

RIGSPOLITIET

Bilag 1
POLITI

Internt notat

Dato : 7. november 2014
J.nr.: 2014-3400-11
Sagsbehandler : MLY

KONCERNSTYRING
Koncernservice
Center for Beredskabskom-
munikation

E-mail: sine@sikkerhedsnet.dk

Telefon: 45 15 21 65

Sletterrutiner for politiets alarm- og vagtcentralsystemer

Formålet med dette notat er at give overblik over de nuværende sletterutiner for personoplysninger, der opbevares i politiets alarm- og vagtcentralsystemer, herunder radiosystemer.

Herudover redegøres i korte træk for den gældende retlige regulering af området.

1. Kort om systemernes samspil

1.1. *Politiets 112-system*

Politiets 112-system bruges i landets to 2 alarmcentraler, der er placeret hos Østjyllands Politi og Sydsjællands og Lolland Falsters-Politi.

112-systemet består overordnet af en call center softwareløsning (Solidus), der integrerer en 112 software applikation og støtteværktøjer som f. eks. digitale kort.

Politiets alarmcentraler modtager opkald, stedfæster disse og alarmerer relevante beredskaber (herunder politiet) ved elektroniske meldinger.

1.2. *Vagtcentralløsninger*

Politikreds 1-10 og 12

Vagtcentralerne i alle landets politikredse bortset fra København benytter samme vagtcentralløsning – den såkaldte Politiklient – til modtagelse af meldinger fra 112-alarmcentralerne. Politiklienten bruges endvidere til responstidsmålinger.

I vagtcentralløsningen indgår Politiklienten, InterVIEW, der fungerer som vagtcentralernes brugergrænseflade til alarmbehandling. Politiklienten er integreret med et flådestyrings- og navigationssystem, InterVIEW Fleet.

Flådestyrings- og navigationssystemet forener koordinatsæt fra 112-systemet med digitale kort og positioner fra GPS udstyr, som er monteret i visse af politiets køretøjer (Garmin) og terminaler (Motolocator).



Operatøren i vagtcentralen kan på et flådestyringskort vælge skadestedet og et patruljekøretøj. Patruljen kan så navigeres ud til den pågældende opgave ved fremsendelse af data, fx skadestedsadresse, til køretøjets udstyr.

Terma Radiodispatch

Politikredsene 1-10 og 12 benytter en radiodispatchløsning leveret af firmaet Terma. Denne kontrolrumssoftware benyttes til at styre vagtcentralens radio-kommunikation og til at sende korte databeskeder (SDS) til politikøretøjerne. Dette foregår via beredskabernes fælles radionetværk, SINE, og det dertil godkendte radioudstyr.

Københavns Politi

Vagtcentralen i Københavns Politi benytter en særskilt og samlet softwareløsning, disponeringssystemet HS2, som består af en radiodispatch, et flådestyringssystem og et meldeblanketsystem. HS2-systemet er integreret med KR, 118 og digitale kort. I dette system modtages meldinger fra Københavns Brands alarmcentral, der dækker det storkøbenhavnske område.

Anden systemunderstøttelse af vagtcentralerne

Udover de nævnte systemer benytter vagtcentralerne et antal andre systemer, såsom sagsbehandlingssystemet POLSAS, politiets centrale registre m.fl. Anvendelsen af disse systemer behandles ikke i dette notat.

2. Typer af oplysninger

2.1. Politiets 112-system

I 112-systemet behandles oplysninger om anmelderen, herunder anmelders/skadelidtes telefonnummer og typisk navn og adresse, og om hændelsen.

Alarmoperatørerne identificerer skadestedsadresse med evt. koordinatsæt, vælger en årsag/hændelse på en årsagspickliste, og supplerer evt. med yderligere oplysninger i fritekst. Opgaven tidsstemples, og det registreres, hvilke beredskaber opgaven sendes til.

2.2. Vagtcentralløsninger

Politikreds 1-10 og 12

En melding fra 112-systemet indeholder førnævnte oplysninger.



Herudover behandler flådestyringssystemet oplysninger vedr. køretøjers placering og vagtcentralens fremsendelse af beskeder og oplysninger til patruljerne.

Side 3

Terma Radiodispatch

Radiodispatchløsningen registrerer al tale og datakommunikation mellem vagtcentralen og patruljerne.

Københavns Politi

Oplysninger der tilgår Københavns Politis vagtcentral registreres i HS2-systemet på en særlig meldeblanket, der anvendes til intern udveksling af oplysninger.

Meldeblanketten omfatter oplysninger om opgaven/indsatsen og vejledning i opgaveløsningen samt alle telefonopkald og al radiokommunikation mellem vagtcentralen og politiets køretøjer.

Endvidere er der mulighed for at tilknytte GPS-positioner på digitale kort, fx over et gerningssted.

3. Kort om lovgivningens regulering af slettefrister

Persondataloven regulerer bl.a. offentlige myndigheders behandling af personoplysninger, som finder sted helt eller delvis ved hjælp af elektronisk databehandling (it-systemer). De to mest centrale begreber "personoplysninger" og "behandling" skal herefter forstås i overensstemmelse med de legale definitioner i persondataloven.

Personoplysninger dækker over oplysninger, der kan henføres til en fysisk person, fx stemme, navn og løbenummer, ligesom opbevaring, videregivelse og sletning er former for behandling af disse oplysninger.

Persondataloven indeholder bl.a. en række behandlingsregler, der fastlægger hvornår, hvordan og hvilke oplysninger, der må behandles, jf. lovens kapitel 4.

Pligten til at slette lovligt indsamlede personoplysninger følger af § 5, stk. 5, hvorefter personoplysninger ikke må opbevares i identificerbar form i længere tid end nødvendigt af hensyn til de formål, hvortil oplysningerne indsamles eller behandles. Bestemmelsen har til formål at modvirke unødigt dataophobning, som øger risikoen for bl.a. utilsigtet videregivelse og misbrug. En oplysning skal derfor slettes, når den på grund af alder eller af andre grunde har mistet sin betydning for varetagelsen af registerets opgaver.

Det påhviler den dataansvarlige at anmelde behandling (medmindre undtaget) til Datatilsynet og i den forbindelse oplyse tidspunktet for sletning, jf. § 43, stk. 2, nr. 9.



Det er i sagens natur ikke muligt at opstille en generel regel for i hvilket tidsrum opbevaring af identificerbare oplysninger må ske. Dette må afgøres i det konkrete tilfælde.

Datatilsynet opstiller ikke specifikke sletningsfrister, men efterprøver om der på behørig vis er fastsat procedurer for sletning i forhold til formålet med behandlingen.

Det er herefter op til den dataansvarlige at fastsætte sletterutiner og vurdere, hvilke slettefrister, der er nødvendige under iagttagelse af ovennævnte. Opbevaring og behandling skal i øvrigt skal ske under iagttagelse af reglerne i såvel persondatalovens kapitel 11 som sikkerhedsbekendtgørelsen, herunder reglerne om autorisation, adgangskontrol og logning af anvendelse.

Sikkerhedsbekendtgørelsen fastslår desuden, at den dataansvarlige myndighed skal fastsætte instrukser som fastlægger ansvar for og beskriver behandling og destruktion af ud- og inddatamateriale, jf. § 5, stk. 1, 3. pkt., samt fastsætte slettefrister vedrørende samme, jf. § 10, stk. 2 og § 13, stk. 4.

Med baggrund i sikkerhedsbekendtgørelsens regler og sikkerhedsstandarden DS 484 har Rigspolitiet udarbejdet en Sikkerhedshåndbog med interne bestemmelser om sikkerhedsforanstaltninger, gældende for alle politiets it-systemer og it-udstyr.

Rigspolitiet har samtidigt udsendt Rundskrivelse af 9. september 2008 med tre fællesanmeldelser over de anmeldelsespligtige behandlinger af personoplysninger der udføres i medfør af bl.a. politiloven.

Personoplysninger, som senere overgår til konkret sagsbehandling i fx straffesager, vil tilgå andre systemer, hvorefter spørgsmålet om senere arkivmæssig opbevaring reguleres af arkivlovgivningen.

4. Sletterutiner i alarm- og vagtcentralssystemerne

4.1. *Politiets 112-system*

Politiets alarmcentralers behandling af personoplysninger blev anmeldt til Datatilsynet i 2002, hvorved slettefristen blev angivet til 13 måneder fra hændelsestidspunktet. Samtidigt trådte Kundgørelse B nr. 54 "*Politiets PC Alarmcentral (112)*" i kraft.

Af kundgørelsen fremgår det, at der lagres oplysninger i en voicelog og en hændelseslog. Begge indeholder anmeldelsespligtig behandling af personoplysninger.



Hændelsesloggen opbevares i alarmcentralens system og indeholder al data vedrørende henvendelser til alarmcentralen, jf. afsnit 2 ovenfor.

Voiceloggen indeholder al lydkommunikation, der har fundet sted i forbindelse med et opkald til alarmcentralen.

Den 1. december 2004 trådte en ændret kundgørelse i kraft, hvorved reglerne blev ændret, således at data og lydfiler skulle slettes efter 6 måneder.

Slettefristen blev senest ændret ved orienteringsbrev til Datatilsynet i 2006, hvorefter fristen blev ændret fra 13 måneder til 3 måneder fra hændelsestidspunktet. Undtaget er fortsat oplysninger til brug for behandlingen af en straffesag, i hvilket tilfælde arkivreglerne følges.

Det fremgår af slettereglerne i den gældende kundgørelse (senest rettet den 13. marts 2008) pkt. V, at det er politikredsen, hvor alarmcentralen er placeret, der er ansvarlig for sletning. Voice- og hændelsesloggen skal slettes efter 3 måneder fra hændelsestidspunktet.

I praksis er KIT ansvarlig for de servere, der håndterer voiceloggen på al telefoni, 114, vagtcentral og alarmcentral. Sletning af voicelog sker efter 3 måneder.

Efter det oplyste slettes hændelsesloggen i praksis efter 6 måneder.

Sletningerne foregår automatisk.

4.2. Vagtcentralløsninger

Politikreds 1-10 og 12

Flådestyringssystemet og Politiklienten

Af Rundskrivelse af 17. januar 2008, "*Politiets flådestyrings- og navigationssystem*", fremgår det, at der i systemet genereres data, som omfatter information fra 112-systemet om politikøretøjers kørselsforløb samt kommunikation mellem vagtcentralerne og de tilsluttede køretøjer. Disse data logges i systemet, og Rigspolitiet forestår sletning heraf. Sletning af historiske personhenførbare data skal efter Kundgørelsen ske efter 7 dage fra hændelsestidspunktet.

Efter det oplyste er dette på et senere tidspunkt ændret, således at GPS-data fra politiets tjenestekøretøjer i dag anonymiseres i Flådestyringssystemet efter 72 timer.

Andre oplysninger, der sendes i Politiklienten, f. eks.



- Input fra 112-systemerne,
- Adresser eller oplysninger sendt til patruljekøretøjerne,
- Responstidsdata

slettes i dag ikke med et fast interval, men gemmes principielt så længe der er plads på harddisken, muligt i op til 5 år.

I "*Retningslinjer for Politiets Operative Anvendelse af SINE*", 2012, pkt. 7.3 og 7.5, fremgår det, at tracking (logning) i flådestyringen, altså hvordan køretøjer og mobile terminaler har bevæget sig på kortmaterialet, er tilgængeligt i op til 3 døgn til brug for analyser og statistikker. Trackingen er anonym og vil ikke vise brugeren af køretøjet men alene typen af køretøj.

Terma Radio Dispatch og Witness

I "*Retningslinjer for Politiets Operative Anvendelse af SINE*", 2012, pkt. 4.3, omtales to talelogningssystemer på vagtcentralerne, hhv. til korttids- og langtidsoptagelse af radiokommunikation.

Korttidsoptagelse sker i en 24 timers log i selve radiodispatch-applikationen.

Langtidsoptagelse sker i en 3 måneders log i systemet *Witness*, som er opsat på hver vagtcentral. Det kan herefter anvendes til at optage og afspille lyd i op til 3 måneder efter optagelsen har fundet sted.

Al kommunikation på den primær og, den sekundære talegruppe logges, dvs. tale fra terminaler til og fra operatøren i vagtcentralen.

Af pkt. 7.2 følger det, at alle brugere på vagtcentralen må bruge, se og høre data fra SINE-loggen (24 timers log), men at kun udvalgte personer i politikredsene efter lokale aftaler kan indhente oplysninger fra SINE loggen (3 måneders log). Denne log ligger i selve radiodispatchen sammen med relevante tekniske data. Alle data i loggen slettes automatisk efter 3 måneder.

I forhold til korttidsoptagelse, fremgår det i øvrigt af "*T.react Radio Dispatch Brugervejledning v. 2.6.5.*", pkt. 2.3, at lydoptageren på betjeningspladsen automatisk optager al talekommunikation til og fra betjeningspladsen. Der registreres i den forbindelse relevante informationer, såsom tidsregistrering mv., så lydoptagelserne kan identificeres. Lydoptagelserne slettes automatisk i korttidslydoptageren, når de bliver ældre end 24 timer.

Kundgørelse B nr. 18, "*Om politiets radioudstyr*", som senest er rettet den 25. juni 2003, indeholder ikke selvstændig information om sletterutiner.

Københavns Politi



I HS2-systemet lagres alle oplysninger vedrørende en hændelse, som er omfattet af meldeblanketten, dvs. bl.a. GPS-data, lyd og hændelsesdata. Slettefristen for de lagrede oplysninger er som udgangspunkt 3 år.

Flådestyringsoplysninger lagres ligeledes i 3 år.

Det har ikke været muligt at identificere yderligere instrukser omkring sletterutiner i HS2, som administreres af Københavns Politi og KIT.

5. Problemstillinger

Følgende problemstillinger er identificeret:

- Slettefristerne for ens data er forskellig i forskellige systemer
- Der er visse steder uoverensstemmelse sletteregler og praksis
- Sletterutiner, herunder også instrukser til databehandler om opbevaring, må klarlægges ved dokumentation fx skriftligt aftalegrundlag
- Visse gældende slettefrister forekommer meget korte set i en efterforskningsmæssig sammenhæng
- Der er behov for en generel gennemgang og sanering af de gældende regelsæt

6. Bilagsoversigt

- Bilag 1 - Sletterutiner i skematisk oversigt
- Bilag 2 - Oversigt over regulering
- Bilag 3 - Oversigt over leverandøraftaler



Bilag 1 – Sletterutiner i skematisk oversigt

	Politiets Alarmcentraler	Vagtcentralerne i politikreds 1-10, 12		Vagtcentralen i Københavns Politi
Sletterfrister fordelt på indholdstype	112-system (Solidus)	Kontrolrumssoftware (Radio Dispatch)	Politiklienten og Flådestyring (Interview + Fleet)	HS2
• Lyd	3 mdr. (i voicelog)	<ul style="list-style-type: none"> • 24 timer • 3 mdr. (Witness og Terma) 	•	3 år
• Personhenførbare GPS-data	•	•	72 timer	3 år
• Anden personhenførbare data	3 mdr. (i hændelseslog). I praksis 6 måneder.	•	I praksis så længe plads haves, dvs. 5+ år	3 år
Dokumentation/instrukts	<ul style="list-style-type: none"> • Kundgørelse 2008, pkt. V. • Databehandlingsinstruks ukendt 	<ul style="list-style-type: none"> • Retningslinjer for POAS fra 2012, pkt. 4.3 og 7.2 • Brugervejledning, pkt. 2.3 • Slettefrist ikke i kontrakt 	<ul style="list-style-type: none"> • Rundskrivelse 2008 • Retningslinjer for POAS 2012, pkt. 7.3 • Databehandlingsinstruks ukendt 	Databehandlingsinstruks ukendt
Systemejer	CFB (KIT står for daglig drift)	CFB	CFB (KIT står for daglig drift)	Københavns Politi og KIT
Leverandør	NetDesign	Terma	IBS	Systematic
Senest anmeldt/orienteret	Anmeldt til Datatilsynet 2002. Senest orienteret om ændring i 2006	Fællesanmeldelse	Fællesanmeldelse	Fællesanmeldelse
Slette metode	Automatisk	Automatisk	Automatisk	Ukendt

Alle tidsangivelser er fra hændelses-/optagetidspunkt.

Bilag 2 – Oversigt over regulering***Retlig regulering***

- Persondataloven - nr. 429 af 31. maj 2000 med senere ændringer.
- Sikkerhedsbekendtgørelsen - nr. 528 af 15. juni 2000 med senere ændringer
- Bekendtgørelse om undtagelser til anmeldelsespligten - nr. 529 af 15/06/2000
- Vejledning til sikkerhedsbekendtgørelsen - nr. 37 af 02/04/2001
- Vejledning om anmeldelse - nr. 125 af 10/07/2000
- Statsministeriets Sikkerhedscirkulære, nr. 9846 af 21. december 2013

Interne retningslinjer

- "Om politiets radioudstyr" - Kundgørelse B nr. 18, senest rettet den 25. juni 2003.
- "Politiets PC Alarmcentral (112)" - Kundgørelse B nr. 54, senest rettet den 13. marts 2008.
- "Politiets flådestyrings- og navigationssystem" - Rundskrivelse af 17. januar 2008.
- "Retningslinjer for Politiets Operative Anvendelse af SINE" (POAS), opdateres af CFB, senest i 2012 til version 1.1.
- "Politiet og it-sikkerhed" Rigspolitiet, IT og Tele, Sikkerhedshåndbog for politiet (rev. 1.9.2009, ver 6.0)

Brugervejledninger

- "T.react Radio Dispatch Brugervejledning v. 2.6.5", TERMA A/S, senest opdateret 3. december 2013.
- "Vagtcentralen HS København – et overblik", Københavns Politi, IT afd., april 2011.
- "InterVIEW-fleet systemmanual, version 2.4", IBS, 1. oktober 2010.
- "alarm112 Brugervejledning 24-11-2005", IBS, fra november 2005.
- "Quick guide iv politiklient 100205", IBS, fra februar 2005.
- "Måling af responstid på alarm 112-opgaver i politiklienten", Rigspolitiet, fra november 2005.
- "En kort guide til ivNotes", IBS, september 2010.

IT standarder for informationssikkerhed

- DS 484 Dansk Standard for Informationssikkerhed (international best practice)
- ISO-27001 – International IT-sikkerhedsstandard, som statens institutioner fra januar 2014 skal følge i stedet for DS484, jf. Finansministeriets plan "Enkel administration i staten" (2010).



Leverandører

- 112-systemet, Solidus vedligeholdes af NetDesign.
- 112 software applikation er udviklet af Innovative Business Software A/S (IBS).
- Politiklienten, InterVIEW, og flådestyrings- og navigationssystemet, InterVIEW Fleet, er udviklet og vedligeholdes af IBS.
- GPS kortudstyr fra Garmin Ltd.
- Motolocator er leveret af Dansk Beredskabskommunikation A/S (DBK).
- Radio Dispatch er leveret og vedligeholdes af Terma A/S.
- HS2 vedligeholdes af Systematic A/S.

Aftalegrundlag

112-systemet vedligeholdes efter driftsaftale mellem KIT og Koncernindkøb med NetDesign.

Vagtcentralløsningen (Politiklienten og flådestyring) vedligeholdes efter samarbejdsaftale mellem Rigspolitiet og IBS, samt forligsaftale fra 2010 mellem Rigspolitiet og TERMA A/S (Radio Dispatch).

HS2 er udviklet på SKI 17.10 aftale med Roving (Frontline). Nuværende vedligeholdelsesaftale er indgået på SKI 02.18 aftale mellem KIT og Systematic.

