Sagsnr.: 2018-790-0276 Akt: 37 Dok.: 718161 Titel: Fra RP om spm. fra Jesper Tyne...

Fra: BMM001@politi.dk <BMM001@politi.dk>
Sendt: 17. april 2018 09:25
Til: Jakob Spangsberg Lundsager <lnj@jm.dk>
Cc: JGP005@politi.dk; MKR002@politi.dk
Emne: VS: Jesper Tynells 15 spørgsmål af 5 februar 2018_udkast til svar_12032018 (2)

Kære Jakob

Til din orientering er Rigspolitiet tilbage i januar 2018 på baggrund af Tibetkommissionens beretning blevet kontaktet af journalist Jesper Tynell fra P1 med 17 spørgsmål vedrørende sletning af e-mails. Efter Rigspolitiet besvarede disse spørgsmål stillede Jesper Tynell yderligere 15 spørgsmål, som KIT og Databeskyttelsesenheden har udarbejdet vedhæftede udkast til besvarelse af.

Med venlig hilsen

Birgitte Mohr Mersing
specialkonsulent

POLITI

Rigspolitiet
Direktionssekretariatet

Polititorvet 14
1780 København V

Telefon 25168956
E-mail bmm001@politi.dk

Web www.politi.dk
Facebook facebook.com/politi
Twitter twitter.com/rigspoliti

Politiet og Edb-sikkerhed

Må ikke komme til uvedkommendes kendskab.
Skal opbevares på betryggende måde

Rigspolitichefen • Dataafdelingen

Sikkerhedshåndbog for politiet

Politiet
Og
Edb-sikkerhed

Må ikke kommer til uvedkommendes kendskab.
Skal opbevares på betryggende måde.

Rigspolitichefen • Datasafdelingen

Rigspolitichefens
trykkeri
København

Kapitel 9

Retningslinier for anvendelse af elektronisk post internt i politiet

9. 1. Generelle retningslinier

Politiets e-postsystem skal understøtte udførelsen af arbejdsopgaver der henhører under politiet. E-post systemet må ikke anvendes til formål, der er uforenelige hermed.

9. 2. Anvendelse af elektronisk post

9. 2. 1. Elektroniske postkasser

Til medarbejdere med et tjenstligt behov herfor kan der etableret en personlig e-postkasse. Adgang til postkassen skal være beskyttet med adgangskontrol baseret på medarbejderens entydige brugeridentifikation med tilhørende kendeord.

9. 2. 1. 1. Funktionspostkasser

Hvor det skønnes mest hensigtsmæssigt, at e-post sendes til eller fra en gruppe af personer, der varetager en fælles funktion, kan der oprettes en funktionspostkasse.

Adgang til postkassen tildeles medarbejdere efter behov.

Der udpeges blandt medarbejdere tilknyttet funktionspostkassen en postansvarlig. Den postansvarlige skal sikre, at retningslinierne for anvendelse af e-post overholdes.

9. 2. 2. Hvad kan sendes som e-post?

E-post systemet må som hovedregel kun anvendes til at fremsende tjenstlig information, der er relevant for modtageren og, som ikke mere hensigtsmæssigt kan formidles ad andre kommunikationskanaler.

E-postsystemet må ikke anvendes til at oversende sager, der er resultatet af en sagsbehandling i politiets øvrige edb-systemer (f.eks. POLSAS). Sagsoversendelse og fremsendelse af enkelt akter skal ske ved almindelig post eller i hastende tilfælde ved fax. Dette gælder såvel sager og akter, der sendes mellem politikredsene, som internt i politikredsen.

Ved fremsendelse af oplysninger om enkeltpersoners rent private forhold og andre fortrolige oplysninger skal medarbejderen i hvert enkelt tilfælde vurdere, om den, oplysninger sendes til er berettiget til at modtage informationerne. De normale retningslinier for videregivelse af oplysninger om enkeltpersoners rent private forhold og andre fortrolige oplysninger skal iagttages, jf. forvaltningslovens § 28 og 29.

E-post meddelelser, der sendes til en modtager **inden** for afsenderens politikreds kan vedhæftes bilag af intern karakter (eksempelvis udkast til referater o.l).

E-postsystemet kan i begrænset omfang anvendes til korte beskeder af ikke-tjenstlig karakter svarende til den gældende tradition for brug af telefonen til ikke tjenstlige formål. E-post systemet kan eksempelvis bruges ved udveksling af informationer i tilknytning til IPA, politiets idrætsforeninger og faglige organisationer.

9. 2. 3. Behandling af e-post

9. 2. 3. 1. Modtager af e-post

Modtageren af en e-postmeddelelse skal vurdere, om afsenderen af meddelelsen er identificeret i nødvendigt omfang og om meddelelsen fremstår som ægte. Hvis der er tvivl herom, skal modtageren tage personlig kontakt med afsenderen.

E-post meddelelser skal til stadighed fremstå i autentisk form. Modtageren må ikke ændre en modtaget meddelelse.

9. 2. 3. 2. Afsender af e-post

Afsenderen af e-post skal vurdere, om rettidig modtagelse af de fremsendte informationer er vigtig og om nødvendigt søge bekræftelse af, at e-postmeddelelsen er modtaget.

9. 2. 3. 3. Journalisering af e-post

Det påhviler såvel afsender som modtager af en e-post meddelelse at sikre, at alle sagsrelaterede informationer, der afsendes eller modtages som e-post, udskrives på papir, journaliseres og arkiveres efter gældende regler for papirbaseret information.

9. 2. 3. 4. Sletning af e-post

Det påhviler indehaveren af en e-postkasse at sikre, at alle ind og udgående e-post meddelelser, der indeholder sagsrelaterede informationer, slettes senest 30 dage efter afsendelse eller modtagelse. Øvrige e-post meddelelser slettes regelmæssigt.

Den udpegede administrator (jf. pkt. 3) skal foretage kontrol til sikring af, at sletning af sagsrelaterede oplysninger finder sted.

9. 2. 4. Rettigheder til e-postmeddelelser

Ledelsen i politikredsen eller i Rigspolitichefens afdelinger har ret til at se alle e-postmeddelelser, der er modtaget i eller afsendt fra e-postkasser i kredsen/afdelingen. Ledelsen kan bemyndige administratoren - eller efter behov - andre medarbejdere til at gennemse e-post, der er modtaget i eller afsendt fra e-postkasser i kredsen/afdelingen.

9. 2. 5. Tømning af e-postkasser m.v.

9. 2. 5. 1. Gennemgang af modtaget e-post

Medarbejdere med e-postadgang skal løbende og mindst en gang i løbet af en tjenestedag gennemse modtaget e-post. Hvis det på grund af tjenestens tilrettelæggelse ikke er muligt at gennemse e-postkassen som anført, skal den nærmeste foresatte orienteres herom således, at der om nødvendigt kan udpeges en medarbejder til at tømme e-postkassen.

9. 2. 5. 2. Fravær

Ved en medarbejders ferie, sygdom m.v. skal den nærmeste foresatte udpege en medarbejder til

9. 3. Administration af e-postkasser

9. 3. 1. Administratorfunktion

Der skal på hvert tjenestested (politikreds eller Rigspolitichefens afdelinger) udpeges en person, der har ansvaret for administrationen af e-postkasser .

Administratoren har ansvaret for oprettelse og nedlæggelse af postkasser samt håndtering af tekniske problemer. Administratoren skal endvidere føre kontrol med, at sletning af meddelelser i de enkelte postkasser sker i overensstemmelse med fastlagte retningslinier .

9. 3. 2. Fratræden

Fratrådte medarbejderes e-postkasser skal lukkes snarest muligt efter medarbejderens fratræden. Forflyttelse til andet tjenestested udenfor kredsen eller afdelingen betragtes som fratræden.

Den lokale administrator har ansvaret for lukning af e-postkasser.

RIGSPOLITIET

POLITI

Jesper Tynell
Fagmedarbejder, Orientering på P1

Sendt som e-brev til tyne@dr.dk

Dato: 19. marts 2018
Sagsbehandler: Ida Lydolph Bojsen

RIGSPOLITIETS KONCERN IT

Direkte: 2080 2184
E-mail: ilb001@politi.dk
Web: www.politi.dk

Svar på Deres 15 spørgsmål af 5. februar 2018
Ved e-mail af den 5. februar 2018 har De bedt om svar på 15 spørgsmål med udgangspunkt i deres mail af 5. januar med 17 spørgsmål.

Indledningsvist – og i forlængelse af de redegørelser Rigspolitiet tidligere har meddelt Dem telefonisk – kan Rigspolitiet oplyse, at lov nr. 429 af 29. maj 2001 om behandling af personoplysninger (persondataloven) fastsætter under hvilke betingelser, Rigspolitiet og de enkelte politikredse (herefter "politiet") må behandle personoplysninger til formål, der ikke sker i retshåndhævelsesøjemed, herunder behandling af personoplysninger som led i medarbejdernes brug af deres tildelte e-mailkonto.

Persondatalovens § 5 fastsætter en række grundlæggende krav, som enhver behandling af personoplysninger skal efterleve. Lovens § 5, stk. 5, fastsætter, at indsamlede personoplysninger ikke må opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles. Denne bestemmelse fastsætter således en generel retlig forpligtelse for politiet til dels at vurdere, hvor længe det er nødvendigt at opbevare en given samling personoplysninger, dels rent praktisk at sikre, at denne opbevaringsperiode efterleves i praksis. Som det fremgår, er vurderingen efter § 5, stk. 5, skønsmæssig, idet det vil bero på de nærmere omstændigheder, hvor længe en konkret samling af personoplysninger må opbevares. Der er imidlertid ingen tvivl om, at bestemmelsen indeholder en generel forpligtelse for bl.a. politiet– og enhver anden dataansvarlig omfattet af bestemmelsen – til at fastsætte en konkret opbevaringsfrist i overensstemmelse med bestemmelsen og under iagttagelse af lovens øvrige regler. Når den fastsatte frist udløber, skal oplysningerne slettes, hvilket efter persondataloven kan omfatte arkivering i overensstemmelse med arkivlovens regler.

Det bemærkes, at en arbejdsgivers anvendelse af en medarbejders personlige e-mailadresse indebærer behandling af personoplysninger, hvilket også fremgår af den tidligere fremsendte udtalelse fra Datatilsynet.

De øvrige grundlæggende krav i persondatalovens § 5 er navnlig kravene om god databehandlingsskik, saglighed, proportionalitet, datakvalitet og formålsbestemt-

hed. Disse krav skal således ligeledes efterleves, når der fastlægges en konkret slettefrist.

Hertil kommer, at persondataloven indeholder en række nærmere betingelser/hjemler for, hvornår politiet må indsamle og registrere personoplysninger, videregive dem osv. Hvilke hjemler, politiet skal følge i den enkelte situation, afhænger af oplysningernes karakter og formålet med databehandlingen. Hvis der er tale om behandling af følsomme personoplysninger, skal hjemlerne i persondatalovens §§ 7-8 iagttages, hvorimod hjemlen i persondatalovens § 6 skal iagttages, hvis der er tale om behandling af almindelige personoplysninger.

Det ovenfornævnte indebærer, at politiet ikke lovligt kan gemme personoplysninger, hvis eksempelvis det grundlæggende krav om proportionalitet ikke iagttages, eller hvis hjemlen/betingelserne i § 6 for behandling af almindelige personoplysninger ikke iagttages.

Endelig er det værd at bemærke, at de ovenfornævnte grundlæggende krav og juridiske hjemler ikke regulerer spørgsmålet om, hvorvidt politiet *skal* foretage en bestemt behandling af personoplysninger, men kun om behandlingen *kan* eller *må* foretages.

2.1. Foruden det under pkt. 1 anførte indeholder persondataloven et overordnet krav om datasikkerhed. For den offentlige forvaltning – herunder politiet – er dette krav nærmere udmøntet i sikkerhedsbekendtgørelsens regler, hvori der fastsættes en række minimumskrav til sikkerhed ved elektronisk behandling af personoplysninger.

Hvilke regler, der skal efterleves i sikkerhedsbekendtgørelsen, afhænger af, om de behandlede oplysninger er omfattet af anmeldelsespligten til Datatilsynet – altså om oplysningerne er følsomme og/eller fortrolige (dog med undtagelse af CPR-numre).

Som udgangspunkt skal enhver behandling af personoplysninger leve op til sikkerhedskravene i sikkerhedsbekendtgørelsens kapitel 1 og kapitel 2, mens anmeldelsespligtige oplysninger tillige skal iagttage sikkerhedskravene i sikkerhedsbekendtgørelsens kapitel 3.

Kravet om logning (og eventuelle undtagelser hertil) er fastlagt i § 19 sikkerhedsbekendtgørelsens kapitel 3 – og gælder altså kun for anmeldelsespligtige oplysninger.

2.2. Særligt for så vidt angår logning, er udgangspunktet således, at der skal foretages logning af de ovennævnte typer af personoplysninger. Hertil gælder bl.a. undtagelsen i bekendtgørelsens § 19, stk. 2 om, at dokumenter, som foreligger i endelig form, ikke skal logges, hvis der sker sletning inden for en af den dataansvarlige myndighed nærmere fastsat kortere frist.

I vejledningen til sikkerhedsbekendtgørelsen er det til § 19, stk. 2, beskrevet, at *"Bestemmelsen om logning [ikke] gælder færdige dokumenter og lignende, som opbevares en vis kortere periode, inden de - f.eks. efter en fastlagt arbejdsgang - enten slettes eller anonymiseres ved, at alle identifikationsoplysninger, der kan henføre oplysningerne til bestemte personer, fjernes. Den dataansvarlige skal tage stilling til længden af den omtalte kortere periode, der generelt bør være af en størrelsesorden på højst en måned, og udfærdige retningslinier for, hvorledes medarbejderne skal forholde sig."*

Det ovenfornævnte indebærer, at e-mails indeholdende personoplysninger kan opbevares i en kortere periode uden at være omfattet af logning, uden at dette er i strid med sikkerhedskravene i sikkerhedsbekendtgørelsen. Det er dog en forudsætning, at politiet har fastlagt en kortere periode for, hvor længe de pågældende e-mails kan opbevares, som dog ikke må være længere end en måned.

Politiet har på denne baggrund fastsat retningslinjer for medarbejdernes brug af bl.a. e-mail i politiets sikkerhedshåndbog, hvoraf det fremgår, at den enkelte medarbejder har pligt til at påse, at e-mails, der måtte indeholde anmeldelsespligtige personoplysninger, slettes inden 30 dage. Der henvises til politiets sikkerhedshåndbog § 25, som De har fået udleveret uddrag fra i forbindelse med en aktindsigtsanmodning.

Bemærk venligst, at persondatalovens betingelserne for, hvornår politiet må indsamle og registrere personoplysninger, jf. pkt. 1, samt sikkerhedskravene, jf. pkt. 2 gælder sideløbende.

For så vidt angår Deres konkrete spørgsmål, kan politiet herefter oplyse følgende:

1. **Har I logning på jeres e-mail-system, så man kan se, hvilke medarbejdere, der har haft adgang til en medarbejders e-mails?**

Politiet har forstået spørgsmålet således, at der spørges til, om der er logning på e-mailsystemet – således at man kan se hvilke medarbejdere, der har fået tildelt adgang til en anden medarbejderes mailboks.

Politiet kan bekræfte, at politiets e-mailsystem i begrænset omfang har logning, og at det med denne logning er muligt at se hvilke medarbejdere, der har fået tildelt adgang til en anden medarbejders mailboks.

Politiet skal gøre opmærksom på, at den ovennævnte begrænsede logning ikke er en logning som defineret i Sikkerhedsbekendtgørelsens § 19, jf. ovenfor under pkt. 2.1 og 2.2 ovenfor, hvor registreringen mindst skal indeholde oplysning om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium.

2. **Har I logning på jeres back-up-system, så man kan se, hvilke medarbejdere, der har haft adgang til backup af en medarbejders e-mails?**

Politiet har forstået spørgsmålet således, at der spørges til, om det via logningen er muligt at se hvilke medarbejdere, der har haft adgang til en back-up kopi af en anden medarbejders e-mails.

Politiet kan oplyse, at såfremt en back-up kopi af en medarbejders mailboks indlæses, vil det også i dette tilfælde være muligt at se, hvem der har fået tildelt adgang til den indlæste back-up kopi, jf. svar på spørgsmål 1.

3. **Hvis I har logning på jeres e-mail-system, præcis hvad forhindrer jer så rent juridisk i at opbevare tidligere medarbejderes e-mails i længere tid end 30 dage?**

Som tidligere meddelt Dem, er der ikke noget juridisk, som hindrer en opbevaring af oplysninger i længere tid end 30 dage, så længe opbevaringen sker inden for de rammer, der er beskrevet under pkt. 1 og pkt. 2 i indledningen ovenfor.

Praksis i politiet har siden 2005 været, at mail-systemet ved en medarbejders fratrædelse automatisk sletter den pågældende medarbejderes mailboks 30 dage efter fratrædelsesdatoen.

4. **Hvis I har logning på jeres back-up-system, præcis hvad forhindrer jer så rent juridisk i at opbevare back-up af tidligere medarbejderes e-mails i længere tid end 30 dage?**

Se ovenfor under svaret til spørgsmål nr. 3.

5. **Hvis I har logning på jeres back-up-system, præcis hvad forhindrer jer så rent juridisk i at opbevare back-up af nuværende medarbejderes e-mails i længere tid end 30 dage?**

Se ovenfor under svaret til spørgsmål nr. 3.

6. **Hvis I ikke har logning på jeres mail-system, hvorfor indfører I så ikke det?**

Se ovenfor under svaret til spørgsmål nr. 1.

7. **Hvis I ikke har logning på jeres back-system, hvorfor indfører I så ikke det?**

Se ovenfor under svaret til spørgsmål nr. 2.

8. **Er I enige i, at I ville kunne opbevare emails i længere tid end nu, hvis I havde logning på jeres mailsystemer?**

Henset til, at Justitsministeriet har iværksat en proces med henblik på nærmere at vurdere praksis og de retlige rammer for offentlige myndigheders opbevaring af e-mails fra fratrådte medarbejdere mv., finder politiet ikke anledning til at udtale sig nærmere herom.

9. Er I enige i, at I ville kunne opbevare back-up af emails i længere tid end nu, hvis I havde logning på jeres back-up-systemer?

Henset til, at Justitsministeriet har iværksat en proces med henblik på nærmere at vurdere praksis og de retlige rammer for offentlige myndigheders opbevaring af e-mails fra fratrådte medarbejdere mv., finder politiet ikke anledning til at udtale sig nærmere herom.

10. Svaret på spørgsmål 9 begrunder I med henvisning til Datatilsynets praksis for, hvor længe man må gemme og behandle fratrådte medarbejderes mails. Hvilken praksis fra Datatilsynet er her tale om? (Når jeg spørger, er det fordi, den udtalelse fra Datatilsynet, I henviser til i svaret på spørgsmål 9, intet siger op tiden for opbevaring af gamle mails, men alene udtaler sig om, hvor længe man må holde en fratrådt medarbejders mailkonto åben for at modtage nye mails).

Henset til, at Justitsministeriet har iværksat en proces med henblik på nærmere at vurdere praksis og de retlige rammer for offentlige myndigheders opbevaring af e-mails fra fratrådte medarbejdere mv., finder politiet ikke anledning til at udtale sig nærmere herom.

11. Når I svarer "Nej (…) næppe" på spørgsmål 10 og i svaret på spørgsmål 16 skriver, at "Det er der ikke hjemmel til i loven", hvilket hjemmelsgrundlag mener I så helt præcist forhindrer jer i at opbevare en back-up af fratrådte medarbejderes e-mails i fx 5 eller 10 år?

Henset til, at Justitsministeriet har iværksat en proces med henblik på nærmere at vurdere praksis og de retlige rammer for offentlige myndigheders opbevaring af e-mails fra fratrådte medarbejdere mv., finder politiet ikke anledning til at udtale sig nærmere herom.

12. Når I svarer "Nej (…) næppe" på spørgsmål 10 og i svaret på spørgsmål 16 skriver, at "Det er der ikke hjemmel til i loven", hvilket hjemmelsgrundlag mener I så helt præcist forhindrer jer i at opbevare en back-up af nuværende medarbejderes e-mails i fx 5 eller 10 år?

Henset til, at Justitsministeriet har iværksat en proces med henblik på nærmere at vurdere praksis og de retlige rammer for offentlige myndigheders opbevaring af e-mails fra fratrådte medarbejdere mv., finder politiet ikke anledning til at udtale sig nærmere herom.

13. Når I svarer, at der "var en uensartet praksis på området fra kreds til kreds" i svaret på spørgsmål 5, vil jeg gerne spørge helt specifikt til, hvordan praksis for opbevaring var for hhv. nuværende og tidligere medarbejdere ansat hos hhv. Københavns Politi og hos Rigspolitiet. Hvordan var praksis for opbevaring af hhv. daværende og tidligere ansatte hos disse to myndigheders e-mails (Københavns Politi og Rigspolitiet), før de nuværende retningslinjer blev hhv. implementeret i 2012 og før de nuværende retningslinjer fra 2010?

Politiet er blevet opmærksom på, at svaret på Deres spørgsmål nr. 2, 4, 5, og 6 af den 17. januar 2018 ikke var fyldestgørende. På baggrund af en yderligere gennemgang af historikken forbundet med retningslinjerne for sletning af fratrådte medarbejderes mailkonti kan politiet oplyse, at der også før 2012 eksisterede retningslinjer på området. Politiet sender derfor nedenstående historiske gennemgang.

Gennemgangen skal ses som en uddybning og præcisering af Deres spørgsmål nr. 2, 4, 5, og 6 af den 17. januar 2018 samt som besvarelse af spørgsmål nr. 13 af 5. februar 2018.

Retningslinjer og praksis for sletning af e-mails for fratrådte medarbejdere ved politiet

I september 1992 besluttede Rigspolitichefens Centrale Teknologiudvalg, at der på grund af den stærkt øgede anvendelse af edb-teknologi i politiet skulle udarbejdes en edb-Sikkerhedshåndbog som et hjælpemiddel for de enkelte politimyndigheder.

Sikkerhedshåndbogen blev distribueret til alle politikredse og til Rigspolitichefens afdelinger. Af den reviderede (version 2.0) edb-Sikkerhedshåndbog fra 2000[1] fremgår af retningslinjerne for sletning af e-mails, at det påhvilede den enkelte indehaver af mailboks at sikre, at alle ind- og udgående e-mails, der indeholdt sagsrelaterede informationer, blev slettet senest 30 dage efter afsendelse eller modtagelse. Øvrige e-mails skulle indehaveren af mailboksen slette regelmæssigt, jf. den daværende edb-Sikkerhedshåndbog.

Det var den kredslokale administrators ansvar at føre kontrol med, at sletning af meddelelser i de enkelte mailbokse skete i overensstemmelse med de fastlagte retningslinjer. Det fremgår endvidere af edb-Sikkerhedshåndbogen, at fratrådte medarbejderes mailbokse skulle lukkes snarest muligt efter medarbejderens fratræden, og at dette ansvar påhvilede den kredslokale administrator. Det fremgår slutteligt af edb-Sikkerhedshåndbogen, at det var en forudsætning for anvendelse af politiets centrale registre, at Sikkerhedshåndbogen blev sat i kraft i politikredsene og Rigspolitichefens afdelinger.

Det har desværre ikke umiddelbart været muligt for politiet at genfinde de beslutningsdokumenter, der ledte op til Rigspolitichefens Centrale Teknologiudvalgs be-

[1] Politiet har som bilag 1 til indeværende e-brev vedlagt et uddrag fra denne udgave af Edb-sikkerhedshåndbogen.

slutning om, at de ansatte skulle slette e-mails, der indeholdte sagsrelaterede informationer, senest 30 dage efter afsendelse, og at fratrådte medarbejderes mailbokse skulle lukkes snarest muligt efter medarbejderens fratrædelse. Referatet fra mødet er enten bortkommet eller arkiveret i Statens Arkiver. Såfremt De ønsker, at politiet undersøger, hvorvidt referatet er arkiveret i Statens Arkiver, bedes De anmode politiet herom via en ny aktindsigtsanmodning.

I 2005 fik politiet et landsdækkende e-mail system. Før 2005 havde hver enkelt kreds deres eget mailsystem, som kun kunne sende mails internt i kredsen.

I perioden 2004-2008 implementerede politiet et it-system til styring af brugeridentitet og brugergrupper på tværs af politiets systemer. I denne periode blev der indført automatisk sletning af fratrådte medarbejderes mailbokse 30 dage efter medarbejderens fratrædelse. Imidlertid skulle den automatiske proces igangsættes af den lokale systemadministrator i kredsen, som skulle notere i systemet, at medarbejderen havde fratrådt sin stilling. Oplysningen om fratrædelse blev givet af den lokale personaleafdeling. Processen var som beskrevet lokalt forankret og blev forvaltet uensartet i kredsene.

Nuværende retningslinjer for sletning af e-mails for fratrådte medarbejdere ved politiet

I 2011 blev personaleadministrationen i politiet centraliseret hos Rigspolitiets Koncern HR. I forbindelse med centraliseringen blev der implementeret kontroller, som sikrer, at alle fratrådte medarbejdere rettidigt registreres som fratrådte i politiets personalesystem. Når Koncern HR har markeret en medarbejder som fratrådt, igangsætter politiets it-systemer automatisk, at den fratrådte medarbejderes mailboks slettes 30 dage efter fratrædelse.

Retningslinjer og praksis for sletning af e-mails for ikke-fratrådte medarbejdere ved politiet

Det fremgår af "Driftshåndbogen til Rigspolitiets Windows miljø" af 24. september 2008, at der tidligere har været begrænsning på størrelsen af den enkelte medarbejders mailboks. En mailboks kunne dengang maksimalt fylde 50 Mb. Når grænsen blev nået, kunne medarbejderen ikke længere afsende e-mails. Medarbejderen modtog en advarsel, når mailboksen fyldte 45 Mb, og var da nødsaget til at slette mails fra mailboksen for igen at kunne afsende e-mails. Når medarbejderen slettede en slettet e-mail (e-mailen var opbevaret i mailboksen "slettet post"), kunne medarbejderen genskabe denne i syv dage efter sletning. Alle slettede e-mails blev automatisk slettet af systemet efter 30 dage.

Nuværende retningslinjer for sletning af e-mails for ikke-fratrådte medarbejdere ved politiet

I 2012 blev databegrænsningen på medarbejderes mailboks fjernet, ligesom reglen om, at alle slettede e-mails automatisk blev permanent slettet efter 30 dage blev fjernet. Herefter er proceduren den, at alle e-mails gemmes, indtil medarbejderen fratræder, hvorefter vedkommendes mailboks slettes permanent 30 dage efter me-

darbejderens fratrædelse. Undtagelsen til ovenstående forekommer i det tilfælde, hvor medarbejderen af egen drift permanent sletter en e-mail (når e-mailen slettes fra mailboksen "slettet post"). I dette tilfælde slettes den pågældende e-mail efter 30 dage, og kan ikke længere fremsøges. Medarbejderen har imidlertid mulighed for at genskabe den permanent slettede e-mail i 30 dage efter sletning.

Afsluttende bemærkning

Politiet beklager på baggrund af ovenstående gennemgang, at politiet ikke i besvarelsen af Deres spørgsmål nr. 15 af den 17. januar 2018, formulerede svaret med tilstrækkelig tydelighed. Svaret på deres spørgsmål er således: "(...) Nuværende medarbejderes e-mails slettes ikke af Rigspolitiet som arbejdsgiver, men der sker løbende sletning efter 30 dage, når den enkelte medarbejder selv sletter en mail fra sin mailboksen "slettet post"".

14. **Når I svarer, at der "var en uensartet praksis på området fra kreds til kreds" i svaret på spørgsmål 5, vil jeg gerne spørge helt specifikt til, hvordan praksis var for backup for hhv. nuværende og tidligere medarbejdere ansat hos hhv. Københavns Politi og hos Rigspolitiet. Hvordan var praksis for opbevaring af backup af hhv. daværende og tidligere ansatte hos disse to myndigheders e-mails (Københavns Politi og Rigspolitiet), før de nuværende retningslinjer blev hhv. implementeret i 2012 og før de nuværende retningslinjer fra 2010?**

Politiet er blevet opmærksom på, at svaret på Deres spørgsmål nr. 12 den 17. januar 2018 ikke er korrekt. Politiet beklager dette.

Siden 2005, hvor politiet fik et landsdækkende mail system som nævnt under svar til spørgsmål 13, har politiets mailsystem været sat op til at tage en automatisk backup af alle medarbejderes mailbokse. Denne backup gemmes i 14 dage, hvorefter den slettes.

Når en medarbejder fratræder, vil vedkommendes mailboks som tidligere beskrevet automatisk blive slettet 30 dage efter fratrædelsen. Eftersom der tages en automatisk backup af alle medarbejderes mailbokse hver 14. dag, vil en fratrådt medarbejders mailboks således kunne genskabes i 44 dage efter fratrædelse.

15. **Hvornår forventer I at besvare den begæring om aktindsigt, jeg sendte jer den 17. januar 2018?**

De modtog svar på Deres aktindsigtsanmodning den 20. februar 2018.

Afsluttende bemærkning til Deres henvendelse af 5. februar 2018

På baggrund af Tibet-kommissionens bemærkninger vedrørende sletning af e-mails har politiet igangsat en revurdering af procedurerne for sletning af fratrådte medarbejderes e-mails samt af hvor længe back-up'en af alle medarbejderes mailbokse gemmes.

Med venlig hilsen

Ida Lydolph Bojsen
Specialkonsulent
Koncern IT, Landlystvej 34, 2650 Hvidovre

Mobil: 2080 2184
Mail:ilb001@politi.dk

RIGSPOLITIET