JD

JUSTIS- OG BEREDSKAPSDEPARTEMENTET

# Høringsnotat

Politiavdelingen
Dato: 20. november 2024
Saksnr: 24/7353
Høringsfrist: 20. januar 2025

## Høring – forslag til endringer i politiregisterloven, politiregisterforskriften, straffeprosessloven, politiloven og grenseloven – testing og utvikling av informasjonssystemer og PSTs behandling av åpent tilgjengelig informasjon mv.

## Innhold

# 1 Innledning

Justis- og beredskapsdepartementet sender med dette på høring forslag til endringer i politiregisterloven, grenseloven, straffeprosessloven, politiloven og politiregisterforskriften.

Endringene gjelder for det første regulering av bruk av opplysninger til testing og utvikling av informasjonssystemer innenfor politiregisterlovens og grenselovens virkeområde, se høringsnotatet punkt 2.

Det foreslås å innta i politiregisterloven at loven gjelder når opplysninger behandles for testing og utvikling av informasjonssystemer til formål som er omfattet av loven. Videre foreslås det en ny bestemmelse i politiregisterforskriften for å ramme inn bruken av opplysninger til testing og utvikling. Det stilles blant annet krav om at opplysninger bare kan brukes til testing og utvikling dersom det

vil være umulig eller uforholdsmessig å oppnå formålet ved bruk av anonyme eller fiktive/syntetiske opplysninger. Videre kan enkelte typer opplysninger ikke brukes til testing og utvikling, det stilles krav om den behandlingsansvarliges godkjenning og det åpnes for at den behandlingsansvarlige kan stille nærmere krav til behandlingen. I tillegg foreslås det å innføre krav om forhåndsdrøftelser med Datatilsynet ved testing og utvikling som kan medføre høy risiko for de registrertes rettigheter og friheter.

Det foreslås også endringer i straffeprosessloven og politiloven slik at informasjon innhentet ved kommunikasjonskontroll, romavlytting og dataavlesing skal kunne brukes til testing og utvikling.

Forslagene gir ingen utvidet mulighet til å innhente eller lagre opplysninger, men åpner for at opplysninger politiet allerede har rettsgrunnlag i politiregisterlovgivningen til å behandle, også kan brukes til å teste og utvikle informasjonssystemer som skal brukes til å behandle opplysninger til formål som omfattes av loven.

Høringsnotatet inneholder også forslag om at PST skal kunne benytte åpent tilgjengelig informasjon innhentet etter politiregisterloven ny § 65 a til testing og utvikling av informasjonssystemer til bruk i forbindelse med analyser og etterretningsvurderinger, herunder automatiserte analyseverktøy. En slik utvikling var forutsatt i Prop. 31 L (2022–2023), men kommer ikke til uttrykk i lovteksten.

Det foreslås også hjemler for bruk av opplysninger til testing og utvikling av informasjonssystemer i forbindelse med grensekontroll. Her foreslås det også å åpne for at ansiktsfoto og fingeravtrykk opptatt i grensekontrollen kan lagres for en avgrenset periode utelukkende til bruk for testing og utvikling av informasjonssystemer med grensekontrollformål.

For det andre inneholder høringsnotatet forslag om en ny forskriftsbestemmelse som regulerer nærmere PSTs behandling av åpent tilgjengelig informasjon til etterretningsformål etter politiregisterloven ny § 65 a, se høringsnotatet punkt 3. Forskriftsforslaget utfyller og presiserer den vedtatte lovbestemmelsen, som foreløpig ikke har trådt i kraft. Forslagene utvider ikke adgangen til å innhente eller å behandle informasjon sammenlignet med de vedtatte lovendringene.

For det tredje foreslås det enkelte andre presiserende endringer i politiregisterforskriften uten sammenheng med de ovennevnte temaene. Disse gjelder sletting av opplysninger som behandles for utarbeidelse av analyser og etterretningsvurderinger som nevnt i politiloven § 17 a, se høringsnotatet punkt 4, og tydeliggjøring av PSTs tilgang til politiets registre for sin oppgaveløsning, se høringsnotatet punkt 5.

# 2 Testing og utvikling

## 2.1 Overordnet om bakgrunnen for forslagene

Den teknologiske utviklingen i samfunnet går raskt, og politiet må holde tritt med denne utviklingen. Utvikling og testing av eksisterende og nye systemer er en forutsetning for at politiet kan utføre oppgavene de er pålagt på en effektiv måte. Politiet må derfor både ha ressurser til å utvikle og teste nye teknologiske

løsninger, og regelverket må være tilpasset utvikling, testing og bruk av slike løsninger.

I Prop. 1 S (2023–2024) for Justis- og beredskapsdepartementet på s. 93 er det uttalt at det er «viktig at verksemdene nyttar seg av moglegheitene som den teknologiske utviklinga gir til å auke kvaliteten og effektiviteten i oppgåveløysinga». Videre vises det på samme sted til at politiet, for å løse sitt samfunnsoppdrag, er avhengig av å bruke ny teknologi og moderne løsninger for å bekjempe nye former for kriminalitet. Dette nødvendiggjør at ny teknologi kan testes, nye tekniske løsninger utvikles og tas i bruk og eksisterende tekniske løsninger må kunne videreutvikles.

Kompleksiteten i politiets og påtalemyndighetens oppgaver og informasjonsbehandling, samt behovet for ivaretakelse av krav til blant annet rettssikkerhet, notoritet, personvern og samfunnssikkerhet medfører at politiet i stor grad er avhengige av egenutviklede løsninger eller hyllevare (dvs. ferdig utviklede informasjonssystemer og verktøy som tilbys av kommersielle aktører) med meget gode tilpasningsmuligheter. Når nye informasjonssystemer skal tas i bruk, må de være utviklet med utgangspunkt i eller være tilpasset de særlige behov politiet har. Herunder må systemene være tilpasset hvilke opplysninger som skal behandles, hvilke formål opplysningene skal brukes til og hvordan ulike opplysninger henger sammen.

Utvikling av informasjonssystemer må videre være basert på god forståelse av hvordan behandlingen kan bidra til å løse politiets arbeidsoppgaver. For å opparbeide seg denne forståelsen, må IT-utviklere ofte ha tilgang til opplysninger fra eksisterende registre og saksbehandlingssystemer for å få oversikt over hvilke opplysninger som behandles, hvordan de behandles og hvordan behandlingen kan forbedres eller effektiviseres. Videre krever all utvikling og oppdatering av informasjonssystemer omfattende testing før de tas i bruk for å sikre at informasjonssystemet fungerer etter intensjonen og ikke får utilsiktede konsekvenser for den registrerte, samt at krav til informasjonssikkerhet og forsvarlig håndtering av personopplysninger ivaretas. For å kvalitetssikre systemene og unngå informasjonssikkerhetsbrudd, herunder brudd på personopplysningssikkerheten, kan være helt nødvendig å teste systemene med reelle opplysninger.

## 2.2 Nærmere om begreper mv.

Høringsnotatet inneholder forslag om hjemler for «utvikling» og «testing» av «informasjonssystemer». Ingen av disse begrepene har en entydig eller allmenn definisjon, og innholdet i begrepene kan utvikle og endre seg over tid som følge av den teknologiske utviklingen. Med informasjonssystemer menes i denne sammenheng ulike tekniske løsninger som politiet kan benytte i sin oppgaveløsning, som for eksempel saksbehandlingssystemer, registre, IT-systemer, IT-verktøy, modeller for beslutningsstøtte og systemer for sammenstilling av informasjon, oversettelse og analyse mv. Det omfatter også systemer som benytter maskinlæring og kunstig intelligens (KI).

Med testing menes tradisjonelt det å kontrollere at et IT-system fungerer slik det skal. Testing kan skje både for å sikre at et eksisterende system fungerer, og for å kontrollere at nye systemer som er under utvikling fungerer etter intensjonen. Med utvikling menes tradisjonelt det å lage, oppgradere eller på andre måter endre et

IT-system slik at det er klart for testing. Utvikling omfatter dermed både videreutvikling av eksisterende systemer og at helt nye systemer lages. Begrepene testing og utvikling er i dette høringsnotatet ment å dekke hele utviklingsfasen og alle steg i denne, samt ulike former for testing av informasjonssystemer. De inkluderer dermed blant annet feilretting, analyse av testresultater, for eksempel for å avdekke årsaken til at systemene ikke gir det resultat eller den kvaliteten som er forventet, samt annen løpende forbedring og endring av et system. Utvikling omfatter også endring av ferdig utviklede systemer for å tilpasse dem til politiets behov. Testing omfatter også testing og kvalitetssikring av verktøy og modeller som er utviklet og/eller trent av andre, samt trening av modeller politiet selv utvikler. Begrepene avgrenses mot den daglige driften av informasjonssystemene, for eksempel at brukere melder inn feil i systemet som deretter rettes, som regnes som «drift og administrasjon», jf. politiregisterforskriften § 8-2. For slik løpende drift gjelder ikke forslagene i høringsnotatet her.

Utvikling og testing kan enten foregå med anonyme eller fiktive (også kalt syntetiske) opplysninger eller med opplysninger om identifiserte eller identifiserbare personer. Med anonyme og fiktive opplysninger menes henholdsvis reelle opplysninger som ikke kan knyttes til bestemte personer, og opplysninger som er skapt uavhengig av reelle opplysninger. Som utgangspunkt bør testing og utvikling skje ved bruk av anonyme eller fiktive opplysninger, og slik testing og utvikling krever heller ingen særskilt regulering. Av ulike grunner er det ikke alltid mulig utelukkende å bruke anonyme eller fiktive opplysninger, for eksempel fordi det ikke er mulig å skape et stort nok eller realistisk datasett som kan benyttes i arbeidet. Dette omtales nærmere i punkt 2.6.2@ og 2.9.2@.

Utvikling og testing kan skje på ulike måter og i ulike systemer, og metodene endrer seg over tid som følge av den teknologiske utviklingen. I noen tilfeller etableres det egne test- og utviklingsmiljøer separat fra ordinære systemer, der eventuelle reelle personopplysninger som er nødvendige kopieres over fra ordinære systemer. Når testingen og utviklingen er fullført, vil endringene implementeres og tas i bruk i det ordinære systemet, og de kopierte opplysningene kan slettes. I andre tilfeller skjer testing og utvikling mer fortløpende og integrert i det aktuelle systemet der opplysninger ellers behandles. Opplysninger brukes i slike tilfeller der de er registrert, men med tekniske sperrer som gjør at de originale opplysningene ikke påvirkes. Det kan også være mellomvarianter, for eksempel at utvikling skjer i et separat miljø, men løsningen testes helt eller delvis i det faktiske systemet for å sikre at det fungerer etter intensjonen.

Hvilke personer i organisasjonen som involveres i testing og utvikling kan også variere. Mens utvikling krever særskilt teknisk kompetanse og gjerne skjer ved bruk av dedikert IT-personell, kan testing både utføres av IT-personell og av brukerne av systemet. Sistnevnte er kanskje særlig aktuelt i sluttfasen av utviklingen, nær den faktiske produksjonssettingen/implementeringen av løsningen.

## 2.3 Rettslige rammer

### 2.3.1 Grunnloven og EMK

Grunnloven § 102 og EMK artikkel 8 verner om borgernes rett til respekt for sitt privatliv. Grunnloven § 102 første ledd første punktum slår fast at enhver har rett

til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. At opplysninger som er innhentet for et formål viderebehandles til andre formål enn de er innhentet for, herunder testing og utvikling, vil kunne utgjøre et inngrep i rettighetene som vernes av disse bestemmelsene. Det samme gjelder å lagre opplysninger utelukkende for å bruke dem til testing og utvikling. Inngrep i vernede rettigheter må ha hjemmel i lov, ivareta et legitimt formål og være nødvendig og forholdsmessig.

### 2.3.2 Personvernforordningen

Personvernforordningen (EU) 2016/679 (heretter GDPR) gjelder for politiets forvaltningsvirksomhet, herunder grensekontroll. Forordningen kommer i sin helhet til anvendelse for bruk av personopplysninger for testing og utvikling innenfor forordningens virkeområde, jf. artikkel 2 og personopplysningsloven § 2. Her nevnes bare enkelte artikler som særlig har betydning for behovet for regulering av behandling av personopplysninger til testing og utvikling.

Prinsippet om formålsbegrensning i GDPR artikkel 5 nr. 1 bokstav b innebærer at personopplysninger ikke kan viderebehandles på en måte som er «uforenlig» med det opprinnelige formålet. Etter bokstav c skal personopplysninger være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for (prinsippet om dataminimering).

Det kreves i utgangspunktet ikke noen eksplisitt hjemmel for å viderebehandle opplysninger som er innhentet til et formål til et annet, så lenge det nye formålet anses forenlig med det opprinnelige, jf. artikkel 6 nr. 4 og fortalepunkt nr. 50. Er derimot det nye formålet uforenlig med formålet opplysningene ble innhentet for, må viderebehandlingen ha grunnlag i samtykke eller lov, jf. Prop. 56 LS (2017–2018) punkt 6.6.

At testing og utvikling i konteksten av GDPR ofte vil være et annet formål enn det opplysningene opprinnelig behandles for, er lagt til grunn både av Datatilsynet og i EU-domstolens praksis, se C-77/21 avsnitt 45:

«[…] Article 5(1)(b) of Regulation 2016/679 must be interpreted as meaning that the principle of 'purpose limitation', laid down in that provision, does not preclude the recording and storage by the controller, in a database created for the purposes of carrying out tests and correcting errors, of personal data previously collected and stored in another database, where such further processing is compatible with the specific purposes for which the personal data were initially collected, which must be determined in the light of the criteria in Article 6(4) of that regulation.»

### 2.3.3 Personverndirektivet

Direktiv (EU) 2016/680 (heretter LED) regulerer rettshåndhevende myndigheters behandling av personopplysninger til kriminalitetsbekjempende formål mv. Direktivet er gjennomført i politiregisterloven og politiregisterforskriften. Direktivets regler er på en del punkter sammenfallende med GDPR, men med tilpasninger på grunn av særlige behov ved kriminalitetsbekjempelse.

LED har i motsetning til GDPR ingen regler om viderebehandling til «forenlige» formål. Etter LED artikkel 9 nr. 1 kommer GDPR til anvendelse når opplysninger som omfattes av direktivet behandles for andre formål enn de som er nevnt i artikkel 1 nr. 1, det vil si behandling av personopplysninger «med sikte på å

forebygge, etterforske, avsløre eller rettsforfølge straffbare handlinger eller fullbyrde strafferettslige reaksjoner, herunder hindre trusler mot og verne om offentlig sikkerhet».

Testing og utvikling ikke er nevnt i direktivet. Det er likevel flere artikler som forutsetter at teknisk utvikling vil skje, se for eksempel reglene i artikkel 27 om vurderinger av personvernkonsekvenser ved bruk av ny teknologi. Tiltak som kan bidra til å redusere personvernkonsekvensene av ny teknologi kan bygges inn i utviklingsfasen, og grundig testing kan bidra til å identifisere uheldige eller utilsiktede konsekvenser som kan avhjelpes før systemet settes i verk.

Også krav til informasjonssikkerhet og den behandlingsansvarliges kontroll innebærer at systemer må kunne testes og videreutvikles for at sikre at kravene etterleves, uten at dette sies eksplisitt.

### 2.3.4 Internasjonalt regelverk om kunstig intelligens mv.

EUs forordning om kunstig intelligens (EU) 2024/1689 (heretter KI-forordningen) gir regler for markedsplassering og bruk av KI-systemer. Forordningen skal begynne å gjelde i EU fra august 2026, med enkelte unntak, jf. artikkel 113. Forordningen er ennå ikke inntatt i EØS-avtalen, og arbeidet med dette samt gjennomføring i norsk rett følger et eget løp. Her beskrives derfor bare enkelte artikler som kan ha betydning for politiets testing og utvikling av informasjonssystemer.

Forordningen artikkel 3 nr. 1 definerer et KI-system på følgende måte:

«a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.»

Systemer som utelukkende følger forhåndsprogrammerte regler, for eksempel automatisert saksbehandling som fullt ut er regelstyrt og systemer som ikke opererer med noen form for autonomi eller tilpasser seg etter å bli tatt i bruk, faller derfor utenfor forordningens virkeområde. Etter artikkel 96 nr. 1 bokstav f skal kommisjonen utvikle retningslinjer om den praktiske gjennomføringen av forordningen, særlig anvendelsen av definisjonen av et KI-system.

KI-forordningen regulerer ikke bruk av kunstig intelligens som utelukkende benyttes i forbindelse med nasjonal sikkerhet, jf. artikkel 2 nr. 3. Forordningen legger derfor ikke begrensninger for PSTs bruk av kunstig intelligens innenfor dette området. Systemer som brukes for flere formål, for eksempel at de også benyttes til rettshåndhevelse, omfattes derimot av forordningen, jf. fortalepunkt 24. Det er dermed ikke nødvendigvis systemet i seg selv, men hvordan det tas i bruk, som avgjør om KI-forordningen kommer til anvendelse eller ikke.

KI-forordningens virkeområde avgrenser mot forskning, testing og utvikling av systemer før de tilbys på markedet eller settes i verk, jf. artikkel 2 nr. 8. Slike aktiviteter skal utføres på en måte som respekterer relevant EU-regelverk. Forordningen legger likevel føringer for testing og utvikling av systemer som skal tilbys på markedet eller tas i bruk, særlig for systemer som defineres som høyrisikosystemer. Høyrisikosystemer er blant annet systemer for biometrisk fjernidentifisering, med unntak av systemer for biometrisk verifisering utelukkende for å bekrefte at personen er den hen oppgir å være, jf. vedlegg III nr.

1 bokstav a. Det omfatter også en rekke former for systemer dersom de brukes av rettshåndhevende myndigheter, blant annet systemer som skal vurdere risikoen for at en person vil bli utsatt for eller vil begå lovbrudd, samt systemer for profilering, jf. vedlegget nr. 6. Også systemer som benyttes i forbindelse med grensekontroll vil kunne være høyrisikosystemer, dersom de blant annet brukes til å vurdere om en person utgjør en risiko eller for å oppdage, gjenkjenne eller identifisere personer, ut over verifikasjon av reisedokumenter, jf. vedlegget nr. 7.

Artikkel 9 nr. 6 krever at høyrisikosystemer skal testes for å sikre at de fungerer konsistent for de intenderte formålene, og det følger av nr. 8 at testing skal skje gjennom utviklingsfasen og uansett før de settes i verk. Artikkel 10 stiller krav til data og datastyring ved høyrisikosystemer, og inneholder blant annet regler om trenings-, validerings- og testdatasett som inneholder særlige kategorier av personopplysninger. Slike opplysninger kan behandles dersom det er strengt nødvendig for å oppdage og korrigere skjevheter og nærmere vilkår er oppfylt, jf. artikkel 10 nr. 5.

Europarådskonvensjonen om kunstig intelligens (KI-konvensjonen) ble vedtatt 17. mai 2024. Norge undertegnet konvensjonen 5. september 2024.Konvensjonen er mer overordnet enn KI-forordningen, og stiller ikke strengere eller mer detaljerte krav til testing og utvikling enn det som følger av forordningen.

### 2.4 Hjemler for testing og utvikling i annet regelverk

De senere år er det etablert flere hjemler for at opplysninger som et offentlig organ behandler i sin lovregulerte virksomhet, også kan brukes til testing og utvikling av informasjonssystemer. Se blant annet skatteforvaltningsloven § 5-12, som lyder:

§ 5-12 *Bruk av personopplysninger ved utvikling og testing av IT-systemer*

(1) Skattemyndighetene kan behandle innhentede personopplysninger for å utvikle og teste IT-systemer dersom det vil være umulig eller uforholdsmessig vanskelig å oppnå formålet ved å bruke anonyme eller fiktive opplysninger.

(2) Departementet kan i forskrift gi nærmere regler om behandling etter første ledd.

Lignende bestemmelser finnes blant annet i vareførselsloven § 7-17, skattebetalingsloven § 3-6, folkeregisterloven § 9-5, lov om statens pensjonskasse § 45 b, husbankloven § 12 og a-opplysningsloven § 6 a.

Begrunnelsen for at det er gitt egne hjemler for bruk av innhentede opplysninger for testing og utvikling på disse områdene er ifølge Prop. 1 LS (2018–2019) kapittel 18 at dette som regel vil være et annet formål enn opplysningene ble innhentet for. Testing og utvikling kan være forenlig med det opprinnelige formålet, og personvernforordningen vil i så fall ikke stille krav om et eget rettsgrunnlag for behandlingen, jf. artikkel 6 nr. 4. Om bruken er forenlig med innhentingsformålet vil avhenge av en konkret vurdering, og det kan være uklart hvor langt adgangen strekker seg. Egne hjemler for testing og utvikling gir en klar rettslig adgang for slik bruk, og skaper bedre forutsigbarhet for den registrerte.

Også innenfor helselovgivningen er det gitt hjemler for testing og utvikling. For eksempel angir pasientjournalloven § 11 annet ledd at «[d]irekte identifiserbare helseopplysninger kan behandles i lukkede testmiljøer for å utvikle og teste behandlingsrettede helseregistre dersom det er umulig eller uforholdsmessig vanskelig å oppnå formålet ved å bruke pseudonyme, anonyme eller fiktive

opplysninger». I Prop. 91 L (2021–2022) punkt 7.4 er det lagt til grunn at fiktive opplysninger ikke alltid kan gi tilstrekkelig kompleksitet i testsituasjoner som er nødvendig for å kvalitetssikre systemer før produksjonssetting i helsetjenesten. Hensikten med forslaget var å gi en klarere hjemmelssituasjon, og proposisjonen slår fast at selv om utvikling og test av journalsystemer eller andre behandlingsrettede helseregistre utgjør et annet formål enn det opplysningene i utgangspunktet er innhentet for, vil det ikke være uforenlig med det opprinnelige formålet.

I proposisjonen er det uttalt at utviklings- og testvirksomheten ikke skal ha større omfang, og helseopplysninger skal ikke lagres lenger, enn det som er nødvendig for å gjennomføre arbeidet.

Helsepersonelloven § 29 første ledd bokstav a åpner for at departementet etter søknad kan bestemme at opplysninger fra pasientjournaler og andre behandlingsrettede helseregistre skal tilgjengeliggjøres uten hinder av taushetsplikt når opplysningene skal brukes til et uttrykkelig angitt formål knyttet til utvikling og bruk av klinisk beslutningsstøtteverktøy. Ifølge spesialmerknadene til bestemmelsen i Prop. 112 (2020–2021) er begrepet «beslutningsstøtteverktøy» vidt og omfatter i utgangspunktet alle typer kunnskapsbaserte hjelpemidler eller støttesystemer som kan gi råd og støtte og veilede helsepersonell ved ytelse av helsehjelp. Det omfatter utvikling og bruk av systemer som bygger på kunstig intelligens og systemer som bygger på maskinlæring.

Bestemmelsen inneholder en rekke ytterligere vilkår for tilgjengeliggjøring, blant annet skal det ikke tilgjengeliggjøres flere opplysninger enn det som er nødvendig for formålet, og opplysningene skal tilgjengeliggjøres uten navn, fødselsnummer eller andre direkte personentydige kjennetegn med mindre slike opplysninger av særlige grunner er nødvendige. Opplysningene kan bare tilgjengeliggjøres dersom det er ubetenkelig ut fra etiske, medisinske og helsefaglige hensyn.

Helsepersonelloven § 29 regulerer kun dispensasjon fra taushetsplikten, og ikke andre sider ved utvikling og bruk av beslutningsstøtteverktøy og kunstig intelligens.

### 2.5 Andre lands rett

Verken *svensk* eller *dansk* regelverk har egne bestemmelser om bruk av opplysninger som behandles til politimessige formål til testing eller utvikling av informasjonssystemer. Heller ikke innenfor grensekontroll finnes det slike bestemmelser.

Den *finske* lag om behandling av personuppgifter vid Gränsbevakningsväsendet har i § 16 annet ledd en hjemmel for at opplysninger i Gränsbevakningsväsendets personregister kan brukes for analyser, planlegging og utvikling. I registeret lagres både opplysninger fra reisedokumenter og signalementsopplysninger for å fastsette identitet, herunder ansiktsbilde, jf. § 6 nr. 15 og § 7 andre ledd nr. 9. Også bestemmelsene i lag om behandling av personuppgifter i polisens verksamhet §§ 13, 15 og 55 åpner for at henholdsvis opplysninger i politiets personregister, opplysninger som behandles for kvalitetssikring av DNA-prøver og opplysninger i skyddspolisens informasjonssystem uten hinder av taushetspliktsregler kan brukes til lovlighetsovervåking, (analyse – kun etter § 13,) planlegging og utvikling. Bestemmelsene og forarbeidene til disse konkretiserer ikke nærmere hva slags

utvikling bestemmelsene hjemler, for eksempel om det er snakk om utvikling av informasjonssystemer.

## 2.6 Regulering av testing og utvikling i politiregisterlovgivningen

### 2.6.1 Gjeldende rett

Politiregisterloven og politiregisterforskriften regulerer politiets behandling av opplysninger til politimessige formål, samt PSTs forvaltningsvirksomhet og etterretningsvirksomhet, jf. politiregisterloven § 3. Politiregisterforskriften § 1-3 både presiserer og utvider lovens virkeområde i nærmere angitte tilfeller.

Etter politiregisterloven § 3 gjelder politiregisterloven for «politiets og påtalemyndighetens behandling av opplysninger», med unntak av behandling av opplysninger etter nr. 1 (behandling som reguleres av SIS-loven) og 2 (behandling av opplysninger som er en del av politiets forvaltningsvirksomhet eller sivile gjøremål). Testing og utvikling av informasjonssystemer er ikke eksplisitt nevnt, og omfattes verken av nr. 1 eller nr. 2.

Behandling av opplysninger er definert i politiregisterloven § 2 nr. 2 som «enhver elektronisk eller manuell bruk av opplysninger, som for eksempel innsamling, registrering, systematisering, strukturering, oppbevaring, tilpasning, endring, gjenfinning, søking, videreformidling ved overføring, spredning eller andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, sperring, sletting eller tilintetgjøring eller en kombinasjon av slike bruksmåter». Definisjonen er vid, og omfatter også behandling som skjer ved bruk av ulike informasjonssystemer.

Regelverket er utformet teknologinøytralt, det vil si at det regulerer alle former for behandling av opplysninger til formål som er omfattet av loven. Det legger ikke føringer på hvilken teknologi som skal benyttes i oppgaveløsningen.

I utgangspunktet er det derfor ikke behov for egne hjemler i politiregisterloven for bruk av ulike former for informasjonssystemer, herunder systemer som benytter kunstig intelligens. I politiregisterloven § 65 a er det likevel eksplisitt inntatt at behandling kan skje ved hjelp av automatiserte analyseverktøy, noe som blant annet kan omfatte ulike former for maskinlæring. Bestemmelsen er nærmere omtalt i høringsnotatet punkt 2.8 og 3.

Behandlingsregelverket er imidlertid ikke utformet med tanke på testing og utvikling av informasjonssystemer. I den grad bruk av identifiserbare opplysninger til utviklings- og testformål i dag ikke omfattes av politiregisterloven, vil personopplysningsloven og personvernforordningen komme til anvendelse.

Personopplysningsloven gjelder etter § 2 første ledd for all behandling av personopplysninger, med mindre annet er bestemt i eller i medhold av lov. Politiregisterloven er et eksempel på en slik lov, jf. Prop. 56 LS (2017–2018) punkt 4.5.2 der det uttales:

> Nasjonale regler som gjennomfører direktiv (EU) 2016/680, vil være et eksempel på slike regler, og reglene vil dermed gå foran bestemmelsene i personopplysningsloven og forordningen. Hvorvidt reglene i personopplysningsloven og forordningen kommer til supplerende anvendelse i disse tilfellene, eller om de er fraveket i sin helhet, må avgjøres på bakgrunn av en tolkning av de aktuelle reglene.

Hvorvidt behandling av opplysninger til testing og utvikling av informasjonssystemer som skal brukes til politimessige formål reguleres i sin helhet av politiregisterloven, eller om personopplysningsloven og personvernforordningen helt eller delvis kommer til (supplerende) anvendelse, må dermed bero på en konkret tolkning.

### 2.6.2 Nærmere om behovet

I den grad det er mulig, bruker politiet syntetiske data til testing, utvikling og forvaltning av informasjonssystemer. Det er i dag noe usikkert i hvilken grad politiet kan benytte reelle opplysninger til testing og utvikling, og hvilket personvernregelverk som i tilfelle gjelder.

Det vil i en del tilfeller være nødvendig at politiets systemer testes og utvikles med reelle opplysninger. Testing med reelle opplysninger kan være nødvendig dersom syntetiske eller anonymiserte opplysninger ikke simulerer virkeligheten godt nok til at man kan være sikker på at systemet fungerer som tiltenkt. Det kan være ressurskrevende, og noen ganger tilnærmet umulig, å lage et realistisk syntetisk datasett som tar høyde for alle forhold. Datasettene kan i tillegg bli svært omfangsrike. Dette gjelder særlig ved utvikling av informasjonssystemer som bruker komplekse analyser eller statistiske modeller, eller der utviklingen av informasjonssystemet krever store mengder opplysninger, for eksempel systemer som benytter maskinlæring. De opplysningene politiet behandler skiller seg fra opplysninger andre organer har behov for i sin test- og utviklingsvirksomhet, slik at det som regel ikke vil være mulig å benytte syntetiske testdata utviklet av andre. Politiet må med andre ord selv sørge for utvikling av testdata.

Behovet for å bruke opplysninger til testing og utvikling av informasjonssystemer spenner over et vidt spekter, fra utvikling av helt nye systemer fra bunnen av, til testing og tilpasning av verktøy og systemer som er utviklet av andre. Det er derfor ikke mulig å gi en uttømmende beskrivelse av hva slags systemer det er behov for å utvikle og teste på det nåværende tidspunkt og i fremtiden. Her nevnes likevel noen konkrete eksempler for å illustrere bredden i mulige informasjonssystemer der det kan være nødvendig å bruke reelle opplysninger. Politiet har eksempelvis behov for å kunne bryte ned og hente ut typer av opplysninger (som navn, adresser, IP-adresser, kjennemerker, osv.) i større mengder tekstlig materiale, for eksempel politirapporter. Politiet benytter et eget språk og en egen struktur i egenproduserte rapporter og dokumenter. Det er svært tidkrevende og til dels umulig å produsere tilsvarende syntetisk materiale som representerer virkeligheten. Dersom modeller testes, tilpasses eller trenes på feil datagrunnlag vil dette kunne påvirke resultatene i stor grad.

Det eksisterer et stort utvalg av ferdige KI-modeller til ulike formål som det også kan være aktuelt for politiet å benytte. Disse modellene er imidlertid generelt utviklet, og må testes med opplysninger politiet sitter på for å kunne verifiseres før de tas i bruk.

Et annet aktuelt tilfelle er testing av nye versjoner av programvare, for eksempel i systemer for passasjerinformasjon (PNR), jf. politiregisterforskriften kapittel 60. PNR-data er til dels ustrukturert data og det er stor grad av variasjon i innholdet i meldingene PNR-enheten mottar fra flyselskaper. Enheten mottar store mengder data hver dag og databasen inneholder mange millioner PNR-meldinger som systemet til enhver tid må prosessere. Dette gjør det igjen vanskelig å lage

syntetisk data som speiler data i produksjon, og det er risiko for avvik og feil dersom programvare ikke testes med reelle opplysninger.

Enkelte særlige behov som gjør seg gjeldende i forbindelse med etterforsking og bruk av tvangsmidler omtales i punkt 2.6.3.6@ og 2.7 @.

### 2.6.3 Forslag til endringer

#### 2.6.3.1 *Innledning*

Det er etter departementets syn et klart behov for at politiet kan teste og videreutvikle eksisterende tekniske løsninger og utvikle og teste nye informasjonssystemer som kan bidra til en effektiv og tidsriktig oppgaveløsning. I den forbindelse kan det være behov for å benytte reelle opplysninger i større eller mindre omfang. Spørsmålet i det følgende er i hvilken grad det er behov for en eksplisitt regulering av bruk av opplysninger til testing og utvikling, og hvor omfattende denne reguleringen bør være.

Det kan argumenteres for at bruk av opplysninger i forbindelse med utvikling og testing av informasjonssystemer der opplysninger skal behandles til formål som omfattes av loven, allerede er omfattet av politiregisterloven og LED. Dette som følge av at behandlingen skal resultere i systemer som skal brukes til formål som er omfattet av politiregisterloven. Etter det departementet kjenner til har en slik tolkning av LED vært lagt til grunn i praksis i våre naboland.[1] For å unngå tvil om adgangen til å bruke opplysninger til testing og utvikling og hvilket personvernregelverk som gjelder i disse tilfellene, mener departementet likevel at bruk av opplysninger til testing og utvikling av systemer som skal brukes til formål som omfattes av politiregisterloven bør reguleres nærmere.

Som omtalt i punkt 2.3.2 anses testing og utvikling etter GDPR som et eget eller annet formål enn det opprinnelige. For behandling som følger GDPR skaper ikke dette problemer, ettersom forordningen vil gjelde selv om behandlingen har et annet formål.

For LED og politiregisterloven blir vurderingen av om testing og utvikling skal anses som et eget formål en annen. LED åpner som nevnt i punkt 2.3.3 ikke for at direktivet kan komme til anvendelse dersom opplysninger behandles til andre formål enn de som er omfattet av direktivets virkeområde. Dersom testing og utvikling av systemer med kriminalitetsbekjempelsesformål anses som et annet formål enn kriminalitetsbekjempelse, vil GDPR gjelde for denne behandlingen. Bruk av opplysninger til testing og utvikling av systemer som skal brukes til å ivareta kriminalitetsbekjempende formål, har så nær sammenheng med det opprinnelige formålet at de samme personvernreglene bør gjelde også for denne behandlingen. Riktig nok har EU-domstolen i flere saker uttalt at unntakene i personvernforordningen artikkel 2 nr. 2 skal «tolkes strengt», se bl.a. C-180/21 avsnitt 73. Uttalelsene har imidlertid kommet i saker som dreier seg om bruk til formål som klarere skiller seg fra kriminalitetsbekjempelse enn testing og utvikling av informasjonssystemer med kriminalitetsbekjempelsesformål. Domstolen har hittil ikke tatt stilling til hvorvidt testing og utvikling av systemer som skal brukes i kriminalitetsbekjempelsen kan falle innenfor LEDs virkeområde.

[1] Opplyst fra Kripos.

Departementet mener derfor at testing og utvikling av systemer som skal brukes til politimessige formål, må kunne innfortolkes i formålene som er nevnt i LED artikkel 1 nr. 1 og i politimessige formål, og at LED dermed gjelder for denne behandlingen.[2] Dette finner også til dels støtte i KI-forordningens regler om utvikling av høyrisiko KI-systemer der systemet trenes ved bruk av trenings-, validerings- og testdatasett. Artikkel 10 nr. 5 angir at ut over bestemmelsene i GDPR og LED må en rekke andre vilkår være oppfylt for at treningsdata skal kunne inneholde særlige kategorier av personopplysninger. Dersom slik utvikling skulle reguleres utelukkende av GDPR, ville det ikke vært nødvendig å vise til LED i denne artikkelen.

I det følgende anses derfor testing og utvikling ikke som et eget eller annet formål enn politimessige formål. Det er likevel behov for å gi en klar hjemmel for at reelle opplysninger kan brukes til testing og utvikling og å regulere denne formen for behandling nærmere.

For noen typer opplysninger gjelder særskilte formålsbegrensninger slik at de ikke kan behandles til alle politimessige formål, jf. også politiregisterloven § 4. Dette gjelder for eksempel opplysninger fra enkelte skjulte tvangsmidler, jf. straffeprosessloven § 216 i og politiloven § 17 f. Videre kan opplysninger som er sperret, for eksempel opplysninger som behandles etter politiregisterloven ny § 65 a, bare brukes til de formålene som er særskilt angitt. For slike opplysninger må det tas stilling til om testing og utvikling faller innenfor noen av de tillatte formålene. Faller testing og utvikling utenfor, må det inntas som egne formål. Se høringsnotatet punkt 2.7 og 2.8.

Som omtalt i punkt 2.4 finnes det hjemler for testing og utvikling i annen lovgivning. Forslaget i dette punktet har likhetstrekk med disse hjemlene og har til dels samme begrunnelse. Departementet foreslår likevel en noe mer omfattende regulering for politiets behandling av opplysninger til test og utvikling. Begrunnelsen for dette er hovedsakelig at politiet har adgang til å behandle opplysninger som er beheftet med usikkerhet eller som er innhentet ved bruk av tvangsmidler.

#### 2.6.3.2 *Forslag til lovendringer*

Departementet foreslår å utvide politiregisterlovens virkeområde i § 3, slik at loven også gjelder når opplysninger behandles for testing og utvikling av informasjonssystemer som skal brukes til formål innenfor lovens virkeområde. Dette omfatter både politimessige formål og PSTs etterretningsvirksomhet og forvaltningsvirksomhet. Forslaget medfører at opplysninger som i bruksfasen av et informasjonssystem er omfattet av politiregisterloven, også vil være omfattet av loven når politiet og påtalemyndigheten behandler opplysningene for test og utvikling av systemet. Det vil blant annet innebære at krav til informasjonssikkerhet, sporing, kvalitet, formålsbestemthet osv. vil gjelde også når opplysningene behandles i forbindelse med testing og utvikling.

Det er etter departementets syn likevel behov for å gi særlige bestemmelser i forskriften for denne typen behandling. Politiregisterloven § 69 om hva det kan gis

[2] Datatilsynet har i Politihøgskolen, sluttrapport: PrevBOT punkt 5 kommet til en annen konklusjon med henvisning til at unntaket i GFPR artikkel 2 nr. 2 bokstav d etter sin ordlyd retter seg mot mer tradisjonelle og utpregede «politioppgaver»: Politihøgskolen, sluttrapport: PrevBOT | Datatilsynet

forskrifter om er ikke uttømmende, men er utformet slik at den «i størst mulig grad gir oversikt over på hvilke områder det kan gis forskrift», jf. Ot.prp. nr. 108 (2008–2009) punkt 18.3.4. Bestemmelsen er endret en rekke ganger for å sikre dette. Departementet foreslår derfor at det gis en forskriftshjemmel i politiregisterloven § 69 slik at det kan gis nærmere regler i forskrift om behandling av opplysninger i forbindelse med testing og utvikling av informasjonssystemer. De nærmere forskriftsreglene omtales i de følgende punktene.

Det understrekes at forslaget her ikke åpner for at politiet kan innhente opplysninger de ikke ellers ville hatt hjemmel til å behandle for å bruke dem til testing og utvikling. Forslaget åpner bare for at opplysninger som allerede behandles, også kan brukes til testing og utvikling av systemer som skal benyttes til formål innenfor loven. Det åpner derfor heller ikke for at opplysninger kan brukes for å teste eller utvikle systemer med formål som faller utenfor politiregisterlovens virkeområde.

#### 2.6.3.3 *Nærmere om forskriftsreguleringen*

Departementet foreslår at det gis en egen forskriftsbestemmelse som regulerer testing og utvikling, se forslag til politiregisterforskriften ny § 1-5. Som et grunnleggende utgangspunkt bør testing og utvikling av informasjonssystemer skje ved bruk av anonyme eller fiktive data. Hvis bruk av slike opplysninger er tilstrekkelig for å oppnå formålet, er bruk av reelle opplysninger ikke nødvendig. Hjemler for testing og utvikling i annet regelverk viser som regel til at reelle data kan brukes dersom det ville være umulig eller uforholdsmessig vanskelig å oppnå formålet ved å bruke anonyme eller fiktive opplysninger. At det er «umulig» å oppnå formålet omfatter både tilfeller der testingen eller utviklingen faktisk ikke lar seg gjennomføre, eller der bruk av syntetiske data er teoretisk mulig, men vil gi et vesentlig dårligere resultat eller uakseptabel risiko for feil. At det er «uforholdsmessig vanskelig» å bruke anonyme eller fiktive data kan være tilfelle der det vil være svært tid- eller ressurskrevende å lage et representativt fiktivt datasett eller å anonymisere reelle data fullt ut.

Departementet foreslår at det forskriftsfestes et tilsvarende krav om at det vil være umulig eller uforholdsmessig vanskelig å oppnå formålet ved bruk av anonyme eller syntetiske data, jf. forslag til § 1-5 første ledd. Kravet skal forstås på samme måte som i annet regelverk, men for informasjonssystemer som benyttes av politiet kan det være flere tilfeller der kravet er oppfylt enn for andre offentlige etater. Politiets IT-systemer er store og komplekse, og inneholder opplysninger om et stort antall personer. Opplysninger fra et register kan i tillegg sammenstilles med opplysninger fra andre registre, slik at det er behov for å se hvordan opplysninger fra ulike systemer virker sammen når det testes og utvikles. I praksis kan et for strengt krav om å benytte anonyme eller fiktive opplysninger føre til at IT-systemer ikke blir erstattet eller oppgradert tilstrekkelig ofte og med tilstrekkelig god kvalitet. Testing og utvikling ved bruk av reelle opplysninger vil kunne være et viktig tiltak for å sikre kvalitet og sikkerhet i systemene.

Utviklings- og testingsvirksomheten skal ikke ha større omfang enn det som er nødvendig for å oppnå formålet. Dette følger av det generelle kravet om dataminimering i LED artikkel 4 nr. 1 bokstav c om at opplysningene ikke skal være «for omfattende» ut fra formålet de behandles for. Det må derfor tas stilling til hvilke opplysninger som er nødvendige å bruke, og omfanget må ikke være mer omfattende enn nødvendig. En for streng tolkning vil imidlertid kunne legge

uhensiktsmessige begrensninger på testing og utvikling av systemer som benytter for eksempel maskinlæring eller kunstig intelligens. Slike systemer trenger store mengder data for å lære. Direktivets krav til dataminimering innebærer ikke nødvendigvis at politiet må vurdere om hver enkelt opplysning som inngår i materialet modellen trenes på isolert sett er nødvendig eller ikke. Det må imidlertid sikres at treningsdata er representative og tilstrekkelige for det modellen skal trenes til.

Opplysninger skal ikke brukes til testing og utvikling lenger enn nødvendig, noe som foreslås forskriftsfestet i første ledd. Departementet har vurdert om det bør settes en konkret tidsfrist for hvor lenge opplysninger kan brukes til testing og utvikling, men finner en forskriftsfestet tidsfrist vanskelig. Hvor lenge opplysningene er nødvendige vil kunne variere avhengig av det konkrete tilfellet. Utvikling av nye systemer kan gå over lang tid, og det kan være nødvendig å teste og videreutvikle eksisterende systemer mer eller mindre kontinuerlig. Et ytterpunkt vil uansett være de gjeldende slettefristene, særlig de som følger av politiregisterforskriften del 11. Det vil ikke være anledning til å beholde opplysninger som skulle vært slettet kun fordi de er nødvendige for testing og utvikling.

Ved trening av maskinlæringsmodeller ved bruk av reelle data er det en potensiell risiko for at modellen «husker» deler av dataen den er trent på. Ved treningen vil opplysningene kunne omformes til såkalte «vekter» (tall som representerer vektorer/tensorer) i modellen. Opplysningene vil dermed bli en integrert del av modellen, som det ikke er mulig å fjerne uten å slette hele modellen. Etter departementets vurdering vil disse vektene ikke anses som personopplysninger i LEDs forstand da de ikke lenger kan knyttes til fysiske personer som kan identifiseres direkte eller indirekte, og de omfattes dermed ikke av slettekravet.

#### 2.6.3.4 *Krav om den behandlingsansvarliges godkjenning*

Den behandlingsansvarlige må sikre at testing og utvikling skjer i tråd med regelverket. Dette følger i og for seg av de alminnelige reglene om internkontroll i politiregisterforskriften kapittel 39, men reglene der er ikke spesielt utformet med tanke på testing og utvikling. Departementet mener derfor at det bør gis mer utfyllende regler om den behandlingsansvarliges kontroll med denne typen behandling. Dette vil sikre at den behandlingsansvarlige i det enkelte tilfelle må ta stilling til hvordan testingen og utviklingen bør og skal innrettes.

Kripos, som er behandlingsansvarlig for de fleste registrene som er regulert i politiregisterforskriften, har allerede utviklet rutiner for å gi tillatelse til bruk av opplysninger til testing og utvikling. Dersom reelle opplysninger ønskes brukt til testing og utvikling må det blant annet redegjøres for hva som skal testes og utvikles og til hvilket formål, hva slags opplysninger som er tenkt brukt, hvem det vil behandles opplysninger om, mengden opplysninger, om det kan brukes anonymiserte og/eller fiktive data, hvor lenge behandlingen er nødvendig og risiko og tiltak for å minske denne. Dette bidrar til å ramme inn behandlingen.

Departementet foreslår at det stilles krav i forskriften om at den behandlingsansvarlige skal godkjenne behandling av opplysninger til testing og utvikling av informasjonssystemer, jf. forslaget til § 1-5 annet ledd. Videre foreslås det at den behandlingsansvarlige kan stille nærmere krav til behandlingen, og det gis noen eksempler på særlig aktuelle krav. Disse er behandlingens

varighet, hvilke typer opplysninger som skal brukes og omfanget av behandlingen. Opplistingen i forslaget er ikke uttømmende, og stenger ikke for at andre vilkår og krav kan stilles, avhengig av hva som anses egnet for den aktuelle testingen og utviklingen.

Videre foreslås det å forskriftsfeste at kravene må kunne dokumenteres.

#### 2.6.3.5 *Hvilke opplysninger som kan brukes til testing og utvikling*

Politiregisterlovgivningen oppstiller ulike vilkår og terskler for å behandle opplysninger, avhengig av typen opplysninger og hvor de er registrert. Disse kravene vil også gjelde for behandling i forbindelse med testing og utvikling, selv om det ikke reguleres særskilt.

Etter politiregisterloven § 7 kan behandling av særlige kategorier av personopplysninger bare finne sted dersom det er strengt nødvendig ut fra formålet med behandlingen. Det strenge nødvendighetskravet vil som utgangspunkt også gjelde dersom særlige kategorier av personopplysninger skal brukes til testing og utvikling. Dette vil for eksempel kunne være tilfelle ved systemer som er ment å behandle eller analysere biometriske opplysninger som ansiktsfoto, da det i liten grad er mulig å utføre tilfredsstillende testing og utvikling med syntetiske biometriske opplysninger. Det vil ikke nødvendigvis være mulig å sortere ut særlige kategorier av personopplysninger fra eksempelvis straffesaksdokumenter eller registre der opplysningene finnes sammen med annen informasjon. Departementet mener at i slike tilfeller må dokumentene/opplysningene likevel kunne brukes til testing og utvikling, dersom vilkårene ellers er oppfylt. At materialet kan inneholde særlige kategorier av personopplysninger vil imidlertid måtte tas i betraktning ved den behandlingsansvarliges vurdering av om behandlingen skal tillates, herunder hvilke vilkår som skal stilles for behandlingen. At behandlingen inkluderer bruk av særlige kategorier av personopplysninger vil også være et moment som taler for at behandlingen kan medføre høy risiko og dermed utløser krav om forhåndsdrøftelser, jf. politiregisterforskriften § 41-2 og punkt 2.6.3.9@ i høringsnotatet.

En begrensning som allerede følger av regelverket er at sperrede opplysninger ikke kan brukes til testing eller utvikling med mindre dette reguleres særskilt. Ut over opplysninger som er sperret etter politiregisterloven § 65 a, ser departementet det ikke som aktuelt å åpne for at sperrede opplysninger kan brukes til testing og utvikling av informasjonssystemer. Endringene i politiregisterloven § 65 a omtales i punkt 2.8.

Departementet foreslår at opplysninger som behandles etter politiregisterloven § 8 eller § 65 ikke skal kunne brukes testing og utvikling, jf. forslag til § 1-5 tredje ledd. Dette er opplysninger som politiet og PST ikke vet om oppfyller kravene til formålsbestemthet, nødvendighet og kvalitet, og som kan behandles i inntil fire måneder med sikte på å avklare om disse kravene er oppfylt. Å åpne for at slike opplysninger også skal kunne brukes til testing og utvikling vil kunne gjøre det mer betenkelig at det tillates at slike opplysninger i det hele tatt behandles. Departementet foreslår derfor en eksplisitt avgrensning mot at slike opplysninger kan brukes til testing og utvikling. I lys av at forskriften § 5-4 første ledd stiller krav om at slike opplysninger enten skal holdes atskilt fra opplysninger som oppfyller lovens alminnelige krav eller merkes særskilt, legger departementet til

grunn at det vil være håndterbart for politiet og PST å sikre at denne typen opplysninger ikke benyttes til testing og utvikling.

Ustrukturerte data og ikke-verifiserte opplysninger vil ikke nødvendigvis ha en form eller kvalitet som egner seg for bruk til testing og utvikling. Departementet mener likevel at det ikke bør avgrenses mot bruk av ikke-verifiserte opplysninger. Det kan være nødvendig å bruke ikke-verifiserte opplysninger i en del former for testing og utvikling, for eksempel når et register som inneholder slike opplysninger skal videreutvikles, eller dersom hensikten er å utvikle eller teste et system som skal bistå i å vurdere troverdighet og pålitelighet til ikke-verifiserte opplysninger. Videre inneholder straffesaksdokumenter ofte ikke-verifiserte opplysninger, og det kan være nødvendig å bruke slike for eksempelvis å utvikle systemer for sammendrag eller sammenstilling av opplysninger.

Ut over begrensningene som allerede følger av regelverket og den eksplisitte avgrensningen mot §§ 8 og 65-opplysninger, antar departementet at det ikke bør legges for store begrensninger på hvilke opplysninger som kan brukes til testing og utvikling. Avhengig av typen system som skal testes, utvikles eller videreutvikles, kan det være behov for å benytte forskjellige typer opplysninger. Skal et av politiets register videreutvikles eller fornyes, kan det være nødvendig å benytte alle slags opplysninger som er registrert der for å teste systemet, herunder hvordan det samvirker med andre registre og systemer.

Et annet moment departementet har lagt vekt på i vurderingen av hvilke opplysninger som skal kunne brukes, er at maskinlæringsmodeller krever store mengder data for å lære. Resultatene av slike modeller blir sikrere dersom de trenes på større og representative datamengder. Det kan være større risiko ved at politiet kjøper ferdige modeller, uten mulighet til å teste modellene med politiets egne opplysninger for å se hvordan de fungerer eller justere for skjevheter eller feil, enn at politiet selv utvikler modeller og informasjonssystemer som trenes på egne data. Dersom visse typer opplysninger utelukkes helt fra treningsmaterialet, kan det medføre skjevheter, diskriminering og feil som i ytterste konsekvens kan få betydning for personer som får sine opplysninger behandlet i systemene når de tas i bruk. Trening på ufullstendige eller ikke-representative datasett kan også være i strid med kravene i KI-forordningen artikkel 10.

For informantregisteret, jf. politiregisterforskriften kapittel 57, anser departementet det likevel som betenkelig å åpne for at reelle opplysninger skal kunne brukes til testing og utvikling. Dersom en informants identitet blir kjent, kan dette medføre alvorlig fare for personens liv eller helse. Det er derfor svært få personer som har tilgang til dette registeret, jf. politiregisterforskriften § 57-5. Departementet ber særlig om høringsinstansenes syn på om det bør stenges helt for at reelle opplysninger fra informantregisteret kan brukes til testing og utvikling. I så fall kan testing og videreutvikling av dette registeret utelukkende skje ved bruk av anonymiserte eller fiktive opplysninger,

#### 2.6.3.6 *Særlig om opplysninger fra digitale beslag*

Noen særlige problemstillinger gjør seg gjeldende for digitale beslag, jf. straffeprosessloven § 203. Ved digitale beslag tar politiet gjerne midlertidig beslag i en databærer (for eksempel en telefon eller en PC), som ofte speilkopieres. Speilkopien gjennomgås og opplysninger som antas å ha betydning som bevis

hentes ut. De uthentede opplysningene inngår i sakens dokumenter, mens speilkopien etter rettspraksis ikke gjør det, jf. HR-2018-1901-U avsnitt 17 og 19:

(17) Gjennomgangen kan lede til at politiet tar beslag i dokumenter som finnes på speilkopien. Slike beslag besluttes av påtalemyndigheten etter straffeprosessloven § 205, hvor ett vilkår er at dokumentet «antas å ha betydning som bevis», jf. § 203. Dette innebærer at beslag i bestemte dokumenter ikke skjer allerede på det tidspunktet politiet får treff i et elektronisk søk i en speilkopi, hvor søket har skjedd med hjelp av visse søkeord eller lignende. Det kreves i tillegg en vurdering og en beslutning. Relevansvurderingen kan ikke gjøres før beslutningstakeren har sett selve dokumentet.

(19) Etter ankeutvalgets syn vil et dokument fra en speilkopi ikke gå inn i «sakens dokumenter» før det er gjennomgått av politiet eller påtalemyndigheten, og det dessuten er tatt en beslutning om å innlemme dokumentet, typisk ved beslag. Ikke før dette har skjedd, er det naturlig å betrakte dokumentet som «hentet ut» fra speilkopien.

For å gjennomgå databærere for å finne bevis kan det være behov for informasjonssystemer som for eksempel kan transkribere mediefiler, oversette, sammenstille og gjenkjenne objekter i bilder og videoer (for eksempel kjøretøy og våpen). Et annet eksempel er løsninger for å finne kryptovalutaadresser og tilhørende mnemonics (en rekkefølge av tilfeldige ord som gir tilgang til en kryptovalutakonto) i beslag. Disse følger en fast struktur og lar seg lett syntetisere, men for å finne ut hvor og hvordan dette blir gjemt må politiet basere seg på tidligere beslag hvor slike opplysninger er funnet. Det er nyttig for utviklere å få tilgang til beslag hvor det er funnet kryptovaluta og mnemonics for å skjønne hvordan disse gjemmes og dermed hvilke teknikker og metoder som er nødvendig å benytte i en slik løsning.

En speilkopi vil inneholde store mengder informasjon, der det aller meste vil være overskuddsinformasjon uten betydning for den konkrete saken. Selv om speilkopien er i politiets besittelse og det kan tenkes at det er behov for å benytte reelle speilkopier for å teste verktøy for å hente ut informasjon fra speilkopier, mener departementet at det ikke bør åpnes for at speilkopier kan brukes til testing og utvikling. Slik bruk vil kunne innebære et betydelig personverninngrep. Selv om dette gjør at eventuelle nye verktøy ikke kan testes på reelle data før de tas i bruk, og dette kan medføre en viss risiko for at verktøyet ikke fungerer som forventet, mener departementet at hensynet til personvernet her må veie tyngst. Departementet foreslår derfor at informasjon fra beslag og utleveringspålegg bare kan brukes til testing og utvikling dersom opplysningene inngår i straffesakens dokumenter. På denne måten åpnes det ikke for å benytte selve speilkopien til testing og utvikling.

#### 2.6.3.7 *Særlig om sletting i test- og utviklingsmiljøer*

Dersom testing og utvikling skjer i samme tekniske løsning som annen behandling, vil opplysningene ikke lenger være tilgjengelig for testing og utvikling når slettefristen inntrer, uten at dette reguleres særskilt.

Dersom behandlingen skjer i egne utviklings- og testmiljøer, må det derimot etableres mekanismer som sikrer at opplysningene slettes når de ikke lenger er nødvendige for testing og utvikling, og at de heller ikke lever videre i disse miljøene etter at de slettes i systemet opplysningene er hentet fra. Departementet foreslår å forskriftsfeste at opplysningene i slike tilfeller skal slettes senest når slettefristen for den opprinnelige registreringen inntrer. I tillegg foreslås det presisert at opplysninger i slike situasjoner skal tilintetgjøres. Opplysningene i

test- og utviklingsmiljøene vil være kopier av opplysninger som finnes i andre systemer, og de har derfor ikke selvstendig arkivfaglig verdi. De er heller ikke gjenstand for saksbehandling i vanlig forstand. Ved sletting i kilderegisteret vil opplysningene uansett arkiveres eller tilintetgjøres etter reglene for det aktuelle registeret. At det forskriftsfestes at opplysninger i test- og utviklingsmiljøer skal tilintetgjøres innebærer dermed bare en tydeliggjøring av hvordan opplysningene skal slettes, og ikke et unntak fra arkivlovens kassasjonsforbud.

#### 2.6.3.8 *Tilgang ved testing og utvikling*

Politiregisterforskriften § 8-2 første ledd nr. 4 åpner for at det kan gis tilgang til opplysninger når det er nødvendig for drift og administrasjon av informasjonssystemet. Dette vil til en viss grad omfatte tilgang i forbindelse med testing og utvikling for å sikre at et eksisterende informasjonssystem fungerer og for retting av feil mv., men bestemmelsen bør ikke etterlate tvil om at det kan gis tilgang til testing og utvikling.

Departementet foreslår derfor en endring i politiregisterforskriften § 8-2 så det kommer klart frem at tilgang til opplysninger kan gis når det er nødvendig til testing og utvikling.

En del opplysninger som behandles av politiet er underlagt særskilte tilgangsbegrensninger. For eksempel er tilgangen til referat fra bekymringssamtaler etter politiregisterforskriften § 58-6 begrenset til «et mindre antall personer som har fått særskilt bemyndigelse». Tilsvarende krav finnes for tilgang til DNA-registerets profildatabase, jf. § 45-11. Den behandlingsansvarlige må i slike tilfeller vurdere konkret om det skal gis tilgang til opplysningene til bruk for testing og utvikling, og i så fall gi de aktuelle personene slik særskilt bemyndigelse som bestemmelsene krever.

#### 2.6.3.9 *Konsekvensutredning og forhåndsdrøftinger*

Politiregisterforskriften § 41-1 stiller krav om at den behandlingsansvarlige før visse behandlinger iverksettes skal foreta en vurdering av konsekvensene behandlingen vil ha for personopplysningsvernet. Kravet oppstår dersom det er trolig at en type behandling, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, vil medføre en høy risiko for fysiske personers rettigheter og friheter, jf. § 41-1 første ledd. Annet ledd inneholder en nærmere opplisting av hva vurderingen minst skal inneholde, herunder skal risikoen vurderes og det skal planlegges tiltak for å redusere den. Bestemmelsen gjennomfører krav som følger av LED artikkel 27.

Bestemmelsens ordlyd tar høyde for at det kan være nødvendig å vurdere personvernkonsekvensene før utvikling og testing både av nye og eksisterende informasjonssystemer. Departementet ser derfor ikke behov for endringer i denne bestemmelsen.

Etter politiregisterforskriften § 41-2 skal den behandlingsansvarlige rådføre seg med Datatilsynet dersom vurderingen etter § 41-1 tilsier at behandlingen vil medføre en høy risiko, eller dersom behandlingen på grunn av ny teknologi, nye mekanismer eller prosedyrer innebærer høy risiko for de registrertes rettigheter og friheter. Plikten er begrenset til behandling av personopplysninger i registre, både i og utenfor straffesak, og for sammenstilling av opplysninger fra registre som omfattes av forskriften del 11, jf. annet ledd. Begrunnelsen for begrensningen er at kravet om forhåndsdrøftelser er snevrere etter LED enn etter GDPR. LED artikkel

28 stiller bare krav om forhåndsdrøftinger ved behandling som vil inngå i et nytt register. LED er ikke til hinder for at det fastsettes strengere tiltak for å verne den registrertes rettigheter og friheter, jf. fortalepunkt 15. Det kan derfor etableres krav om forhåndsdrøftinger i flere tilfeller enn det som følger av LED.

Noen former for testing og utvikling av informasjonssystemer kan få konsekvenser av en slik art at forhåndsdrøftinger bør gjennomføres, selv om behandlingen ikke inngår i et register eller en sammenstilling. Departementet mener derfor at plikten til å rådføre seg med Datatilsynet generelt bør gjelde ved testing og utvikling som kan medføre en høy risiko for de registrertes rettigheter og friheter, uavhengig av om behandlingen inngår i et register eller en sammenstilling. Datatilsynet vil kunne gi skriftlige råd dersom den behandlingsansvarlige ikke i tilstrekkelig grad har identifisert eller redusert risikoen ved den planlagte behandlingen, jf. forskriften § 41-3. I denne forbindelse kan tilsynet også benytte seg av virkemidlene som nevnt i politiregisterloven § 60, noe som blant annet omfatter å gi pålegg og stille vilkår for å sikre at lovens krav om informasjonssikkerhet og internkontroll oppfylles.

Datatilsynets tilsynskompetanse avgrenses etter politiregisterforskriften § 42-1 mot politiets og påtalemyndighetens behandling av saker etter straffeprosessloven kapittel 16a, § 216 m og § 216 o, jf. straffeprosessloven § 216 h. Som følge av dette vil ikke kravet om forhåndsdrøftelser med Datatilsynet komme til anvendelse for testing og utvikling ved bruk av opplysninger som er innhentet ved kommunikasjonskontroll, romavlytting eller dataavlesing, jf. forslaget om å åpne for dette i punkt 2.7. Ettersom det er snakk om inngripende tvangsmidler, kan det være et særskilt behov for å sikre en grundig vurdering av konsekvensene før testing og utvikling med opplysninger fra slike tvangsmidler settes i verk.

Departementet er noe i tvil om det på dette området bør innføres et krav om forhåndsdrøftelser med Datatilsynet selv om behandlingen ellers kontrolleres av Kontrollutvalget for kommunikasjonskontroll (KK-utvalget). Forhåndsdrøftelser kan gjennomføres uten at Datatilsynet gis innsyn i de faktiske opplysningene som er innhentet, noe som taler for at kravet om forhåndsdrøftelser også bør gjelde på dette feltet. Samtidig kan det tenkes noen uheldige konsekvenser dersom et tilsynsorgan gir skriftlige råd om den forestående behandlingen og kan gi pålegg og anmerkninger i den forbindelse, jf. politiregisterforskriften § 41-3 og politiregisterloven § 60, mens et annet tilsynsorgan kan gi anmerkninger i etterkant. Departementets foreløpige vurdering er likevel at kravet om forhåndsdrøftelser også bør gjelde ved bruk av opplysninger fra skjulte tvangsmidler til testing og utvikling, men at Datatilsynet i slike tilfeller kun kan gi skriftlige råd og anmerkninger, men ikke pålegg. At det ikke kan gis pålegg i slike tilfeller foreslås inntatt i § 41-3. Det bes særlig om høringsinstansenes syn på spørsmålet.

Det foreslås ikke å innføre et krav om forhåndsdrøftelser med Datatilsynet for PSTs behandling av opplysninger til testing og utvikling, uavhengig av hvordan opplysningene er innhentet. Her vil EOS-utvalget føre kontroll på vanlig måte.

#### 2.6.3.10 *Særlig om meldeplikt ved testing og utvikling*

Kravet om vurdering av personvernkonsekvenser og forhåndsdrøftelser med Datatilsynet gjør at tilsynet blir kjent med testing og utvikling som politiet vurderer at kan medføre høy risiko. Tilsynet vil imidlertid ikke få beskjed om

testing og utvikling som ikke vurderes å medføre slik risiko. Som ledd i arbeidet med dette høringsnotatet har departementet hatt et møte med Datatilsynet. Datatilsynet ytret i møtet ønske om i større grad å kunne ha oversikt over den samlede bruken av kunstig intelligens i politiet, særlig med tanke på at behandlingen som regel ikke vil være kjent for offentligheten. Tilsynet skisserte som en mulighet å etablere en meldeplikt til Datatilsynet om testing og utvikling, særlig av systemer som bruker kunstig intelligens.

Departementet ser at det er argumenter som taler for en slik meldeplikt og at dette vil kunne lette tilsynsvirksomheten. Det er i tilfelle viktig at plikten innrettes på en måte som verken påfører politiet eller tilsynet unødvendig ressursbruk. En eventuell meldeplikt bør begrenses til testing og utvikling av en viss størrelse og/eller som kan tenkes å medføre personvernkonsekvenser av et visst omfang. Det er ikke nødvendig eller ønskelig at enhver endring av et informasjonssystem skal meldes til Datatilsynet. Videre må det være klart i hvilke tilfeller plikten utløses, særlig dersom plikten skal knyttes til kunstig intelligens. Definisjonen av et KI-system etter KI-forordningen artikkel 3 nr. 1 gir rom for tolkning, og kommisjonen skal som omtalt i punkt 2.3.4 utarbeide retningslinjer for anvendelsen av denne definisjonen. Definisjonen i KI-konvensjonen artikkel 2 er ikke fullt ut sammenfallende med KI-forordningens definisjon. Det er med andre ord utfordrende på det nåværende tidspunkt å avgrense hvilke KI-systemer som bør omfattes av en eventuell meldeplikt.

Departementet har derfor ikke utformet forslag regelverksendringer om en meldeplikt for testing og utvikling av informasjonssystemer, men ber særlig om høringsinstansenes syn på om en slik ordning bør etableres og hvordan den i tilfelle kan innrettes.

#### 2.6.3.11 *Personvernkonsekvenser av forslaget*

Politiets behandling av opplysninger etter politiregisterloven er ikke betinget av samtykke fra den registrerte, og personen vil i en del tilfeller ikke vite at hen er registrert. Bestemmelsene om den registrertes rettigheter vil gjelde på vanlig måte når opplysningene behandles til testing og utvikling. Den registrerte vil dermed for eksempel ikke kunne få større innsyn i opplysninger som brukes til testing og utvikling enn det som følger av de alminnelige innsynsreglene i politiregisterloven. Regelverksendringene vil imidlertid gjøre det klart at opplysninger politiet behandler kan bli brukt til testing og utvikling, og på den måten sikre større forutberegnelighet.

Selv om denne formen for behandling er noe annet enn det som ga grunnlag for at personen ble registrert i første omgang, vurderer departementet at den i utgangspunktet har relativt begrensede konsekvenser for de registrerte. Testingen og utviklingen vil ikke medføre konsekvenser for den enkeltes rettsstilling, og det skal ikke treffes noen avgjørelser overfor den registrerte. Den registrerte vil dermed selv ikke merke noe til at opplysningene brukes på denne måten. Kravet om den behandlingsansvarliges godkjenning og mulighet til å stille vilkår for å ramme inn behandlingen bidrar også til at behandlingen ikke får større omfang enn nødvendig. Videre gjør kravet om forhåndsdrøftelser at Datatilsynet vil bli involvert før testing og utvikling som kan medføre høy risiko settes i verk.

Forslaget medfører ikke at opplysningene skal kunne utleveres til andre. Det åpner heller ikke for at opplysninger kan innhentes eller behandles utelukkende for

testing og utvikling. Opplysningene vil ikke kunne lagres lenger enn det de kan etter de alminnelige slettereglene. Det vil si at de ikke kan beholdes utelukkende for testing og utvikling, dersom de ellers skulle vært slettet.

Forslaget er begrenset til bruk av opplysninger til testing og utvikling. Det åpner derfor ikke for at politiet kan ta i bruk informasjonssystemer som er av en slik inngripende art at de krever særskilt hjemmel.

Departementet mener derfor at personvernkonsekvensene samlet sett står i et rimelig forhold til de formålene bestemmelsen skal oppnå.

## 2.7 Særlig om bruk av informasjon fra skjulte tvangsmidler til testing og utvikling

Et særlig spørsmål er om informasjon som er innhentet ved hjelp av skjulte tvangsmidler skal kunne brukes til testing og utvikling.

Straffeprosessloven § 216 i og politiloven § 17 f setter rammer for hvilke formål opplysninger fra skjulte tvangsmidler i henholdsvis straffesaker og PSTs forebyggende saker kan brukes til. Testing og utvikling av informasjonssystemer er ikke nevnt. På grunn av den inngripende karakteren slike tvangsmidler har, er adgangen til å bruke opplysninger fra skjulte tvangsmidler snevrere enn for andre opplysninger politiet behandler. Bestemmelsene er utformet som regler om taushetsplikt og unntak fra denne, men innebærer også en regulering av hvilke formål opplysningene kan brukes til, jf. Ot.prp. nr. 108 (2008–2009) punkt 9.2.5.

Det finnes en rekke eksempler på at det kan være behov for å bruke opplysninger og materiale innhentet ved skjulte tvangsmidler i reelle saker til å teste og utvikle tekniske løsninger som kan bidra til bedre oversikt, ressursbesparelser og at mer informasjon kan utledes av det innhentede materialet. For eksempel kan det være behov for verktøy som kan transkribere, oversette og lage sammendrag av materiale fra kommunikasjonskontroll. Kommunikasjonskontroll kan resultere i store mengder lydopptak og tekst på fremmedspråk, i så store mengder at det praktisk sett er umulig å få oversatt det. Et ferdig utviklet oversettelses- eller transkriberingsprogram vil ikke nødvendigvis kunne ta høyde for eksempelvis slang og intern begrepsbruk i et kriminelt miljø. Ferdigutviklede verktøy for å lage sammendrag eller sammenstille informasjon vil heller ikke nødvendigvis være tilpasset hvilken informasjon politiet er ute etter i materialet, slik at det kan være nødvendig å teste og gjøre justeringer slik at det ivaretar politiets særlige behov. Ved å tilpasse modellene basert på informasjon politiet sitter på om typisk språkbruk og kontekst, vil de kunne bli mer egnet for formålet.

Departementet ser at det er innvendinger mot at opplysninger som er underlagt formålsbegrensningene i straffeprosessloven § 216 i og politiloven § 17 f skal kunne brukes til testing og utvikling. Tvangsmidlene er inngripende, noe som tilsier at adgangen til å bruke de innhentede opplysningene ikke bør være for vid. Samtidig er det nettopp på dette området et særlig behov for å ha verktøy som kan bidra til enklere oversikt, sammenstilling og oversettelse, samt for å finne relevante bevis. Slike verktøy kan bidra til å redusere den manuelle gjennomgangen av opplysninger, noe som igjen kan være positivt i et personvernperspektiv.

Departementet har derfor, under noe tvil, kommet til at også opplysninger innhentet ved kommunikasjonskontroll, romavlytting og dataavlesing bør kunne

brukes til testing og utvikling av informasjonssystemer. Formålene som straffeprosessloven § 216 i første ledd tredje punktum bokstav a til k og politiloven § 17 f bokstav a til e i dag åpner for at opplysninger kan behandles til, er snevrere enn definisjonen av politimessige formål i politiregisterloven § 2 nr. 13. Etter departementets syn kan ikke testing og utvikling innfortolkes i noen av alternativene som allerede er inntatt. Det foreslås derfor at testing og utvikling av informasjonssystemer som skal brukes innenfor politiregisterlovens virkeområde inntas som egne formål i bestemmelsene.

Departementet er usikker på om det bør stilles ytterligere krav for at opplysninger som er omfattet av formålsbegrensningene i § 216 i og politiloven § 17 f skal kunne brukes til testing og utvikling. Departementets foreløpige vurdering er at de krav som foreslås for bruk av andre opplysningskategorier er tilstrekkelige til å ta høyde for de særlige hensyn som gjør seg gjeldende for opplysninger fra skjulte tvangsmidler. I kravet om at den behandlingsansvarlige skal godkjenne behandlingen, jf. punkt 2.6.3.4, ligger også at det må vurderes hvilke typer opplysninger som skal kunne brukes. At det er snakk om opplysninger fra skjulte tvangsmidler vil være et moment som må tas med i vurderingen av om at behandlingen skal godkjennes, og kan tilsi at den behandlingsansvarlige setter strengere rammer enn det som vil være naturlig med mindre inngripende opplysninger.

At det foreslås å innføre krav om forhåndsdrøftelser med Datatilsynet, jf. punkt 2.6.3.9, vil også være en sikkerhetsmekanisme. Testing og utvikling ved bruk av opplysninger fra inngripende tvangsmidler taler for at behandlingen har høy risiko.

Forslaget åpner ikke for at opplysninger som skal slettes etter straffeprosessloven § 216 g annet ledd kan brukes til testing og utvikling. Heller ikke informasjon som er sperret etter politiregisterloven § 50 tredje ledd kan brukes til testing og utvikling. I Prop. 4 L (2019–2020) punkt 5.1.4 uttales det at sperring av opplysningene i innhentingssaken ikke påvirker den videre behandlingen av opplysninger som allerede er overført til andre formål. Opplysninger som skal sperres i innhentingssaken kan derfor «leve videre» for eksempel i en annen straffesak. Dette er ikke ønskelig for testing og utvikling. Det foreslås derfor endringer i forskriften § 25-4 slik at opplysninger som er tatt i bruk til testing og utvikling skal sperres på samme tidspunkt som opplysninger i innhentingssaken.

KK-utvalget fører kontroll med politiets bruk av kommunikasjonskontroll, romavlytting og dataavlesing, med unntak av saker som omfattes av EOS-kontrolloven, jf. straffeprosessloven § 216 h og kommunikasjonskontrollforskriften § 14 første ledd. Etter forskriften § 14 annet ledd skal utvalget kontrollere at «de opplysningene som politiet har fått ved kommunikasjonskontroll, romavlytting og dataavlesing, bare blir brukt på lovlig måte, og at lovens regler om oppbevaring, sperring og sletting av opplysninger blir fulgt». Bruk av opplysninger fra tvangsmidler som er omfattet av kontrollutvalgets mandat til testing og utvikling vil dermed også falle inn under utvalgets kontrollområde.

## 2.8 Bruk av åpent tilgjengelig informasjon innhentet for etterretningsformål til testing og utvikling

### 2.8.1 Gjeldende rett

Ved lov 28. april 2023 nr. 11 ble det tilføyd en ny § 65 a i politiregisterloven som åpner for at PST kan behandle åpent tilgjengelig informasjon dersom det antas å være nødvendig for utarbeidelse av analyser og etterretningsvurderinger. Opplysningene kan for dette formål behandles ved hjelp av automatiserte analyseverktøy. Automatiserte analyseverktøy er ikke definert i loven, men kan for eksempel være ulike former for maskinlæring og systemer som benytter kunstig intelligens. Bestemmelsen har foreløpig ikke trådt i kraft, i påvente av forskriftsbestemmelsene som foreslås i punkt 3 i dette høringsnotatet.

Etter § 65 a annet ledd skal opplysningene være sperret. Sperring innebærer blant annet at formålene opplysningene skal brukes til må være regulert særskilt, noe som er gjort i annet ledd nr. 1 til 3. Etter bestemmelsen kan de sperrede opplysningene bare brukes til følgende formål:

1. utarbeidelse av analyser og etterretningsvurderinger
2. opprettelse av eller bruk i forebyggende sak
3. etterforskning av lovbrudd som nevnt i politiloven § 17 b

Testing og utvikling, verken av automatiserte analyseverktøy eller andre former for informasjonssystemer, er ikke nevnt, og kan ikke innfortolkes i noen av alternativene i nr. 1 til 3. Som følge av dette åpner den vedtatte lovbestemmelsen etter sin ordlyd ikke for at PST kan bruke de sperrede opplysningene til å utvikle og teste automatiserte analyseverktøy til bruk for utarbeidelse av analyser og etterretningsvurderinger, selv om lovteksten åpner for at slike verktøy kan benyttes.

I Prop. 31 L (2022–2023) er det lagt til grunn at PST skal kunne utvikle egne automatiserte analyseverktøy, blant annet uttales det at forslaget «åpner for at det kan utvikles og benyttes maskinlæringsmodeller», og at ved «utvikling og kjøp av nye verktøy må det sikres at kontrollbehovene ivaretas i løsningene», jf. proposisjonen punkt 8.9.3. Proposisjonen sier ingenting om hvordan slike verktøy skal kunne utvikles og testes, herunder hvilke opplysninger som skal kunne brukes.

### 2.8.2 Forslag til endringer

Etter departementets syn er det et klart behov for at PST kan benytte opplysninger som behandles etter politiregisterloven § 65 a for å utvikle og teste informasjonssystemer som bestemmelsen åpner for at kan brukes. Dette gjelder også automatiserte analyseverktøy. Bestemmelsens ordlyd tar imidlertid ikke høyde for slik bruk. Som følge av at formålene de sperrede opplysningene skal kunne brukes til må være eksplisitt regulert, er det nødvendig at test og utvikling inntas i bestemmelsen. Selv om testing og utvikling anses for å falle inn under politimessige formål, kan slik behandling ikke innfortolkes i de formålene bestemmelsen i dag åpner for at opplysningene kan brukes til.

Departementet foreslår derfor at utvikling og testing av informasjonssystemer som skal brukes innenfor bestemmelsens første ledd, tilføyes i annet ledd nytt nr. 4 som et formål de sperrede opplysningene kan brukes til. Dette vil være i tråd med de

intensjoner som er lagt til grunn i proposisjonen. Forslaget vil åpne for at opplysningene kan brukes til å teste og utvikle selve systemet for behandling av åpent tilgjengelig informasjon, samt systemer som skal brukes i forbindelse med analyser og etterretningsvurderinger, blant annet automatiserte analyseverktøy. Det åpnes ikke for å bruke opplysningene til å teste og utvikle systemer med rene forebyggings- eller etterforskingsformål.

At PST selv tester og utvikler verktøyene som skal brukes, eller tilpasser innkjøpte verktøy (hyllevare) til tjenestens særskilte behov, har flere fordeler. For PST selv kan det bidra til at verktøyene er bedre innrettet mot tjenestens behov, og de kan justeres for skjevheter og unøyaktigheter. Dette vil redusere risikoen for at systemene produserer resultater som gir et uriktig bilde av trusler mot nasjonale sikkerhetsinteresser, som igjen kan gi analyser og vurderinger med lav kvalitet som ikke er egnet som beslutningsstøtte. For kontrollformål er det også en fordel at PST har størst mulig kontroll over de tekniske verktøyene og systemene som benyttes. Som nevnt må automatiserte analyseverktøy være innrettet slik at EOS-utvalget kan føre kontroll med innretningen på og bruken av dem. Dette vil lettere kunne ivaretas dersom PST selv utvikler og tester verktøyene, og det kan gi større grad av etterprøvbare resultater.

Det vil være helt nødvendig at faktisk åpent tilgjengelig informasjon kan brukes til å teste og utvikle informasjonssystemer etter bestemmelsen. Det er ikke mulig å skape et stort nok sett med fiktive data som er realistisk nok til å utvikle, teste og trene systemene. Automatiserte analyseverktøy krever et bredt informasjonsgrunnlag for å gi presise resultater, noe som best kan sikres ved en mulighet for at de også testes ved hjelp av reelle data. Som nevnt i punkt 2.3.4 faller bruk av kunstig intelligens utelukkende for nasjonale sikkerhetsformål utenfor KI-forordningen. Forordningen legger dermed ikke føringer for systemer som skal kunne brukes etter politiregisterloven § 65 a første ledd, med mindre de også tas i bruk til andre formål. De verktøy som er aktuelle å bruke for utarbeidelse av analyser og etterretningsvurderinger vil uansett falle utenfor de KI-systemene forordningen forbyr, jf. artikkel 5, og det som defineres som høyrisiko bruk av kunstig intelligens, jf. vedlegg III.

Selv om opplysningene brukes til testing og utvikling vil de fremdeles være sperret. Bruk til dette formålet medfører dermed ikke at opplysningene skal flyttes over til PSTs alminnelige registre eller at personene som berøres anses for å være registrert hos PST. Kravene etter forslaget til ny § 1-5 vil, med unntak av begrensningene i hvilke opplysninger som kan behandles, også gjelde for testing og utvikling etter politiregisterloven § 65 a, jf. forslaget til § 21-8 åttende ledd. Dersom testing og utvikling skjer separat fra de sperrede opplysningene må opplysningene slettes når slettefristen etter § 65 a tredje ledd inntrer.

Forslaget endrer ikke på vilkårene for å kunne innhente informasjon etter bestemmelsen. Grunnvilkåret for behandlingen er at opplysningene må antas å være nødvendige for utarbeidelse av analyser og etterretningsvurderinger. Det kan derfor ikke innhentes åpent tilgjengelig informasjon etter § 65 a utelukkende til bruk for testing og utvikling. Departementet vurderer at personvernkonsekvensene for de berørte er begrenset, og at konsekvensene av at PST ikke kan bruke de innhentede opplysningene til å utvikle eller teste verktøyene før de tas i bruk potensielt kan være mer inngripende for de berørte.

## 2.9 Regulering av testing og utvikling i grenselovgivningen

### 2.9.1 Gjeldende rett

Grensekontroll er en del av politiets forvaltningsvirksomhet, og behandling av opplysninger for grensekontrollformål reguleres av personopplysningsloven og GDPR. Grenseloven § 22 regulerer behandling av opplysninger til gjennomføring av grensekontroll. Den generelle hjemmelen finnes i første ledd, som angir at politiet kan behandle opplysninger som er nødvendige for gjennomføring av grensekontroll etter loven. Dette omfatter også særlige kategorier av personopplysninger. Etter annet ledd kan opplysninger om reisende behandles i et register for gjennomføring av inn- og utreisekontroll. Grense- og territorialkontrollregisteret (heretter GTK) er nærmere regulert i grenseforskriften kapittel 5. Bestemmelsene er teknologinøytrale, slik at de gjelder for behandling av opplysninger til det angitte formålet, uavhengig av den tekniske løsningen. Grenseforskriften § 5-4 tredje ledd åpner for at tilgang til GTK kan gis til ansatte med ansvar for drift, utvikling og administrasjon av informasjonssystemet og for å sikre at behandlingen skjer i samsvar med personopplysningsloven. Ansiktsfoto fra reisedokumenter fra reisende som passerer grensekontrollen lagres i GTK, jf. § 5-3 første ledd nr. 2. Fingeravtrykk lagres ikke, jf. avgrensningen i samme nr.

Grenseloven og forskriften inneholder ellers ingen regulering av testing og utvikling av informasjonssystemer.

Grenseloven § 22 tredje ledd angir at biometrisk personinformasjon (ansiktsfoto og fingeravtrykk) kan innhentes elektronisk av alle som passerer grensekontroll eller annet kontrollsted for kontroll av reisedokumenter. Grenseloven § 22 tredje ledd viderefører tidligere bestemmelse i passloven § 6 a, som ble opphevet ved grenseloven. I passloven § 6 a annet ledd var det angitt at opplysningene skulle slettes så snart som mulig når identiteten er verifisert mot gyldig reisedokument, eller når identiteten er fastslått på annen måte. I Prop. 161 L (2016–2017) s. 87 (merknadene til § 22) er det uttalt at denne sletteregelen skulle videreføres i grenseforskriften, men dette er ikke gjort. Det er imidlertid ingen hjemmel for å lagre verken ansiktsfoto eller fingeravtrykk opptatt i grensekontrollen.

### 2.9.2 Nærmere om behovet

Systemene som benyttes til grense- og territorialkontroll utvikles kontinuerlig, noe som medfører et løpende behov for å verifisere at systemene fungerer som de skal. Det er behov for å kunne teste alt av programvare, opptaksutstyr, integrasjoner, kvalitet på data og algoritmenes nøyaktighet.

Selv om politiet benytter fiktive data til testing og utvikling der det er mulig, er det i mange tilfeller behov for å bruke reelle data. Behovet gjør seg særlig gjeldende for biometriske opplysninger som ansiktsfoto og fingeravtrykk.

Syntetiske data av ansikter, fingeravtrykk, mv. kan brukes på noe testing, men dekker blant annet ikke den fysiske situasjonen med opptak av data fra en fingeravtrykksleser. Politiet har behov for å teste og sikre at opptaksutstyr fungerer som det skal til enhver tid. Produksjon av syntetiske data er svært tidkrevende og gir begrenset innsikt i en reell situasjon. Bruk av syntetiske data er heller ikke tilstrekkelig for å få et representativt utvalg av fingeravtrykk, og politiet får ikke testet kvalitetskravene i tilstrekkelig grad med slike data.

Videre er det et behov for å kunne lagre ansiktsfoto opptatt i grensekontrollen for testing og utvikling av systemer for automatisert kontroll av personer som passerer yttergrensen. Kontrollen skal skje i form av en til en biometrisk sammenligning av ansiktsfoto i databrikken mot ansiktsfoto tatt på grensen (verifisering av identitet). For å sikre en sikker og effektiv automatisert ansiktssammenligning i grensekontrollen må det settes terskelverdier for når ansiktsfoto opptatt i grensekontrollen og ansiktsfoto i reisedokumentet anses for å være samme person. Denne terskelen må settes på et nivå som både avdekker personer som benytter andres reisedokumenter, samtidig som personer ikke skal stanses for unødvendige kontroller (falske treff). For å få dette riktig må et representativt utvalg ansiktsfoto opptatt i grensekontrollen lagres i en periode for å kunne utføre nødvendig utvikling, test, analyse og optimalisering av systemet. Det er svært viktig at dataene er representative ut fra for eksempel kjønn, alder og etnisitet for å unngå at noen grupper plukkes ut for andrelinjekontroll oftere enn andre.

Forordning (EU) 2017/2226 om inn- og utreisesystemet (EES-forordningen) forutsetter at kontroll av ansiktsfoto og fingeravtrykk skal tas i bruk ved grensepassering i større grad enn i dag. Etter artikkel 23 nr. 2 tredje ledd skal det ved grensepassering foretas en kontroll av biometriske opplysnionger opptatt i grensekontrollen med foto registrert i EES eller med fingeravtrykk som er registrert i EES eller VIS (visuminformasjonssystemet). Forordningen sier ingenting om at denne sammenligningen må skje automatisert, men det vil klart være den mest hensiktsmessige måten å gjennomføre kontrollen på for å sikre en effektiv grensekontroll.

Dersom tredjelandsborgeren ikke allerede er registrert i EES, skal det opprettes en individuell saksmappe med alfanumeriske og biometriske data, herunder ansiktsbilde opptatt i grensekontrollen. Etter artikkel 15 nr. 2 skal grensekontrollmyndighetene, i ekstraordinære tilfeller der det ikke er mulig å oppfylle spesifikasjonene for registrering av ansiktsbilde i EES, i stedet trekke ut ansiktsbilde fra den elektroniske brikken i reisedokumentet og registrere dette i EES, etter en elektronisk kontroll av at ansiktsbildet i brikken tilsvarer ansiktsbildet av personen tatt på stedet. I slike tilfeller stiller dermed forordningen krav om at det må foretas en form for automatisert ansiktsgjenkjenning for å verifisere at personen er rette innehaver av reisedokumentet.

Politidirektoratet har opplyst at for persongruppen som er omfattet av EES, dvs. tredjelandsborgere, vil automatisert ansiktssammenligning ved bruk av live opptatt ansiktsfoto bli standard metode for å undersøke identitet.

EES-forordningen skal begynne å gjelde fra 10. november 2024. Også etter at forordningen har begynt å gjelde vil det være behov for å lagre ansiktsfoto for å sikre at systemet fungerer som det skal, og for testing, feilretting og videreutvikling.

Som omtalt i punkt 2.3.4 anses ikke systemer som behandler biometriske opplysninger til biometrisk gjenkjenning som høyrisiko kunstig intelligens etter KI-forordningen dersom behandlingen er begrenset til kontroll mot reisedokumenter for å verifisere identitet, jf. forordningen vedlegg III og definisjonen av biometrisk verifikasjon i artikkel 3 nr. 35. Slik behovet er beskrevet fra Politidirektoratet vil opplysningene ikke brukes til å teste og utvikle systemer som utgjør høyrisiko KI-systemer som vil kreve særskilt hjemmel.

Grenseloven § 15 tredje ledd gir uansett hjemmel til å benytte ansiktsgjenkjenning og kontroll av fingeravtrykk i forbindelse med inn- og utreisekontroll.

### 2.9.3 Forslag til endringer

#### 2.9.3.1 *En klar hjemmel for testing og utvikling i grenseloven*

Departementet foreslår at det gis en uttrykkelig hjemmel for at opplysninger som behandles i forbindelse med grensekontroll kan benyttes til testing og utvikling av informasjonssystemer som brukes til grensekontrollformål. Forslaget er utformet etter mal av reglene som omtalt i punkt 2.4 ovenfor, og vil åpne for at opplysninger som er lagret i systemer som benyttes for grensekontrollformål, som GTK og andre systemer som gjøres tilgjengelige via GTK (som FKL[3] og FKS[4]) også kan benyttes for dette formålet. Forslaget gir ikke hjemmel for å innhente nye opplysninger til bruk i testing og utvikling (med unntak av forslaget i neste punkt), og åpner ikke for at opplysningene kan lagres lenger enn regelverket ellers åpner for.

Det foreslås at behandling av reelle opplysninger til testing og utvikling er betinget av at det er umulig eller uforholdsmessig vanskelig å oppnå formålet ved hjelp av anonyme eller fiktive opplysninger, jf. forslag til § 22 a første ledd. Begrensningen skal forstås på samme måte som i politiregisterlovgivningen, jf. forslaget ovenfor, og i bestemmelsene i annet regelverk, jf. punkt 2.4. Begrensningen har størst betydning for andre opplysninger enn biometriske opplysninger. Som nevnt vil det i dag som regel være umulig eller uforholdsmessig vanskelig å benytte anonyme eller fiktive biometriske opplysninger til testing og utvikling, slik at bruk av reelle opplysninger på dette området vil være hovedregelen snarere enn et unntak.

Selv om behovet for en hjemmel for testing og utvikling særlig er begrunnet i behovet for testing og utvikling av systemer for biometrisk sammenligning, foreslår departementet at hjemmelen ikke begrenses til slike systemer. Den teknologiske utviklingen medfører at det vil åpne seg nye teknologiske muligheter og lages nye verktøy som kan bidra til en effektiv og hensiktsmessig grensekontroll. For at politiet skal kunne benytte seg av disse mulighetene, må systemer kunne utvikles og testes for å sikre at de fungerer etter intensjonen og ikke får utilsiktede konsekvenser for de reisende.

I forslaget presiseres det at opplysningene ikke skal behandles til testing og utvikling lenger enn nødvendig. Hvor lenge dette vil være avhenger av hva den konkrete testingen og utviklingen går ut på. Det åpnes ikke for at opplysninger kan behandles for testing og utvikling etter at de skulle vært slettet etter reglene som ga grunnlag for registreringen.

#### 2.9.3.2 *Hjemmel for lagring av ansiktsfoto og fingeravtrykk opptatt i grensekontrollen til bruk for testing og utvikling*

Som omtalt i punkt 2.9.1 er det i dag ingen hjemmel for å lagre ansiktsfoto og fingeravtrykk opptatt i grensekontrollen, men det fremgår heller ikke klart av

[3] FKL (Forhåndskontroll Luft) er et system for forhåndskontroll av API-data fra flyselskaper som skal støtte politiets oppgaver innen grensekontroll.

[4] FKS (Forhåndskontroll Sjø) er et web-basert system som mottar informasjon om anløp fra Kystverkets rapporteringssystem (SSN-N), inklusive lister over mannskap og passasjerer.

regelverket at de biometriske opplysningene som opptas i grensekontrollen skal slettes. I dette punktet foreslås det å åpne for lagring av ansiktsfoto og fingeravtrykk utelukkende for testing og utvikling. Denne lagringsmuligheten representerer et unntak fra den i dag ulovfestede sletteplikten. Departementet mener derfor at ordlyden i passloven tidligere § 6 a annet ledd bør inntas i grenseloven § 22 tredje ledd, for å tydeliggjøre at fingeravtrykk og ansiktsfoto ikke kan lagres ut over der det er nødvendig for testing og utvikling.

Departementet foreslår å innføre en hjemmel for lagring av ansiktsfoto og fingeravtrykk opptatt i grensekontrollen for en viss periode utelukkende for dette formålet, jf. forslaget til § 22 a annet ledd. Begrunnelsen for forslaget er som omtalt i punkt 2.9.2 at det er behov for å utvikle, teste og vedlikeholde systemene som skal benyttes til verifisering av identitet mot reisedokumenter, og sette korrekte terskelverdier for når identitetsopplysningene samsvarer. I tillegg er det behov for å teste fysisk utstyr for opptak av biometriske opplysninger. Denne typen testing og utvikling er i dag ikke mulig å gjennomføre uten reelle biometriske opplysninger.

Lagring av ansiktsfoto og fingeravtrykk og bruk av opplysningene til testing og utvikling innebærer behandling av særlige kategorier av personopplysninger, det vil si behandling av biometriske opplysninger med det formål å entydig identifisere en fysisk person. Behandling av særlige kategorier av personopplysninger er i utgangspunktet forbudt etter GDPR artikkel 9 nr. 1, men er likevel tillatt dersom et eller flere av vilkårene i nr. 2 er oppfylt.

Det aktuelle grunnlaget i artikkel 9 nr. 2 er bokstav g om at behandlingen er nødvendig av hensyn til viktige allmenne interesser. Å sikre en forsvarlig og effektiv grensekontroll og at personene som passerer grensen faktisk er den personen de utgir seg for å være, er utvilsomt viktige allmenne interesser. Det samme gjelder det å sikre at personer ikke unødvendig blir plukket ut til annenhåndskontroll. Av den grunn må også det å utvikle og teste systemer som ivaretar disse hensynene anses som en viktig allmenn interesse som kan begrunne behandling av biometriske opplysninger.

Behandling av særlige kategorier av personopplysninger til formål som nevnt i artikkel 9 nr. 2 bokstav g krever et grunnlag i nasjonal rett, som må stå i et rimelig forhold til det mål som søkes oppnådd, være forenlig med det grunnleggende innholdet i retten til vern av personopplysninger og sikre egnede og særlige tiltak for å verne den registrertes grunnleggende rettigheter og interesser. Departementet foreslår flere regler for å ivareta disse kravene.

For det første må lagringen av de biometriske opplysningene være nødvendig for å teste og utvikle systemer til bruk for grensekontroll. Det gis dermed ikke en generell hjemmel for lagring av ansiktsfoto og/eller fingeravtrykk av alle som passerer grensekontrollen. I hvilket omfang det er nødvendig å lagre opplysninger må vurderes konkret, og vil kunne variere over tid. Det foreslås ingen nærmere regulering av omfanget av biometriske opplysninger som kan lagres ut over at det må være nødvendig for testing og utvikling.

Som omtalt i forrige punkt må det være umulig eller uforholdsmessig vanskelig å oppnå formålet for at reelle personopplysninger skal kunne brukes til testing og utvikling. Dette vil også gjelde for bruk av ansiktsfoto og fingeravtrykk opptatt i grensekontrollen for testing og utvikling.

For det andre foreslås det en særskilt formålsbegrensning slik at biometriske opplysninger utelukkende kan benyttes til testing og utvikling av systemer for grensekontrollformål. De kan dermed ikke benyttes til andre formål eller i andre sammenhenger. Lagringen vil ikke få konsekvenser for personens mulighet til å passere grensen. Det vil ikke foretas andre undersøkelser opp mot politiets registre, og ansiktsfotoene vil heller ikke kunne utleveres til andre

For det tredje foreslås det at ansiktsfoto og fingeravtrykk skal holdes atskilt fra andre opplysninger som behandles for grensekontrollformål. Dette kan gjøres enten ved at opplysningene lagres i et eget system eller ved at det etableres et logisk skille mellom disse opplysningene og andre opplysninger. Begrunnelsen for kravet er at opplysningene utelukkende skal kunne brukes til testing og utvikling og ikke for andre formål, og de skal ikke være tilgjengelig for eksempel i forbindelse med grensekontroll. I tillegg skal tilgang til ansiktsfoto og fingeravtrykk bare gis til personer som er særskilt bemyndiget. Kravet skal forstås på samme måte som tilsvarende krav etter politiregisterlovgivningen, og innebærer at personene må ha tjenestemessig behov for tilgang, være kvalifisert og ha gjennomgått opplæring. Bemyndigelse gis av den behandlingsansvarlige.

For det fjerde foreslås det en klar begrensning i hvor lenge de biometriske opplysningene kan lagres. Etter forslaget kan ansiktsfoto og fingeravtrykk lagres i inntil seks måneder, og de må deretter slettes. Begrunnelsen for denne fristen er at det er viktig å sikre at opplysninger ikke brukes til testing og utvikling lenger enn nødvendig. Samtidig kan fristen ikke settes så kort at det kontinuerlig må innhentes nye biometriske opplysninger av nye personer.

Ansiktsfoto og fingeravtrykk skal etter forslaget til fjerde ledd slettes i form av tilintetgjøring. Etter arkivlova § 9 bokstav c går kassasjonsforbudet foran sletteregler i annet regelverk. Et forslag til ny arkivlov ble sendt på høring i oktober 2021. Det er ennå ikke fremmet noen proposisjon på bakgrunn av høringsforslaget. Etter departementets syn vil forslaget i dette høringsnotatet ikke være et unntak fra kassasjonsforbudet. Arkivfaglige hensyn tilsier ikke at ansiktsfotoene eller fingeravtrykkene skal lagres for ettertiden. Opplysningene lagres utelukkende for testing og utvikling, og er dermed ikke gjenstand for saksbehandling i tradisjonell forstand. Opplysningene har også begrenset verdi for ettertiden. De vil bestå av et tilfeldig utvalg ansiktsfoto og fingeravtrykk, som skal sikre et representativt utvalg til bruk for testing og utvikling. Dersom opplysningene skal lagres for ettertiden utelukkende fordi personens bilde tilfeldigvis ble valgt ut, kan det i tillegg oppleves som en belastning for den enkelte.

I tillegg til de kravene som foreslås lovfestet, skal opplysningene ifølge Politidirektoratet behandles i en avidentifisert form, det vil si at alfanumeriske opplysninger (som navn) fjernes slik at personen ikke er direkte identifiserbar. Også opplysninger om når og hvor grensepassering skjedde vil fjernes før testing. Dette vil ivareta prinsippet om dataminimering i GDPR artikkel 5 nr. 1 bokstav c.

#### 2.9.3.3 *Personvernkonsekvenser av forslagene*

Konsekvensene for den registrerte av at opplysninger som behandles i forbindelse med grensekontroll også kan brukes til testing og utvikling vurderes å være forholdsvis begrenset. Behandlingen vil ikke ha betydning for deres mulighet til å passere grensen og det vil ikke foretas andre undersøkelser opp mot politiets

registre. Behandlingen vil derimot bidra til å forbedre og effektivisere grensekontrollen og sikre likebehandling, noe som vil komme alle reisende til gode.

Forslaget om å åpne for å lagre ansiktsfoto og fingeravtrykk til bruk for testing og utvikling har noe større personvernkonsekvenser. Dette er opplysninger som politiet ikke har hjemmel til å lagre til grensekontrollformål per i dag, og det representerer dermed noe nytt. Opplysningene er i tillegg særlige kategorier av personopplysninger etter GDPR, noe som gjør at det er særlig viktig at det er gode rammer for behandlingen. Regelverket vil sikre forutberegnelighet ved at det er klart at opplysninger kan bli lagret og hvilke regler som vil gjelde for behandlingen, men den enkelte reisende vil ikke nødvendigvis få vite om vedkommendes ansiktsfoto eller fingeravtrykk vil bli lagret ved en konkret grensepassering. Den enkelte har heller ingen mulighet til å motsette seg lagringen, da passering av grensen ikke vil være mulig uten å avgi biometriske opplysninger for kontroll av identitet og reisedokumenter. Departementet legger til grunn at den behandlingsansvarlige på egnet måte sørger for at det gjøres kjent for de reisende at biometriske opplysninger blir eller kan bli lagret ved grensepassering, for eksempel ved oppslag i grensekontrollen eller ved informasjon på politiets nettsider. Dette vil sikre at de registrerte har mulighet til å utøve sine rettigheter etter GDPR.

Forslaget rammer inn behandlingen for å begrense de personvernmessige konsekvensene og for å sikre at behandlingen ikke blir mer omfattende enn nødvendig. De biometriske opplysningene skal kun lagres for et bestemt formål i en avgrenset tidsperiode, og de skal deretter slettes. Det vil være en snever personkrets som har tilgang til dataene, det stilles krav om at opplysningene skal behandles atskilt og at personer som skal ha tilgang må være særskilt bemyndiget i tillegg til å ha tjenestemessig behov for tilgang. Dette vil samlet sett bidra til å redusere de personvernmessige ulempene av forslaget. Departementet mener at personvernkonsekvensene står i et rimelig forhold til de formålene bestemmelsen skal oppnå.

# 3 Nærmere regulering av PSTs behandling av åpent tilgjengelig informasjon

## 3.1 Kort om de vedtatte lovendringene

Ved lov 28. april 2023 nr. 11 ble det innført nye bestemmelser om PSTs etterretningsoppdrag og om behandling av åpent tilgjengelig informasjon til etterretningsformål i henholdsvis politiloven § 17 a og politiregisterloven § 65 a.

Politiloven § 17 a lovfester at PST, i tillegg til å være en politi- og sikkerhetstjeneste, også er Norges innenlands etterretningstjeneste. Oppgaven som innenlands etterretningstjeneste er formulert som at PST skal utarbeide analyser og etterretningsvurderinger om forhold i Norge som kan true Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser. Bestemmelsen trådte i kraft 1. september 2023.

Politiregisterloven § 65 a åpner for at PST kan lagre, systematisere og analysere åpent tilgjengelig informasjon for etterretningsformål. Det er et vilkår at

behandlingen antas å være nødvendig for utarbeidelse av analyser og etterretningsvurderinger, jf. politiloven § 17 a.

Etter § 65 a fjerde ledd skal det gis nærmere regler om behandlingen i forskrift, herunder om utlevering, utsatt sletting, tilgangsbegrensning og kontroll. Opplistingen er ikke uttømmende. I merknadene til bestemmelsen i Prop. 31 L (2022–2023) er det uttalt:

> Departementet tar blant annet sikte på å gi bestemmelser i forskriften som tydeliggjør krav til sporbarhet, kravene til beslutninger om å beholde opplysninger lenger enn slettefristen, regler om utlevering av sperrede opplysninger og at sperrede opplysninger skal slettes i form av tilintetgjøring. Videre vil departementet vurdere om det bør gis regler som ytterligere tydeliggjør at opplysninger som tas i bruk i konkrete saker må flyttes over i PSTs alminnelige registre, og at den videre behandlingen da vil følge de alminnelige behandlingsreglene i loven og forskriften.

## 3.2 Forslag til forskriftsbestemmelse

### 3.2.1 Innledning

Da forslag til politiregisterloven § 65 a var på høring ble det også foreslått en forskriftsbestemmelse med følgende ordlyd:

> § 21-8 *Særlig om behandling av åpent tilgjengelig informasjon etter politiregisterloven § 65 a*
>
> Opplysninger som behandles etter politiregisterloven § 65 a skal holdes atskilt. Tilgang til opplysningene skal bare gis til personer som har fått særskilt bemyndigelse.
>
> Behandling av opplysningene for etterretningsformål, jf. § 65 a tredje ledd nr. 1, kan skje ved bruk av automatiserte analyseverktøy.
>
> Bruk av opplysningene skal registreres og kunne spores for å kunne kontrollere om søkene og bruken er tillatt eller ikke. Registreringene skal gjennomgås regelmessig med det formål å avdekke uautorisert tilgang til opplysningene.

De vedtatte lovendringene fikk en annen utforming enn det som ble foreslått i høringsnotatet. Departementet mener det er behov for noe mer detaljerte forskriftsbestemmelser for å ramme inn behandlingen. Dette er også forutsatt i Prop. 31 L (2022–2023).

Det foreslås én samlet forskriftsbestemmelse om behandling av åpent tilgjengelig informasjon etter politiregisterloven § 65 a. Dette vil gjøre det lettere å finne frem til de særreglene som gjelder for denne behandlingen. Det er flere regler i politiregisterloven og -forskriften om informasjonssikkerhet, internkontroll, logging og sporing som også vil gjelde for behandlingen selv om det ikke reguleres særskilt. Forslaget er derfor begrenset til forhold som bør reguleres særskilt.

### 3.2.2 Utlevering av opplysninger

#### 3.2.2.1 *Bakgrunn*

Det følger av politiregisterloven § 65 a annet ledd at opplysningene som behandles etter bestemmelsen skal være sperret. Formålene opplysningene kan brukes til fremgår av politiregisterloven § 65 a annet ledd. Så lenge opplysningene er sperret kan de ikke brukes til andre formål enn de oppgitte og de kan heller ikke utleveres

til andre. De sperrede opplysningene vil for eksempel ikke kunne utleveres som følge av opplysningsplikt i annen lovgivning eller etter avvergingsplikten i straffeloven § 196. Det vil heller ikke være mulig å utlevere sperrede opplysninger som kan være relevante for samarbeidspartnere, herunder Etterretningstjenesten.

Opplysningene vil imidlertid kunne utleveres til andre dersom de er tatt i bruk til noen av de tillatte formålene. Dette kan for eksempel være i form av analyser og etterretningsvurderinger, det vil si når de er bearbeidet og funnet relevante for etterretningsformål. Det samme gjelder for opplysninger som er tatt i bruk og registrert i PSTs vanlige registre i forebyggende sak eller i etterforsking. Opplysningene vil i slike tilfeller ikke lenger være sperret, og kan utleveres etter de vanlige reglene i politiregisterloven og -forskriften.

I Prop. 31 L (2022–2023) punkt 8.5.3 er det uttalt at departementet tar sikte på å regulere i forskrift at opplysninger som er sperret og ikke tatt i bruk ikke vil kunne utleveres.

#### 3.2.2.2 *Departementets vurdering*

Selv om loven stenger for at sperrede opplysninger kan brukes, herunder utleveres, til andre formål enn de loven selv åpner for, foreslås det å innta i forskriftsteksten at opplysningene som er sperret etter politiregisterloven § 65 a ikke kan utleveres til andre.

Denne begrensningen gjelder bare for opplysninger som verken inngår i analyser eller etterretningsvurderinger eller er registrert i PSTs alminnelige registre på annet grunnlag. Det vil si at det bare er opplysninger som ligger i det sperrede materialet og som ikke vurderes å være relevant eller nødvendig for PSTs egen virksomhet, som ikke vil kunne utleveres. Heller ikke opplysninger som utelukkende er tatt i bruk til testing og utvikling vil kunne utleveres, ettersom dette ikke medfører at opplysningene registreres i PSTs alminnelige registre.

Departementet bemerker også at det som nevnt i proposisjonen punkt 8.5.3 er slik at dersom PST kommer over opplysninger i det sperrede materialet som normalt ville blitt utlevert etter regler om opplysningsplikt eller avvergingsplikt, kan PST undersøke om opplysningene finnes åpent tilgjengelig på nett og varsle aktuell mottaker om opplysningene. Det samme gjelder dersom PST finner informasjon som kan være relevant for samarbeidende tjenester, herunder for Etterretningstjenesten. Dette kan gjøres uten at de utleveres fra det sperrede materialet.

### 3.2.3 Tilgang til de sperrede opplysningene

#### 3.2.3.1 *Bakgrunn*

Det følger av politiregisterforskriften § 15-2 annet ledd at opplysninger som er sperret skal holdes atskilt fra øvrige registre og at tilgangen til opplysningene skal begrenses til så få personer som mulig og bare gis til personer som har fått særskilt bemyndigelse, jf. § 8-4 annet ledd. I § 8-4 annet ledd er det gitt anvisning på hva en særskilt bemyndigelse innebærer. Det skal kun gis slik bemyndigelse til personer som er kvalifisert og har gjennomgått opplæring. Det er sjef PST som gir bemyndigelsen, jf. tredje ledd.

Det følger av politiregisterloven § 21 første ledd at ansatte i politiet og påtalemyndigheten kun skal ha tilgang til den informasjonen de har et

tjenestemessig behov for. Vilkår for tilgang er nærmere regulert i politiregisterforskriften kapittel 8, hvor tjenestemessig behov er definert i § 8-3 annet ledd. Det følger av bestemmelsen at kravet om tjenestemessig behov er oppfylt dersom «tjenestemannen vil settes i stand til å treffe en riktigere eller mer velbegrunnet avgjørelse, eller utføre en mer effektiv og hensiktsmessig tjeneste, enn om vedkommende ikke hadde hatt tilgang til opplysningene».

I høringsnotatet i forkant av lovendringene foreslo departementet at det skulle fremgå av forskriften at tilgang til opplysningene bare skal gis til personer som har fått særskilt bemyndigelse. Departementet foreslo ikke at tilgangen skulle begrenses til så få personer som mulig, men det ble forutsatt at tilgang ikke skulle gis til flere personer enn nødvendig.

#### 3.2.3.2 *Departementets vurdering*

En viktig grunn til at opplysningene som er innhentet etter politiregisterloven § 65 a skal være sperret er at de skal holdes atskilt. Videre er det en sentral mekanisme for å hindre misbruk at bruk av opplysningene er tilgangsstyrt og krever bemyndigelse.

Departementet foreslår som i forrige høringsnotat at det presiseres i forskriften at opplysningene skal holdes atskilt og at tilgang krever særskilt bemyndigelse. Dette innebærer at opplysningene må holdes atskilt fra PSTs øvrige registre. Tilgang til opplysningene forutsetter at vedkommende må ha et tjenestemessig behov for tilgang, være kvalifisert og ha fått opplæring i bruk av systemet. EOS-utvalget skal til enhver tid kunne kontrollere hvem som har slik bemyndigelse.

Departementet foreslår ikke at tilgangen skal begrenses til så få personer som mulig. Hvor mange personer som skal ha tilgang til sperrede opplysninger avhenger av hva som er grunnen til at opplysningene er sperret. Vanligvis er sperring et surrogat for sletting, noe som gjør at tilgangen kan begrenses til svært få personer. Begrunnelsen for at opplysninger som behandles etter politiregisterloven § 65 a skal være sperret, er å sikre at personer som figurerer i materialet ikke skal anses registrert hos PST og at materialet skal holdes atskilt. De sperrede opplysningene skal kunne lagres, systematiseres og analyseres for å utarbeide analyser og etterretningsvurderinger. Dette gjør at gruppen som skal ha tilgang naturlig nok må være større enn når sperring er et alternativ til sletting. Begrenses tilgangen i for stor grad, er det en risiko for at man ikke oppnår formålet med bestemmelsen.

Personene som har behov for tilgang er ikke nødvendigvis de samme i alle sammenhenger. Det vil være behov for ulik kompetanse avhengig av hvilket steg i prosessen man er, for eksempel innhenting, bearbeiding og strukturering for å gjøre informasjonen tilgjengelig og forståelig for brukeren. Videre vil det være andre personer som vil ha behov for tilgang i forbindelse med en forebyggende sak eller en etterforskingssak, jf. § 65 annet ledd nr. 2 og 3.

En begrensning til «så få personer som mulig» er etter dette et lite egnet avgrensningskriterium, og vil kunne gi inntrykk av at antall personer som har tilgang er atskillig mindre enn det som vil være tilfelle. Departementet foreslår imidlertid at det presiseres i forskriften at tilgang ikke skal gis til flere personer enn nødvendig. Selv om det allerede følger av politiregisterforskriftens alminnelige system at det bare er personer som har et tjenestemessig behov for

tilgang til et system skal ha tilgang, vil presiseringen kunne ha en opplysende og pedagogisk effekt.

### 3.2.4 Registrering og behandling av sperrede opplysninger

#### 3.2.4.1 *Bakgrunn*

Når opplysninger fra det sperrede systemet inngår i ferdige etterretningsvurderinger og analyser, lagres disse i PSTs alminnelige systemer. Det følger da av politiregisterloven og -forskriftens system at de alminnelige reglene for behandling av opplysningene kommer til anvendelse.

Åpent tilgjengelig informasjon som er innhentet for utarbeidelse av analyser og etterretningsvurderinger kan også benyttes til å opprette en forebyggende sak eller etterforskingssak og i allerede opprettede saker hos PST, jf. politiregisterloven § 65 a annet ledd nr. 2 og 3. For at opplysningene skal kunne brukes i slike saker må politiregisterlovens regler om behandling av opplysninger være oppfylt, blant annet at opplysningene er nødvendige og relevante. Som omtalt i punkt 3.1 er det i merknadene til bestemmelsen i Prop. 31 L (2022–2023) uttalt at departementet vil vurdere om det bør gis regler som tydeliggjør at opplysninger som tas i bruk i konkrete saker må flyttes over i PSTs alminnelige registre, og at den videre behandlingen da vil følge de alminnelige behandlingsreglene i loven og forskriften.

#### 3.2.4.2 *Departementets vurdering*

Når opplysningene fra det sperrede systemet inngår i ferdige etterretningsvurderinger og analyser, samt i forebyggende saker eller i etterforsking, vil de måtte registreres i PSTs vanlige registre, og opplysningene vil da ikke lenger være sperret.

For å gjøre det klart at opplysningene må registreres i PSTs alminnelige registre og følge ordinære behandlingsregler dersom de benyttes til formålene som nevnt i politiregisterloven § 65 annet ledd nr. 1 til 3, foreslår departementet at dette fremgår tydelig av forskriftsbestemmelsen, se forslag til tredje ledd. At opplysningene brukes til testing og utvikling, jf. dette høringsnotatet punkt 2.8, medfører ikke at de skal registreres i PSTs alminnelige systemer. Opplysninger som utelukkende er brukt til testing og utvikling vil derfor fremdeles være sperret.

### 3.2.5 Merking

#### 3.2.5.1 *Bakgrunn*

Merking av opplysninger er definert i politiregisterloven § 2 nr. 9 som markering av lagrede opplysninger uten at hensikten er å begrense den fremtidige behandlingen av disse opplysningene. Det fremgår av Ot.prp. nr. 108 (2008–2009) punkt 21.1 at opplysninger som er merket kan behandles på samme måte som før merkingen. Hensikten med merkingen kan være forskjellig, men den vil vise at det er særlige forhold ved opplysningene som brukeren bør være klar over. Politiregisterforskriften stiller krav om merking av opplysninger i ulike sammenhenger. Blant annet skal opplysninger som behandles etter lovens § 8 merkes, jf. forskriften § 5-4. Det samme gjelder opplysninger som behandles utelukkende basert på samtykke, jf. § 6-2 tredje ledd.

I Prop. 31 L (2022–2023) er det uttalt at det skal gå klart frem av den forebyggende saken eller etterforskingssaken hvilke opplysninger som er hentet fra det sperrede materialet. På samme måte skal det fremgå klart dersom en sak er opprettet på bakgrunn av opplysninger som er hentet fra det sperrede materialet. Proposisjonen omtaler ikke nærmere hvordan dette skal skje.

#### 3.2.5.2 *Departementets vurdering*

For at det skal fremgå av opplysninger som tas i bruk i forebyggende sak eller til etterforsking at de er hentet fra det sperrede systemet, foreslår departementet at opplysningene i slike tilfeller skal merkes. Merking vil gjøre at det går klart frem at opplysningene er hentet fra det sperrede systemet, og vil legge til rette for at det kan føres kontroll med hvilke opplysninger som er hentet ut og bruken av dem. I tillegg vil brukeren til enhver tid være kjent med hvor opplysningene er hentet fra. Merkingen vil ikke innebære noen begrensning på videre bruk av opplysningene etter at de er registrert.

### 3.2.6 Krav til sporbarhet

#### 3.2.6.1 *Bakgrunn*

Både politiregisterloven og -forskriften inneholder en rekke krav til informasjonssikkerhet og internkontroll som vil gjelde for behandlingen av de sperrede opplysningene. Denne typen krav er det derfor ikke nødvendig å regulere særskilt for behandling etter politiloven § 65 a. Som eksempel kan nevnes plikt til systematiske tiltak for å sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av opplysninger. Dette innebærer å sikre at informasjonen ikke er tilgjengelig for uvedkommende, at opplysningene ikke endres utilsiktet eller av uvedkommende og at opplysningene er tilgjengelige for rettmessige brukere ved deres behov. I tillegg er PST underlagt særskilte krav til informasjonssikkerhet i sikkerhetsloven som følge av at PST behandler sikkerhetsgradert informasjon i sine systemer. For graderte deler av det sperrede systemet vil kravene i sikkerhetsloven komme til anvendelse.

Viktige krav for å kunne føre kontroll med behandlingen følger av politiregisterloven § 17 og politiregisterforskriften § 40-13, som sier at all bruk av opplysninger skal registreres og kunne spores for å kontrollere om søkene er tillatt eller ikke. Videre skal registreringene gjennomgås regelmessig med det formål å avdekke uautorisert tilgang til opplysningene. Formålet med bestemmelsen er å forebygge og kontrollere brudd på loven, først og fremst om tjenestepersonen hadde et tjenestemessig behov for opplysningene.

I høringsnotatet i forkant av lovendringene ble det foreslått å presisere i forskriften at bruk av opplysningene skal registreres og kunne spores for å kunne kontrollere om søkene og bruken er tillatt eller ikke. Registreringene skal gjennomgås regelmessig med det formål å avdekke uautorisert tilgang til opplysningene. I Prop. 31 L (2022–2023) punkt 8.7.3 er det vist til at all bruk av opplysningene må logges og kunne spores.

#### 3.2.6.2 *Departementets vurdering*

En viktig kontrollmekanisme for behandlingen etter politiregisterloven § 65 a er å kunne kontrollere hvem som har søkt i de sperrede opplysningene og hvorfor. For

å tydeliggjøre at kravene etter politiregisterforskriften § 40-13 også gjelder for de sperrede opplysningene, foreslår departementet at kravene inntas i den nye forskriftsbestemmelsen.

Etter politiregisterloven § 65 a første ledd tredje punktum kan PST bruke automatiserte analyseverktøy ved utarbeidelse av analyser og etterretningsvurderinger. Dersom slike verktøy brukes, vil det ikke nødvendigvis være mulig å spore verktøyenes automatiserte «bruk» av den enkelte opplysning. Verktøyene kan for eksempel være avanserte maskinlæringsmodeller, der det ikke alltid er mulig å vite hvilke konkrete opplysninger modellen baserer utfallet på og hvordan modellen har kommet frem til resultatet. I slike tilfeller er det søkene som er gjort, herunder formålet med søkene og hvem som har gjort dem, samt resultatene, som må spores og kunne kontrolleres.

Dersom det foretas søk i forbindelse med konkrete saker etter § 65 a annet ledd nr. 2 og 3, vil søkene kunne logges og spores på samme måte som bruk av PSTs alminnelige registre. Det samme gjelder søk i forbindelse med utarbeidelse av analyser og etterretningsvurderinger som ikke skjer ved bruk av automatiserte analyseverktøy.

PST må også etablere rutiner hvor det fremgår at det skal være notoritet over hvilke formål søket er foretatt for og av hvem. EOS-utvalget vil ha full tilgang til PSTs systemer og kan kontrollere disse.

### 3.2.7 Utsatt sletting

#### 3.2.7.1 *Bakgrunn*

Opplysningene innhentet etter politiregisterloven § 65 a som ikke er tatt i bruk i analyser og etterretningsvurderinger, forebyggende saker eller etterforskingssaker skal slettes etter fem år, med en mulighet for å beslutte utsatt sletting på nærmere vilkår, jf. bestemmelsens tredje ledd.

Ettersom fristen ble satt til fem år, mot opprinnelige 15 år som var foreslått i høringen til lovbestemmelsen, er det åpnet for at sjef PST eller den denne bemyndiger kan beslutte at opplysningene kan beholdes ytterligere i fem år av gangen, men ikke lenger enn 15 år totalt. En beslutning om utsatt sletting forutsetter at opplysningene etter en konkret vurdering fortsatt er nødvendige for utarbeidelse av analyser og etterretningsvurderinger. Det er forutsatt i proposisjonen at adgangen til å beslutte utsatt sletting skal være en unntaksregel.

I Prop. 31 L (2022–2023) punkt 8.8.3 er det uttalt at departementet i forskrift ville fastsette at beslutninger om utsatt sletting skal være skriftlige og begrunnet. Dette vil sikre at EOS-utvalget kan føre kontroll med hvilke opplysninger som beholdes lenger enn fem år og vurderingen av hvorfor opplysningene fremdeles anses nødvendige.

#### 3.2.7.2 *Departementets vurdering*

I Prop. 31 L (2022–2023) er det erkjent at det i noen tilfeller vil være behov for å beholde opplysningene i lenger tid enn fem år. I proposisjonen ble det vist til at et eksempel på en slik situasjon er behovet for å kartlegge påvirkningsvirksomhet i tilknytning til valg over flere valgperioder. Andre eksempler kan være propaganda og aktivitet som tidligere har vært spredt åpent fra terrorgrupperinger, men som senere blir slettet, og lekkede datasett fra eksempelvis Russland, som bidrar til å

identifisere personer knyttet til russiske etterretningstjenester. Selv om slike opplysninger etter omstendighetene vil kunne registreres i PSTs vanlige registre, vil ikke alle dataene nødvendigvis tilfredsstille politiregisterlovens krav. Det kan også være tilfeller der bare deler av materialet er relevant, men der «råmaterialet» er nødvendig å beholde for å følge utvikling over tid. Valgpåvirkning er et eksempel på sistnevnte.

Det er viktig at det er notoritet om beslutninger om utsatt sletting, og departementet foreslår at det reguleres i forskriften at slike beslutninger skal være skriftlige og begrunnet. Dette vil sikre at det gjøres en konkret vurdering av at opplysningene fremdeles er nødvendige, slik loven gir anvisning på.

Slettefristen etter politiregisterloven § 65 a gjelder så lenge opplysningene er sperret. Dersom opplysningene tas i bruk i forebyggende sak eller i etterforsking, jf. § 65 a annet ledd nr. 2 og 3, vil de som omtalt i punkt 3.2.4 registreres og behandles i PSTs ordinære systemer. De alminnelige slettereglene vil da gjelde for disse opplysningene. Når det gjelder de ferdige analysene og etterretningsvurderingene som er laget på bakgrunn av opplysninger i det sperrede systemet, vil den generelle regelen om at opplysningene skal slettes når de ikke lenger er nødvendige for formålet komme til anvendelse.

### 3.2.8 Sletting i form av tilintetgjøring

#### 3.2.8.1 *Bakgrunn*

Hovedregelen om sletting av opplysninger følger av politiregisterloven § 50 første ledd. Etter bestemmelsen skal opplysninger ikke lagres lenger enn det som er nødvendig for formålet med behandlingen. Opplysningene skal slettes eller sperres, med mindre de skal oppbevares i henhold til arkivloven eller annen lovgivning.

Sletting er nærmere regulert i politiregisterforskriften § 16-2, der det fremgår at sletting etter politiregisterloven eller forskriften innebærer at opplysningene skal fjernes fra registre eller andre systemer. Etter at opplysningene er fjernet fra registrene skal de enten behandles i samsvar med arkivlovgivningen eller tilintetgjøres, jf. § 16-2 annet ledd nr. 1 og 2.

For registrene som er regulert i politiregisterforskriften del 11 er det gitt anvisning på hvordan opplysningene skal slettes, ved en henvisning til politiregisterforskriften § 16-2 annet ledd nr. 1 eller 2. Etter politiregisterforskriften § 22-3 tredje ledd skal sletting av opplysninger i PSTs forebyggende virksomhet utenfor forebyggende sak skal skje i form av tilintetgjøring.

I Prop. 31 L (2022–2023) punkt 8.8.3 er det uttalt at departementet tar sikte på å tydeliggjøre i forskrift at sletting av opplysninger som er sperret etter politiregisterloven ny § 65 a skal skje i form av tilintetgjøring.

#### 3.2.8.2 *Departementets vurdering*

Departementet foreslår at sperrede opplysninger etter § 65 a skal slettes i form av tilintetgjøring. Opplysninger som er sperret er ikke registrert i politiregisterlovens forstand. Politiregisterforskriften § 22-3 tredje ledd gjelder ikke for opplysninger som behandles etter politiregisterloven § 65 a, og det bør gis en egen bestemmelse om hvordan disse opplysningene skal slettes.

Tungtveiende personvernhensyn taler for at opplysningene slettes i form av tilintetgjøring. Det vil kunne dreie seg om opplysninger om et stort antall personer, som er helt uten interesse for PSTs arbeid, og opplysningene er verken tatt i bruk i analyser eller etterretningsvurderinger, forebyggende saker eller i etterforsking. Opplysningene kan sammenlignes med opplysninger som behandles etter politiregisterloven §§ 8 og 65, der det fremgår av forskriften §§ 22-3 tredje ledd og 16-2 tredje ledd at opplysningene alltid skal tilintetgjøres dersom vilkårene for videre behandling ikke er oppfylt.

Det finnes heller ikke tungtveiende argumenter for at opplysninger innhentet fra åpne kilder, som verken har inngått i analyser og etterretningsvurderinger eller konkrete saker, skal bevares for ettertiden. De hensynene som begrunner at opplysninger registrert utenfor forebyggende sak skal tilintetgjøres, gjør seg enda sterkere gjeldende for opplysninger som er sperret etter politiregisterloven § 65 a. I det sperrede systemet vil svært mange av opplysningene være av ingen eller liten interesse for PST. Opplysningene som ikke er tatt i bruk har heller ikke vært gjenstand for noen egentlig saksbehandling i PST. Etter departementets syn tilsier derfor heller ikke arkivfaglige hensyn at opplysningene skal avleveres til Arkivverket ved slettefristens utløp.

## 4 Sletting av opplysninger som behandles for etterretningsformål

PST kan etter politiregisterloven § 64 tredje ledd nr. 6 behandle opplysninger som er nødvendige for å utarbeide analyser og etterretningsvurderinger som nevnt i politiloven § 17 a.

I Prop. 31 L (2022–2023) er det i punkt 7.3.2 angitt at den alminnelige slettebestemmelsen i politiregisterloven § 50 vil komme til anvendelse når opplysninger behandles til dette formålet, det vil si at opplysninger ikke skal lagres lenger enn det som er nødvendig for formålet med behandlingen, og at opplysningene skal slettes eller sperres med mindre de skal oppbevares etter arkivlovgivningen eller annen lovgivning.

Som omtalt i forrige punkt skal opplysninger som behandles til forebyggende formål, utenfor forebyggende sak, slettes i form av tilintetgjøring, jf. politiregisterforskriften § 22-3 tredje ledd jf. § 16-2 annet ledd nr. 2. Begrunnelsen for unntaket for arkiveringsplikten for denne typer opplysninger er at politiregisterloven åpner for vidtgående unntak fra det som ellers gjelder for behandling av personopplysninger etter personopplysningsloven. Eksempelvis kan det registreres ikke-verifiserte opplysninger og opplysninger om personer som utelukkende har en tilknytning til den personen som er av egentlig interesse for politiet. Slike opplysninger bør ikke bevares for ettertiden.

Ettersom opplysninger som behandles for analyser og etterretningsvurderinger faller utenfor det som forstås med PSTs forebyggende virksomhet utenfor forebyggende sak, er det også behov for å regulere hvordan disse opplysningene skal slettes. De samme hensynene som begrunner unntak fra arkiveringsplikten hva gjelder opplysningene PST behandler i forebyggende virksomhet utenfor forebyggende sak, gjør seg også gjeldende for opplysninger som behandles for etterretningsoppdraget i politiloven § 17 a.

Oppgaven etter politiloven § 17 a medfører blant annet at PST kan registrere opplysninger om lovlig virksomhet så fremt opplysningene er nødvendige for

utarbeidelse av analyser og etterretningsvurderinger. PST kan derfor registrere opplysninger om personer i et videre omfang for utarbeidelse av analyser og etterretningsvurderinger enn de opplysningene som registreres i det forebyggende arbeidet. Dette tilsier etter departementets syn at også disse opplysningene bør slettes i form av tilintetgjøring når de ikke lenger er nødvendige for formålet, se forslaget til nytt femte ledd i politiregisterforskriften § 22-3.

# 5 Tilgang til politiets registre for PSTs oppgaveløsning

Politiregisterforskriften § 8-2 regulerer til hvilke formål tilgang til opplysninger kan gis. Bestemmelsen nevner ikke spesifikt PSTs oppgaver, selv om dette er formål som er omfattet av politiregisterloven og PST har tilgang til de fleste av politiets registre som er regulert i politiregisterforskriften del 11.

Verken § 8-2 eller bestemmelsene om tilgang for de ulike registre i forskriften del 11 reflekterer at det kan gis tilgang i form av direkte søk til PSTs oppgaveløsning. Dette kan blant annet skape uklarhet om hvorvidt PST kan benytte eksisterende tilganger til utarbeidelse av analyser og etterretningsvurderinger etter den nye bestemmelsen i politiloven § 17 a.

Departementet foreslår derfor at det tas inn et nytt nr. i § 8-2 som viser til PSTs oppgaver, slik at det ikke er tvil om at PST, i den grad de har tilgang til et politiregister, kan bruke opplysninger i dette registeret til alle formål som nevnt i politiregisterloven § 64. Forslaget gjør ingen endringer i hvilke registre PST har tilgang til. Det innebærer dermed bare en klargjøring av gjeldende rett.

# 6 Økonomiske og administrative konsekvenser

## 6.1 Testing og utvikling

Forslagene om regulering av testing og utvikling vil ikke i seg selv medføre økonomiske eller administrative konsekvenser av betydning. Forslagene pålegger ingen testing eller utvikling, og dette må derfor håndteres innenfor de til enhver tid gjeldende budsjettrammer. Kravet om forhåndsdrøftinger med Datatilsynet ved testing og utvikling av informasjonssystemer som kan medføre høy risiko for personers rettigheter og friheter vil kunne medføre noe økt ressursbruk hos politiet og hos tilsynet i forbindelse med slike drøftinger. Ettersom kravet er begrenset til situasjoner der testingen og utviklingen i seg selv eller den etterfølgende bruken av systemet kan medføre høy risiko, og behandlingen ikke faller inn under de eksisterende alternativene som utløser krav om forhåndsdrøftelser, antar departementet konsekvensene vil være håndterbare både for politiet og for Datatilsynet. Konsekvensene for tilsynet vil utredes nærmere.

Bruk av opplysninger fra kommunikasjonskontroll, romavlytting og dataavlesing til testing og utvikling vil falle innenfor KK-utvalgets kontrollområde, noe som kan medføre noe merarbeid for utvalget. Departementet antar også at konsekvensene for utvalget vil være håndterbare innenfor utvalgets gjeldende budsjettrammer, og viser til at Statens sivilrettsforvaltning i 2024 fikk bevilget midler til å ansette en teknolog i utvalgets sekretariat.

### 6.2 Behandling av åpent tilgjengelig informasjon

Det er foretatt beregninger av økonomiske og administrative konsekvenser i forbindelse med lovforslagene. Disse er omtalt i Prop. 31 L (2022–2023) punkt 9. Forslaget til politiregisterforskriften § 21-8 utfyller og presiserer de vedtatte lovendringene, og det materielle innholdet i forskriftsreglene er forutsatt i proposisjonen. Forskriftsbestemmelsen vil derfor ikke medføre økonomiske eller administrative konsekvenser av betydning ut over det som følger av de vedtatte lovbestemmelsene.

### 6.3 Øvrige forslag

De andre forslagene i høringsnotatet vil ikke ha nevneverdige økonomiske eller administrative konsekvenser.

## 7 Forslag til lov- og forskriftsendringer

### 7.1 Politiregisterloven

Politiregisterloven § 3 fjerde ledd nytt annet punktum skal lyde:

*Loven gjelder også når opplysninger behandles for testing og utvikling av informasjonssystemer som skal brukes innenfor lovens virkeområde.*

Politiregisterloven § 65 a annet ledd nytt nr. 4 skal lyde:

Opplysninger som behandles etter første ledd, skal være sperret og kan bare brukes til følgende formål:

[…]

4. *testing og utvikling av informasjonssystemer som skal brukes innenfor denne bestemmelsens første ledd.*

§ 69 første ledd nytt nr. 27 skal lyde:

Kongen kan i forskrift gi nærmere regler til gjennomføring av denne lov, herunder om

[…]

27. *behandling av opplysninger i forbindelse med testing og utvikling av informasjonssystemer.*

### 7.2 Politiregisterforskriften

Ny § 1-5 skal lyde:

§ 1-5 *Testing og utvikling av informasjonssystemer*

Opplysninger kan bare behandles til testing og utvikling av informasjonssystemer dersom det vil være umulig eller uforholdsmessig vanskelig å oppnå formålet ved å bruke anonyme eller fiktive opplysninger. Opplysningene skal ikke brukes til testing og utvikling lenger enn nødvendig.

Behandling av opplysninger til testing og utvikling skal godkjennes av den behandlingsansvarlige. Den behandlingsansvarlige kan stille nærmere krav til behandlingen, herunder til behandlingens varighet, hvilke typer opplysninger som skal brukes og omfanget av behandlingen. Kravene skal dokumenteres.

Opplysninger som behandles etter §§ 8 og 65 kan ikke behandles til testing og utvikling. Opplysninger som innhentet ved beslag eller utleveringspålegg, jf. straffeprosessloven §§ 203 og 210, kan bare behandles til testing og utvikling dersom de inngår i straffesakens dokumenter.

Dersom behandling til testing og utvikling skjer atskilt fra annen behandling, skal opplysningene slettes når de ikke lenger er nødvendig for testing og utvikling, og senest samtidig med at opplysninger slettes i det registeret vedkommende er registrert. Opplysningene skal tilintetgjøres.

§ 8-2 første ledd skal lyde:

Tilgang til opplysninger kan gis til formål som omfattes av politiregisterloven, jf. politiregisterloven § 21 første ledd når det er nødvendig for

1. behandling av opplysninger til politimessige formål, jf. politiregisterloven § 2 nr. 13,
2. behandling av opplysninger i straffesaker, herunder også påtalemessige formål, jf. også politiregisterloven § 5 nr. 1,
3. å sikre at behandling av opplysninger skjer i samsvar med politiregisterloven og tilhørende forskrift, jf. også § 2-2,
4. *utvikling, testing,* drift og administrasjon av *informasjonssystemer,*
5. opplæring,
6. å utføre oppgaver knyttet til vandelskontroll, jf. kapittel 7 i politiregisterloven,
7. formål som nevnt i politiregisterloven § 32 om statistisk bearbeiding *mv.,*
8. *behandling av opplysninger til formål som nevnt i politiregisterloven § 64, og*
9. *andre formål når det er særskilt bestemt i lov eller i forskrift gitt i medhold av lov.*

§ 9-5 første ledd første punktum skal lyde:

Utlevering av opplysninger etter politiregisterloven § 29 kan også finne sted i form av direkte tilgang, jf. § 8-2 første ledd *nr. 9,* når slik tilgang er hjemlet i forskriften til registrene i del 11.

Ny § 21-8 skal lyde:

§ 21-8 *Særlig om behandling av åpent tilgjengelig informasjon etter politiregisterloven § 65 a*

Opplysninger som behandles etter politiregisterloven § 65 a skal holdes atskilt. Tilgang til opplysningene skal bare gis til personer som har fått særskilt bemyndigelse. Det skal ikke gis tilgang til flere personer enn nødvendig.

Opplysninger som ikke er tatt i bruk til formål som nevnt i politiregisterloven § 65 a annet ledd nr. 1 til 3 kan ikke utleveres.

Opplysninger som inngår i etterretningsvurderinger og analyser, jf. politiloven § 17 a, skal registreres og behandles i samsvar med reglene i forskriften del 6. Det samme gjelder opplysninger som tas i bruk i forebyggende saker, jf. politiregisterloven § 65 a annet ledd nr. 2. Opplysninger som tas i bruk i etterforskning, jf. politiregisterloven § 65 a annet ledd nr. 3, skal registreres og behandles i samsvar med straffeprosessloven og forskriften del 7.

Opplysninger som tas i bruk i saker som nevnt i politiregisterloven § 65 a annet ledd nr. 2 og 3 skal merkes.

Bruk av opplysningene skal registreres og kunne spores for å kunne kontrollere om søkene og bruken er tillatt eller ikke. Registreringene skal gjennomgås regelmessig med det formål å avdekke uautorisert tilgang til opplysningene.

Beslutning om utsatt sletting etter politiregisterloven § 65 a tredje ledd skal være skriftlig og begrunnet.

Opplysninger som ikke er registrert etter tredje ledd skal slettes i samsvar med § 16-2 annet ledd nr. 2.

For testing og utvikling som nevnt i politiregisterloven § 65 a annet ledd nr. 4 gjelder i tillegg § 1-5 første, annet og fjerde ledd. Slettefristen etter § 1-5 fjerde ledd inntrer når opplysningene skal slettes i medhold av politiregisterloven § 65 a tredje ledd.

§ 22-3 femte ledd skal lyde:

*Opplysninger som behandles for formål som nevnt i politiloven § 17 a skal slettes i samsvar med § 16-2 annet ledd nr. 2 når de ikke lenger er nødvendige for formålet*.

Nåværende femte ledd blir nytt sjette ledd.

§ 25-4 første ledd skal lyde:

Før sperring etter politiregisterloven § 50 tredje ledd finner sted, kan opplysninger overføres og brukes til andre formål innenfor rammen av straffeprosessloven § 216 i. Politiregisterloven § 50 tredje ledd gjelder også for opplysninger som er overført etter første punktum. *Opplysninger som kun er tatt i bruk til formål som nevnt i straffeprosessloven § 216 i tredje ledd bokstav l skal sperres når saken opplysningene er innhentet i, er avgjort ved rettskraftig dom eller endelig henleggelsesbeslutning.*

§ 41-2 annet ledd skal lyde:

Plikten etter første ledd gjelder for behandling av personopplysninger i registre, herunder behandling av personopplysninger som nevnt i § *26-2, sammenstillinger* av personopplysninger fra registre som omfattes av forskriften

del 11 dersom behandlingen følger reglene som gjelder for kilderegisteret *og ved testing og utvikling av informasjonssystemer. Kravet om forhåndsdrøftelser ved testing og utvikling av informasjonssystemer gjelder også dersom det skal behandles opplysninger som er innhentet ved kommunikasjonskontroll, dataavlesing og romavlytting, med unntak av opplysninger som behandles av Politiets sikkerhetstjeneste.*

§ 41-3 første ledd skal lyde:

Dersom Datatilsynet mener at den planlagte behandlingen som nevnt i § 41-2 vil være i strid med politiregisterloven eller denne forskriften, særlig dersom den behandlingsansvarlige ikke i tilstrekkelig grad har identifisert eller redusert risikoen, skal Datatilsynet innen seks uker fra mottak av anmodningen om drøftinger gi den behandlingsansvarlige skriftlige råd. I denne forbindelse kan Datatilsynet benytte seg av de virkemidler som nevnt i politiregisterloven § 60. *Ved behandling som nevnt i § 41-2 annet ledd annet punktum kan Datatilsynet kun gi anmerkning.*

### 7.3 Straffeprosessloven

§ 216 i første ledd tredje punktum bokstav k og ny bokstav l skal lyde:

Taushetsplikten er ikke til hinder for at opplysningene brukes

[…]

k. i sak om forbud mot en kriminell sammenslutning etter kapittel *17 c,*

*l. til testing og utvikling av informasjonssystemer som skal brukes innenfor politiregisterlovens virkeområde.*

### 7.4 Politiloven

§ 17 f annet ledd bokstav e, f og ny bokstav g skal lyde:

Taushetsplikten er ikke til hinder for at opplysningene brukes

e. for å forhindre en alvorlig straffbar handling som kan krenke andres liv, helse eller *frihet,*
f. for at Politiets sikkerhetstjeneste kan utlevere opplysninger til Etterretningstjenesten dersom det er nødvendig for forebyggelses- og sikkerhetsmessige formål, *eller*
g. *til testing og utvikling av informasjonssystemer som skal brukes innenfor politiregisterlovens virkeområde.*

### 7.5 Grenseloven

§ 22 tredje ledd skal lyde:

Biometrisk personinformasjon (ansiktsfoto og fingeravtrykk) kan *opptas* elektronisk av alle som passerer grensekontroll eller annet kontrollsted for kontroll av reisedokumenter. *Opplysningene skal tilintetgjøres så snart som mulig etter at identiteten er verifisert mot gyldig reisedokument, eller når identiteten er fastslått på annen måte, med unntak av tilfeller som nevnt i § 22 a annet ledd.*

Ny § 22 a skal lyde:

§ 22 a *Testing og utvikling*

Opplysninger som behandles i medhold av § 22 første og annet ledd og annet ledd i bestemmelsen her kan behandles for å utvikle og teste og informasjonssystemer til bruk for grensekontrollformål dersom det vil være umulig eller uforholdsmessig vanskelig å oppnå formålet ved å bruke anonyme eller fiktive opplysninger. Opplysningene skal ikke brukes til testing og utvikling lenger enn nødvendig.

Politiet kan lagre ansiktsfoto og fingeravtrykk opptatt i medhold av § 22 tredje ledd i inntil seks måneder dersom det er nødvendig for å teste og utvikle informasjonssystemer som nevnt i første ledd. Opplysninger som lagres etter dette leddet kan bare behandles til dette formålet.

Opplysninger som behandles etter andre ledd i bestemmelsen her skal holdes atskilt. Tilgang skal bare gis til personer som er særskilt bemyndiget.

Ansiktsfoto og fingeravtrykk skal slettes i form av tilintetgjøring.

§ 25 nr. 10 skal lyde:

10. behandling av opplysninger, blant annet om innsyn, retting og sletting, *behandling av opplysninger i forbindelse med testing og utvikling* og om behandling, herunder utveksling, av opplysninger i koordineringssenteret for Eurosur, jf. *§§* 22 og *22 a,*