

# Politiet tar opp alle samtaler

Ringer du 02800 blir samtalen tatt opp, uten at du får vite det. Det kan stride mot personopplysningsloven, hevder Datatilsynet.

OLE PETTER BAUGERØD STOKKE

Jages du av en ransmann, ringer du 112. At samtaler til dette nødnummeret blir tatt opp er ikke særlig overraskende. Og at man ikke får beskjed om dette når man ringer, kan rettferdiggjøres med at hvert minutt teller.

Lurer du på hvordan du går frem for å få nytt pass, ringer du 02800. At også disse samtalene tas opp, uten at det opplyses om det, er mer overraskende. Og, ifølge Datatilsynet, sannsynligvis ulovlig.

## SKREVET BREV

— Vi lurert først og fremst på hvorfor de som ringer inn ikke får informasjon, og hva som er formålet med å gjøre opptakene, sier seniorrådgiver Cecilie B. Rønnevik i Datatilsynet på deres nettsider.

Datatilsynet har nå sendt et brev til Politidirektoratet hvor de ber om en avklaring. I brevet påpekes det at personopplysningsloven tilsier at det skal være godt grunnlag for å ta opp telefonsamtaler, samt at man skal ha samtykke fra begge parter. Datatilsynet skriver videre at de ikke kan se at loven opprettholdes så lenge man ikke får opplyst at det blir gjort lydopptak når man ringer 02800.

## POLITIET BEKREFTER

Politidirektoratet skulle egentlig allerede ha svart på brevet, men



FOTO: NARD SCHREURS

**KRITISK:** Cecilie B. Rønnevik i Datatilsynet krever svar fra politiet om potensielle ulovlige lydopptak.

de har nå fått utsatt svarfristen til 26. februar. En pressetalsmann Computerworld får snakket med bekrefter at det gjøres lydopptak av samtalene, og at dette ikke opplyses om til de som ringer inn. Pressetalsmannen vil ikke siteres, men henviser til det som er skrevet på politiets hjemmesider. Talsmannen understreker også at det kun gjøres opptak av samtalene inn til sentralbordet. Bli man satt videre, opphører også lydopptaket.

Vidar Refvik,  
assisterende politidirektør

På politiets utskjulte hjemmesider skrives det følgende om grunnen til opptakene: "Årsaken til at politiet logger sentralbordapparatene er at bombetrusler, meldinger om drap utført av personer i nære relasjoner, tips om vinningskriminalitet og straffbare forhold faktisk kommer langt oftere til distriktets hovednummer eller 02800 enn til nødnummer 112".

## ÅPEN FOR ENDRINGER

— Vi er i dialog med Datatilsynet og de rette personer i egen etat for å få fakta på bordet i denne saken. Dersom det viser seg at politiet bryter personopplysningsloven, vil vi selvsagt endre våre rutiner, sier assisterende politidirektør Vidar Refvik på nettsiden.

OLE.P.B.STOKKE@COMPUTERWORLD.NO



FOTO: ISTOCK

**PROBLEM:** Lagring av persondata i skyen utenfor EU vil kunne bøtelegges.

## Skjær i sjøen for Cloud Computing

Mange er ikke klar over at det knytter seg risiko til lagring i skyen.

Cloud Computing har etter hvert blitt et etablert trendord, som blant annet brukes i forbindelse med lagring av informasjon. Til tross for den svevende ordlyden, er lagringen svært håndfast, noe folk flest i bransjen er klar over. Vi snakker lagring på godt gammeldags «jern». Mange av fordelene knyttet til cloud computing er kjente. Lagringskapasiteten kan blant annet raskt og enkelt utvides eller innskrenkes. Vi tror risikoen knyttet til slik lagring imidlertid er mindre kjent. Det er viktig at kunden vurderer - og begrenser - risikoen før vedkommende velger lagring i skyen.

■ Dagens Cloud Computing løsninger er normalt slik at en ikke har kontroll på hvor opplysningene lagres. Selskapene som tilbyr tjenestene lagrer ofte opplysningene hos en tredjepart, for eksempel hos Amazon.com, som er en av de største tilbydere av slik lagring. Dersom kunden ikke vet hos hvem eller hvor opplysningene lagres, kan kunden heller ikke være sikker på om uvedkommende/uønskede får tilgang eller om informasjonen benyttes til andre formål. De økonomiske konsekvensene kan kunden sikre seg mot gjennom en god avtale. Selve bruddet vil det ikke alltid være like lett å sikre seg mot. Problemet gjelder i og for seg for all lagring hos tredjepart, men problemet kan være større dersom kunden ikke vet hvor informasjonen fysisk lagres. Kunden må også sikre at slik lagring ikke medfører brudd på

regler og prosedyrer for lagring som er fastsatt i det norske lovverk. Dette kan være bokføringsreglens krav om at informasjon skal lagres i Norge, krav i iktforskriften eller det kan være personvernrelaterte lovkrav.

Et eksempel på sistnevnte er de særskilte prosedyrene som norske virksomheter må følge ved overføring av personopplysninger til land utenfor EU/EØS-området etter personopplysningsloven. Disse reglene gjelder gjennom EUs personverndirektiv for hele EU.

■ Behov for sikkerhet og reglene om overføring av personopplysninger til andre land, er antakelig grunnen til at noen leverandører forsikrer om at opplysningene lagres innenfor et nærmere bestemt område, som for eksempel Europa. Uansett vil en slik forsikring gjøre overholdelsen av regelverket enklere for kunden.

Dersom kunden lagrer personopplysninger utenfor EU/EØS-området, og Datatilsynet finner at kunden ikke har hatt tilstrekkelig kontroll eller ikke har fulgt prosedyrene, vil dette kunne få alvorlige følger for omdømmet til virksomheten gjennom negativ mediaomtale. Datatilsynet vil også kunne ilegge vedkommende virksomhet gebyr for brudd på regelverket på over 700.000 kroner.

Arve Føyen og Frode Bergland Bjørnstad, Føyen advokatfirma

« Kunden må også sikre at slik lagring ikke medfører brudd på regler og prosedyrer for lagring som er fastsatt i det norske lovverk.

” Vi lurert først og fremst på hvorfor de som ringer inn ikke får informasjon, og hva som er formålet.  
Cecilie B. Rønnevik, Datatilsynet



## AKTUELT

■ Advokat Arve Føyen er spesialist på it-juss og har jobbet tett på it-bransjen i en årrekke.

