



JUSTITSMINISTERIET

Dato: 30. april 2019  
Kontor: Sikkerhedskontoret  
Sagsbeh: Maja Elkjær Tarpgård  
Sagsnr.: 2017-0094-0833  
Dok.: 903327

## UDKAST

### **Bekendtgørelse om Politiets Efterretningstjenestes behandling af oplysninger om fysiske og juridiske personer m.v. og om sikkerhedsforanstaltninger til beskyttelse heraf**

I medfør af § 7, stk. 2, § 8, stk. 2, § 9 a, stk. 3, og § 14, stk. 2, i lov om Politiets Efterretningstjeneste (PET), jf. lovbekendtgørelse nr. 231 af 7. marts 2017, som ændret ved lov nr. 503 af 23. maj 2018 og lov nr. 1706 af 27. december 2018, fastsættes:

#### Kapitel 1

##### *Politiets Efterretningstjenestes journaler, databaser mv.*

**§ 1.** Politiets Efterretningstjeneste fører elektroniske journaler med sager vedrørende efterretningstjenestens virksomhed.

*Stk. 2.* Politiets Efterretningstjeneste skal senest 10 år fra sagsoprettelsen i en elektronisk journal slette oplysninger om fysiske og juridiske personer, der ikke er omfattet af § 9, stk. 1, i lov om Politiets Efterretningstjeneste.

*Stk. 3.* Politiets Efterretningstjenestes egne personalesager og sager om personsikkerhedsundersøgelser er ikke omfattet af stk. 2.

*Stk. 4.* Sletning efter stk. 2 kan undlades, hvis væsentlige hensyn til varretagelsen af Politiets Efterretningstjenestes opgaver gør det nødvendigt. Efterretningstjenesten underretter Tilsynet med Efterretningstjenesterne om en beslutning om at undlade sletning.

**§ 2.** Politiets Efterretningstjeneste kan føre særlige databaser i tilknytning til efterretningstjenestens operative og administrative opgaver.

Slotsholmsgade 10  
1216 København K.

T +45 7226 8400  
F +45 3393 3510

www.justitsministeriet.dk  
jm@jm.dk

*Stk. 2.* Politiets Efterretningstjeneste fastsætter en slettefrist for den enkelte person eller oplysning i databasen på indtil 5 år fra indførelsen i databasen. Efterretningstjenesten kan efter underretning af Tilsynet med Efterretningstjenesterne undtagelsesvist fastsætte længere frister for sletning af personer, poster eller oplysninger i disse databaser mv.

*Stk. 3.* Slettefrister efter stk. 2 kan ikke overstige fristen i § 9, stk. 1, jf. dog stk. 2, i lov om Politiets Efterretningstjeneste.

**§ 3.** Oplysninger, som ikke inden 4 uger fra modtagelsen eller tilvejebringelsen er lagret i en journal eller i en database, jf. §§ 1 og 2, skal slettes, medmindre oplysningerne efter deres karakter ikke kan lagres elektronisk.

*Stk. 2.* Politiets Efterretningstjeneste underretter Tilsynet med Efterretningstjenesterne, hvis efterretningstjenesten undtagelsesvis ikke kan overholde fristen i stk. 1.

**§ 4.** Fysisk materiale, som knytter sig til oplysninger i en journal eller en database, og som efter dets karakter ikke kan lagres i journalen eller i en database, jf. §§ 1 og 2, behandles efter samme vilkår, som gælder for elektroniske oplysninger.

## Kapitel 2

### *Generelle forpligtelser*

**§ 5.** Politiets Efterretningstjeneste gennemfører og om nødvendigt ajourfører og reviderer de fornødne tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse med lov om Politiets Efterretningstjeneste og bestemmelser fastsat i medfør af denne bekendtgørelse. Står det i rimeligt forhold til behandlingsaktiviteterne, skal Politiets Efterretningstjeneste tillige gennemføre de fornødne databeskyttelsespolitikker.

*Stk. 2.* Foranstaltninger efter stk. 1 omfatter databeskyttelse gennem design og gennem standardindstillinger.

*Stk. 3.* Politiets Efterretningstjeneste skal forud for iværksættelse af behandlingsaktiviteter, der udføres af eller for efterretningstjenesten, overveje de påtænkte behandlingsaktiviteters konsekvenser for de registrerede fysiske personers rettigheder og grundrettigheder, og tage hensyn hertil i fastsættelsen af foranstaltninger efter § 6, stk. 1. Overvejelserne bør omfatte be-

handlingsaktiviteters relevante systemer og processer, men ikke enkeltsager.

## Kapitel 3

### *Behandlingsikkerhed*

§ 6. Politiets Efterretningstjeneste og databehandleren skal under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og behandlingens karakter, omfang, sammenhæng og formål og risicienes varierende sandsynlighed og alvor for fysiske og juridiske personers rettigheder gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.

*Stk. 2.* For så vidt angår automatisk behandling af oplysninger om fysiske og juridiske personer, skal Politiets Efterretningstjeneste og databehandleren på grundlag af en risikovurdering gennemføre passende foranstaltninger til at sikre, at behandlingen endvidere sker i overensstemmelse med bestemmelserne i kapitel 4, jf. dog stk. 3-5.

*Stk. 3.* For så vidt angår automatisk behandling, der sker som led i administrative forhold, skal alene gennemføres foranstaltninger efter stk. 2, når det findes relevant.

*Stk. 4.* Inden for rammerne af lov om Politiets Efterretningstjeneste og regler fastsat i medfør heraf og med henblik på at sikre et passende sikkerhedsniveau, jf. § 6, stk. 1, kan Politiets Efterretningstjeneste i nærmere bestemt omfang gennemføre andre passende tekniske og organisatoriske foranstaltninger end dem, som er fastsat i kapitel 3 og 4.

*Stk. 5.* Gennemførelsen af sådanne foranstaltninger skal begrundes og godkendes af efterretningstjenestens juridiske chef eller dennes stedfortrædere. Efterretningstjenesten underretter Tilsynet med Efterretningstjenesterne om foranstaltninger i medfør af stk. 4.

*Stk. 6.* Oplysninger om fysiske eller juridiske personer, der behandles i databehandlingsystemer, som føres af eller for Politiets Efterretningstjeneste, må hverken helt eller delvist opbevares uden for Danmark, medmindre andet følger af lov eller bestemmelser fastsat i medfør af lov, jf. dog stk. 7.

*Stk. 7.* Helt eller delvist opbevaring uden for Danmark af efterretningstjenestens oplysninger, der behandles i databehandlingsystemer, der føres

af eller for Politiets Efterretningstjeneste, kan dog ske efter forudgående godkendelse af Chefen for Politiets Efterretningstjeneste eller efterretningstjenestens juridiske chef, når det findes forsvarligt.

§ 7. Overlader Politiets Efterretningstjeneste en behandling af oplysninger om fysiske og juridiske personer til en databehandler, skal efterretningstjenesten sikre sig, at databehandleren kan træffe de tekniske og organisatoriske sikkerhedsforanstaltninger, der er nævnt i kapitel 3, og § 5.

*Stk. 2.* Politiets Efterretningstjeneste skal føre tilsyn med, at databehandleren gennemfører og overholder sikkerhedsforanstaltningerne, jf. stk. 1. Der fastsættes på grundlag af en risikovurdering et passende tilsyn, herunder karakteren af og hyppigheden for tilsynet. Ved vurderingen af et passende tilsyn inddrages navnlig karakteren og omfanget af de overladede behandlinger og oplysninger samt eventuelle risici for de registreredes rettigheder. Politiets Efterretningstjeneste kan afhængig af risikovurderingen lade tilsynet gennemføre af en uafhængig tredjepart.

*Stk. 3.* Gennemførelse af en behandling ved en databehandler skal ske i henhold til lov eller en skriftlig aftale mellem databehandleren og Politiets Efterretningstjeneste. Loven eller aftalen skal fastsætte genstanden for og varigheden af behandlingen, behandlingens karakter og formål samt Politiets Efterretningstjenestes forpligtelser og rettigheder. Det skal navnlig fremgå, at databehandleren

- 1) kun må handle efter instruks fra Politiets Efterretningstjeneste,
- 2) sikrer, at de fysiske personer, der er autoriseret til at behandle oplysninger om fysiske og juridiske personer, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt,
- 3) bistår Politiets Efterretningstjeneste på enhver hensigtsmæssig måde med at sikre overholdelse af bestemmelser om den registreredes rettigheder,
- 4) efter Politiets Efterretningstjenestes valg sletter eller tilbageleverer alle oplysningerne om fysiske og juridiske personer til Politiets Efterretningstjeneste, efter at tjenesterne vedrørende behandling er ophørt, medmindre anden lovgivning foreskriver opbevaring af oplysningerne,
- 5) stiller alle oplysninger, der er nødvendige for at påvise overholdelse af denne bestemmelse, til rådighed for Politiets Efterretningstjeneste og giver mulighed for og bidrager til revisioner og kontroller, herunder inspektioner, der foretages af Politiets Efterretningstjeneste eller Tilsynet med Efterretningstjenesterne

6) iværksætter alle foranstaltninger, som kræves i henhold til kapitel 3 og 4, og

7) overholder betingelserne i nr. 1-6 samt stk. 4 med henblik på at gøre brug af en anden databehandler.

*Stk. 4.* En databehandlers overladelse af behandling til en anden databehandler skal ske i henhold til en specifik skriftlig aftale med Politiets Efterretningstjeneste.

*Stk. 5.* Databehandleren, og enhver, der udfører arbejde for Politiets Efterretningstjeneste eller databehandleren, og som har adgang til oplysninger om fysiske og juridiske personer, må kun efter instruks fra Politiets Efterretningstjeneste behandle disse oplysninger.

#### *Brud på datasikkerheden*

**§ 8.** Ved brud på datasikkerheden i forbindelse med behandling af oplysninger om fysiske eller juridiske personer skal Politiets Efterretningstjeneste uden unødigt forsinkelse, efter at efterretningstjenesten er blevet bekendt med bruddet, underrette Tilsynet med Efterretningstjenesterne om bruddet, hvis det er sandsynligt, at bruddet indebærer en høj risiko for fysiske eller juridiske personers rettigheder.

*Stk. 2.* Databehandleren underretter straks Politiets Efterretningstjeneste om et brud på datasikkerheden.

*Stk. 3.* Underretningen efter stk. 1 skal

- 1) beskrive karakteren af bruddet på persondatasikkerheden,
- 2) beskrive de sandsynlige konsekvenser af bruddet på datasikkerheden og
- 3) beskrive de foranstaltninger, som Politiets Efterretningstjeneste har truffet eller påtænker truffet for at håndtere bruddet på datasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

*Stk. 4.* Er det ikke muligt at forelægge oplysningerne, der er nævnt i stk. 3, samlet for Tilsynet med Efterretningstjenesterne, skal oplysningerne meddeles trinvis uden unødigt forsinkelse.

*Stk. 5.* Politiets Efterretningstjeneste skal dokumentere alle brud på data-sikkerheden, jf. dog § 6, stk. 6, som er omfattet af stk. 1, herunder de faktiske omstændigheder vedrørende bruddet, bruddets virkninger og de trufne afhjælpende foranstaltninger.

## Kapitel 4

### *Supplerende sikkerhedsbestemmelser for automatisk behandling*

#### *Generelle bestemmelser*

**§ 9.** Politiets Efterretningstjeneste og databehandleren skal fastsætte nærmere interne bestemmelser om sikkerhedsforanstaltninger til uddybning af reglerne i kapitel 3 og 4. De interne bestemmelser skal gennemgås mindst én gang hvert år med henblik på at sikre, at de i væsentlig grad er fyldestgørende og afspejler de faktiske forhold. Desuden skal der fastsættes retningslinjer for efterretningstjenestens tilsyn med overholdelsen af de sikkerhedsforanstaltninger, der er fastsat for efterretningstjenesten.

**§ 10.** Politiets Efterretningstjeneste og databehandleren skal give den fornødne instruktion til de medarbejdere, som behandler oplysninger om fysiske og juridiske personer, ligesom medarbejderne skal gøres bekendt med de regler, der er fastsat i medfør af § 9.

#### *Kontrol med fysisk adgang til oplysninger om fysiske og juridiske personer*

**§ 11.** Der skal gennemføres passende fysiske sikkerhedsforanstaltninger, herunder i relevant omfang perimetersikring med adgangskontroller, til at sikre, at uautoriserede personer ikke kan få adgang til det behandlingsudstyr, der benyttes til behandling.

*Stk. 2.* For at undgå uautoriseret adgang skal fysiske adgangssteder til Politiets Efterretningstjenestes eller databehandlerens område, eksempelvis områder til af- og pålæsning, kontrolleres og så vidt muligt adskilles fra behandlingsfaciliteter, hvor der sker automatisk behandling af oplysninger om fysiske og juridiske personer.

### *Kontrol med datamedier*

§ 12. Der skal gennemføres passende foranstaltninger, herunder i relevant omfang kryptering, til at sikre, at der ikke sker uautoriseret læsning, kopiering, ændring eller sletning af datamedier, hvorpå der har været eller bliver behandlet oplysninger om fysiske eller juridiske personer.

§ 13. I forbindelse med reparation og service af datamedier, der indeholder oplysninger om fysiske eller juridiske personer, skal der træffes fornødne foranstaltninger for at sikre, at bestemmelsen i § 12 iagttages.

§ 14. Datamedier skal bortskaffes på forsvarlig vis, eksempelvis ved destruktion, og efter nærmere fastsatte procedurer, når de ikke længere skal anvendes til de formål, som behandlingen varetager.

### *Kontrol med opbevaring*

§ 15. Der skal gennemføres passende foranstaltninger, herunder i relevant omfang kryptering, til at sikre, at der ikke sker uautoriseret indlæsning eller uautoriseret læsning, ændring eller sletning af opbevarede oplysninger om fysiske og juridiske personer.

### *Autorisation og brugerkontrol*

§ 16. Der skal gennemføres passende foranstaltninger til at sikre, at automatiske behandlingssystemer ikke via datakommunikationsudstyr, kan benyttes af uautoriserede personer.

*Stk. 2.* Der må kun etableres eksterne kommunikationsforbindelser, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til oplysninger om fysiske og juridiske personer.

§ 17. Oplysninger om fysiske og juridiske personer må kun behandles af personer, som er autoriseret til at varetage de formål, til hvilke behandlingen af oplysningerne foretages.

§ 18. Der må kun autoriseres personer, der er beskæftiget med de formål, hvortil oplysninger om fysiske eller juridiske personer behandles. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for.

*Stk. 2.* Der må endvidere autoriseres personer, for hvem adgang til oplysninger er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver.

*Stk. 3.* Autorisationer skal angive, i hvilket omfang brugeren må indlæse, ændre, forespørge, videregive eller slette oplysninger.

*Stk. 4.* Det skal sikres, at de autoriserede personer fortsat opfylder betingelserne i stk. 1-3. Kontrol heraf skal foretages mindst én gang hvert halve år.

### *Kontrol med dataadgangen*

§ 19. Der skal gennemføres passende foranstaltninger til at sikre, at personer, der autoriseres til at anvende et automatisk behandlingssystem kun har adgang til de oplysninger om fysiske og juridiske personer, der er omfattet af autorisationen.

§ 20. Der skal gennemføres kontrol med dataadgangen i form af relevant registrering af brugeraktiviteter, og sikkerhedshændelser, herunder skal registreres alle afviste adgangsforsøg til behandlingssystemer, hvori der behandles personoplysninger.

*Stk. 2.* Hvis der inden for en fastsat periode registreres et nærmere fastsat antal på hinanden følgende afviste adgangsforsøg fra samme kilde eller med samme brugeridentifikation, skal der blokeres for yderligere forsøg. Der skal løbende ske opfølgning i Politiets Efterretningstjeneste.

### *Kommunikationskontrol*

§ 21. Der skal gennemføres passende foranstaltninger til at sikre, at det er muligt at kontrollere og fastslå de modtagere, til hvilke der er blevet overført eller stillet oplysninger til rådighed, eller kan overføres eller stilles oplysninger til rådighed ved hjælp af datakommunikationsudstyr, herunder gennem relevant logning af søgninger og videregivelse, jf. § 23, stk. 3.



### *Kontrol med indlæsning*

§ 22. Der skal gennemføres passende foranstaltninger til at sikre, at det er muligt efterfølgende at undersøge og fastslå, hvilke oplysninger om fysiske og juridiske personer, der er indlæst i automatiske behandlingssystemer samt hvornår og af hvem oplysningerne er indlæst, herunder gennem relevant logning af indlæsning, jf. § 23, stk. 3.

### *Logning*

§ 23. I automatiske databehandlingssystemer foretages logning af alle anvendelser af oplysninger om fysiske og juridiske personer.

*Stk. 2.* Loggen skal mindst indeholde oplysning om tidspunkt, bruger, type af behandlingsaktivitet og angivelse af den fysiske eller juridiske person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium.

*Stk. 3.* Loggen skal ud over stk. 2 så vidt muligt kunne understøtte kontrol efter §§ 20-22.

*Stk. 4.* Loggen skal opbevares i 6 måneder, hvorefter den skal slettes. I særlige tilfælde kan logoplysninger opbevares i indtil 10 år.

§ 24. Logningskravet i § 23, stk. 1 finder ikke anvendelse for oplysninger, som indgår i tekstbehandlingsdokumenter og lignende, der ikke foreligger i endelig form, samt sådanne dokumenter og lignende, der foreligger i endelig form, hvis der sker sletning inden for en af efterretningstjenesten nærmere fastsat kortere frist.

*Stk. 2.* Hvis behandlingen udelukkende sker ved afvikling af programmer, som foretager en forud defineret massebehandling af oplysninger (batchkørsler), finder logningskravet i stk. 1 ikke anvendelse. Dog skal logges bruger og tidspunkt for behandlingen.

### *Transportkontrol*

§ 25. Der skal gennemføres passende foranstaltninger til at sikre, at der ikke sker uautoriseret læsning, kopiering, ændring eller sletning af oplysninger om fysiske og juridiske personer i forbindelse med overførsel af disse eller under transport af datamedier.

## *Genopretning*

§ 26. Der skal gennemføres passende foranstaltninger til at sikre, at de anvendte systemer i tilfælde af teknisk uheld kan genetableres. I den forbindelse udarbejdes en plan for genopretning.

## *Pålidelighed og integritet*

§ 27. Der skal gennemføres passende foranstaltninger til at sikre, at systemer fungerer, og at opbevarede oplysninger om fysiske og juridiske personer ikke bliver ødelagt som følge af fejlfunktioner i systemet, herunder ved procedurer for fejlhåndtering samt konfigurations- og ændringsstyring.

## Kapitel 5

### *Politiets Efterretningstjenestes egne personalesager og sikkerhedsgodkendelsessager*

§ 28. Europa-Parlamentets og Rådets forordning nr. 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysningers artikel 12-22 og databeskyttelseslovens § 22 og forvaltningslovens kapitel 4-6 finder anvendelse for behandlingen af personoplysninger for Politiets Efterretningstjeneste vedrørende tjenestens egne personalesager og sikkerhedsgodkendelsessager.

## Kapitel 6

### *Fremgangsmåde ved undersøgelser og godkendelse af visse efterforskningskridt*

§ 29. Chefen for Politiets Efterretningstjeneste fastsætter nærmere retningslinjer for fremgangsmåden i forbindelse med brug af undersøgelser, jf. § 5 i lov om Politiets Efterretningstjeneste.

§ 30. Straffeprocessuelle tvangsindgreb, herunder indgreb i meddelelshemmeligheden, skal i hvert enkelt tilfælde godkendes af chefen for Politiets Efterretningstjeneste eller efterretningstjenestens juridiske chef eller dennes stedfortrædere.

*Stk. 2.* Hvis det pågældende tvangsindgreb kræver retskendelse, skal den i stk. 1 nævnte godkendelse finde sted, inden sagen forelægges retten i overensstemmelse med retsplejelovens regler.

*Stk. 3.* Særligt for så vidt angår iværksættelse af telefonaflytninger eller indhentelse af teleoplysninger baseret på retskendelser, der vedrører en navngiven person i stedet for et bestemt telefonnummer, jf. retsplejelovens § 783, stk. 2, skal der i hvert enkelt tilfælde, hvor der iværksættes indgreb vedrørende nye telefonnumre, ske forudgående godkendelse af chefen for Politiets Efterretningstjeneste eller efterretningstjenestens juridiske chef eller dennes stedfortrædere.

## Kapitel 7

### *Indhentelse og videregivelse af oplysninger*

**§ 31.** I tilfælde, hvor Politiets Efterretningstjeneste i medfør af § 4, stk. 1, jf. § 3 i lov om Politiets Efterretningstjeneste indhenter oplysninger om alle personer, der inden for et givent tidspunkt har rettet henvendelse til en given offentlig myndighed, eller andre grupper af personer, som på tilsvarende måde ikke på forhånd er identificeret, skal efterretningstjenesten, så hurtigt som forholdene tillader det, foretage en vurdering af, om de personer, som oplysningerne vedrører, er af relevans for efterretningstjenestens opgavevaretagelse. I den udstrækning dette vurderes ikke at være tilfældet, skal de ikke relevante oplysninger straks slettes.

*Stk. 2.* Indhentelse af oplysninger af den i stk. 1 nævnte art kan alene ske efter forudgående godkendelse af chefen for Politiets Efterretningstjeneste eller efterretningstjenestens juridiske chef eller dennes stedfortrædere. Det samme gælder indhentelse af oplysninger om psykiatriske diagnoser eller tilsvarende særligt følsomme helbredsoplysninger.

*Stk. 3.* I tilfælde, hvor Politiets Efterretningstjeneste i medfør af lov om indsamling, anvendelse og opbevaring af oplysninger om flypassagerer indhenter oplysninger om alle personer, der inden for et givent tidspunkt rejser med luftfartøjer til eller fra bestemte destinationer eller med bestemte rejsemønstre, eller andre grupper af personer, som på tilsvarende måde ikke på forhånd er identificeret, skal efterretningstjenesten, så hurtigt som forholdene tillader det, foretage en vurdering af, om de personer, som oplysningerne vedrører, er af relevans for efterretningstjenestens opgavevaretagelse. I den udstrækning dette vurderes ikke at være tilfældet, skal de ikke rele-

vante oplysninger straks slettes eller anonymiseres hos efterretningstjenesten.

*Stk. 4.* Chefen for Politiets Efterretningstjeneste fastsætter nærmere retningslinjer for indhentelse af oplysninger efter § 4 i lov om Politiets Efterretningstjeneste.

**§ 32.** Videregivelse af følsomme personoplysninger til udenlandske myndigheder kan alene ske efter forudgående godkendelse af chefen for Politiets Efterretningstjeneste eller efterretningstjenestens juridiske chef eller dennes stedfortrædere.

*Stk. 2.* Chefen for Politiets Efterretningstjeneste fastsætter nærmere retningslinjer for videregivelse af oplysninger.

## Kapitel 8

### *Intern kontrol*

**§ 33.** Politiets Efterretningstjeneste foretager løbende stikprøvekontrol med sletning, logning, iværksættelse af undersøgelser, indhentelse af oplysninger, indgreb under efterforskningen og videregivelse af oplysninger.

**§ 34.** Chefen for Politiets Efterretningstjeneste fastsætter nærmere retningslinjer for stikprøvekontrol.

## Kapitel 9

### *Orientering af Tilsynet med Efterretningstjenesterne*

**§ 35.** Politiets Efterretningstjeneste orienterer Tilsynet med Efterretningstjenesterne om tjenestens beslutninger i medfør af § 9, stk. 2, i lov om Politiets Efterretningstjeneste om at undlade at slette oplysninger, som har nået slettefristen i § 9, stk. 1, i lov om Politiets Efterretningstjeneste.

**§ 36.** Politiets Efterretningstjeneste orienterer løbende Tilsynet med Efterretningstjenesterne om anvendelsen af § 4 i lov om Politiets Efterretningstjeneste.

§ 37. Politiets Efterretningstjeneste orienterer løbende Tilsynet med Efterretningstjenesterne om sager om sikkerhedsgodkendelse, hvor efterretningstjenesten videregiver oplysninger fra tjenestens journaler eller databaser, jf. §§ 1 og 2, til andre myndigheder end Justitsministeriet, anklagemyndigheden eller øvrige dele af politiet.

§ 38. Politiets Efterretningstjeneste orienterer løbende Tilsynet om Efterretningstjenesterne om alle væsentlige spørgsmål vedrørende efterretningstjenestens behandling af oplysninger.

§ 39. Politiets Efterretningstjeneste orienterer løbende Tilsynet med Efterretningstjenesterne om tjenestens interne kontrol, jf. §§ 33 og 34, med behandlingen af oplysninger om fysiske og juridiske personer.

§ 40. Politiets Efterretningstjeneste orienterer Tilsynet med Efterretningstjenesterne om nye administrative retningslinjer af betydning for tilsynets kontrol.

*Stk. 2.* Politiets Efterretningstjeneste orienterer Tilsynet med Efterretningstjenesterne om andre retningslinjer, hvis tilsynet anmoder herom.

## Kapitel 10

### *Bevaring til Rigsarkivet*

§ 41. Fysiske eller elektroniske oplysninger, som i medfør af bestemmelser om bevaring og kassation udstedt af Rigsarkivet skal bevares for eftertiden, må ikke destrueres eller slettes. Sådanne oplysninger skal i stedet overføres til Rigsarkivet.

*Stk. 2.* Kan de i stk. 1 nævnte oplysninger af praktiske eller sikkerhedsmæssige grunde ikke overføres til Rigsarkivet, skal oplysningerne, fra det tidspunkt hvor destruktion eller sletning skulle være sket, behandles adskilt fra efterretningstjenestens øvrige oplysninger, således at alene medarbejdere, der af chefen for Politiets Efterretningstjeneste er særligt autoriseret hertil, har adgang til oplysningerne.

*Stk. 3.* Oplysninger, som skal overføres til Rigsarkivet, jf. stk. 1, og oplysninger, som af praktiske eller sikkerhedsmæssige grunde ikke kan overføres til Rigsarkivet, jf. stk. 2, må, fra det tidspunkt, hvor destruktion eller sletning skulle være sket, kun behandles af Politiets Efterretningstjeneste, hvis det må antages at have væsentlig betydning for varetagelsen af tjene-

stens opgaver vedrørende forebyggelse og efterforskning af en overtrædelse af straffelovens kapitel 12 og 13 eller sker i forbindelse med behandling af arkiv- indsigts-, tilsyns- og lignende sager.

## Kapitel 11

### *Ikrafttræden*

**§ 42.** Bekendtgørelsen træder i kraft den xx.xx.2019.

*Stk. 2.* Følgende bekendtgørelser ophæves

- 1) bekendtgørelse nr. 763 af 20. juni 2014 om Politiets Efterretningstjenestes behandling af oplysninger om fysiske og juridiske personer m.v. og
- 2) bekendtgørelse nr. 516 af 23. maj 2018 om sikkerhedsforanstaltninger til beskyttelse af oplysninger om fysiske og juridiske personer, som behandles for Politiets Efterretningstjeneste.

**§ 43.** Bekendtgørelsens § 3 finder ikke anvendelse på oplysninger, som på ikrafttrædelsestidspunktet alene foreligger hos Politiets Efterretningstjeneste i fysisk form.

*Stk. 2.* Politiets Efterretningstjeneste skal lagre oplysninger som nævnt i stk. 1 i en journal eller en database, jf. §§ 1 og 2, medmindre lagringen strider mod arkivloven eller regler fastsat i medfør heraf.

*Stk. 3.* For de i stk. 1 nævnte oplysninger regnes de i § 1, stk. 2, og § 2, stk. 2, nævnte slettefrister fra tidspunktet for lagring i en journal eller en database, jf. stk. 2.

**§ 44.** Bekendtgørelsens § 5 gælder alene i forhold til ny behandling af oplysninger om fysiske personer, der iværksættes den [x] eller senere.