för om grunden för behandlingen har varit olovligt brukande av en avgiftsbelagd informationssamhällstjänst, ett kommunikationsnät eller en kommunikationstjänst eller röjande av en företagshemlighet. Ur redogörelsen skall både under året upphörda manuella behandlingar och under förevarande år pågående, möjligtvis redan tidigare påbörjade, behandlingar av identifieringsuppgifter framgå.

När en redogörelse över avslutade manuella behandlingar av identifieringsuppgifter, som ges till användaren i enlighet med 13 g § i lagen om dataskydd för elektronisk kommunikation, har lagrats för första gången av sammanslutningsabonnenten, skall ett registerutdrag över det personregister som har bildats bifogas till årsanmälan till dataombudsmannen.

Modellblanketter, som dataombudsmannens byrå har utarbetat för att styra uppgörandet av anmälningar, samt de avgifter som uppbärs vid behandlingen av anmälningar, hittas på byråns hemsida på adressen, <http://www.tietosuoja.fi>. Blanketterna kan även beställas per post.