



DATAOMBUDSMANNENS BYRÅ

BEHANDLING AV IDENTIFIERINGSUPPGIFTER I FALL AV MISSBRUK

- Anvisning för verksamhetens organisering

Publiserad 3.8.2010

www.tietosuoja.fi

INLEDNING	2
ÖVERVAKNING AV MISSBRUK OCH ÖVRIG BEHANDLING AV IDENTIFIERINGSUPPGIFTER.....	3
SOM GRUND EN RISKANALYS	5
PLANERING	6
UTREDNING OCH ÅTGÄRDER.....	16
FRÅGOR OCH SVAR.....	18
BILAGA 1, KOMMUNIKATIONSVERKETS TOLKNING 268/64/2010	

Inledning

Denna anvisning beskriver stegvis vad som skall beaktas vid behandling av identifieringsuppgifter och då fall av missbruk av kommunikationsnät eller företagshemligheter observeras eller utreds. Anvisningen strävar till att åskådliggöra de särskilda kraven och åtgärderna för att observera och utreda fall av missbruk, som lagen om dataskydd vid elektronisk kommunikation (LDSEK, 516/2004) 13 a - 13 k §, stadgar om. Anvisningen hjälper vid utarbetandet av konkreta verksamhetsmodeller och anvisningar för var och en organisation.

Anvisningen har indelats i två delar. Den första delen är avsedd att vara ett stöd vid planeringen identifieringsuppgifternas behandlingspraxis för de kretsar som styr dataförvaltningen, säkerhetsfunktionerna eller den interna granskningen. I planeringsdelen går för varje åtgärd igenom 1) säkrandet av datasäkerhetsnivån 2) användarnas handledning 3) bestämmandet av identifieringsuppgifternas behandlingspraxis samt 4) informering. Anvisningens andra del är avsedd till representanter av dem som i praktiken behandlar identifieringsuppgifter inom dataförvaltningen, säkerhetsfunktionerna eller den interna granskningen. I delen genomgås de olika skedena vid bedömningen av en avvikelse i datanätet samt de åtgärder som följer en utredning av missbruk. Den andra delen innehåller även en del med frågor och svar, i vilken grunderna för behandling av identifieringsuppgifter har eftersträvat att klargöras genom praktiska exempel. Genom praktiska exempel har särskilt eftersträvat att klargöra förhållandet mellan LDSEK 13 § och behandlingen av identifieringsuppgifter i datasäkerhetssyften i LDSEK 20 §.

Användaren av denna anvisning förutsätts identifiera sig som en sammanslutningsabonnent som avses i 2 § 11 punkt i lagen om dataskydd vid elektronisk kommunikation (516/2004) och förutsätts vara medveten om att denne behandlar identifieringsuppgifter i enlighet med 8 punkten. Anvisningen kompletterar dataombudsmannens byrås broschyr om en sammanslutningsabonnents rätt att behandla identifieringsuppgifter i fall av missbruk¹, i vilken behandlingsrätten av identifieringsuppgifter i 13 a – k § i lagen om dataskydd vid elektronisk kommunikation behandlas särskilt från lagstiftningens synpunkt.

Övervakning av missbruk och övrig behandling av identifieringsuppgifter

Lagen om dataskydd vid elektronisk kommunikation tillåter behandling av identifieringsuppgifter å sammanslutningsabonnentens vägnar för producerande och användandet (9 §), faktureringen (10 §), marknadsföringen (11 §), tekniska utvecklingen (12 §) och statistiska analysen (12 a §) av tjänster samt utredning av fall av missbruk (13 §), iakttagandet av tekniska fel (14 §) och förverkligandet av datasäkerheten (20 §).

Det är viktigt att vara medveten om på vilken av de ovan nämnda grunderna identifieringsuppgifter behandlas i alla olika fall. Med tanke på fall av missbruk är det väldigt viktigt att särskilja från varandra gränserna för verksamheten mellan bestämmelserna om fall av

¹ En sammanslutningsabonnents rätt att behandla identifieringsuppgifter i fall av missbruk, <http://www.tietosuojafi/47723.htm>

missbruk (13 a – k §) och bestämmelserna om grunderna för datasäkerhetens förverkligande (20 §). Verktögen och åtgärderna är i dessa fall ofta de samma eftersom endast verksamhetens syfte skiljer åt rättsgrunderna från varandra.

Det är även skäl att särskilja utredning av missbruk vilken grundar sig på behandlingen av identifieringsuppgifterna i kommunikationsnätet, från andra utredningssätt inom dataförvaltningen, i vilka identifieringsuppgifter inte behandlas. Datasystemens inre mekanismer, så som inloggning och logguppgifterna för datasystemets användning hör inte till LDSEK:s 13 a – k §.

I denna anvisning är fokus på att guida utredningen av fall av missbruk i kommunikationsnätet i enlighet med 13 a – k § i lagen om dataskydd vid elektronisk kommunikation, genom att behandla identifieringsuppgifter. I anvisningens del "Frågor och svar" eftersträvas att ta fram gränsdragningsituationer mellan missbruksutredningar och skyldigheten att sörja för datasäkerheten, vilka uppkommer vid datanätets dagliga underhållning.

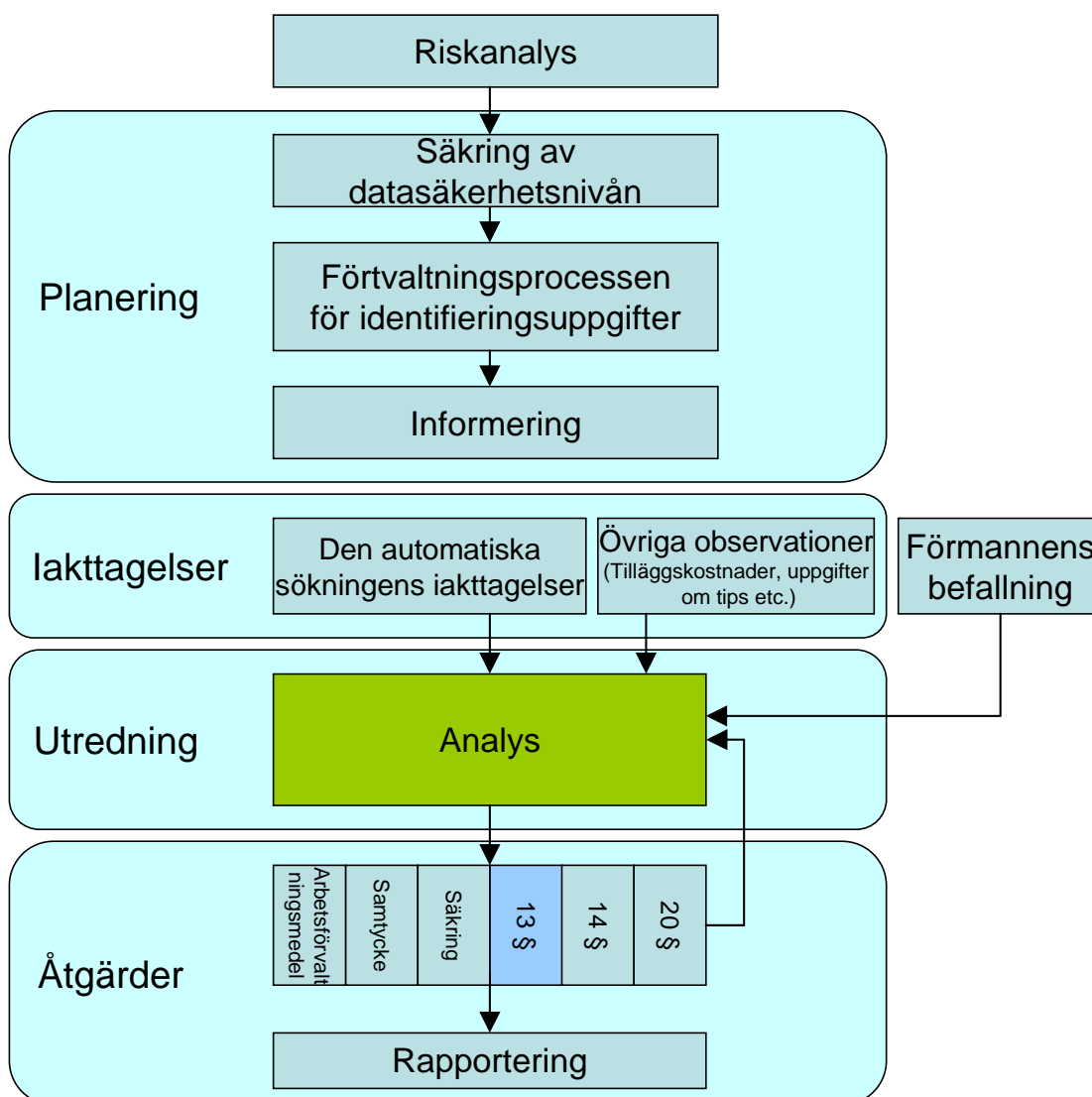


Bild 1. Processschema om ibruktagande och användning av identifieringsuppgifternas behandlingsrättigheter vid utredning av fall av missbruk

Som grund en riskanalys

En sammanslutningsabbonents beslut att börja behandla identifieringsuppgifter i fall av missbruk grundar sig på den av organisationen utförda riskanalysen. Till stöd för beslutet

- kartläggs i organisationen de mål som skall skyddas (centrala företagshemligheter) och de mot anvisningarna stridande situationerna som förorsakar betydande skada²;
- identifieras riskerna i organisationen och deras verkningar samt de förvaltnings sätt som är i bruk och deras tillräcklighet.

Organisationens ledning beslutar huruvida behandlingsrätt för identifieringsuppgifterna behövs för att iaktta och utreda fall av missbruk. Enligt det beslut som fattats kan behandlingsrättens ibruktagande förberedas enligt de skeden som framgår ur schemat (bild 1, s.4) eller så kan behandlingsrätten gällande identifieringsuppgifterna begränsas så att ifrågavarande behandling inte sker för att iaktta och utreda missbruk enligt LDSEK 13 §. Vid begränsandet av behandlingsåtgärderna är kommunikationsverkets ställningstaganden och föreskrifter samt de till denna anvisning bifogade frågorna och svaren riktgivande.

Hjälpmiddel och modeller

- Kommunikationsverkets föreskrifter och beslut <http://www.ficora.fi/sv/index/saadokset.html>
- SME-företagens riskhantering <http://www.pk-rh.com/sv>
- Statskontorets Kaiku–Luotain: <http://www.valtiokonttori.fi/public/default.aspx?nodeid=19073>
- Anvisningarna från statsförvaltningens ledningsgrupp för datasäkerhet http://www.vm.fi/vm/sv/13_forvaltningsutveckling/09_datasakerhet/index.jsp
- Nationella säkerhetsauditeringskriterierna KATAKRI <http://www.defmin.fi/files/1525/Katakri.pdf>

² Företagshemligheters centrala ställning bestäms genom den egna verksamheten, verksamhetsområdet och den praxis och de samarbetsformer som där tillämpas samt genom de anvisningar som användarna har getts. Betydande skada eller olägenhet kan orsakas genom ökade kostnader eller dataöverföringskapacitetens användning eller andra motsvarande orsaker, som äventyrar, försvårar eller saktar ner kommunikationsnätets eller tjänstens användning till det ändamål de är avsedda till.

Planering

När en organisation bestämmer sig för att börja avvärja användningen av kommunikationsnätet eller -tjänsten till sådana ändamål som strider mot anvisningarna samt börja skydda företagshemligheterna från olaga avslöjande, genom utnyttjande av egna datanät enligt LDSEK 13 i §, skall denne planera och förverkliga identifieringsuppgifternas livslängd för alla enskilda åtgärders och behandlingsskedens del. Ansvar för planeringen och beslutsfattandet gällande identifieringsuppgifternas behandling åligger ledningen, men det är även bra att involvera representanter från personalförvaltningen, dataförvaltningen, kommunikationsavdelningen och den juridiska avdelningen.

I planeringen skall beaktas följande förhandsåtgärder som lagen förutsätter:

1. Säkra datasäkerhetens nivå
2. Vägled användarna
3. Definiera behandlingspraxisen gällande identifieringsuppgifterna samt namnge och skola identifieringsuppgifternas behandlare
4. Informera om ärendet (behandla i samarbetsförhandlingarna) och gör en anmälan till dataombudsmannen.

Efter detta har företaget rätt att behandla identifieringsuppgifter för de ändamål som lagen anger.

Åtgärd 1 Tryggande av datasäkerhetsnivån	
Mål	Behandlingen av identifieringsuppgifter är begränsad till situationer där förebyggandet och utredandet av missbruk inte är möjligt genom de datasäkerhetsåtgärder som sammanslutningsabbonenten vidtar för att skydda sitt datakapital och datasystem. Sammanslutningsabbonenten har strävat till att med hänsyn till hotens allvarlighet, tekniska utvecklingsnivå och kostnader, begränsa identifieringsuppgifternas behandlingssituationer och föremålen för behandling till endast de mest nödvändiga ändamålen.
Åtgärd 1.1	Bedöm ifall tillgången till kommunikationsnätet och kommunikationstjänsten och deras användning samt centrala företagshemligheter har begränsats ändamålsenligt.
Åtgärd 1.2	<p>Bedöm användningen av användningsbegränsningar och skyddsmetoder för att förebygga olovligt avslöjande av övriga företagshemligheter, t.ex.</p> <ul style="list-style-type: none"> - uppgörande av sekretessavtal med arbetstagare och affärspartners; - anskaffande av säkerhetsutredningar enligt lagen om säkerhetsutredningar (177/2002); - kameraövervakning och annan teknisk övervakning om vilken stadgas i lagen om integritetsskydd i arbetslivet; - isolerandet av databehandlingstjänsterna, användarna och datasystemen från varandra i näten t.ex. med en brandmur eller andra tillämpningar för hämning av intrång; - begränsning av tillträde till vissa tidpunkter samt endast från vissa bestämda och gemensamma adresser eller anordningar; - hemlighållande av uppgifter som skall överföras och definierande av den metod för hemlighållande vilken används; - begränsning av typer av bilagor och - förhindrande av sändande av meddelanden till vissa sorters eller vissa måladresser.
Åtgärd 1.3	<p>Överväg användning av andra begränsningar och skydd vilka förebygger användning mot anvisningarna, t.ex.</p> <ul style="list-style-type: none"> - filtrering av förbjudna måladresser med hjälp av analys av existerande listor och analys av dem; - uppföljning av nätets och nätanordningarnas belastningssituation (övervakning av kapaciteten) och saklig informering av de största användargrupperna;

	<ul style="list-style-type: none"> - teknisk begränsning av de meddelanden som sänds eller som mottas (t.ex. begränsning av meddelandenas maximiantal eller maximistorlek) - förhindrande av installering/körning av icke godkända program eller anordningar; - förhindrande av automatiskt genomförande av en programkod i ett meddelande; - förbud mot kringgående av de tekniska begränsningarna.
Åtgärd 1.4	Insamla och förvara logguppgifter gällande användarnas verksamhet, avvikelser, störningar och datasäkerhetshändelser för en bestämd tid.
Exempel över god praxis	Åtgärd 1.1: Till uppgifterna och nättjänsterna har endast de befulldäktade användarna tillgång enligt den godkända tillgångsövervakningspolitiken. Användarrättigheterna förvaltas enligt bestämda förvaringssätt.
Observationer	Då behandlingsverksamheter för identifieringsuppgifter utkontrakteras förutsätts av underleverantörerna och samarbetspartnerna minst samma datasäkerhetsnivå som av sammanslutningsabbonenten själv.
Hjälpmiddel och modeller	ISO 27001 och 27002 och statsförvaltningens datasäkerhetsnivåer.

Åtgärd 2		Handledning av användare
Mål		Användaren av sammanslutningsabbonentens datanät vet hur och till vad kommunikationsnätet eller -tjänsten får användas och hur man skall förfara i oklara situationer.
Åtgärd 2.1		<p>Dokumentera, upprätthåll och håll reglerna om godkänd användning av kommunikationsnätet och -tjänsterna tillgängliga för alla användare av datanätet. Individualisera med tillräcklig precisering åtminstone</p> <ul style="list-style-type: none"> - begränsningarna som har tillsatts kommunikationsnätets användning, så som t.ex. det huruvida kommunikation begränsas till vissa typer eller vissa måladresser, - anvisningarna för förfarandet vid behandling av data-material i kommunikationsnätet och - hur efterlevnaden av reglerna övervakas, hur man ingriper i avvikelser samt vad som följer av brytande av dem.
Exempel över god praxis		<p>Användningsreglerna genomgås i orienteringssituationen och de behandlas regelbundet i den skolning som ordnas.</p> <p>Av de personer som har rätt att få uppgifter om centrala företags-hemligheter, upprätthålls en separat förteckning.</p>
Observationer		I skriftliga bruksanvisningar för nät- och kommunikationstjänster kan godkända sätt för användning definieras vitt men identifieringsuppgifter får behandlas med stöd av LDSEK 13 a-k § endast för iakttagande och utredning av olovlig användning av avgiftsbelagda data-samhällstjänster, kommunikationsnät eller kommunikationstjänster, vilken orsakar betydande skada eller olägenhet, eller avslöjande av centrala företags-hemligheter.

Åtgärd 3 Bestämning av identifieringsuppgifternas behandlingspraxis	
Mål	Förvaltningsanvisningar för missbruk har utarbetats och utbildats
Åtgärd 3.1	<p>Identifiera och bestäm</p> <ul style="list-style-type: none"> - de centrala företagshemligheterna vars olovliga avslöjande m.h.a. kommunikationsnät eller kommunikationstjänst vill förebyggas och utredas eller - de organisationens anvisningar och praxis för vars efterlevnad nätets övervakning används eller det är nödvändigt att ta i bruk (de användningssituationer som strider mot anvisningarna för organisationens kommunikationsnät och kommunikationstjänster) samt - de kommunikationsnät som sammanslutningsabonnenten förvaltar eller som förvaltas för dennes del, vars lagrade identifieringsuppgifter används vid övervakningen av missbruk och - de sammanslutningsabonnentens kommunikationstjänster, som övervakas för att förebygga och utreda missbruk.
Åtgärd 3.2	Namnge klara ansvarspersoner, uppgifter eller verksamhetsenheter för behandlingen av identifieringsuppgifterna, Dessa personer skall sörja för nätets upprätthållande, datasäkerhet och säkerhet.
Åtgärd 3.3	Handled och utbilda handhavarna av identifieringsuppgifterna sakligt.
Åtgärd 3.4	Kartlägg de system som används vid sökning av avvikelser som tyder på missbruk i det automatiska kommunikationsnätet och bestäm de sökkriterier som då används. Sökkriterierna kan grunda sig på meddelandenas storlek, typ, kontaktsätt, trafikmängd eller måladresser.
Åtgärd 3.5	Bestäm den manuella praxisen för behandling av identifieringsuppgifter för att utreda missbruk.
Åtgärd 3.6	Bestäm till vem och på vilka förutsättningar identifieringsuppgifter kan lämnas ut. Märk att överföring av identifieringsuppgifter mellan sammanslutningsabonnenten och underleverantören inte är utlämnande av uppgifter, utan databehandling i sammanslutningsabonnentens egen verksamhet.
Exempel på god praxis	<p>Åtgärd 3.1: Bestäm för de olika behandlingssituationerna, om din organisation är en utav kommunikationens parter eller en sammanslutningsabonnent som ordnar kommunikationsmöjligheter.</p> <p>Åtgärd 3.2: Används rollbeskrivningar istället för personliga arbets-</p>

	<p>bilder (se VAHTI 3/2007 bilaga 2: Tietoturvvavastuut rooleittain (endast på finska)).</p> <p>Åtgärd 3.2: Utarbeta med personerna sekretessavtal.</p> <p>Åtgärd 3.2: Definiera kompetenserna, som behövs för genomförandet av identifieringsuppgifternas behandlinguppgifter.</p> <p>Åtgärd 3.3: Utarbeta tillräckligt detaljerade anvisningar för förfarandet vid behandling av identifieringsuppgifter i fall av missbruk.</p> <p>Åtgärd 3.3: Upprätthåll sakenliga lagringar utav skolning, färdigheter, erfarenhet och kvalifikationer.</p> <p>Åtgärd 3.4: Då du anskaffar färdiga programvaror för att övervaka missbruk, säkra dig om att systemet möjliggör</p> <ul style="list-style-type: none"> - efterlevnaden av bestämda behandlingspraxisar samt - svaret på granskningsframställningar gällande identifieringsuppgifter eller deras behandlingshändelser uppgifter. <p>Åtgärd 3.5: Bestäm vem i din organisation som bestämmer om påbörjandet av utredningen eller en annan intern utredning av missbruk. Om tagandet av identifieringsuppgifterna till manuell behandling för att utreda missbruk kan t.ex. en förman som svarar för nätets uppehåll, datasäkerhet eller säkerhet eller en annan förman fatta beslut.</p> <p>Åtgärd 3.5: Sörj för att denna</p> <p>Åtgärd 3.5: Bestäm vem som deltar i utredningen av det iakttagna missbruket.</p> <p>Åtgärd 3.5: Bestäm vem i din organisation som bestämmer om vidtagande av åtgärder för att reagera på missbruk.</p> <p>Åtgärd 3.5: Sammankoppla och innefatta identifieringsuppgifternas behandlings praxis, som sker i syfte att utreda missbruk, i verksamhetsmodellerna och anvisningarna angående den interna utredningen eller reagerande på datasäkerhetens avvikelser.</p> <p>Åtgärd 3.5: Utav de samlade identifieringsuppgifterna sparas utredningskopior på det dataverktyg, till vilket endast de som undersöker missbruket eller deras förmän har tillgång.</p> <p>Åtgärderna 3.1 - 3.6: I en situation gällande utkontraktering skall du som sammanslutningsabonnent sörja för att</p> <ul style="list-style-type: none"> - det med en utomstående tjänsteproducent har noggrant avtalats om vem som övervakar nätet och i vilket syfte, - att en utomstående tjänsteleverantör följer avtalad praxis, - att man har kommit överens om de förfaranden som följs vid överföring av uppgifter
<p>Observationer</p>	<p>En sammanslutningsabonnent får inte behandla uppgifter gällande telefonsamtal, textmeddelanden eller övriga motsvarande meddelanden, till den del som de överförs i fasta eller mobila telefontät-</p>

verk. Detta begränsar dock inte behandling av telefonsamtalsräkningens specifikationsuppgifter i enlighet med 24.2 § i lagen om datskydd vid elektronisk kommunikation.

I utkontrakteringssituationer skall en sammanslutningsabonnent försäkra sig om definierande av den utomstående tjänstegivarens uppgifter och verksamheter.

Sådana sökkriterier som typiskt används i nätets övervakningsverktyg omfattar vitt exempelvis olika datasäkerhetsavvikelser. Då avvikelser som tyder på missbruk söks skall kriterierna bestämmas på ett sätt som begränsar sökningen till endast sådana fall av missbruk som orsakar betydande skada.

Sökningen får inte användas till att få reda på uppgifter som faller under källskyddet.

Den person som beslutar om identifieringsuppgifternas manuella behandling skall bedöma på nytt uppfyllande av förutsättningarna för betydande skada och centrala företagshemligheter för de identifieringsuppgifters del som blir föremål för manuell behandling.

Föremålen för behandling och de identifieringsuppgifter som tas till behandling skall på förhand begränsas från fall till fall m.h.a. de övriga uppgifter som finns i användning. Tidsmässigt kan till behandling tas endast de identifieringsuppgifter som är nödvändiga för att utreda det ifrågavarande fallet.

Behandlingen av identifieringsuppgifter skall avslutas och uppgifterna förstöras då behandlingens ändamål upphör exempelvis då, polisen slutar utredningen av ett fall, arbetsrättsliga åtgärder har förverkligats och fallet har inte lett till en polisundersökning eller det under utredningen framgår att utredningen inte är ekonomiskt meningsfull (har inte lösts eller förts till polisen inom en viss tid).

Åtgärd 4 Informera	
Mål	Informationen är organiserad och ansvaras för
Åtgärd 4.1	Bestäm vem/vilka som svarar för delgivningar och anmälningar samt för samlandet av de uppgifter som behövs vid dem.
Åtgärd 4.2	<p>Bestäm vem som informeras om:</p> <p>1) Informera på förhand, då behandlingsrättigheter för identifieringsuppgifter tas i bruk;</p> <p>a) användarna i sammanslutningsabonnentens datanät,</p> <p>b) de som behandlar företagshemligheter,</p> <p>c) dataombudsmannen.</p> <p>2) Informera i efterhand, då identifieringsuppgifter har behandlats manuellt;</p> <p>a) kommunikationsnätets användare vars identifieringsuppgifter har behandlats manuellt (bör också informeras till föremålen för behandling, vilka inte är sammankopplade till misstankar om missbruk) och</p> <p>b) arbetstagarnas representanter samt</p> <p>c) dataombudsmannen.</p>
Åtgärd 4.3	<p>Bestäm vad som informeras:</p> <p>1. Informera på förhand;</p> <p>a) förfarandenas grunder och praxis som följs vid behandlingen av identifieringsuppgifter,</p> <p>b) omständigheterna och grunderna på basis av vilka en automatisk eller manuell behandling vore möjlig,</p> <p>c) uppgifterna i vilka identifieringsuppgifter kan behandlas samt</p> <p>d) besluten som fattas i samarbetsförhandlingar.</p> <p>2. Information i efterhand till föremålet för behandlingen;</p> <p>a) grunderna, tidpunkten och längden på behandlingen av identifieringsuppgifterna,</p> <p>b) orsaken för vilken behandlingen av identifieringsuppgifterna har påbörjats</p> <p>c) behandlarna och</p> <p>d) den person som har fattat beslut om behandlingen.</p> <p>3. En årlig utredning till arbetstagarnas representant och dataombudsmannen;</p> <p>a) mängden behandlingsgånger för identifieringsuppgifternas manuella behandling och grunderna.</p>
Åtgärd 4.4	<p>Planera informationsprocessen, hur informeras:</p> <p>1. Information på förhand</p>

	<ul style="list-style-type: none"> a) reservera arbetstagarna och deras representanter en möjlighet att bli hörda (om du omfattas av samarbets-skyldigheten), b) informera arbetstagarna om övervakningens syfte, ibruktagande och de metoder som då används samt om användningen av e-posten och datanätet satm c) överväg hur alla får vetskap om bruksanvisningarna och övervakningsmekanismerna. <p>2. Information i efterhand till föremålet för behandlingen;</p> <ul style="list-style-type: none"> a) sörj för att alla som deltar i övervakningen undertecknar den utredning som ges till användaren av nätverket. b) Skicka den utredning som du har gjort till personen/personerna vars identifieringsuppgifter har behandlats, när det är möjligt utan att äventyra behandlingens syfte. c) Spara utredningen i 2 år. d) Utarbeta en registerbeskrivning i enlighet med personuppgiftslagens (523/1999) 10 § över alla utredningar som har sparats och håll den tillgänglig för alla. <p>En årlig utredning till arbetstagarnas representanter och dataombudsmannen görs endast då identifieringsuppgifter har behandlats manuellt under året.</p>
<p>Exempel över god praxis</p>	<p>Åtgärd 4.3, underpunkt 2: Över all verksamhet gällande utredning av iakttagna missbruk, inklusive behandling av identifieringsuppgifter, förs en händesedagbok, i vilken antecknas åtgärder, tidpunkter, beslut</p> <p>Åtgärd 4.3 underpunkt 2: Utarbeta grundmodeller för den utredning som ges i efterhand över den manuella behandlingen av identifieringsuppgifterna. Mer detaljerad information om den givna utredningens innehåll finns senare på sid 16, i utredning och åtgärder - kapitlets nedre del B.</p> <p>Åtgärd 4.4 underpunkt 1: Sammanslutningsabbonenten kan välja sätt att informera. Skriftlig information förebygger bevisningsproblem.</p> <p>Åtgärd 4.4 underpunkt 2: Utredningen delges den som misstänks för missbruk personligt å polisens eller den behöriga förmannens vägnar (personalavdelningens representants närvaro enligt organisationens interna anvisningar). Till de föremål för behandling av identifieringsuppgifter, som inte enligt utredningen hade att göra med den misstänktes missbruk, kan delges t.ex. genom e-post.</p>
<p>Observationer</p>	<p>Tidpunkten för uppgörande av den utredning som skall ges till dataombudsmannen årligen räknas från den tid då till dataombudsmannen har skickats förhandsanmälan eller från den föregående årsanmälan. Förutom den manuella behandling som har avslutats under året skall ur utredningen framgå också de behandlingar av identifieringsuppgifter som under det ifrågakvarande året har pågått eller som</p>

	möjligtvis har påbörjats redan tidigare.
Hjälpmedel och modeller	Modellblanketter för anmälningar som skall göras till dataombudsmannen hittas på adressen http://www.tietosuoja.fi/50005.htm och registerbeskrivning jämte ifyllningsanvisningar på adressen http://www.tietosuoja.fi/50001.htm

Utredning och åtgärder

Då man börjar utreda ett iakttaget olovligt avslöjande av en företagshemlighet eller börjar reagera på en iakttagen avvikelse i datanätet, är behandlingen av identifieringsuppgifter endast ett medel av flera möjliga. Representanter för dataförvaltningen, säkerhetsåtgärderna eller den interna granskningen, vilka deltar i utredningen skall med stöd i sin yrkeskunskap bedöma behovet av behandling av identifieringsuppgifter i enskilda fall och sörja för att identifieringsuppgifternas behandling är sakenlig med hänsyn till den praxis och de anvisningar som organisationen har utfärdat.

A. Då du har märkt en avvikelse i datanätet

- 1) bedöm avvikelens möjliga inverkan på datanätet och dess anordningars funktion (analys av situationen);
 - a) hur omfattande är avvikelsen och hur snabbt sprider den sig,
 - b) vad är dess inverkan på verksamheten och hurudan skada har uppstått eller kommer sannolikt att uppstå (t.ex. uppgifternas eller tjänsternas åtkomst, uppgifternas konfidentialitet eller riktighet, systemets helhet, ekonomiska skador eller hot om skada, personskador),
- 2) om avvikelsen hotar nätets eller dess anordningars datasäkerhet skall du vidta omedelbara åtgärder för att avvärja hotet eller för att begränsa dess inverkan (avstängning av måladresser; LDSEK 20 §);
- 3) bedöm om det är frågan om ett fel som härstammar från systemet eller om mänsklig verksamhet;
- 4) om avvikelsen orsakas av missbruk, bedöm om utredningen skall fortsättas;
- 5) avväg om det finns skäl att misstänka brott (uppfylls brottets rekvisit) och ta kontakt med polisen.

Utred ditt uppdrags gränser - hur långt bestämmer du självständigt om dina åtgärder och när bör du konsultera din förman.

Ta i utredningen med de behövliga medverkarna från organisationens olika enheter på ett specifikt bestämt sätt.

B. När missbrukets utredning inleds, bestäm och anteckna

- 1) vad utreds (hurudan avvikelse/störning är det fråga om; är det fråga om olovliga användning av en misstänkt avgiftsbelagd datasamhällestjänst, ett kommunikationsnät eller en kommunikationstjänst, avslöjande av en företagshemlighet eller orsakande av annan fara för databehandlingen)
- 2) 2.hur har avvikelsen/störningen/det möjliga missbruket eller dataläckaget iakttagits:
 - a) en automatisk sökningsfunktion iakttog avvikelsen i kommunikationen
 - b) tjänstens användningskostnader har stigit ovanligt mycket,
 - c) en företagshemlighet har offentliggjorts eller den används olovligt,
 - d) en anordning, ett program eller en tjänst som inte hör dit har uppmärksamats i datanätet,
 - e) annan motiverad omständighet som kan jämföras med de ovan nämnda (individualisera)

- 3) har hänt när och var
- 4) till vilket system eller vilken uppgift riktar sig avvikelserna: bedöm och anteckna
 - a) är det fråga om en central företagshemlighet; hur är den central (på basis av de kriterier som organisationen har bestämt),
 - b) är det fråga om en uppgift som faller under källskyddet
- 5) vem är ansvarig för detta system eller denna uppgift
- 6) individualisera systemen, vars identifieringsuppgifter behandlas (organisationens e-post, nätsidor, interna nätets tjänster, någonting annat)
- 7) vem har beslutat om utredningen och vem behandlar identifieringsuppgifterna samt av vem får man mera information om de ovan nämnda iakttagelserna (kontaktuppgifter)
- 8) vems identifieringsuppgifter behandlas; samla vid behov namnen på utredningens föremål till en separat lista.
- 9) när har utredningen påbörjats och när avslutats.

Frågor och svar

Skadeprogram

Fråga: Får upprätthållaren söka i datorer som har blivit angripna av skadeprogram från datakommunikationsloggar m.h.a. den kommunikation som är kännetecknande för skadeprogrammet?

Fråga: En utomstående part meddelar att sammanslutningsabonnentens datanäts anordning sprider ett skadeprogram. Får den ifrågavarande anordningen utredas från datakommunikationens logg?

Svar: Båda är sådana datasäkerhetsåtgärder som omfattas av LDSEK 20§.

Fråga: En viss användare får fortlöpande skadeprogramms vidhäftning på sin dator. Får sammanslutningsabonnenten från datakommunikationsloggen utreda vilka internetsidor som användaren besöker?

Svar: Ifall besökandet av de ifrågavarande internetsidorna är förbjudet i uppförandekodexen och användaren har sakentligt informerats om det, kan man med stöd i LDSEK 13 § utreda om användaren har besökt de förbjudna sidorna.

Phishing

Fråga: Får sammanslutningsabonnenten filtrera uppgifter i vilka användarna försöker luras till att avslöja sammanslutningsabonnentens uppgifter till utomstående?

Svar: Ja, som en datasäkerhetsåtgärd i LDSEK 20 §.

Fråga: Får sammanslutningsabonnenten utreda vilken användare som emottog meddelandet, med vilket användaren försöks luras till att avslöja företagshemligheter till utomstående?

Svar: Om det i meddelandet försöktes snokas uppgifter om betalningsförbindelser eller uppgifter som kan användas till äventyrande av sammanslutningsabonnentens kommunikationstjänsters datasäkerhet eller kommunikationsmöjligheter, kan meddelandenas mottagare med beaktande av de allmänna behandlingsreglerna för identifieringsuppgifter utredas med stöd i LDSEK 20 §. Om det i meddelandet försöks snokas efter sammanslutningsabonnentens företagshemligheter, får meddelandenas mottagare utredas med stöd i LDSEK 13 § i övriga fall än de som ovan anfördes.

Fråga: Får sammanslutningsabonnenten utreda från kommunikationens logg de användare som svarade på ett phishing-meddelande och stänga deras lösenord för den tid som ärendet utreds?

Svar: Om det i kommunikationen försöktes snokas efter uppgifter som kan användas för äventyrande av sammanslutningsabonnentens kommunikationstjänsters datasäkerhet eller kommunikationsmöjligheter kan sammanslutningsabonnenten vidta säkerhetsåtgärder

med grund i LDSEK 20 §. Om phishing-meddelandets innehåll var annat, sker utredningen med grund i LDSEK 13 §.

Störande i externa tjänster

Fråga: får sammanslutningsabonnenten utreda vilken användare som har stört en tredje part i nättjänst?

Svar: Användarnas missbruk i externa tjänster kan utredas enligt LDSEK 13 a §, när verksamheten klart strider mot de sakenligt utarbetade användarnas handledning. En användare som stör en tredje parts nättjänst kan identifieras i vissa situationer också med stöd i LDSEK 20 §, om de ramar som kommunikationsverkets ställningstagande 268/64/2919 anger uppfylls (se bilaga 1).

Viestintäviraston arvion mukaan muiden käyttäjien viestintäpalvelun käyttömahdollisuuksia merkittävästi ja välittömästi rajoittavan käyttäjän toimia voidaan pitää sähköisen viestinnän tietosuojalaissa tarkoitettuna tietoturvatyökaluun ryhtymiseen oikeuttavana viestintäpalvelulle haittaa aiheuttavana häiriönä. Tietoturvatyökaluun ryhtymistä voidaan pitää perusteltuna myös viestintäpalvelun muiden käyttäjien viestintämahdollisuuksien turvaamiseksi.

Arvioitaessa käyttömahdollisuuksien rajoittamisen merkittävyyttä, on huomiota kiinnitettävä ainakin siihen, että toimilla saavutettavan hyödyn on oltava olennaisesti luottamuksellisen viestin suojalle aiheuttavaa haittaa suurempi. Arvioinnissa on syytä kiinnittää huomiota ainakin kohteena olevan palvelun merkittävyyteen sekä mahdollisten rajoitustoimien todennäköisyyteen ja vaikuttavuuteen käyttäjien keskuudessa.

Arvioitaessa käyttömahdollisuuksien rajoittamisen välittömyyttä, on huomiota kiinnitettävä rajoitustoimenpiteiden toteutumisen todennäköisyyteen. Välittömyyden arviointi perustuu tyypillisesti käsittelytarvetta arvioivan toimijan omaan kokemukseen rajoitustoimenpiteiden todennäköisyydestä. Jo aloitettujen rajoitustoimenpiteiden osalta ei välittömyysarviointia tarvitse tehdä. Viestintäviraston tulkinnan mukaan kolmannen osapuolen palvelussa häiriköivät käyttäjät voidaan tunnistaa tunnistamistietoja käsittelemällä yllä kuvatut reunaehdot huomioiden. Tunnistamistietojen käsittelyn edellytyksenä on kuitenkin aina se, että käsittelyn tavoitetta ei voida saavuttaa millään muulla tavoin. Viestintämahdollisuuksien rajoittamista lievempänä toimenpiteenä käyttäjä voidaan vain tunnistaa yhteydenottoa varten.

Skräppost

Fråga: Får sammanslutningsabonnenten filtrera skräppost?

Svar: Ja. (LDSEK 20 §)

Fråga: Får sammanslutningsabonnenten utreda den användare som skickar skräppost från dennes datanät?

Svar: När sändandet av skräppost är förbjudet i sammanslutningsabonnentens uppförandecodex, kan efterlevnaden av förbudet övervakas enligt LDSEK 13 a §. Om den stora mängden avsänd skräppost märkbart försvagar kommunikationstjänstens användning, kan användaren få utredas också för att sörja för datanätets datasäkerhet (LDSEK 20 §).

Fråga: Får sammanslutningsabonnenten utreda och isolera den dator från sitt nätverk, vilken skickar skräppost och vilken antagligen har nedsmutsats av ett skadeprogram?

Svar: Ja. (LDSEK 20 §)

Tjänster som användarna har installerat

Fråga: Får en sammanslutningsabonnent med hjälp av datakommunikationens identifieringsuppgifter från sitt nätverk söka tjänster, så som fil- och www-servrar, P2P-trackers eller trådlösa basstationer, som har installerats i strid med anvisningarna?

Svar: Om tjänsterna stör datanätets andra anordningar eller stör betydligt datanätets kommunikationstjänsters användning eller annars tydligt äventyrar datanätets datasäkerhet, får de utredas enligt LDSEK 20 § som en datasäkerhetsåtgärd. För övrigt får verksamhet som strider mot anvisningarna utredas med stöd i LDSEK 13 §.

Fråga: Hur är det ifall det är fråga om en olovlig e-posttjänst?

Svar: För sammanslutningen skadlig verksamhet, p.g.a. e-posttjänster som användaren har installerat, borde kunna förhindras m.h.a. datanätets brandmur (outbound SMTP), då spårandet av själva tjänsten är utredning av verksamhet mot anvisningarna, vilket LDSEK 13 § stagar om.

Andra frågor

Fråga: Får underhållaren övervaka kommunikationsnätets trafikmängd (s.k. flow-data) för att iaktta störningar och avvikelser?

Svar: Ja, med stöd av LDSEK 12 a §, får man som statistisk analys göra det, då det inte går att identifiera en enskild användare av den.

Fråga: Får underhållaren granska filer, inloggningsuppgifter eller bokmärken vilka finns på användarens dator för att utreda missbruk?

Svar: LDSEK 13 § behandlar endast behandling av kommunikationens identifieringsuppgifter. Datasystemens interna mekanismer, så som t.ex. inloggningar och datasystemets användnings logguppgifter hör inte till LDSEK 13 a-k §. Historiska uppgifter från nätsurffing är dock sådana identifieringsuppgifter som LDSEK omfattar.

Fråga: Den automatiska sökningens kriterier är för snäva! Får inte misslyckade inloggningsförsök övervakas?

Svar: Sammanslutningsabonnenten är i kommunikationen mellan användaren och sammanslutningens datasystem den andra parten och berättigad till att med stöd i LDSEK 8 § behandla identifieringsuppgifter.

Fråga: Kan sammanslutningsabonnenten genom avtal flytta över skyldigheterna och ansvaren i LDSEK till erbjudaren av datakommunikationstjänsten, m.a.o. utkontraktera övervakningen enligt principen "nycklarna direkt i handen"?

Svar: Sammanslutningsabonnenten svarar alltid för sin verksamhet, men kan enligt huvudregeln genom avtal utkontraktera åtgärder, som denne själv är berättigad till att sköta.