



DET KONGELIGE
JUSTIS- OG BEREDSKAPSDEPARTEMENT

Prop. 36 L

(2025–2026)

Proposisjon til Stortinget (forslag til lovvedtak)

Endringer i politiregisterloven
og grenseloven mv.
(testing og utvikling av informasjonssystemer)

Innhold

1	Proposisjonens hovedinnhold	5	6.4.2	Hvilket personvernregelverk som gjelder for behandlingen	21
2	Bakgrunnen for lovforslagene	7	6.4.3	Utlevering	22
2.1	Bruk av opplysninger til testing og utvikling	7	6.5	Departementets vurderinger	22
2.1.1	Generelt	7	6.5.1	Generelt	22
2.1.2	Nærmere om testing og utvikling av informasjonssystemer	7	6.5.2	Hvilket personvernregelverk som regulerer behandlingen	23
2.1.3	Høringen	8	6.5.3	Utlevering	25
2.2	Endringer i politiregisterloven og utlendingsloven – taushetsplikt for databehandlere og Tilsynsrådet for tvangsreturer og utlendingsinternatet mv.	9	7	Bruk av informasjon fra skjulte tvangsmidler til testing og utvikling	26
2.2.1	Databehandlers taushetsplikt	9	7.1	Gjeldende rett	26
2.2.2	Tilsynsrådet for tvangsreturer og utlendingsinternatets taushetsplikt	9	7.2	Forslaget i høringsnotatet	26
2.2.3	Høringen	10	7.3	Høringsinstansenes syn	26
2.3	Krav om politiattest ved opptak til videreutdanning og høyere grads studier ved Politihøgskolen	11	7.4	Departementets vurderinger	27
2.3.1	Bakgrunn	11	8	Bruk av åpent tilgjengelig informasjon innhentet for etterretningsformål til testing og utvikling	31
2.3.2	Høringen	11	8.1	Gjeldende rett	31
3	Bruk av personopplysninger til testing og utvikling – rettslige rammer	12	8.2	Forslaget i høringsnotatet	31
3.1	Grunnloven og EMK	12	8.3	Høringsinstansenes syn	31
3.2	Personvernforordningen	12	8.4	Departementets vurderinger	31
3.3	Personverndirektivet	13	9	Regulering av bruk av opplysninger til testing og utvikling i grenseloven	33
3.4	Internasjonalt regelverk om kunstig intelligens mv.	13	9.1	Gjeldende rett	33
4	Hjemler for testing og utvikling i annet regelverk	15	9.2	Nærmere om behovet	33
5	Andre lands rett – testing og utvikling	17	9.3	Forslaget i høringsnotatet	34
6	Regulering av testing og utvikling i politiregisterloven ...	18	9.3.1	Hjemmel for bruk av opplysninger til testing og utvikling	34
6.1	Gjeldende rett	18	9.3.2	Lagring av ansiktsbilde og fingeravtrykk til bruk for testing og utvikling	34
6.2	Nærmere om behovet	18	9.4	Høringsinstansenes syn	35
6.3	Forslaget i høringsnotatet	19	9.5	Departementets vurderinger	36
6.4	Høringsinstansenes syn	20	9.5.1	Hjemmel for bruk av opplysninger til testing og utvikling	36
6.4.1	Generelle og overordnede synspunkter	20	9.5.2	Lagring av ansiktsbilde og fingeravtrykk	36
			10	Databehandlers taushetsplikt	38
			10.1	Gjeldende rett	38
			10.2	Forslaget i høringsnotatet	38
			10.3	Høringsinstansenes syn	38
			10.4	Departementets vurderinger	39

11	Registrering og anmerkning på politiattest av overføring til barnevernet	40	13.2	Forslaget i høringsnotatet	44
11.1	Gjeldende rett	40	13.3	Høringsinstansenes syn	44
11.2	Forslaget i høringsnotatet	40	13.4	Departementets vurderinger	45
11.3	Høringsinstansenes syn	40	14	Økonomiske og administrative konsekvenser	46
11.4	Departementets vurderinger	40	15	Merknader til bestemmelsene	47
12	Tilsynsrådet for tvangsreturer og utlendingsinternatets taushetsplikt	42	15.1	Straffeprosessloven	47
12.1	Forslaget i høringsnotatet	42	15.2	Politi-loven	47
12.2	Høringsinstansenes syn	42	15.3	Utlendingsloven	47
12.3	Departementets vurderinger	42	15.4	Politiregisterloven	47
13	Krav om politiattest og plettfriandel ved opptak til videre-utdanning og høyere grads studier ved Politihøgskolen	44	15.5	Grenseloven	48
13.1	Gjeldende rett	44	Forslag til lov om endringer i politiregisterloven og grenseloven mv. (testing og utvikling av informasjonssystemer)		50



DET KONGELIGE
JUSTIS- OG BEREDSKAPSDEPARTEMENT

Prop. 36 L

(2025–2026)

Proposisjon til Stortinget (forslag til lovvedtak)

Endringer i politiregisterloven og grenseloven mv. (testing og utvikling av informasjonssystemer)

*Tilråding fra Justis- og beredskapsdepartementet 13. mars 2026,
godkjent i statsråd samme dag.
(Regjeringen Støre)*

1 Proposisjonens hovedinnhold

I denne proposisjonen foreslår Justis- og beredskapsdepartementet endringer i politiregisterloven, grenseloven, straffeprosessloven, politiloven og utlendingsloven.

Endringene er i hovedsak knyttet til bruk av opplysninger til testing og utvikling av informasjonssystemer. Flere offentlige organer har de senere årene fått hjemler til å benytte personopplysninger til disse formålene for de tilfellene hvor det er umulig eller uforholdsmessig vanskelig å oppnå formålet ved å benytte fiktive eller anonymiserte opplysninger. I denne proposisjonen foreslås det hjemler for bruk av opplysninger til testing og utvikling innenfor politiregisterlovens og grenselovens virkeområder.

Det foreslås en endring i politiregisterloven § 3 om lovens virkeområde som gjør det klart at loven gjelder for behandling av opplysninger i forbindelse med testing og utvikling av informasjonssystemer som skal brukes innenfor politiregisterlovens virkeområde. Det foreslås også en forskriftshjemmel, slik at behandlingen kan reguleres nærmere i forskrift. Videre foreslås det at

også opplysninger som PST har innhentet med hjemmel i politiregisterloven § 65 a om behandling av åpent tilgjengelig informasjon til etterretningsformål skal kunne benyttes til testing og utvikling av informasjonssystemer som skal brukes i forbindelse med utarbeidelse av analyser og etterretningsvurderinger etter politiloven § 17 a. Sistnevnte bestemmelse regulerer PSTs oppgaver som innenlands etterretningstjeneste.

Det foreslås også endringer i straffeprosessloven § 216 i og politiloven § 17 f for å legge til rette for at opplysninger som er innhentet ved hjelp av skjulte tvangsmidler som ledd i henholdsvis etterforskning og forebygging kan benyttes til testing og utvikling.

I tillegg foreslås det en hjemmel i grenseloven for å kunne benytte opplysninger som behandles i forbindelse med grensekontroll til testing og utvikling av informasjonssystemer til bruk for grensekontrollformål, etter mal av bestemmelser i annet regelverk. I grenseloven foreslås det også en hjemmel for å kunne lagre ansiktsbilde og fingeravtrykk innhentet i grensekontrollen, men

utelukkende til bruk for testing og utvikling. Det foreslås også nærmere rammer for behandlingen av disse opplysningene.

Det foreslås også enkelte andre endringer i politiregisterloven som ikke har sammenheng med forslagene som gjelder testing og utvikling. I § 18 om databehandlers rådighet over personopplysninger foreslås det endringer som åpner for å avtalefeste omfanget av taushetsplikten. Det foreslås i tillegg å oppheve § 40 nr. 3 bokstav f om anmerkning av opplysninger om overføring til

barnevernet på politiattest, da bestemmelsen er utdatert.

I utlendingsloven foreslås det endringer som lovfester og utvider taushetsplikten for Tilsynsrådet for tvangsreturer og utlendingsinternatet.

Endelig foreslås det endringer i politiloven § 24 b, slik at Politihøgskolen kan fastsette krav til plettfri vandel og kreve fremlagt uttømmende og utvidet politiattest fra personer som skal tas opp til videreutdanning og høyere grads studier ved Politihøgskolen.

2 Bakgrunnen for lovforslagene

2.1 Bruk av opplysninger til testing og utvikling

2.1.1 Generelt

Den teknologiske utviklingen i samfunnet går raskt, og politiet må holde tritt med denne utviklingen. Utvikling og testing av eksisterende og nye informasjonssystemer er en forutsetning for at politiet skal kunne utføre oppgavene etaten er pålagt på en effektiv måte. Politiet må derfor ha ressurser til å utvikle og teste nye teknologiske løsninger. I tillegg må regelverket være tilpasset utvikling, testing og bruk av slike løsninger.

I Prop. 1 S (2025–2026) for Justis- og beredskapsdepartementet på side 113–114, vises det til at et sentralt funn i Riksrevisjonens undersøkelse av digitalisering i politiet er at det digitale etterslepet er stort, og at mange av systemene som er avgjørende for politiets virksomhet er utdaterte. Dette begrenser mulighetene som den teknologiske utviklingen gir til å øke kvaliteten og effektiviteten i oppgaveløsningen. Videre uttales det:

Det trengst ei digital omstilling over tid. Dette er avgjerande både for å sikre god operativ evne, ein meir effektiv kamp mot kriminalitet og adekvat beredskap, og for å kunne yte betre tenester til innbyggjarane.

En slik digital omstilling forutsetter at ny teknologi kan testes, nye tekniske løsninger utvikles og tas i bruk og at eksisterende tekniske løsninger kan videreutvikles.

Kompleksiteten i politiets og påtalemyndighetens oppgaver og informasjonsbehandling, og behovet for ivaretagelse av krav til blant annet rettssikkerhet, notoritet, personvern og samfunnssikkerhet, medfører at politiet i stor grad er avhengig av egenutviklede løsninger eller hyllevare (dvs. ferdig utviklede informasjonssystemer og verktøy som tilbys av kommersielle aktører) med meget gode tilpasningsmuligheter. Nye informasjonssystemer må være utviklet med utgangspunkt i eller være tilpasset de særlige behov politiet har, herunder må systemene være tilpasset

opplysningskategoriene som skal behandles, formålene opplysningene skal behandles for og sammenhengen mellom ulike opplysninger.

2.1.2 Nærmere om testing og utvikling av informasjonssystemer

I denne proposisjonen foreslås det hjemler for bruk av opplysninger til «utvikling» og «testing» av «informasjonssystemer». Ingen av disse begrepene har en entydig eller allmenn definisjon, og innholdet i og forståelsen av dem kan endre seg over tid som følge av den teknologiske utviklingen. Med informasjonssystemer menes i denne sammenheng systemer for innsamling, lagring, bearbeiding, overføring og presentasjon av opplysninger basert på informasjons- og kommunikasjonsteknologi. Eksempler er saksbehandlingssystemer, modeller for beslutningsstøtte og analysesystemer. Det omfatter også systemer som benytter maskinlæring og kunstig intelligens (KI).

Med testing menes tradisjonelt det å kontrollere at et informasjonssystem 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. Det omfatter også testing og kvalitetssikring av verktøy og modeller som er utviklet og trent av andre, samt trening av modeller politiet selv utvikler.

Med utvikling menes tradisjonelt det å lage, oppgradere eller på andre måter endre et informasjonssystem for å gjøre det klart for testing og senere bruk. Utvikling omfatter dermed både videreutvikling av eksisterende systemer og at helt nye systemer lages. Utvikling omfatter også endring av ferdig utviklede systemer for å tilpasse dem til politiets behov.

Begrepene testing og utvikling i de foreslåtte lovbestemmelsene er ment å dekke hele utviklingsfasen og alle steg i denne, herunder ulike former for testing av informasjonssystemer. Også feilretting og analyse av testresultater, for eksempel for å avdekke årsaken til at systemene ikke gir det resultatet eller den kvaliteten som er for-

ventet, samt annen løpende forbedring og endring av et system, vil omfattes.

Utvikling og testing kan enten skje ved bruk av 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 laget for test- og utviklingsformål. Som utgangspunkt bør testing og utvikling skje ved bruk av anonyme eller fiktive opplysninger for å unngå at personopplysninger behandles unødvendig, og testing og utvikling krever da ingen særskilt regulering. Av ulike grunner er det likevel ikke alltid mulig utelukkende å bruke anonyme eller fiktive opplysninger ved testing og utvikling.

Utvikling og testing kan skje på ulike måter og i ulike systemer. I noen tilfeller etableres det egne test- og utviklingsmiljøer, separat fra de ordinære systemene, der eventuelle reelle personopplysninger som er nødvendige kopieres over fra de ordinære systemene. 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 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, mens løsningen testes helt eller delvis i det faktiske systemet for å sikre at det fungerer etter intensjonen.

2.1.3 Høringen

Forslag til endringer i politiregisterloven, grenseloven, straffeprosessloven og politiloven ble sendt på høring 20. november 2024. Høringsfristen var 20. januar 2025. Høringsnotatet ble sendt til følgende høringsinstanser:

Departementene

Arbeids- og velferdsdirektoratet
 Arbeidstilsynet
 Arkivverket
 Barneombudet
 Barne-, ungdoms- og familiedirektoratet
 Datatilsynet
 Digitaliseringsdirektoratet
 Direktoratet for samfunnssikkerhet og beredskap
 Domstoladministrasjonen

Etterretningstjenesten
 Forsvarsstaben
 Helsedirektoratet
 Integrerings- og mangfoldsdirektoratet
 Kommisjonen for gjenopptakelse av straffesaker
 Kontrollutvalget for kommunikasjonskontroll
 Kriminalomsorgsdirektoratet
 Kripos
 Likestillings- og diskrimineringsombudet
 Nasjonal kommunikasjonsmyndighet
 Nasjonal sikkerhetsmyndighet
 Norges institusjon for menneskerettigheter (NIM)
 Politidirektoratet
 Politihøgskolen
 Politiets sikkerhetstjeneste (PST)
 Regjeringsadvokaten
 Riksadvokaten
 Sametinget
 Sekretariatet for konfliktrådene
 Sivil klareringsmyndighet
 Sivilombudet
 Skattedirektoratet
 Spesialenheten for politisaker
 Statens sivilrettsforvaltning
 Statistisk Sentralbyrå
 Statsadvokatembetene
 Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget)
 Sysselmesteren på Svalbard
 Tolletaten
 Utlendingsdirektoratet
 Utlendingsnemnda
 ØKOKRIM

Amnesty International Norge
 Antirasistisk Senter
 Den Norske Advokatforening
 Den Norske Dommerforening
 DIXI Ressurssenter
 Nok. Norge
 Forandringsfabrikken
 Juridisk rådgivning for kvinner (JURK)
 Jussbuss
 Jussformidlingen
 Norges idrettsforbund
 Norges politilederlag
 Norsk forening for kriminalreform
 Norsk Journalistlag
 Norsk Presseforbund
 Norsk Redaktørforening
 Næringslivets Hovedorganisasjon
 OMOD (Organisasjon mot offentlig diskriminering)

Politiets Fellesforbund
 Redd Barna, Rettighetssenteret
 Rettspolitisk forening
 Røde kors
 Stiftelsen for en Kritisk og Undersøkende Presse

Det juridiske fakultet ved Universitetet i Bergen
 Det juridiske fakultet ved Universitetet i Oslo
 Det juridiske fakultet ved Universitetet i Tromsø
 Forsvarets forskningsinstitutt
 Forsvarets høyskole
 Institutt for forsvarsstudier
 Institutt for fredsforskning
 Norsk Utenrikspolitisk Institutt

Følgende instanser hadde merknader til lovfor-
 slagene:

Datatilsynet
 Digitaliseringsdirektoratet
 Kontrollutvalget for kommunikasjonskontroll
 Kripos
 Politidirektoratet
 Politiets IT-enhet
 Politiets sikkerhetstjeneste
 Politiets utlendingsenhet
 Politihøgskolen
 Statens sivilrettsforvaltning
 Stortingets kontrollutvalg for etterretnings-,
 overvåkings- og sikkerhetstjeneste
 (EOS-utvalget)
 Utlendingsdirektoratet
 Øst politidistrikt

Advokatforeningen

Følgende instanser meldte at de ikke hadde merk-
 nader eller ikke ønsket å uttale seg:

Arbeids- og velferdsdirektoratet
 Domstoladministrasjonen
 Nasjonal kommunikasjonsmyndighet
 Skatteetaten
 Statistisk sentralbyrå

2.2 Endringer i politiregisterloven og utlendingsloven – taushetsplikt for databehandlere og Tilsynsrådet for tvangsreturer og utlendingsinternatet mv.

2.2.1 Databehandlers taushetsplikt

Overfor departementet har Kripos, i kraft av å
 være behandlingsansvarlig for de fleste av poli-

tiets registre, redegjort for enkelte utfordringer
 knyttet til politiregisterloven § 18 tredje ledd
 første punktum om pålegg om taushetsplikt for
 databehandlere. Bestemmelsen har vist seg vans-
 kelig å praktisere overfor databehandlere som
 opererer med standardavtaler, typisk større uten-
 landske IT-selskaper. I slike avtaler kan det være
 begrensede muligheter for individuelle tilpas-
 ninger. Kripos har opplyst at det i standard-
 avtalene vil være inntatt en avtalefestet bestem-
 melse om at den som er ansatt hos eller utfører
 tjeneste eller arbeid for databehandler, og som
 behandler taushetsbelagte opplysninger, er under-
 lagt taushetsplikt. De nærmere formuleringene
 og omfanget av taushetsplikten kan imidlertid
 variere, og kan dermed skille seg noe fra taushets-
 plikten for personer som er ansatt i eller utfører
 tjeneste eller arbeid for politiet eller påtalemyndig-
 heten, slik denne er regulert i politiregisterloven
 § 23.

I tilfeller hvor taushetsplikten følger av stan-
 dardavtaler og det ikke kreves fremlagt politiattest
 slik det er adgang til etter politiregisterloven § 18
 tredje ledd tredje punktum, har Kripos lagt til
 grunn at deres behov for opplysninger om hvem
 hos databehandler som har tilgang til opplysnin-
 gene er mindre. Kripos mener at databehandlers
 plikt til å opplyse om hvem som får tilgang til opp-
 lysningene bør bestå, men at plikten først bør inn-
 tre ved forespørsel – for eksempel i forbindelse
 med en revisjon av databehandleravtalen.

2.2.2 Tilsynsrådet for tvangsreturer og utlendingsinternatets taushetsplikt

Ved lov 11. juni 2021 nr. 72 om endringer i politi-
 registerloven og utlendingsloven ble det gitt en ny
 § 107 a i utlendingsloven om Tilsynsrådet for
 tvangsreturer og utlendingsinternatet. Bestem-
 melsen trådte i kraft 1. januar 2023.

Forskrift om tilsynsrådet for tvangsreturer og
 utlendingsinternatet § 7 regulerer tilsynsrådets
 taushetsplikt. Bestemmelsen lyder:

Forvaltningslovens regler om taushetsplikt
 gjelder for tilsynsrådets virksomhet. Taushets-
 plikten omfatter også forhold av betydning for
 sikkerheten ved utlendingsinternatet.

Da forskriften var på høring høsten 2019, mente
 Politidirektoratet og Politiets utlendingsenhet at
 taushetsplikten også burde omfatte forhold knyttet
 til forestående tvangsreturer og opplysninger som
 det av hensyn til politiets operative virksomhet er
 nødvendig å holde hemmelig.

2.2.3 Høringen

Justis- og beredskapsdepartementet sendte 11. februar 2022 på høring forslag til endringer i blant annet politiregisterloven §§ 18 og 40 om henholdsvis databehandlere og ordinære politiattester og utlendingsloven § 107 a om Tilsynsrådet for tvangsreturer og utlendingsinternatet.

Høringsfristen var 20. april 2022. Høringsnotatet ble sendt til følgende instanser:

Departementene

Arbeids- og velferdsdirektoratet
 Arkivverket
 Barneombudet
 Barne-, ungdoms- og familiedirektoratet
 Datatilsynet
 Digitaliseringsdirektoratet
 Direktoratet for samfunnssikkerhet og beredskap
 Domstoladministrasjonen
 Helsedirektoratet
 Integrerings- og mangfoldsdirektoratet
 Kriminalomsorgsdirektoratet
 Kripos
 Ligestillings- og diskrimineringsombudet
 Medietilsynet
 Nasjonal kommunikasjonsmyndighet
 Nasjonal sikkerhetsmyndighet
 Norges institusjon for menneskerettigheter
 Personvernkommisjonen
 Politidirektoratet
 Politiets sikkerhetstjeneste
 Politihøgskolen
 Regjeringsadvokaten
 Riksadvokaten
 Sametinget
 Sivil klareringsmyndighet
 Sivilombudet
 Skattedirektoratet
 Spesialenheten for politisaker
 Statens sivilrettsforvaltning
 Statistisk Sentralbyrå
 Statsadvokatembetene
 Sysselmasteren på Svalbard
 Tilsynsrådet for politiets utlendingsinternat,
 Trandum
 Utlendingsdirektoratet
 Utlendingsnemnda
 ØKOKRIM

Amnesty International Norge
 Antirasistisk Senter
 Den Norske Advokatforening
 Den Norske Dommerforening

DIXI Ressurssenter for voldtatte i Oslo og Stavanger

Fellesskap mot seksuelle overgrep
 Finansnæringens Fellesorganisasjon
 Innvandrernes landsorganisasjon
 Juridisk rådgivning for kvinner
 Jussbuss
 Jussformidlingen
 Kommunesektorens organisasjon
 Landsorganisasjonen i Norge
 Norges idrettsforbund
 Mediebedriftenes landsforening
 Norges politilederlag
 Norsk forening for kriminalreform
 Norsk Journalistlag
 Norsk Presseforbund
 Norsk Redaktørforening
 Næringslivets Hovedorganisasjon
 OMOD (Organisasjonen mot offentlig diskriminering)
 Politiets Fellesforbund
 Tekna
 Redd Barna, Rettighetssenteret
 Rettspolitisk forening
 Røde kors
 Samarbeidsrådet for tros- og livssynssamfunn
 Stiftelsen for en Kritisk og Undersøkende Presse

Det juridiske fakultet ved Universitetet i Bergen
 Det juridiske fakultet ved Universitetet i Oslo
 Det juridiske fakultet ved Universitetet i Tromsø
 Forsvarets forskningsinstitutt
 Forsvarets høgskole
 Institutt for forsvarsstudier
 Institutt for fredsforskning
 Norsk Utenrikspolitisk Institutt

Følgende høringsinstanser hadde realitetsmerknader:

Datatilsynet
 Finnmark politidistrikt
 Kripos
 Oslo politidistrikt
 Politidirektoratet
 Politiets utlendingsenhet
 Øst politidistrikt

Advokatforeningen

Følgende instanser meldte at de ikke hadde merknader eller ikke ønsket å uttale seg:

Forsvarsdepartementet
 Helse- og omsorgsdepartementet

Domstoladministrasjonen
 Politiets sikkerhetstjeneste
 Skattedirektoratet

2.3 Krav om politiattest ved opptak til videreutdanning og høyere grads studier ved Politihøgskolen

2.3.1 Bakgrunn

Det planlegges for et ettårig etterforskningsstudium som skal tilbys ved Politihøgskolen fra høsten 2026 som påbygning til bachelorgrad. Etter planen skal dette studietilbudet være åpent også for søkere som ikke har bachelorgrad fra Politihøgskolen. Etter politiloven § 24 b første ledd stilles det krav om plettfriandel, skikkethet og fremleggelse av uttømmende og utvidet politiattest for opptak til Politihøgskolens grunnutdanning. Det er i dag ikke tilsvarende krav for opptak til videreutdanning eller høyere grads studier.

2.3.2 Høringen

Justis- og beredskapsdepartementet sendte 13. oktober 2025 på høring forslag til endring i politiloven § 24 b, som oppstiller krav om plettfriandel og hjemler krav om fremleggelse av uttømmende og utvidet politiattest fra søkere til opptak til videreutdanning og høyere grads studier ved Politihøgskolen.

Høringsfristen var 26. november 2025.

Høringsnotatet ble sendt til følgende høringsinstanser:

Forsvarsdepartementet
 Kunnskapsdepartementet

Datatilsynet
 De nasjonale forskningsetiske komiteene
 Direktoratet for høyere utdanning og kompetanse
 Kriminalomsorgsdirektoratet
 Nasjonalt organ for kvalitet i utdanningen

Norges forskningsråd
 Politidirektoratet
 Politiets sikkerhetstjeneste
 Samordna opptak
 Statens lånekasse for utdanning
 Utdanningsdirektoratet

Akademikerne
 Forskerforbundet
 Norges politilederlag
 Norsk studentorganisasjon
 Norsk studentunion
 Norsk tjenestemannslag
 Parat
 Politiets Fellesforbund
 Universitets- og høgskolerådet

Forsvarets høgskole
 Høgskolen på Vestlandet
 Kriminalomsorgens høgskole- og utdannings-
 senter
 Nord universitet
 Norges miljø- og biovitenskapelige universitet
 Norges tekniske- og naturvitenskapelige
 universitet
 OsloMet
 Politihøgskolen
 Universitetet i Agder
 Universitetet i Bergen
 Universitetet i Innlandet
 Universitetet i Oslo
 Universitetet i Stavanger
 Universitetet i Tromsø

Følgende høringsinstanser hadde merknader:

Politidirektoratet
 Norges politilederlag
 Parat politiet
 Politiets Fellesforbund
 Politihøgskolen
 Sikt
 Tekna

3 Bruk av personopplysninger til testing og utvikling – rettslige rammer

3.1 Grunnloven og EMK

Grunnloven § 102 og Den europeiske menneskerettskonvensjon (EMK) artikkel 8 verner om borgernes rett til respekt for sitt privatliv. Det følger av lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven) § 2 at EMK gjelder som norsk lov. Ved motstrid går konvensjonen foran bestemmelser i annen lovgivning, jf. § 3. Grunnloven § 102 første ledd første punktum slår fast at enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon.

EMK artikkel 8 lyder:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Den europeiske menneskerettsdomstolen (EMD) har i flere avgjørelser fastslått at EMK artikkel 8 også innebærer en rett til vern av personopplysninger, se for eksempel *Leander mot Sverige*, 26. mars 1987 (sak nr. 9248/81).

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 Grunnloven § 102 og EMK artikkel 8. Det samme gjelder det å lagre opplysninger utelukkende for å bruke dem til testing og utvikling. For at et inngrep i retten til privatliv etter EMK artikkel 8 skal være lovlig, må det være foreskrevet ved lov, forfølge et eller flere nærmere angitte legitime formål og være nødvendig i et

demokratisk samfunn av hensyn til de aktuelle formålene, jf. artikkel 8 nr. 2.

3.2 Personvernforordningen

Personvernforordningen, (EU) 2016/679 (heretter GDPR), gjelder som norsk lov, jf. personopplysningsloven § 1. Personopplysningsloven gjelder etter § 2 første ledd for all behandling av personopplysninger, med mindre annet er bestemt i eller i medhold av lov.

Personopplysningsloven og GDPR gjelder dermed i utgangspunktet for alt av politiets virksomhet, herunder forvaltningsoppgaver som grensekontroll, med mindre annet er bestemt. Politiregisterloven er et eksempel på en lov som gjør unntak fra dette utgangspunktet, jf. nærmere omtale i punkt 6.1.

GDPR 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 et annet rettslig grunnlag enn det som ligger til grunn for innsamlingen for å viderebehandle opplysninger, så lenge det nye formålet anses forenlig med det opprinnelige innsamlingsformålet, 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) *Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til*

deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen punkt 6.6.

At testing og utvikling i konteksten av GDPR kan være et annet, men ikke nødvendigvis uforenlig, formål enn det opplysningene opprinnelig behandles for, er lagt til grunn i EU-domstolens praksis, se C-77/21, 20. oktober 2022, 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.

3.3 Personverndirektivet

Direktiv (EU) 2016/680 (heretter LED) regulerer rettshåndheverende myndigheters behandling av personopplysninger til kriminalitetsbekjempende formål mv. Direktivet er gjennomført i politiregisterloven og politiregisterforskriften hva gjelder politiets og påtalemyndighetens behandling av opplysninger. Direktivets regler er på en del punkter sammenfallende med reglene i GDPR, men med tilpasninger på grunn av særlige behov som gjør seg gjeldende ved kriminalitetsbekjempelse.

LED har i motsetning til GDPR ingen eksplisitte regler om viderebehandling til forenlig formål. Ifølge LED artikkel 4 nr. 1 bokstav b skal medlemsstatene fastsette at personopplysninger skal innsamles til uttrykkelig angitte og legitime formål og ikke behandles på en måte som er uforenlig med disse. Videre fremgår det av LED artikkel 4 nr. 2 at viderebehandling til andre formål som nevnt i artikkel 1 nr. 1 enn det formålet personopplysningene er innsamlet til, er tillatt i den grad a) dette følger av EU-retten eller nasjonal rett og b) behandlingen er nødvendig og forholdsmessig i forhold til det andre formålet etter EU-retten eller nasjonal rett. Etter artikkel 4 nr. 3 kan behandling som foretas av den samme eller en annen behandlingsansvarlig omfatte arkivering i samfunnets interesse eller til vitenskapelig, stati-

stisk eller historisk bruk for formålene i artikkel 1 nr. 1, med forbehold om tilstrekkelige tiltak for å sikre de registrertes rettigheter og friheter.

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 er ikke nevnt i direktivet. Det er likevel flere artikler som forutsetter at rettshåndheverende myndigheter vil kunne ta i bruk nye teknologiske løsninger, se for eksempel 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 tas i bruk.

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

3.4 Internasjonalt regelverk om kunstig intelligens mv.

EUs forordning om kunstig intelligens (EU) 2024/1689 (heretter KI-forordningen) gir regler for markedsplassing og bruk av KI-systemer. Forordningen skal gjelde i EU fra 2. august 2026, med enkelte unntak, jf. artikkel 113. Forordningen er ennå ikke inntatt i EØS-avtalen. Digitaliserings- og forvaltningsdepartementet sendte 30. juni 2025 på høring forslag om gjennomføring av KI-forordningen i norsk rett, med høringsfrist 30. september 2025.

Her beskrives bare enkelte artikler i forordningen 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, recommenda-

tions, 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 og ikke tilpasser seg etter at det er tatt i bruk, faller derfor utenfor forordningens virkeområde.

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 også til rettshåndhevelse, omfattes derimot av forordningen, jf. fortalepunkt 24. Det er dermed ikke nødvendigvis systemet i seg selv, men hvordan det brukes, som avgjør om KI-forordningen kommer til anvendelse eller ikke.

KI-forordningens virkeområde avgrenser mot forskning, testing og utvikling av systemer før de bringes i omsetning eller tas i bruk, jf. artikkel 2 nr. 8. Slike aktiviteter skal utføres i samsvar med gjeldende unionsrett. Forordningen legger likevel føringer for testing og utvikling av systemer som skal bringes i omsetning 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 hvis eneste formål er å bekrefte at en bestemt fysisk person er den som han eller hun utgir seg for å være, jf. ved-

legg III nr. 1 bokstav a. En rekke former for systemer regnes også som høyrisiko dersom de brukes av rettshåndhevende myndigheter, blant annet systemer som skal vurdere risikoen for at en person vil bli utsatt for eller begå straffbare handlinger, og systemer for profilering, jf. vedlegget nr. 6. Også systemer som benyttes i forbindelse med grensekontroll vil kunne være høyrisikosystemer, blant annet systemer som skal brukes til å vurdere om en person utgjør en risiko eller for å oppdage, gjenkjenne eller identifisere fysiske personer, ut over verifisering av reisedokumenter, jf. vedlegget nr. 7.

Artikkel 9 nr. 6 krever at høyrisikosystemer skal testes for å sikre at de fungerer konsekvent for sine tiltenkte formål, og det følger av nr. 8 at testing skal skje gjennom utviklingsfasen og under alle omstendigheter før systemet bringes i omsetning eller tas i bruk. Artikkel 10 regulerer data og dataforvaltning i 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 påvise og korrigere skjevheter, og gitt at 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 verken strengere eller mer detaljerte krav til testing og utvikling enn det som følger av forordningen.

4 Hjemler for testing og utvikling i annet regelverk

De senere årene er det innført flere hjemler for at opplysninger som et offentlig organ behandler i sin lovregulerte virksomhet, også skal kunne brukes til testing og utvikling av informasjonssystemer. Et eksempel er 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) *Skatter, avgifter og toll 2019* kapittel 18 at testing og utvikling som regel vil være et annet formål enn opplysningene ble innhentet for. Om bruken er forenlig med innhentingsformålet vil ifølge proposisjonen 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 de registrerte.

Også innenfor helselovgivningen er det gitt hjemler for bruk av opplysninger til 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) *Endringer i pasientjournalloven*

mv. (nasjonal digital samhandling) 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. I proposisjonen slås det fast at utvikling og testing av journalsystemer eller andre behandlingsrettede helseregistre ikke vil være uforenlig med det opprinnelige formålet.

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 merknadene til bestemmelsen i Prop. 112 L (2020–2021) *Endringer i helsepersonelloven og pasientjournalloven (bruk av helseopplysninger for å lette samarbeid, læring og bruk av kunstig intelligens i helse- og omsorgstjenesten mv.)* punkt 11.1, 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. Ved lov 20. juni 2025 nr. 71 om endringer i helseforskningsloven mv. (vilkår for medisinsk og helsefaglig forskning og for bruk av helseopplysninger i forskning) ble helsepersonelloven § 29 første ledd bokstav a endret slik at det ikke lenger er krav om at beslutningsstøtteverktøy må være «klinisk». Det ble samtidig foretatt endringer i helseregisterloven § 19 e for å gjøre det klart at det kan tilgjengeliggjøres opplysninger og gis dispensasjon fra taushetsplikten til utvikling og bruk av beslutningsstøtteverktøy i helse- og omsorgstjenesten. Endringene har foreløpig ikke trådt i kraft.

Helsepersonelloven § 29 og helseregisterloven § 19 e 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 til-

gjengeliggjøres 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.

5 Andre lands rett – testing og utvikling

Verken svensk eller dansk regelverk har egne bestemmelser om bruk av opplysninger som behandles til politimessige formål eller til grensekontrollformål til testing eller utvikling av informasjonssystemer. Departementet har fått opplyst fra det danske justisministeriet at behandlingen reguleres av de generelle hjemlene for politiets virksomhet.

I Sverige har det vært lagt til grunn at det ikke er nødvendig med en særskilt regulering av, eller behandlingsgrunnlag for, bruk av personopplysninger til testing og utvikling dersom behandlingen er nødvendig for at myndighetene skal kunne utføre sin virksomhet, se blant annet Prop. 2023/24:29 *En ny dataskyddsreglering på socialförsäkringsområdet* side 45–46 og Prop. 2019/20:113 *En mer ändamålsenlig dataskyddsreglering för studiestödsverksamheten* side 19–21. I sistnevnte proposisjon uttales blant annet at det «[a]tt testverksamhet inte behöver regleras som ett särskilt ändamål måste således anses vara en slags huvudprincip».

I SOU 2025:49 *Säkerhetspolisens behandling av personuppgifter* punkt 8.1.2 på side 303 uttales det:

It-system och olika behandlingsmetoder har kontinuerligt utvecklats och vidareutvecklats i syfte att effektivisera myndighetens kärnverksamhet. Sådan teknisk utveckling har inte ansetts nödvändig att härleda till något uttryck-

ligt uppdrag eller någon särskild rättslig grund, då det ansetts följa indirekt av andra uppdrag eller varit en nödvändig förutsättning för att myndighetens förvaltning och funktion.

Vi anser att it-utveckling som syftar till att öka myndighetens förmåga att bearbeta och analysera personuppgifter utgör en del av den brottsbekämpande verksamheten.

Den finske lag (639/2019) 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 annet ledd nr. 9. Også bestemmelsene i lag (616/2019) 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 blant annet lovligheitsovervåking, 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.

6 Regulering av testing og utvikling i politiregisterloven

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 nr. 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 ikke av noen av unntakene.

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 i den forstand at det regulerer alle former for behandling av opplysninger til formål som er omfattet av loven, uavhengig av måten det gjøres på. Det legger ikke føringer for hva slags 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 punkt 8.1.

Regelverket 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 som nevnt i punkt 3.2 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 i utgangspunktet bero på en konkret tolkning.

I Ot.prp. nr. 108 (2008–2009) *Om lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven)* punkt 8.4.1 er det imidlertid uttalt at departementet tok sikte på å gi en komplett og utfyllende lov for politiets behandling av opplysninger, slik at det ikke ville bli behov for å supplere med den tidligere personopplysningslovens bestemmelser.

6.2 Nærmere om behovet

Politiet bruker i dag fiktive opplysninger til testing, utvikling og forvaltning av informasjonssystemer som brukes innenfor politiregisterlovens virkeom-

råde i den grad det er mulig. Imidlertid vil det i en del tilfeller være nødvendig at politiets systemer testes og utvikles med reelle opplysninger, blant annet dersom fiktive eller anonymiserte opplysninger ikke simulerer virkeligheten godt nok til at man kan være sikker på at systemet fungerer som tiltenkt. Det kan videre være ressurskrevende, noen ganger tilnærmet umulig, å lage et realistisk syntetisk datasett som tar høyde for alle variasjoner i virkelige 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 dessuten 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. For å kvalitetssikre systemene og unngå informasjonssikkerhetsbrudd, herunder brudd på personopplysningssikkerheten, kan det være helt nødvendig å teste systemene med reelle opplysninger.

Behovet for å bruke opplysninger til testing og utvikling av informasjonssystemer gjør seg gjeldende i mange ulike situasjoner og for mange ulike typer systemer, fra utvikling av helt nye systemer fra bunnen av og til testing og tilpasning av verktøy og systemer som er utviklet av andre. Det er ikke mulig å gi en uttømmende beskrivelse av hva slags systemer det er behov for å utvikle og teste på nåværende tidspunkt og i fremtiden. Her nevnes likevel noen konkrete eksempler for å illustrere bredden i situasjoner 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. Det er svært tidkrevende og til dels umulig å produsere tilsvarende syntetisk materiale som representerer virkeligheten. Der som modeller testes, tilpasses eller trenes på feil datagrunnlag vil dette kunne påvirke resultatene i stor grad.

Det finnes 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 kvalitetssikres før de tas i bruk.

Det kan også være behov for testing av nye versjoner av programvare, for eksempel i systemer for passasjerinformasjon (PNR), jf. politiregisterforskriften kapittel 60. PNR-data er til dels ustrukturerte 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 syntetiske data som speiler data i produksjon, samtidig som det er risiko for avvik og feil dersom programvaren ikke testes med reelle opplysninger.

Det kan i tillegg være nødvendig 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 tilpassede verktøy som kan transkribere, oversette og lage sammendrag av store mengder materiale fra kommunikasjonskontroll. 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 den informasjonen politiet er ute etter i materialet, slik at det kan være nødvendig å teste og gjøre justeringer for å ivareta politiets særlige behov.

6.3 Forslaget i høringsnotatet

Departementet mente i høringsnotatet at det var 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 ble det lagt til grunn at det kan være behov for å benytte reelle opplysninger i større eller mindre omfang. Det ble vist til at det i dag er noe usikkert i hvilken grad politiet kan benytte reelle opplysninger til testing og utvikling, og hvilket personvernregelverk som i tilfelle gjelder.

I høringsnotatet uttalte departementet at 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. Begrunnelsen var at behandlingen skal resultere i systemer som skal brukes til formål som er omfattet av politiregisterloven.

Departementet viste til at LED ikke åpner 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 til bruk i kriminalitetsbekjempelsen anses som et annet formål enn kriminalitetsbekjempelse, vil GDPR gjelde for denne behandlingen. Departementet mente at bruk av opplysninger til testing og utvikling av informasjonssystemer som skal brukes til kriminalitetsbekjempende formål, har så nær sammenheng med det opprinnelige formålet at de samme personvernreglene bør gjelde også for denne behandlingen. Selv om EU-domstolen i flere saker har uttalt at unntakene i personvernforordningen artikkel 2 nr. 2 skal tolkes strengt, se blant annet C-180/21, 8. desember 2022, avsnitt 73, har uttalelsene 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.

Departementet mente derfor at testing og utvikling av systemer som skal brukes til politimessige formål, måtte kunne innfortolkes i formålene som er nevnt i LED artikkel 1 nr. 1 og politimessige formål, og at LED dermed gjelder for denne behandlingen. Det ble vist til at dette til dels støttes av KI-forordningens regler om utvikling av høyrisiko KI-systemer der systemet trenes ved bruk av trenings-, validerings- og testdatasett. KI-forordningen 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.

Selv om testing og utvikling ikke anses som et eget eller annet formål enn politimessige formål, mente departementet at det likevel var behov for å gi en klar hjemmel for bruk av reelle opplysninger til testing og utvikling og regulere denne formen for behandling nærmere. Departementet foreslo derfor endringer i 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.

I høringsnotatet ble det også foreslått en hjemmel til å gi nærmere regler i forskrift om behandling av opplysninger i forbindelse med testing og

utvikling av informasjonssystemer. Høringsnotatet inneholdt også forslag til slike forskriftsbestemmelser, herunder at det måtte være umulig eller uforholdsmessig vanskelig å oppnå formålet ved å bruke anonyme eller fiktive opplysninger, krav om den behandlingsansvarliges godkjenning og utvidelse av plikten til forhåndsdrøftelser med Datatilsynet.

I høringsnotatet ble det understreket at forslaget ikke åpnet for at politiet kan innhente opplysninger de ikke ellers ville hatt hjemmel til å behandle for å bruke dem til testing og utvikling. Det ble også vist til at forslaget ikke medførte at opplysningene skulle kunne utleveres til andre.

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

6.4 Høringsinstansenes syn

6.4.1 Generelle og overordnede synspunkter

Politidirektoratet, Kripas, Politiets utlendingsenhet, Øst politidistrikt, Politiets IT-enhet, Politihøgskolen og Politiets sikkerhetstjeneste støtter endringsforslagene. Ingen høringsinstanser er negative til å regulere testing og utvikling av informasjonssystemer som skal brukes til politimessige formål.

Politidirektoratet og Kripas viser til at forslaget vil klargjøre rettstilstanden på et område som stadig blir viktigere både for politiets digitalisering og for digitalt politiarbeid. Bruk av reelle opplysninger til testing og utvikling vil bidra til å sikre tilstrekkelig kvalitet og sikkerhet i informasjonssystemer som er av stor betydning for politiets kriminalitetsbekjempende virksomhet.

Politidirektoratet legger, i likhet med *Politiets utlendingsenhet*, til grunn at bestemmelsen er ment å omfatte registre hvor opplysninger behandles dels til politimessige formål og dels til forvaltningsformål, jf. politiregisterforskriften § 1-3 første ledd nr. 3. Politiregisterforskriften kapittel 56 om politiets utlendingsregister er gitt i medhold av denne bestemmelsen. Disse instansene ser samtidig behov for klargjøring av hvorvidt lovforslaget også omfatter systemer som brukes både til forvaltningsformål og politimessige formål, men hvor systemet ikke er regulert i politiregisterforskriften del 11.

Øst politidistrikt mener at forslagene er hensiktsmessige og fornuftige. Distriktet er enig i at det bør gis klare hjemler for behandling av opplysninger til slike formål, både for å sikre politiets

behov for teknologisk utvikling og for å gi klare rammer i forhold til de registrertes rettigheter.

Politiets IT-enhet ønsker forslagene velkomne. Politiet utvikler og tester en rekke løsninger som samvirker med systemer fra samarbeidende etater. Det er da viktig at hjemlene for testing og utvikling som gjelder for de ulike aktørene er compatible. Politiets IT-enhet oppfatter at de foreslåtte hjemlene følger samme mønster som tilsvarende hjemler gitt andre etater, og støtter dette.

Politiets utlendingsenhet støtter departementets forslag, og mener det er viktig at politiets adgang til å benytte reelle data til testing og utvikling lovreguleres eksplisitt. En lovregulering vil også styrke de registrertes rettigheter. Enheten mener det også bør gis tilsvarende regler om testing og utvikling i utlendingsloven, og viser til at det foregår en omfattende utvikling av nye data-systemer for utlendingsforvaltningen.

Politihøgskolen mener det er viktig at lovgiver tilrettelegger for at politidata kan brukes til testing og utvikling.

Utlendingsdirektoratet er positivt til at adgangen til å bruke reelle data til testing og utvikling reguleres også på politiregisterlovens område. Direktoratet forstår forslaget som at det også kan omfatte testing og utvikling av utlendingsregisteret, som er en logisk atskilt del av politiets ABIS-register, ettersom politiet blant annet har søketilgang til utlendingsregisteret i straffesaker over en definert strafferamme.

Datatilsynet støtter også forslaget om lovregulering, men mener det er viktig å vurdere forslagene opp mot mulighetene som åpnes for utvikling av kunstig intelligens og maskinlæring, som medfører en risiko for potensielt store inngrep i den enkeltes personvern og som kan ha store konsekvenser for samfunnet. Datatilsynet påpeker at de foreslåtte endringene utfordrer de generelle personvernprinsippene ved at opplysningene ikke er frivillig avgitt og ved at de registrerte ikke nødvendigvis vil få informasjon om innhenting og bruk av opplysningene. Tilsynet mener det er problematisk at det åpnes for å utvikle verktøy uten at det nødvendigvis finnes lovhjemmel for å bruke verktøyene. Det er i tillegg utfordrende at politiregisterloven, slik den er utformet i dag, er lite egnet til å regulere bruk av kunstig intelligens i politiet og påtalemyndigheten.

EOS-utvalget fremhever viktigheten av at det legges til rette for intern og ekstern kontroll av utviklingen av kunstig intelligens, herunder hvordan modellene settes opp. Med henvisning til at KI-forordningen ikke regulerer bruk av kunstig intelligens som utelukkende benyttes i for-

bindelse med nasjonal sikkerhet, mener utvalget at departementet bør klargjøre hvilke krav som skal gjelde for utviklingen av kunstig intelligens når behandlinger faller utenfor KI-forordningens virkeområde, og generelt hvordan det skal legges til rette for kontroll.

Advokatforeningen mener overordnet at begrunnelsen for forslagene virker å være fornøftig, og registrerer at departementet vurderer at de personvernmessige konsekvensene av forslaget står i et rimelig forhold til de formålene bestemmelsen skal oppnå.

6.4.2 Hvilket personvernregelverk som gjelder for behandlingen

Høringsinstansene er delte i synet på om LED eller GDPR regulerer behandlingen som er beskrevet i høringsnotatet. *Politidirektoratet* og *Politihøgskolen* er enige i at testing og utvikling kan innfortolkes i formålene i LED artikkel 1 nr. 1 og politimessige formål. *Datatilsynet* og *Digitaliseringsdirektoratet* mener derimot at testing og utvikling vanskelig kan innfortolkes i LEDs virkeområde.

Politidirektoratet mener det er viktig at grensedragningen mellom LED og GDPR er tydelig vurdert og beskrevet i det videre lovarbeidet.

Datatilsynet viser til at unntaket fra personvernforordningens virkeområde i artikkel 2 nr. 2 bokstav d, etter sin ordlyd er rettet mot mer tradisjonelle og utpregede politioppgaver. I og med at unntakene skal tolkes strengt, er det vanskelig å innfortolke utvikling av verktøy basert på kunstig intelligens i disse unntakene. Heller ikke politiregisterlovens definisjon av «politimessige formål», jf. § 2 nr. 13, omfatter teknologiutvikling som sådan. Etter Datatilsynets syn vil derfor bruk av personopplysninger til utvikling av kunstig intelligens i politisektoren i alminnelighet kunne reguleres av personvernforordningen. Dette synspunktet kan imidlertid nyanseres noe, blant annet med henvisning til LEDs fortalepunkt 27 og en artikkel i *European Journal of Law and Technology*, Vol. 15 No. 3 (2024), som argumenterer for at forskning og utvikling i noen tilfeller kan falle inn under begrepet «forebygging». Datatilsynet støtter departementet i at det må vurderes konkret hvilket regelverk som får anvendelse for hver behandling. Tilsynet ser at dette kan by på vanskelige grensedragninger, men mener det vil være et sentralt moment å vurdere formålet med behandlingen av de aktuelle opplysningene og om det er nødvendig gjøre behandlingen under virkeområdet til politiregisterloven.

Datatilsynet viser til at GDPR gir et sterkere vern for den registrertes rettigheter enn politiregisterloven. Det sentrale for tilsynet er at de registrertes rettigheter ivaretas, og at det ikke gjøres større unntak fra retten til informasjon og innsyn enn nødvendig. Datatilsynet mener derfor at det bør vurderes konkret i hvert enkelt prosjekt eller behandling om det er nødvendig å unnta behandlingen fra de registrertes rettigheter, og i hvilken grad åpenhet skal praktiseres. Selv om det i mange tilfeller er andre hensyn som må vektlegges, for eksempel ved bruk av opplysninger fra skjulte metoder, bør det som et utgangspunkt tilstrebes størst mulig åpenhet om utvikling og bruk av KI i politiet. Datatilsynet ber derfor spesielt om at det tas stilling til hvilket regelverk som regulerer testing og utvikling i det videre lovarbeidet.

Digitaliseringsdirektoratet oppfordrer departementet til å foreta en mer inngående vurdering av hvorvidt GDPR eller LED er riktig rettslig utgangspunkt, og viser blant annet til at Datatilsynet i sin sandkasserapport om «Prevbot» har kommet til motsatt konklusjon enn departementet om hvilket personvernregelverk som gjelder for testing og utvikling på området. Viderebehandling for å trene og teste maskinvare vil etter Digitaliseringsdirektoratets syn klart utgjøre en behandling som har et annet formål enn det opplysningene opprinnelig ble innhentet for. Direktoratet oppfordrer til en nærmere vurdering av om særlig viderebehandlingen fortsatt er innenfor det saklige virkeområdet til LED, og om behandlingen er nødvendig og forholdsmessig for å oppnå formålet.

Direktoratet viser til at ikke enhver behandling som har en mer indirekte kriminalitetsforebyggende intensjon vil falle innenfor LEDs saklige virkeområde. Formålene i LED artikkel 1 nr. 1 er uttømmende og tar først og fremst sikte på å regulere operativ virksomhet. I utgangspunktet er derfor ikke formålet å legge til rette for utvikling av nye tekniske løsninger. Digitaliseringsdirektoratet viser videre til at begrensningene i GDPRs virkeområde skal tolkes strengt. Direktoratet fremhever også at rettssystematiske hensyn taler mot å innfortolke maskinlæring mv. i LEDs saklige virkeområde. Etter deres skjønn vil en slik fortolkning i realiteten medføre en utvidelse av LEDs virkeområde, og dermed muligens gå på bekostning av virkeområdet til GDPR.

6.4.3 Utlevering

Flere høringsinstanser har kommentert uttalelsen i høringsnotatet om at forslaget ikke medfører at opplysningene skal kunne utleveres til andre.

Politidirektoratet ber om at departementet i det videre lovarbeidet angir nærmere hva som ligger i denne forutsetningen. Herunder bør det angis om dette skal forstås som en begrensning i bruk av reelle personopplysninger til verdikjedetesting, for eksempel eventuell testing av system-til-system-kommunikasjon med andre aktører, bruk av eksterne databehandlere og testing og utvikling av skybaserte tjenester.

Politihøgskolen mener det også innenfor rammen av anvendt forskning er behov for at politidata kan brukes til testing og utvikling av informasjonssystemer til politimessige formål. Det innebærer et behov for å kunne dele dataene med forskningsinstitusjonen i prosjektet, som besitter den tekniske kompetansen. Politihøgskolen anser at når det først legges til grunn at testing og utvikling av informasjonssystemer utført av politiet selv, direkte omfattes av politimessige formål, må utlevering av data til en forskningsinstitusjon for tilsvarende formål anses som viderebehandling for et formål som er forenlig med det opprinnelige, jf. LED artikkel 4 nr. 2. I tillegg følger det av artikkel 4 nr. 3 at viderebehandling kan skje for «scientific use» for direktivets formål.

Politihøgskolen foreslår at det tas inn et nytt ledd i politiregisterloven § 33 om at taushetsplikten kan oppheves for anvendt forskning som har til formål å teste og utvikle informasjonssystemer som skal understøtte politimessige formål. Alternativt kan det tas inn en ny setning i § 32 om at taushetsplikten ikke er til hinder for at opplysninger brukes for dette formålet. Gjennom henvisning til andre relevante bestemmelser bør det etableres tilsvarende sikkerhetsgarantier som de som gjelder for testing og utvikling som utføres av politiet selv.

Advokatforeningen peker på at utlevering av opplysninger vil være en mulighet dersom testingen og godkjenningen gjelder skybaserte tjenester hvor opplysningene må behandles i en tredjeparts dataløsninger, eller dersom testingen eller utviklingen gjøres ved hjelp av IT-leverandører eller konsulenter.

6.5 Departementets vurderinger

6.5.1 Generelt

Høringen bekrefter departementets vurdering av at det er behov for en nærmere regulering av bruk av opplysninger til testing og utvikling av informasjonssystemer som skal brukes innenfor politiregisterlovens virkeområde. Forslaget i proposisjonen her vil gjøre at politiet i større grad vil

kunne ta i bruk de mulighetene den teknologiske utviklingen gir, og det vil samtidig sikre at informasjonssystemer som benyttes i kriminalitetsbekjempelsen er tilpasset politiets særlige behov.

En del høringsinstanser har hatt kommentarer til forslaget til forskriftsbestemmelse som nærmere regulerer rammene for bruk av opplysninger til testing og utvikling av informasjonssystemer som skal brukes innenfor politiregisterlovens virkeområde. Enkelte innspill berører også tekniske forhold som ikke direkte har tilknytning til de foreslåtte lovforslagene. Disse innspillene vil kun bli gjengitt og kommentert i den grad de har betydning for forslaget om å utvide politiregisterlovens virkeområde til også å omfatte testing og utvikling av informasjonssystemer. Departementet vil vurdere innspillene knyttet til forskriftsbestemmelsen i forbindelse med ferdigstillingen av denne.

Departementet understreker at forslaget her utelukkende gjelder behandling av opplysninger som reguleres av politiregisterloven. Det vil dermed også omfatte opplysninger som behandles delvis til politimessige formål og delvis til forvaltningsmessige formål i et sentralt register, jf. politiregisterforskriften § 1-3 og politiregisterloven § 14. Det vil i utgangspunktet ikke omfatte testing og utvikling av systemer som har som hovedformål å behandle opplysninger som ledd i politiets forvaltningsvirksomhet, selv om det forekommer enkeltstående behandlinger i slike systemer som har et politimessig formål. Dersom det likevel er mulig å skille utviklingen av den «politimessige» delen av systemet klart fra øvrig utvikling, vil politiregisterloven kunne gjelde for utvikling og testing av denne delen. Dette vil måtte vurderes konkret for det enkelte system.

EOS-utvalget har stilt spørsmål ved hvilke regler som vil gjelde for PSTs utvikling av KI-systemer der behandlingen faller utenfor KI-forordningens virkeområde. PSTs testing og utvikling vil reguleres av de alminnelige reglene i politiregisterlovgivningen, noe som også vil omfatte de nærmere forskriftsbestemmelsene om slik behandling. Dette gjelder uavhengig av om informasjonssystemet utgjør et KI-system eller ikke. PST må på vanlig måte og i dialog med EOS-utvalget legge til rette for at utvalget kan ivareta sine kontrolloppgaver.

Departementet ser det ikke som problematisk at bruk av informasjonssystemer som kan ha inngripende konsekvenser kan kreve særskilt hjemmel, mens hjemmelen for testing og utvikling foreslås å skulle være generell. Dette er også tilfelle for hjemler for testing og utvikling i annet regelverk. Konsekvensene av bruken av et system vil være

atskillig mer inngripende enn det utvikling og testing av systemet vil være. Kravene til et klart og tydelig regelverk gjør seg dermed i større grad gjeldende for bruk. Også KI-forordningen skiller mellom testing og utvikling og bruk av systemer. Forordningen gjelder ikke for forsknings-, test- eller utviklingsaktiviteter med hensyn til KI-systemer eller KI-modeller før de bringes i omsetning eller tas i bruk, jf. forordningen artikkel 2 nr. 8. For bruk av visse inngripende systemer krever forordningen at bruken må reguleres i nasjonal rett, men den er ikke til hinder for at systemene utvikles.

Ingen høringsinstanser har kommentert forslaget til forskriftshjemmel for å kunne gi nærmere bestemmelser om testing og utvikling i forskrift. Forslaget til endringer i politiregisterloven § 69 er likelydende som det som ble foreslått i høringsnotatet.

Utlendingsregisteret reguleres av utlendingsloven og personvernforordningen, uavhengig av om politiet har tilgang til det og at Kripos er databehandler. Bruk av reelle personopplysninger fra utlendingsregisteret for å teste og videreutvikle dette registeret faller derfor utenfor forslaget her.

6.5.2 Hvilket personvernregelverk som regulerer behandlingen

Lovendringen som foreslås tar utgangspunkt i at det er politiregisterloven, som gjennomfører LED, som skal regulere behandling av opplysninger til testing og utvikling av informasjonssystemer som skal brukes innenfor lovens virkeområde. Flere høringsinstanser har hatt synspunkter på departementets vurdering av hvilket personvernregelverk som regulerer denne behandlingen, og har oppfordret til at spørsmålet vurderes og omtales nærmere i proposisjonen.

Som omtalt i punkt 6.1 er politiregisterlovens anvendelsesområde i lovens § 3 utformet slik at den gjelder for all behandling av opplysninger i politiet og påtalemyndigheten, med visse spesifikke unntak. Disse unntakene omfatter ikke testing og utvikling av informasjonssystemer som skal brukes til formål som omfattes av loven. Etter bestemmelsens ordlyd reguleres dermed slik behandling av politiregisterloven. Som nevnt tok departementet med forslaget til politiregisterloven sikte på å gi en komplett lov om politiets behandling av opplysninger, og personopplysningsloven var ikke ment å skulle komme supplerende til anvendelse.

Det følger imidlertid av EØS-loven § 2 at bestemmelser i lov som tjener til å oppfylle Norges forpliktelser etter EØS-avtalen, i tilfelle

konflikt skal gå foran andre bestemmelser som regulerer samme forhold. Dette gjør det også nødvendig å vurdere om det er GDPR eller LED som utgjør det folkerettslige rammeverket for den aktuelle behandlingen, da det kun er GDPR som er del av EØS-avtalen.

Hvilket personvernregelverk som kommer til anvendelse ved testing og utvikling av informasjonssystemer til bruk for politimessige formål er ikke klart regulert verken i LED eller GDPR. EU-domstolen har i sin praksis lagt til grunn at unntakene fra GDPRs virkeområde skal tolkes strengt. Videre har domstolen uttalt at ved viderebehandling til et annet av formålene som er nevnt i LED artikkel 1 nr. 1 enn det opplysningene opprinnelig ble innsamlet for, må de ulike formålene betraktes som «specific and distinct», jf. C-180/21, 8. desember 2022, avsnitt 56. Departementet er enig med Datatilsynet og Digitaliseringsdirektoratet i at formålene i artikkel 1 nr. 1 etter sin ordlyd retter seg mot de tradisjonelle politiopp-gavene, og ikke direkte mot teknologisk utvikling. Etter departementets syn vil dette imidlertid ikke sette en skranke mot at også testing og utvikling som har til formål å bidra til politiets kriminalitetsbekjempende virksomhet, reguleres av politiregisterloven og LED.

Slik departementet ser det, har testing og utvikling av informasjonssystemer som skal brukes til politimessige formål så nær sammenheng med den kriminalitetsbekjempende virksomheten at LED må komme til anvendelse. Behandlingen skjer med sikte på å utvikle, teste og forbedre verktøy og systemer som er nødvendige i politiets og påtalemyndighetens kriminalitetsbekjempende virksomhet. For at disse systemene skal kunne brukes er det en forutsetning at de tilpasses politiets behov og i tillegg testes for å sikre at de fungerer etter intensjonen. Utvikling og testing som bedrer eller effektiviserer politiets kriminalitetsbekjempende virksomhet, vil dermed etter departementets syn falle innenfor det samme formålet.

Departementet legger dessuten vekt på at LED artikkel 4 nr. 3 åpner for at behandlingen kan inkludere «scientific use» for formålene som nevnt i artikkel 1 nr. 1, forutsatt at behandlingen er omfattet av tilstrekkelige tiltak for å sikre de registrertes rettigheter og friheter. Vitenskapelig bruk kan også inkludere utvikling av nye metoder og systemer til bruk i kriminalitetsbekjempelsen. Dette har, slik også Datatilsynet viser til, støtte i enkelte forskningsartikler. Behandlingen vil bli nærmere regulert i forskrift. På denne måten vil det etableres egnede sikkerhetsmekanismer, slik LED artikkel 4 nr. 3 gir anvisning på.

Departementet peker også på at det vil være vanskelig praktisk gjennomførbart dersom politiet i det enkelte tilfelle skal vurdere om personopplysningsloven eller politiregisterloven kommer til anvendelse når testing og utvikling skjer for å ivareta formål innenfor politiregisterlovens virkeområde. Opplysningene som benyttes i ulike utviklingsprosjekter kan være de samme eller hentet fra samme register, men behandlingsreglene vil kunne bli ulike, avhengig av utfallet av vurderingen i det enkelte tilfelle. Konsekvensene av vekslende bruk av de to personvernregelverkene vil kunne være uoversiktlige, og vil øke risikoen for mangelfull etterlevelse.

Det vil i tillegg legge uhensiktsmessige begrensninger på hvilke opplysninger som kan brukes til testing og utvikling av systemer som skal brukes til politimessige formål dersom GDPR regulerer behandlingen. Særlig reglene om innsyn er ulike etter politiregisterloven og personopplysningsloven. Etter LED og politiregisterloven § 54 er det mulig å gi en alternativ begrunnelse dersom innsyn ikke gis, slik at vedkommende ikke får vite om han eller hun er registrert. Etter personopplysningsloven § 16 tredje ledd skal den som nekter å gi innsyn, begrunne dette skriftlig med en presis henvisning til unntakshjemmelen. Den som ber om innsyn etter personopplysningsloven vil dermed kunne få vite at han eller hun er registrert dersom opplysninger om vedkommende er tatt i bruk til testing og utvikling, selv om innsyn i opplysningene for øvrig kan nektes av hensyn til kriminalitetsbekjempelsen. Dette vil kunne fordre at politiet gjør en konkret vurdering av den enkelte opplysning og konsekvensene av at den enkelte får vite om registrering før opplysningen eventuelt brukes til testing og utvikling. I så fall vil det både være ressurskrevende og øke risikoen for at datagrunnlaget ikke blir representativt.

Departementet kan heller ikke se at den registrertes rett til informasjon utfordres ved at LED kommer til anvendelse. Også etter GDPR er retten til informasjon begrenset dersom bruken av opplysninger til et nytt formål er lovregulert, jf. GDPR artikkel 14 nr. 5 bokstav c, jf. nr. 4. Reglene som skal fastsettes i forskrift vil inneholde egnede tiltak for å verne den registrertes rettigheter.

LED kommer ikke til anvendelse for aktiviteter som faller utenfor unionsretten, jf. artikkel 2 nr. 3 bokstav a og fortalepunkt 14. Dette omfatter blant annet tiltak for nasjonal sikkerhet. PSTs testing og utvikling av informasjonssystemer som skal brukes til etterretningsvirksomhet eller fore-

byggende virksomhet vil dermed reguleres utelukkende av politiregisterloven.

6.5.3 Utlevering

I høringsnotatet ble det uttalt at bruk av opplysninger til testing og utvikling ikke medfører at opplysningene skal kunne utleveres til andre, noe flere høringsinstanser har kommentert at kan være nødvendig. Det gjøres ingen endringer i politiregisterloven kapittel 6 om begrensninger i taushetsplikten, slik at forslaget her ikke gir noen utvidet adgang til å utlevere opplysninger sammenlignet med gjeldende rett.

Forslaget er imidlertid ikke til hinder for ulike former for bistand til å utføre testing og utvikling, for eksempel ved bruk av innleid personell eller databehandlere. Innleide konsulenter mv. vil kunne omfattes av politiregisterforskriften § 1-3 nr. 1 om at loven også får anvendelse for personer som gjør tjeneste ved politiet og påtalemyndigheten uten å være tilsatt. Ved bruk av et eksternt

firma for å utføre testing og utvikling på politiets vegne vil firmaet som regel være databehandler for politiet, og opplysningene vil ikke kunne behandles på annen måte enn den som følger av skriftlig avtale eller instruks, jf. politiregisterloven § 18. Verken bruk av databehandlere eller personell som omfattes av politiregisterforskriften § 1-3 nr. 1 innebærer utlevering av opplysninger i politiregisterlovens forstand.

Departementet ser ikke grunn til å endre politiregisterloven § 33 om utlevering til forskning for å ta høyde for at forskningen kan ha til formål å teste eller utvikle informasjonssystemer, der både politiet og forskningsinstitusjonen har interesse i prosjektet. En eventuell utvidet adgang til å utlevere opplysninger i forbindelse med visse former for forskning har ikke vært hørt eller utredet nærmere. Politiregisterloven § 33 stiller ikke krav med hensyn til formålet med forskningen, og departementet mener at bestemmelsen er tilstrekkelig fleksibel til å ivareta de hensyn Politi-høgskolen trekker frem.

7 Bruk av informasjon fra skjulte tvangsmidler til testing og utvikling

7.1 Gjeldende rett

Straffeprosessloven § 216 i og politiloven § 17 f regulerer taushetsplikt for opplysninger innhentet med skjulte tvangsmidler i henholdsvis etterforskning og som ledd i PSTs forebyggende virksomhet. Bestemmelsene fastslår at alle skal bevare taushet om opplysninger om at det er benyttet skjulte tvangsmidler, og om opplysninger som fremkommer ved bruk av slike tvangsmidler. Det er i begge bestemmelsene uttrykkelig angitt at taushetsplikten ikke er til hinder for bruk av opplysningene til nærmere angitte formål. Testing og utvikling av informasjonssystemer er ikke nevnt verken i straffeprosessloven § 216 i eller politiloven § 17 f.

Kontrollutvalget for kommunikasjonskontroll (KK-utvalget) fører kontroll med politiets bruk av kommunikasjonskontroll, romavlytting og dataavlesing, med unntak av saker som omfattes av EOS-kontrollloven, 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».

7.2 Forslaget i høringsnotatet

I høringsnotatet bemerket departementet at skjulte tvangsmidlers inngripende karakter kan være en innvending mot at opplysninger som er underlagt formålsbegrensningene i straffeprosessloven § 216 i og politiloven § 17 f, skal kunne brukes til testing og utvikling. Samtidig ble det vist til at det nettopp på dette området er et særlig behov for verktøy som kan bidra til enklere oversikt, sammenstilling og oversettelse, samt å finne frem til relevante bevis. Slike verktøy kan bidra til å redusere den manuelle gjennomgangen av opplysninger, noe som igjen kan være positivt i et personvernperspektiv.

Departementet foreslo derfor, under noe tvil, at også opplysninger innhentet ved kommunikasjonskontroll, romavlytting og dataavlesing bør kunne brukes til testing og utvikling av informasjonssystemer som skal brukes innenfor politiregisterlovens virkeområde.

I høringsnotatet ble det uten nærmere drøftelse lagt til grunn at selv om straffeprosessloven § 216 i og politiloven § 17 f er utformet som regler om taushetsplikt og unntak fra denne, innebærer de også en regulering av hvilke formål opplysningene kan brukes til. Testing og utvikling ble derfor foreslått inntatt i nye bokstaver i straffeprosessloven § 216 i første ledd tredje punktum og politiloven § 17 f annet ledd, ettersom testing og utvikling ikke kan innfortolkes i noen av alternativene som allerede er opplistet i bestemmelsene.

Departementet var i høringsnotatet usikker på om det burde stilles ytterligere krav for at opplysninger som er omfattet av straffeprosessloven § 216 i og politiloven § 17 f skal kunne brukes til testing og utvikling, men vurderte at de foreslåtte forskriftsreglene for bruk av andre opplysningskategorier var tilstrekkelige til også å ta høyde for de særlige hensyn som gjør seg gjeldende for opplysninger fra skjulte tvangsmidler. Det ble imidlertid foreslått forskriftsfestet at også denne formen for testing og utvikling skulle underlegges krav om forhåndsdrøftelser med Datatilsynet.

I høringsnotatet ble det vist til at bruken av opplysninger som er underlagt formålsbegrensningene i straffeprosessloven § 216 i til testing og utvikling, vil falle inn under KK-utvalgets kontrollområde.

7.3 Høringsinstansenes syn

Kripas viser til at riksadvokaten har uttalt at straffeprosessloven § 216 i kun regulerer i hvilken utstrekning opplysningene kan brukes utad, og ikke legger begrensninger på politiets interne bruk. I lys av dette finner Kripas det uklart hva departementet legger til grunn når det uttales at bestemmelsen også «innebærer en regulering av

hvilke formål opplysningene skal brukes til», og at nevnte bestemmelser har karakter av formålsbegrensninger. Legges riksadvokatens utgangspunkt til grunn, vil det etter Kripas' oppfatning ikke være like stort behov for endring i straffeprosessloven. Kripas foreslår derfor at behovet for lovendring vurderes på ny. *Politidirektoratet* viser til Kripas sitt innspill.

Datatilsynet har enkelte prinsipielle innvendinger mot bruk av informasjon fra skjulte tvangsmidler til testing og utvikling. De verktøyene som høringsnotatet påpeker at det er behov for, kan ifølge tilsynet betraktes som ganske grunnleggende bruk av KI, men det vil også være mulig å lage systemer som kan gjenkjenne biometriske kjennetegn, som utseende, stemme eller talemåte. *Datatilsynet* understreker at slike verktøy må vurderes opp mot profilering, som politiregisterloven ikke omfatter, ettersom LED artikkel 11 om automatiserte individuelle avgjørelser ikke er implementert i loven.

Datatilsynet ser at det i mange tilfeller åpenbart er nødvendig å unnta behandling av personopplysninger fra denne typen kilder fra retten til innsyn og informasjon. Tilsynet anbefaler at departementet vurderer om det skal gjøres endringer i personopplysningsloven § 16, som åpner for å gjøre unntak fra de registrertes rettigheter blant annet av hensyn til forebygging, etterforskning, avsløring og rettslig forfølgning av straffbare handlinger, til også å omfatte slike handlinger som er omfattet av forslaget.

Kontrollutvalget for kommunikasjonskontroll (KK-utvalget) tar ikke stilling til om maskinlæringsmodeller skal utvikles og benyttes, men påpeker at det er viktig at eventuell bruk av treningsdata innhentet fra skjult metodebruk begrenses så mye som mulig. Utvalget ser at anonymiserte treningsdata ikke nødvendigvis i tilstrekkelig grad tilfredsstiller kravene i KI-forordningen til relevante, representative, feilfrie og fullstendige treningsdata for trening av høyrisiko maskinlæringsmodeller. Det er viktig at hele prosessen fra innsamling av data til distribusjon av ferdig utviklede modeller blir kontrollert. Dette må legges inn under utvalgets kontroll.

KK-utvalget forutsetter at utvalget kan føre kontroll med alle ledd, fra innsamling av data, testing, utvikling, distribusjon og til bruk av ferdig utviklede modeller. Siden utvikling av modellene og bruk av opplysninger fra skjult metodebruk lite trolig vil bli prøvd for domstolen, bør utvalget få et særskilt ansvar for å føre kontroll på dette området. Det er derfor viktig at politiet gjennomfører adekvate risikovurderinger og at disse vurde-

ringene er protokollført slik at de er etterprøvbare. Utvalget mener at politiet og påtalemyndigheten i startfasen må dokumentere hvilke tekniske løsninger, maskinvare og programvare som skal brukes, og dens egenskaper med sikte på etterfølgende kontroll. Under testing og utvikling må KK-utvalget kunne kontrollere hvordan gjennomføringen faktisk foregår, og om politiet følger fastsatte planer og retningslinjer. Før modellene settes i produksjon, må KK-utvalget kunne vurdere om gjennomføringen har gått etter planen, og at treningsdata ble håndtert og slettet eller sperret på riktig måte i etterkant.

For å muliggjøre tilsyn i alle faser må det etter utvalgets syn utarbeides detaljerte og sammenhengende rapporter som beskriver hvert steg i prosessen i detalj. Etter KK-utvalgets vurdering er det mye som taler for at politiet må følge samme prinsipper for protokollføring og innrapportering ved bruk av modellene som ved dataavlesning.

EOS-utvalget viser til at bruk av innhentede opplysninger til testing og utvikling utgjør et innbryt i personvernet, og savner en nærmere forholdsmessighetsvurdering av bruken av innhentede opplysninger til testing og utvikling generelt, og opplysninger innhentet ved bruk av tvangsmidler i forebyggende øyemed spesielt.

EOS-utvalget påpeker at politiloven § 17 f regulerer alle tvangsmidlene som PST kan anvende etter politiloven § 17 d, også beslag og utleveringspålegg, mens straffeprosessloven § 216 i regulerer taushetsplikt om opplysninger fra kommunikasjonskontroll, romavlytting, dataavlesning og tvangsmidler i avvergende øyemed. Utvalget viser til at opplysninger som skal slettes etter straffeprosessloven § 216 g annet ledd, ikke kan brukes til testing og utvikling. Departementet bør avklare om opplysninger som er omfattet av straffeprosessloven § 216 g annet ledd, men som inngår i en forebyggende sak, kan anvendes til testing og utvikling.

7.4 Departementets vurderinger

Departementet opprettholder vurderingen om at opplysninger som omfattes av straffeprosessloven § 216 i og politiloven § 17 f bør kunne brukes til testing og utvikling av informasjonssystemer som skal brukes innenfor politiregisterlovens virkeområde. Fordi det ofte er omfattende mengder informasjon som innhentes ved bruk av de aktuelle tvangsmidlene, er det på dette området et særlig stort behov for å kunne ta i bruk egnede informasjonssystemer. Materiale som er innhentet med

skjulte tvangsmidler, som opptak fra kommunikasjonskontroll og materiale fra dataavlesing, er unikt i sin karakter, og det vil ofte ikke være mulig å anonymisere opplysningene fullt ut eller skape et fullverdig fiktivt datasett. I en del tilfeller vil det dermed være nødvendig å teste og utvikle informasjonssystemer ved hjelp av den typen materiale de er tiltenkt brukt på. Det kan for øvrig også ha personvernmessige fordeler at ny teknologi kan benyttes, da det vil kunne redusere behovet for manuell gjennomgang av materialet.

Innhenting av opplysninger gjennom visse skjulte tvangsmidler, som kommunikasjonskontroll, romavlytting og dataavlesing, er særlig inngripende. Dette taler for at bruk av slike opplysninger til annet enn det de var innhentet for, begrenses. Departementet mener likevel at det vil være forholdsmessig å kunne bruke slike opplysninger til testing og utvikling. Dette skyldes både det faktiske behovet for å kunne bruke opplysningene til dette formålet, konsekvensene av å bruke informasjonssystemer som ikke er tilstrekkelig testet eller tilpasset til opplysningene de skal brukes på og at behandlingen vil bli rammet inn av forskriftsbestemmelser som begrenser inngrepet til det nødvendige.

Bruk av nye systemer som ikke er testet og tilpasset til politiets behov medfører en risiko for feilslutninger, skjevheter og unøyaktigheter i systemet som kan ha konsekvenser både for etterforskningen og for den berørte selv. Etterforskningen skal klarlegge både det som taler mot og det som taler for den mistenkte, jf. straffeprosessloven § 226 tredje ledd. Mangelfull testing og utvikling før systemene tas i bruk kan medføre en risiko for at systemene ikke avdekker relevante opplysninger som kan være både til fordel og ugunst for den mistenkte. Tilsvarende kan mangelfull testing av informasjonssystemer som brukes i PSTs forebyggende virksomhet medføre en risiko for at inngripende tvangsmiddelbruk varer lenger enn den ellers ville gjort, fordi informasjonen som hentes inn må gjennomgås og vurderes manuelt. Dette taler klart for å åpne for bruk av opplysninger fra skjulte tvangsmidler til testing og utvikling.

Det vil være en forutsetning for bruk av opplysninger fra skjulte tvangsmidler at ikke bruk av andre og mindre inngripende opplysningstyper vil være tilstrekkelig til å oppnå formålet. Behandlingen av opplysningene må også være nødvendig og forholdsmessig i det enkelte tilfelle. At opplysninger er innhentet ved skjult tvangsmiddelbruk, er et moment som må tas med i denne vurderingen. Måten opplysningene er innhentet på vil også få betydning for hvilke rammer som bør settes

for den enkelte behandlingen, herunder omfanget av opplysninger som skal brukes, hvem som skal ha tilgang til dem og varigheten av behandlingen.

Departementet legger også vekt på at testingen og utviklingen ikke vil medføre konsekvenser for den enkeltes rettsstilling eller at det treffes avgjørelser overfor de personene som omfattes av behandlingen. Behandlingen har dermed få paralleller til LED artikkel 11 om automatiserte individuelle avgjørelser. Det er først og fremst bruken av informasjonssystemer for å treffe avgjørelser som har negativ virkning for eller som berører den registrerte som må vurderes opp mot denne artikkelen. Slike avgjørelser legges det ikke opp til med forslaget her. At LED artikkel 11 ikke er gjennomført i politiregisterloven, kan derfor ikke ses å få noen betydning i denne sammenheng.

På bakgrunn av høringsinnspillet fra Kripos har departementet foretatt en ny vurdering av behovet for å endre straffeprosessloven § 216 i. Det aktuelle spørsmålet er hvorvidt bestemmelsen skal forstås som en bestemmelse om taushetsplikt som kun setter begrensninger på bruken av slike opplysninger utad, eller om bestemmelsen også setter begrensninger i politiets adgang til å benytte slike opplysninger internt.

Straffeprosessloven § 216 i første ledd tredje punktum angir at taushetsplikten ikke er til hinder for at opplysninger fra kommunikasjonskontroll mv. brukes i nærmere angitte situasjoner. I Ot.prp. nr. 64 (1998–99) *Om lov om endringer i straffeprosessloven og straffeloven m v (etterforskningsmetoder m v)* kapittel 23 punkt IV, merknadene til § 216 i, uttaler departementet at tredje punktum er et unntak fra taushetsplikten i første og annet punktum, og dermed bare regulerer i hvilken utstrekning opplysningene kan brukes utad, ved at de meddeles til andre. Det uttales at bestemmelsen dermed ikke legger begrensninger på politiets adgang til å benytte opplysninger fra kommunikasjonskontroll internt, så lenge opplysningene ikke meddeles andre. Lignende uttalelser finnes i samme proposisjon punkt 8.9.3.3 og i Prop. 61 L (2016–2017) *Endringer i straffeprosessloven og politiloven (utlevering av informasjon fra PST til E-tjenesten)* punkt 5.2. I enkelte andre proposisjoner forekommer derimot uttalelser som legger til grunn at bestemmelsen også innebærer begrensninger på den interne bruken av opplysninger fra skjult etterforskning, jf. blant annet Prop. 114 L (2012–2013) *Endringer i politiregisterloven mv.* punkt 4.2.3. Sistnevnte proposisjon har imidlertid karakter av etterarbeider til straffeprosessloven § 216 i, og har dermed begrenset vekt ved tolkningen av bestemmelsen.

I lys av det ovennevnte, kan det være grunn til å vurdere nærmere hvordan § 216 i er å forstå på dette punkt. Det kan også være grunn til å vurdere en lovendring for å klargjøre eller eventuelt endre rettstilstanden. Dette vil departementet eventuelt komme tilbake til på et senere tidspunkt. Med utgangspunkt i høringen som ligger til grunn for proposisjonen her, finner departementet det hensiktsmessig å begrense forslaget til en presisering av § 216 i som gjør det klart at opplysninger som omfattes av bestemmelsen, uansett kan brukes internt til testing og utvikling av informasjonssystemer. Departementet foreslår at dette reguleres i en ny bokstav l i § 216 i første ledd tredje punktum.

Det presiseres for ordens skyld at departementet med dette ikke har tatt stilling til om bestemmelsen legger begrensninger på andre former for intern bruk av opplysninger fra kommunikasjonskontroll.

Departementet opprettholder den foreslåtte endringen i politiloven § 17 f om bruk av opplysninger innhentet med tvangsmidler i forebyggende øyemed. Forarbeidene til denne bestemmelsen, særlig Ot.prp. nr. 60 (2004–2005) *Om lov om endringer i straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre alvorlig kriminalitet)*, skiller ikke mellom intern og ekstern bruk. I denne proposisjonen, punkt 9.4.4.1, uttales det:

For departementet er det en ufravikelig betingelse for å åpne for bruk av tvangsmidler i forebyggende øyemed at det skal gjelde strenge regler om taushetsplikt, og strenge begrensninger for hva opplysningene kan brukes til.

Etter departementets vurdering tilsier dette at bestemmelsen bør endres for å unngå usikkerhet om hvorvidt opplysninger innhentet ved skjulte tvangsmidler i forebyggende øyemed skal kunne brukes til testing og utvikling.

Selv om tvangsmiddelbruk i etterforskning og forebygging har ulike formål og skjer i ulike spor, er det mange av de samme hensynene som gjør seg gjeldende ved den videre behandlingen av opplysningene som innhentes. Formålene opplysningene kan brukes til uten hinder av taushetsplikt er til dels overlappende, selv om de er snevrere for de som er innhentet med tvangsmiddelbruk som ledd i forebygging. Begrunnelsen for de snevrere rammene var særlig hensynet til å unngå at det oppstår et press i retning av bruk av tvangsmidler i forebyggende øyemed fremfor som ledd i

etterforskning, noe som ville undergrave rettssikkerhetsgarantiene i strafforfølgningen, jf. Ot.prp. nr. 60 (2004–2005) punkt 9.4.4.1. Adgangen til å bruke opplysninger innhentet ved forebyggende tvangsmiddelbruk i etterforskning og som bevis i straffesak er derfor begrenset. Opplysningene kan bare brukes i etterforskning av lovbrudd som kan begrunne forebyggende tvangsmiddelbruk og som bevis for terrorlovbrudd, jf. politiloven § 17 f annet ledd bokstav b og c. Departementet ser imidlertid ikke at det er noen grunn til å etablere strengere rammer for bruk av opplysninger innhentet ved skjult tvangsmiddelbruk i forebyggende øyemed til testing og utvikling enn for bruk av andre opplysninger til dette formålet.

EOS-utvalget har bedt om at det avklares om opplysninger som omfattes av straffeprosessloven § 216 g annet ledd, men som inngår i en forebyggende sak, kan brukes til testing og utvikling. Straffeprosessloven § 216 g annet ledd pålegger en plikt til å slette blant annet kommunikasjon med nærstående og med personer som er underlagt kallsmessig taushetsplikt, med mindre vedkommende mistenkes for en straffbar handling som kunne ha gitt selvstendig grunnlag for kontrollen. Sletting skal skje så snart som mulig, jf. politiregisterloven § 50 tredje ledd tredje punktum, og det vil derfor ikke være mulig å bruke opplysningene til testing og utvikling. Straffeprosessloven § 216 g gjelder derimot ikke for opplysninger innhentet etter politiloven § 17 d. Dersom PST har registrert opplysninger som omfattes av straffeprosessloven § 216 g annet ledd, vil de etter forslaget her kunne brukes til testing og utvikling på samme måte som øvrige opplysninger innhentet ved skjulte tvangsmidler i forebyggende øyemed.

Departementet bemerker at KK-utvalgets kontroll er etterfølgende, og vil være begrenset til å kontrollere at opplysningene blir brukt på lovlig måte og at lovens regler om oppbevaring, spering og sletting av opplysninger blir fulgt, jf. kommunikasjonskontrollforskriften § 14. Departementet legger som utvalget likevel til grunn at prosesser og planer for behandlingen er godt dokumentert, slik at KK-utvalget kan føre effektiv kontroll med at opplysningene er brukt på lovlig måte.

Forslagene i proposisjonen her regulerer ikke bruk av maskinlæringsmodeller eller andre former for kunstig intelligens. Departementet tar derfor ikke nå stilling til eventuelle mekanismer for å sikre muligheten til å føre kontroll med bruk av maskinlæringsmodeller, men forutsetter at dette vil inngå i de relevante tilsynsorganenes til-

syn på vanlig måte. Hvordan det skal tilrettelegges for kontroll må løses i dialog mellom tilsynsorganene og politiet og påtalemyndigheten.

Datatilsynets merknad om eventuell endring av personopplysningsloven § 16 oppfattes å være relatert til tilsynets vurdering av at GDPR vil kunne gjelde for behandling av personopplysninger ved testing og utvikling, også der syste-

mene skal brukes til politimessige formål. Som omtalt i punkt 6.5.2, mener departementet at denne behandlingen kan og skal reguleres av politiregisterloven. Dette medfører at politiregisterlovens innsynsregler samt retten til dokumentinnsyn etter straffeprosessloven vil gjelde på vanlig måte, og at det ikke er nødvendig med endringer i personopplysningsloven.

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

8.1 Gjeldende rett

Politiregisterloven § 65 a 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. Bestemmelsen trådte i kraft 1. juli 2025.

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 bestemmelsens 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.

I Prop. 31 L (2022–2023) *Endringer i politiloven og politiregisterloven (PSTs etterretningsoppdrag og bruk av åpent tilgjengelig informasjon)* 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 eller hvilke opplysninger som skal kunne brukes til dette.

8.2 Forslaget i høringsnotatet

Departementet ga i høringsnotatet uttrykk for at det er et klart behov for at PST skal kunne benytte opplysninger som behandles etter politiregister-

loven § 65 a for å utvikle og teste informasjonssystemer som bestemmelsen åpner for at kan brukes. Det ble derfor foreslått å tilføye «utvikling og testing av informasjonssystemer som skal brukes innenfor bestemmelsens første ledd» som et nytt formål de sperrede opplysningene kan brukes til.

I høringsnotatet ble det vist til at det for kontrollformål vil være en fordel at PST har størst mulig kontroll over de tekniske verktøyene og systemene som benyttes. Det ble også påpekt at automatiserte analyseverktøy må være innrettet slik at EOS-utvalget kan føre kontroll med innretningen på og bruken av dem, noe som ble antatt å lettere kunne ivaretas dersom PST selv utvikler og tester verktøyene.

Det ble understreket at forslaget ikke åpnet for å innhente åpent tilgjengelig informasjon etter § 65 a utelukkende til bruk for testing og utvikling. Departementet vurderte i høringsnotatet at personvernkonsekvensene for de berørte ville være 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 kunne være mer inngripende for de berørte.

8.3 Høringsinstansenes syn

Politiets sikkerhetstjeneste gir generelt uttrykk for støtte til forslagene og vurderingene departementet har gjort. Ingen øvrige høringsinstanser har særskilt kommentert forslaget til endringer i politiregisterloven § 65 a.

8.4 Departementets vurderinger

Departementet opprettholder forslaget. Det fremstår som helt nødvendig at åpent tilgjengelig informasjon som lagres med hjemmel i § 65 a, kan brukes til å teste og utvikle informasjonssystemer som skal brukes for å behandle opplysningene. Det er ikke mulig å skape et stort nok sett med

fiktive data som er realistisk nok til å utvikle, teste og trene systemene.

Det at PST selv kan teste og utvikle verktøyene som skal brukes, alternativt tilpasse innkjøpte verktøy til tjenestens særskilte behov, har flere fordeler sammenlignet med å ta ferdigutviklede verktøy direkte i bruk. Med egen testing og utvikling vil verktøyene kunne innrettes bedre mot tjenestens behov, og justeres for å unngå 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 lede til analyser og vurderinger med lav kvalitet som ikke er egnet som beslutningsstøtte. Som omtalt i punkt 6.5.1 må utvikling og testing av systemene innrettes på en måte som legger til rette for at EOS-utvalget kan ivareta sine kontrolloppgaver.

9 Regulering av bruk av opplysninger til testing og utvikling i grenseloven

9.1 Gjeldende rett

Grensekontroll er en del av politiets forvaltningsvirksomhet. Behandlingen av opplysninger for grensekontrollformål reguleres av personopplysningsloven og GDPR. Grenseloven § 22 regulerer behandling av opplysninger til gjennomføring av grensekontroll. Den generelle hjemmelen i første ledd angir at politiet kan behandle personopplysninger som er nødvendige for gjennomføring av grensekontroll etter loven. Dette omfatter også særlige kategorier av personopplysninger. Etter annet ledd første punktum 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.

Forskriftsbestemmelsene er teknologinøytrale, i den forstand at de gjelder for behandling av opplysninger til det angitte formålet, uavhengig av hvilken tekniske løsning som benyttes. Ansiktsbilde fra reisedokumenter fra reisende som passerer grensekontrollen lagres i GTK, jf. § 5-3 første ledd nr. 2. Fingeravtrykk lagres ikke, jf. avgrensningen i samme nummer. 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. 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. Bestemmelsen viderefører tidligere bestemmelse i passloven § 6 a første ledd. Passloven § 6 a ble opphevet ved ikraftsettingen av 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) *Lov om grensetilsyn og grensekontroll av per-*

soner (grenseloven), særmerknaden til § 22 i kapittel 14, er det uttalt at denne sletteregelen skulle videreføres i grenseforskriften, men dette er ikke gjort. Det er imidlertid ingen hjemmel for å lagre verken ansiktsbilde eller fingeravtrykk innhentet i grensekontrollen, slik at opplysningene uansett vil måtte slettes.

9.2 Nærmere om behovet

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

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

Syntetiske data av ansikter, fingeravtrykk mv. kan brukes på noe testing, men kan ikke erstatte 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 dessuten svært tidkrevende og kan i begrenset grad speile en reell situasjon. Bruk av syntetiske data er heller ikke tilstrekkelig for å få et representativt utvalg av ansiktsbilder og fingeravtrykk, og politiet får ikke testet kvalitetskravene i tilstrekkelig grad med slike data.

Videre har politiet behov for å kunne lagre et representativt utvalg ansiktsbilder som er opptatt i grensekontrollen i en periode for testing og utvikling av systemer for automatisert kontroll av personer som passerer yttergrensen. Slik kontroll skal skje i form av en-til-en biometrisk sammenligning av ansiktsbilde i databrikken mot ansiktsbilde tatt i grensekontrollen. For å sikre en sikker og effektiv automatisert ansiktssammenligning i grensekontrollen, må det settes terskelverdier for

når ansiktsbilde opptatt i grensekontrollen og ansiktsbilde i reisedokumentet skal anses for å være av samme person. Denne terskelen må settes på et nivå som avdekker personer som benytter andres reisedokumenter, samtidig som personer ikke skal stanses for unødvendige kontroller (falske treff). 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 utreisepasssystemet (EES) (EES-forordningen) forutsetter at kontroll av ansiktsbilde og fingeravtrykk skal foretas ved grensepassering i større grad enn i dag, også i form av automatisert kontroll. Politidirektoratet har opplyst at for persongruppen som er omfattet av EES, dvs. tredjelandborgere, vil automatisert sammenligning ved bruk av ansiktsbilde og fingeravtrykk opptatt i grensekontrollen bli standard metode for å kontrollere identitet.

Den 12. oktober 2025 trådte forordning (EU) 2025/1534 om gradvis innføring av EES i kraft. Forordningen åpner for at Schengen-landene kan ta EES gradvis i bruk i en periode på 180 dager. Også etter at denne perioden utløper, vil det være behov for å lagre ansiktsbilder for å sikre at systemet fungerer som det skal, og for testing, feilretting og videreutvikling.

9.3 Forslaget i høringsnotatet

9.3.1 Hjemmel for bruk av opplysninger til testing og utvikling

Departementet foreslo i høringsnotatet en uttrykkelig hjemmel for bruk av opplysninger som behandles i forbindelse med grensekontroll til testing og utvikling av informasjonssystemer som skal brukes til grensekontrollformål. Forslaget var utformet etter mal av hjemler for bruk av opplysninger til testing og utvikling i annet regelverk, herunder ble det foreslått som vilkår for behandling av reelle opplysninger til testing og utvikling at det er umulig eller uforholdsmessig vanskelig å oppnå formålet ved hjelp av anonyme eller fiktive opplysninger.

Selv om forslaget særlig var begrunnet i behovet for testing og utvikling av systemer for biometrisk sammenligning, foreslo departementet ikke å begrense bestemmelsen til slike systemer. Det ble vist til en forventning om at den teknologiske utviklingen vil åpne for nye teknologiske muligheter og nye verktøy som kan bidra til en effektiv og hensiktsmessig grensekontroll. For at politiet skal kunne benytte seg av disse mulig-

hetene, må systemer kunne utvikles og testes for å sikre at de fungerer etter intensjonen og ikke får utilsiktede konsekvenser for de reisende.

Det ble foreslått å presisere i lovbestemmelsen at opplysningene ikke skal behandles til testing og utvikling lenger enn nødvendig. Departementet understreket også at forslaget ikke åpnet for at opplysninger kan behandles til testing og utvikling etter at de skulle vært slettet i henhold til reglene som ga grunnlag for registreringen.

Departementet vurderte at konsekvensene for den registrerte av at opplysninger som behandles i forbindelse med grensekontroll også kan brukes til testing og utvikling, ville være forholdsvis begrensede, utover å bidra til å forbedre og effektivisere grensekontrollen og sikre likebehandling av reisende.

I høringsnotatet ble det i tillegg foreslått en hjemmel for å kunne gi nærmere regler i forskrift om behandling av opplysninger i forbindelse med testing og utvikling.

9.3.2 Lagring av ansiktsbilde og fingeravtrykk til bruk for testing og utvikling

Departementet foreslo å innta den tidligere slette-regelen i passloven § 6 a annet ledd i grenseloven § 22, slik at det vil fremgå at biometriske opplysninger innhentet i grensekontrollen skal slettes når identiteten er fastslått, med unntak av der opplysningene lagres til testing og utvikling.

Det ble samtidig foreslått en hjemmel for lagring av ansiktsbilde og fingeravtrykk innhentet i grensekontrollen for en viss periode utelukkende til bruk for testing og utvikling av informasjonssystemer. Forslaget var begrunnet i behovet 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 la departementet vekt på behovet for å teste fysisk utstyr for opptak av biometriske opplysninger, noe som ikke er gjennomførbart uten bruk av reelle biometriske opplysninger.

I høringsnotatet ble det vist til at lagring av ansiktsbilde og fingeravtrykk og bruk av opplysningene til testing og utvikling innebærer behandling av særlige kategorier av personopplysninger. Det aktuelle grunnlaget for behandlingen ble uttalt å være GDPR artikkel 9 nr. 2 bokstav g om at behandlingen er nødvendig av hensyn til viktige allmenne interesser. Det ble vist til at det å utvikle og teste systemer som skal sikre en forsvarlig og effektiv grensekontroll, og kontroll med at per-

sonene som passerer grensen faktisk er den de utgir seg for å være, anses som viktige allmenne interesser som kan begrunne behandling av biometriske opplysninger.

Departementet foreslo i høringsnotatet nærmere rammer for å sikre at behandlingen står i et rimelig forhold til det mål som søkes oppnådd, er forenlig med det grunnleggende innholdet i retten til vern av personopplysninger og sikrer egnede og særlige tiltak for å verne den registrertes grunnleggende rettigheter og interesser, slik GDPR artikkel 9 nr. 2 bokstav g krever.

Lagringen av de biometriske opplysningene måtte etter forslaget være nødvendig for å teste og utvikle systemer til bruk for grensekontroll. Det ble dermed ikke foreslått en generell hjemmel for lagring av ansiktsbilde eller fingeravtrykk av alle som passerer grensekontrollen.

Også bruk av reelle personopplysninger i form av ansiktsbilde og fingeravtrykk innhentet i grensekontrollen for testing og utvikling ble foreslått gjort betinget av at det måtte være umulig eller uforholdsmessig vanskelig å oppnå formålet uten slike opplysninger. Det ble videre foreslått en særskilt formålsbegrensning i form av en bestemmelse om at biometriske opplysninger utelukkende kan benyttes til testing og utvikling av systemer for grensekontrollformål. I tillegg ble det foreslått innført et krav om at ansiktsbilder og fingeravtrykk skal holdes atskilt fra andre opplysninger som behandles for grensekontrollformål, og at tilgang bare gis til personer som er særskilt bemyndiget. Kravet om særskilt bemyndigelse skulle 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. Etter forslaget skulle ansiktsbilder og fingeravtrykk kunne lagres i inntil seks måneder, og deretter slettes i form av tilintetgjøring.

Departementet vurderte at de foreslåtte rammene for behandlingen ville bidra til å redusere de personvernmessige ulempene av forslaget. Departementet la 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.

9.4 Høringsinstansenes syn

De høringsinstansene som har uttalt seg om forslagene til endringer i grenseloven, støtter at det

gis en hjemmel for bruk av opplysninger til testing og utvikling og for lagring av ansiktsbilde og fingeravtrykk for slike formål. Disse er *Politidirektoratet*, *Politiets utlendingsenhet* og *Øst politidistrikt*. Ingen høringsinstanser har hatt innvendinger mot forslagene.

Politidirektoratet viser til at bruk av reelle opplysninger til testing og utvikling vil bidra til å sikre tilstrekkelig kvalitet og sikkerhet i informasjonssystemer som er av stor betydning for politiets oppgaver knyttet til grensekontroll. For å sikre samsvar med fagterminologien på feltet foreslås «fiktive» opplysninger i forslaget til grenseloven ny § 22 a første ledd erstattet med «syntetiske» opplysninger.

Direktoratet mener det bør fremkomme eksplisitt dersom den foreslåtte ordlyden skal dekke situasjonen der man har behov for å kontrollere og teste at utstyret som benyttes i grensekontrollen fungerer korrekt før det benyttes i ordinær drift. Det kan for eksempel være nødvendig å avgi fingeravtrykk på opptaksplaten og oppta ansiktsbilde for å kontrollere at det fungerer optimalt. Formålet, som vil være å teste kontrollutstyr, dekkes ikke nødvendigvis av ordlyden i forslaget. *Politidirektoratet* foreslår at det eventuelt tas inn en ny setning i § 22 tredje ledd om at biometriske opplysninger også kan innhentes for å teste utstyr som er nødvendig for å gjennomføre grensekontroll.

Direktoratet påpeker at forslaget ikke oppstiller klare kriterier for hvordan utvalget av ansiktsbilder og fingeravtrykk skal skje, og tar til orde for at det i forarbeidene bør fremkomme at den behandlingsansvarlige har et ansvar for at utvalget av personopplysninger til testing og utvikling skal bidra til å forhindre bias og diskriminering.

Politidirektoratet mener at § 22 tredje ledd om innhenting av biometrisk informasjon ved grensekontroll bør endres, slik at bestemmelsens ordlyd ikke avgrenses til spesifikke typer biometriske opplysninger. Med teknologisk utvikling kan det bli nødvendig å inkludere også andre biometriske opplysninger ved gjennomføring av inn- og utreisekontroll, som irisskanning eller stemmegjenkjenning. Slik bruk vil også kreve testing og utvikling.

Øst politidistrikt påpeker at dersom opplysningene lagres i avidentifisert form, bør det sikres tekniske løsninger for å kunne gjenopprette koblingen mellom foto eller fingeravtrykk og navn i tilfeller der innsynsbegjæring mottas, slik at de registrertes rett til innsyn mv. kan etterleves på en praktisk og effektiv måte.

9.5 Departementets vurderinger

9.5.1 Hjemmel for bruk av opplysninger til testing og utvikling

Ingen høringsinstanser har hatt innvendinger mot forslaget om å gi en hjemmel i grenseloven for bruk av reelle opplysninger til testing og utvikling av informasjonssystemer. Departementet opprettholder forslaget. En slik hjemmel vil legge til rette for at politiet kan ta i bruk nye teknologiske muligheter og verktøy for en effektiv og hensiktsmessig grensekontroll. Testing og utvikling ved bruk av reelle opplysninger vil bidra til å sikre at systemene som benyttes i grensekontrollen fungerer etter intensjonen og ikke får utilsiktede konsekvenser for de reisende. Behandlingen vil ikke ha betydning for de reisendes mulighet til å passere grensen, og det vil ikke foretas andre undersøkelser opp mot politiets registre. Konsekvensene for de registrerte vurderes derfor å være forholdsvis begrensede.

Som vilkår for bruk av reelle opplysninger foreslås det at det må være umulig eller uforholdsmessig vanskelig å oppnå formålet ved bruk av anonyme eller fiktive opplysninger. Begrepene skal forstås på samme måte som i tilsvarende bestemmelser i annet regelverk. Departementet følger ikke opp Politidirektoratets forslag om å erstatte begrepet «fiktive» med «syntetiske» opplysninger. Det er lagt vekt på at hjemler for bruk av opplysninger til testing og utvikling i annen lovgivning bruker begrepet «fiktive» personopplysninger. For å unngå tolkningstvil er det ønskelig at hjemler for testing og utvikling benytter like lydende begreper om det som er ment å ha samme meningsinnhold.

Ingen høringsinstanser har kommentert forslaget til forskriftshjemmel, som opprettholdes.

9.5.2 Lagring av ansiktsbilde og fingeravtrykk

Det er ingen instanser som har hatt innvendinger mot at det åpnes for at ansiktsbilder og fingeravtrykk som innhentes ved grensepassering skal kunne lagres utelukkende til bruk for testing og utvikling av informasjonssystemer til bruk for grensekontrollformål. Det er heller ingen høringsinstanser som har hatt særskilte kommentarer til de foreslåtte rammene for behandlingen. Departementet opprettholder forslaget.

Selv om det kan tenkes at andre former for biometriske opplysninger vil benyttes i fremtiden for å verifisere identiteten til personer som passe-

rer grensekontrollen, følger departementet ikke opp Politidirektoratets forslag å åpne for å innhente flere typer biometriske opplysninger av de reisende. En slik utvidelse må vurderes og utredes nærmere hvis, og i tilfelle når, det oppstår behov for å innhente andre biometriske opplysninger av alle reisende for å verifisere identitet.

Politidirektoratet mener det bør inntas en hjemmel i grenseloven § 22 tredje ledd for å innhente ansiktsbilde og fingeravtrykk som ledd i testing av fysisk utstyr. Bestemmelsen regulerer behandling av opplysninger til gjennomføring av grensekontroll. I høringsnotatet ble det understreket at forslaget ikke ga hjemmel til å innhente nye opplysninger til bruk for testing og utvikling, men bare åpnet for at biometriske opplysninger som allerede innhentes fra de reisende vil kunne lagres til bruk for testing og utvikling. Departementet følger derfor ikke opp innspillet.

Etter forslaget kan ansiktsbilde og fingeravtrykk lagres dersom det er nødvendig for å teste og utvikle informasjonssystemer til bruk for grensekontrollformål. Det gis dermed ikke en generell hjemmel for lagring av ansiktsbilder og fingeravtrykk av alle som passerer grensekontrollen. Dette ivaretar etter departementets syn behovet for fleksibilitet i vurderingen av hvilke ansiktsbilder og fingeravtrykk, og i hvilket omfang, som det er behov for å lagre for dette formålet.

Personer som er omfattet av artikkel VII nr. 3 i tilleggssavtale 10. juni 2022 mellom Norge og USA om forsvarssamarbeid (SDCA) og artikkel III nr. 1 siste punktum i avtale 19. juni 1951 mellom partene i Traktat for det nordatlantiske område om status for deres styrker (NATO SOFA), er unntatt fra bestemmelser og lovgivning om registrering og kontroll av utlendinger. Departementet legger til grunn at forslagene i denne proposisjonen ikke kommer i konflikt med disse bestemmelsene.

Departementet er enig med Politidirektoratet i at det er viktig at utvelgelsen av ansiktsbilder og fingeravtrykk skjer på en måte som sikrer et representativt datagrunnlag. Formålet med å lagre de biometriske opplysningene til bruk for testing og utvikling er nettopp å sikre at informasjonssystemet gjør korrekte vurderinger, herunder at ikke enkelte grupper plukkes ut til kontroll oftere enn andre, eksempelvis basert på hudfarge, alder eller kjønn. For å kunne avdekke og korrigere slike mulige skjevheter og diskriminering, må den behandlingsansvarlige påse at de biometriske opplysningene som benyttes til testing er representative.

Som nevnt i høringsnotatet, legger departementet til grunn at de reisende opplyses på egnet måte om at ansiktsbilde og fingeravtrykk kan eller vil bli lagret til bruk for testing og utvikling. Det må også sikres at opplysningene behandles på en måte som gjør at de registrertes rettigheter etter GDPR, som retten til innsyn, retting og sletting, kan oppfylles.

Lov 20. juni 2025 nr. 96 om dokumentasjon og arkiv (arkivlova) erstatter den tidligere arkivlova og trådte i kraft 1. januar 2026. Det følger av ny arkivlov § 13 annet ledd at bestemmelser om plikt til å slette opplysninger, bare gir grunnlag for kassasjon når det er klart fastsatt eller forutsatt at opplysningene ikke skal finnes i arkivene for ettertiden. Etter forslaget til grenseloven § 22 a fjerde

ledd skal ansiktsbilde og fingeravtrykk slettes i form av tilintetgjøring. En slik regel gjør det etter departementets syn tilstrekkelig klart at opplysningene ikke skal finnes i arkivene for ettertiden. Som omtalt i høringsnotatet, anser departementet at forslaget ikke innebærer noe unntak fra den tidligere arkivlovas kassasjonsforbud, og at arkivfaglige hensyn ikke tilsier at opplysningene skal lagres for ettertiden. For å unngå tvil om forholdet til arkivlova foreslår departementet likevel av pedagogiske hensyn å innta en henvisning til arkivlova § 13 annet ledd i bestemmelsen.

I tillegg er det presisert i lovforslaget at særskilt bemyndigelse gis av den behandlingsansvarlige.

10 Databehandlers taushetsplikt

10.1 Gjeldende rett

Etter politiregisterloven § 18 tredje ledd første punktum skal den som er ansatt hos eller utfører tjeneste eller arbeid for databehandler, og som får tilgang til opplysninger som er underlagt taushetsplikt i henhold til politiregisterloven, pålegges taushetsplikt etter politiregisterloven § 35. Bestemmelsen hjemler pålegg om taushetsplikt når mottaker får opplysninger undergitt taushetsplikt i forbindelse med at de uttaler seg til, eller på annen måte bistår, politiet eller påtalemyndigheten. Av særmerknaden til § 18 tredje ledd i Ot.prp. nr. 108 (2008–2009), punkt 21.4, fremgår at databehandlerne «skal pålegges taushetsplikt, og at dette spørsmål alltid skal fremgå eller være regulert i avtalen eller instruksen mellom den behandlingsansvarlige og databehandleren».

Videre følger det av § 18 tredje ledd at taushetsplikt for den som er ansatt hos eller utfører tjeneste eller arbeid for databehandler skal fremgå av avtalen med den behandlingsansvarlige. Bestemmelsen angir også at databehandler plikter å oppgi hvem som får tilgang til de taushetsbelagte opplysningene.

Verken § 18 eller § 35 sier noe om omfanget av taushetsplikten som skal pålegges. Det fremstår derfor som noe uklart om taushetsplikten som pålegges må være identisk med taushetsplikten etter politiregisterloven § 23, eller om det er rom for tilpasninger. Uttalelser i forarbeidene kan tyde på at taushetsplikten skal være sammenfallende med den som følger av § 23 om omfanget av taushetsplikten. I Ot.prp. nr. 108 (2008–2009) punkt 10.4.4 er det uttalt at det er «viktig at det for databehandlerne gjelder de samme taushetspliktsreglene som for politiet når de behandler opplysninger på vegne av politiet».

Av LED artikkel 22 nr. 3 bokstav b følger det at databehandler, i avtalen med den behandlingsansvarlige, skal være forpliktet til å påse at de som behandler data enten er underlagt lovfestet eller avtalefestet taushetsplikt. Direktivet legger ellers ikke føringer for omfanget av taushetsplikten.

10.2 Forslaget i høringsnotatet

I høringsnotatet anførte departementet at det burde være rom for at omfanget av den taushetsplikten som databehandler skal påse, og som er regulert i databehandleravtalen, ikke fullt ut sammenfaller med politiregisterlovens taushetsplikt. Det sentrale er at opplysningenes konfidensialitet vernes. Departementet foreslo derfor endringer i politiregisterloven § 18 slik at omfanget av taushetsplikten skal fremgå av databehandleravtalen. En slik formulering ville gi større fleksibilitet, samtidig som kravet i LED artikkel 22 om at det må foreligge en avtalefestet taushetsplikt ligger fast.

Departementet viste videre til at dagens ordlyd i politiregisterloven § 18 tredje ledd første punktum kan misforstås, ettersom den gir inntrykk av at den behandlingsansvarlige skal pålegge den enkelte ansatte hos databehandleren taushetsplikt. Departementet foreslo derfor å omformulere bestemmelsen noe for å gjøre det klart at det av databehandleravtalen skal fremgå at de ansatte mv. hos databehandleren skal være underlagt taushetsplikt. I høringsnotatet ble det presisert at endringen ikke innebærer noen realitetsendring.

Departementet foreslo også en endring i § 18 tredje ledd fjerde punktum, slik at plikten til å opplyse om hvem som får tilgang til opplysningene, kun gjelder ved forespørsel.

10.3 Høringsinstansenes syn

Datatilsynet stiller seg positivt til den foreslåtte endringen, og har ikke innvendinger mot at det åpnes for at taushetsplikten som reguleres i databehandleravtalen ikke fullt ut må sammenfalle med taushetsplikten som følger av politiregisterloven. Datatilsynet deler departementets vurdering av at det sentrale må være at opplysningenes konfidensialitet vernes.

Advokatforeningen er prinsipielt enig i at det er uheldig at dagens ordlyd i § 18 er uklar med hensyn til omfanget av taushetsplikten databehandler

skal påse. Foreningen har ingen innvendinger mot at fastsettelsen av taushetsplikten vurderes konkret i det enkelte tilfellet og at den kan avvike fra taushetsplikten i politiregisterloven. Advokatforeningen påpeker likevel at det fremstår som uklart hvordan forslaget til ny ordlyd skal løse utfordringen knyttet til standardiserte vilkår som benyttes av store og internasjonale selskaper i rollen som databehandler. Foreningen ber departementet vurdere om det er behov for å justere den foreslåtte ordlyden for å sikre at taushetsplikten i alle tilfeller må fastsettes slik at den i tilstrekkelig grad hensyntar mengden og arten av opplysningene som skal behandles.

Politidirektoratet støtter en endring i politiregisterloven § 18 tredje ledd hvor plikten til å pålegge databehandler taushetsplikt etter politiregisterloven § 35 bortfaller, men med noen presiseringer. Direktoratet forstår forslaget slik at det gir rom for at deler av taushetsplikten som følger av § 23 ikke nødvendigvis skal gjelde for databehandler, og uttaler i denne sammenheng at det bør fremgå tydelig av bestemmelsens ordlyd og lovens forarbeider at det ikke er adgang til å fravike omfanget av taushetsplikten som er fastsatt i politiregisterloven § 23 i en databehandleravtale.

Direktoratet støtter at plikten til å opplyse om hvem som får tilgang til opplysningene hos databehandler kun skal gjelde ved forespørsel.

Kripos støtter de foreslåtte endringene, og anser at de vil gi større fleksibilitet til å tilpasse databehandlers taushetsplikt til de opplysninger som behandles. Kripos har selv fremmet behovet for lovendringene, og viser til at bakgrunnen for det er todelt. For det første vil det i noen tilfeller der det benyttes utenlandske databehandlere gi bedre sikkerhetsmessig utbytte å forhandle om andre økte sikkerhetstiltak enn å fastholde en lovbestemt taushetsplikt i databehandleravtalevilkårene som eneste alternativ. For det andre kan det overfor databehandlere som opererer med standardavtaler, typisk større selskaper med et stort antall ansatte som opererer fra forskjellige land, være vanskelig å gjennomføre pålegg om krav til lovbestemt taushetsplikt.

Kripos påpeker at det nærmere innholdet i og omfanget av taushetsplikten vil måtte inngå i en overordnet vurdering av om valget av databehandler vil gi tilfredsstillende informasjonssikkerhet, jf.

politiregisterloven § 15. Pålegg om lovbestemt taushetsplikt er, slik Kripos ser det, et viktig tiltak for å sikre dette i en del tilfeller. Det er imidlertid andre tiltak som i vel så stor grad kan sikre tilfredsstillende informasjonssikkerhet, særlig når opplysningene behandles i utlandet. Det er viktig at politiet gis adgang til å differensiere kravene ut fra avtalen som skal inngås.

10.4 Departementets vurderinger

Departementet merker seg at ingen av høringsinstansene har hatt vesentlige innvendinger mot endringsforslaget, som opprettholdes. Som det fremgår av høringsnotatet innebærer forslaget at det åpnes for større fleksibilitet i måten opplysningenes konfidensialitet sikres i ulike databehandleravtaler. Departementet er enig med Kripos i at også andre sikkerhetstiltak vil kunne være viktig for å sikre tilfredsstillende informasjonssikkerhet, og at taushetspliktens innhold og omfang må inngå i en helhetlig vurdering. Der vil også mengden og arten av opplysningene som skal behandles være et moment, slik Advokatforeningen påpeker. Departementet mener imidlertid at det ikke er behov for endringer i lovbestemmelsen for å ivareta dette.

Dersom omfanget av taushetsplikten fremgår av databehandleravtalen fremfor å pålegges etter politiregisterloven § 35, vil brudd på taushetsplikten ikke kunne straffes etter straffeloven § 209 om brudd på taushetsplikt. Straffeloven § 209 rammer brudd på taushetsplikt i henhold til lov eller forskrift, men ikke krenkelser av avtalebasert taushetsplikt. Overfor ansatte i større utenlandske IT-selskaper vil strafforfølging for brudd på taushetsplikten uansett være lite praktisk. Politiet vil etter endringen fortsatt kunne pålegge databehandlere taushetsplikt med hjemmel direkte i politiloven § 35 første ledd om mottakere som får opplysninger undergitt taushetsplikt i forbindelse med at de uttaler seg til eller på annen måte bistår politiet eller påtalemyndigheten. Departementet mener derfor at det vil ha begrensede negative konsekvenser at taushetsplikten for databehandler fremover kan være avtalefestet fremfor lovbestemt.

11 Registrering og anmerkning på politiattest av overføring til barnevernet

11.1 Gjeldende rett

Det følger av politiregisterloven § 40 nr. 3 bokstav f at overføring til barneverntjenesten som hovedregel ikke anmerkes på ordinær politiattest. Etter politiregisterforskriften § 44-4 første ledd nr. 12 skal imidlertid slik overføring registreres i reaksjonsregisteret. Dette innebærer at en overføring til barneverntjenesten i utgangspunktet anmerkes på en uttømmende politiattest, jf. politiregisterloven § 41, med mindre unntakene for unge lov- brytere etter politiregisterforskriften § 30-3 og overgangsregelen i § 86-4, som gir § 30-3 tilbakevirkende kraft, kommer til anvendelse.

Etter den tidligere barnevernloven (lov 17. juli 1953 nr. 14) § 57 kunne påtalemyndigheten avslutte en sak mot en person mellom 15 og 18 år ved å overføre den til helse- og sosialstyret istedenfor å reise tiltale eller gi påtaleunntatelse. Denne bestemmelsen ble ikke videreført da loven ble erstattet av lov 17. juni 1992 nr. 100 om barneverntjenester. Heller ikke den gjeldende barnevernsloven (lov 18. juni 2021 nr. 97), som trådte i kraft 1. januar 2023, har slike regler. Overføring til barneverntjenesten er dermed ikke lenger en mulighet for personer over den kriminelle lavalder.

Når noen som ikke har fylt 15 år har begått en ellers straffbar handling, kan påtalemyndigheten i medhold av straffeprosessloven § 71 b beslutte at saken skal overføres til barneverntjenesten. Dette er ikke en strafferettslig reaksjon, og det vurderes ikke som nødvendig eller rimelig at et slikt tiltak mot en mindreårig under kriminell lavalder skal registreres i reaksjonsregisteret eller fremgå på en uttømmende politiattest. Det antas heller ikke å ha vært tilsiktet da politiregisterloven ble innført. Slik politiregisterforskriften § 44-4 er formulert, fremstår det imidlertid som at en slik overføring skal registreres i reaksjonsregisteret.

11.2 Forslaget i høringsnotatet

Departementet foreslo å presisere i politiregisterloven § 40 at kravet om registrering og anmerkning

om overføring til barneverntjenesten, kun gjelder overføring besluttet med hjemmel i lov 17. juli 1953 nr. 14 om barnevern § 57. På denne måten blir det klart at overføring til barneverntjenesten etter straffeprosessloven § 71 b verken skal registreres i reaksjonsregisteret eller fremkomme på en uttømmende politiattest.

11.3 Høringsinstansenes syn

Datatilsynet, Advokatforeningen, Politidirektoratet, Finnmark politidistrikt og Kripas støtter forslaget. *Finnmark politidistrikt* påpeker at endringsforslaget kun innebærer en kodifisering av gjeldende praksis.

Advokatforeningen bemerker likevel at det er et spørsmål om den foreslåtte ordlyden er hensiktsmessig, da barnevernloven av 1953 er opphevet. Advokatforeningen mener det er vanskelig å se for seg at slik overføring som den foreslåtte ordlyden skisserer i praksis vil finne sted, og foreslår i stedet at det vurderes om politiregisterforskriften § 44-4 nr. 12 bør utgå i sin helhet.

Kripas støtter de foreslåtte endringene i politiregisterloven § 40 og politiregisterforskriften § 44-4 om at overføring til barneverntjenesten etter straffeprosessloven § 71 b, for fremtiden ikke skal registreres i reaksjonsregisteret, og at historiske opplysninger om dette ikke skal fremkomme på en uttømmende politiattest. *Kripas* legger til grunn at eksisterende registreringer etter straffeprosessloven § 71 b kan sperres i registrene, jf. politiregisterloven § 50 første ledd, etter at de foreslåtte forskriftsendringene er trådt i kraft.

11.4 Departementets vurderinger

Departementet har etter en nærmere vurdering kommet til at politiregisterloven § 40 nr. 3 bokstav f bør oppheves. Som Advokatforeningen påpeker vil slike overføringer til barneverntjenesten ikke lenger finne sted, som følge av at barnevernloven

av 1953 er opphevet. Eventuelle overføringer vil dermed være svært gamle, og vil med all sannsynlighet være sperret etter reglene i politiregisterforskriften §§ 30-3 eller 44-12, slik at de uansett ikke lenger vil vises på attesten.

Departementet tar sikte på å gjøre tilsvarende endring i politiregisterforskriften § 44-4, slik at reaksjonene heller ikke skal registreres i reaksjonsregisteret.

12 Tilsynsrådet for tvangsreturer og utlendingsinternatets taushetsplikt

12.1 Forslaget i høringsnotatet

Tilsynsrådet for tvangsreturer og utlendingsinternatets taushetsplikt følger i dag bare av forskrift, uten at det fremgår direkte av utlendingsloven § 107 a at det kan gis forskriftsbestemmelser om taushetsplikt. Departementet mente i høringsnotatet at tilsynsrådets taushetsplikt burde fremgå direkte av bestemmelsen. Det ble vist til at tilsynsrådets taushetsplikt går lenger enn den alminnelige taushetsplikten etter forvaltningsloven § 13, ettersom også sikkerhetsmessige forhold er taushetsbelagt.

I tillegg foreslo departementet at taushetsplikten også skulle omfatte opplysninger knyttet til forestående tvangsreturer og opplysninger som det av hensyn til politiets operative virksomhet er nødvendig å holde hemmelig. Sistnevnte er for politiets del taushetsbelagt etter politiregisterloven § 23 annet ledd. Det ble vist til at tilsynsrådet vil få denne typen opplysninger som ledd i tilsynsoppgaven, og at det vil kunne vanskeliggjøre retur av utlendinger uten lovlig opphold dersom slike opplysninger blir gjort kjent for utenforstående.

12.2 Høringsinstansenes syn

Alle høringsinstansene som har uttalt seg om spørsmålet, støtter at tilsynsrådets taushetsplikt lovfestes og utvides. Dette gjelder *Datatilsynet*, *Politidirektoratet*, *Oslo politidistrikt*, *Kripos* og *Politiets utlendingsenhet*.

Politiets utlendingsenhet uttaler at det er helt nødvendig at taushetsplikten utvides til også å gjelde for opplysninger om tvangsreturer og politiets operative virksomhet, siden det ikke er gitt at dette er opplysningskategorier som vil være taushetsbelagt etter bestemmelsene i forvaltningsloven. Til taushetsplikten om tvangsreturer foreslår *Politiets utlendingsenhet* at «forestående» sløyfes. Selv om en tvangsretur er gjennomført, kan det fortsatt være nødvendig å bevare hemmelighold om en del opplysninger knyttet til returarbeidet. Mye av dette vil være omfattet av «poli-

tiets operative virksomhet», men det kan også fremkomme opplysninger av ikke-operativ art, for eksempel knyttet til dialogen og samhandlingen med hjemlandets myndigheter, flyselskaper eller andre som det er nødvendig å bevare hemmelighold om selv om tvangsreturen er gjennomført.

Politiets utlendingsenhet mener at taushetsplikten også bør omfatte forhold av betydning for sikkerheten ved særskilt tilrettelagte innkvarteringssteder, ettersom tilsynsrådet også skal føre tilsyn med slike steder.

Oslo politidistrikt fremhever at taushetsplikt om opplysninger knyttet til gjennomføringen av uttransport har et viktig sikkerhetsaspekt, og at en tydelig lovhjemlet taushetsplikt vil kunne bidra til å forhindre utilsiktede informasjonslekkasjer. Dersom en utlending selv eller gjennom andre får kjennskap til når en retur skal foregå, kan det innebære en alvorlig sikkerhetsrisiko for utlendingen og andre i forbindelse med gjennomføringen av uttransporten. Videre vil en retur som må avlyses eller som blir avbrutt medføre ekstra bruk av ressurser. Distriktet legger til grunn at tilsynsrådets medlemmer får tilstrekkelig opplæring, herunder om straffbarheten ved brudd på taushetsplikten.

Politidirektoratet støtter innspillene fra *Politiets utlendingsenhet* og *Oslo politidistrikt*.

12.3 Departementets vurderinger

Departementet opprettholder forslaget om at tilsynsrådets taushetsplikt lovfestes, og at også forhold av betydning for sikkerheten ved utlendingsinternatet, opplysninger knyttet til forestående tvangsreturer og opplysninger som det av hensyn til politiets operative virksomhet er behov for å holde hemmelig skal være omfattet av tilsynsrådets taushetsplikt.

Departementet er enig med *Politiets utlendingsenhet* i at også forhold av betydning for sikkerheten ved særskilt tilrettelagte innkvarteringssteder bør være underlagt taushetsplikt, og har endret lovforslaget i tråd med dette.

Til forslaget fra Politiets utlendingsenhet om at ikke bare opplysninger om «forestående» tvangsreturer skal være omfattet av taushetsplikten, viser departementet til at hensikten med bestemmelsen er å unngå at konkrete returer vanskeliggjøres. Etter departementets syn vil forslaget fra Politiets utlendingsenhet være uheldig, ettersom det etter sin ordlyd medfører at alle opplysninger om tvangsreturer vil være taushetsbelagt. Dette vil etter departementets syn gjøre

taushetsplikten mer omfattende enn nødvendig. Samtidig ser departementet at det kan være en risiko for at fremtidige tvangsreturer kan vanskeliggjøres dersom visse opplysninger blir gjort kjent, for eksempel opplysninger om dialog med myndigheter i andre land. Departementet har derfor tilføyd i forslaget til bestemmelse at taushetsplikten også omfatter opplysninger som det av hensyn til politiets arbeid med tvangsreturer er behov for å holde hemmelig.

13 Krav om politiattest og plettfriandel ved opptak til videreutdanning og høyere grads studier ved Politihøgskolen

13.1 Gjeldende rett

Etter politiloven § 24 b første ledd annet punktum er det krav om plettfriandel for opptak til bachelorstudiet ved Politihøgskolen, og søkere må fremlegge utvidet og uttømmende politiattest etter politiregisterloven § 41. Det er ikke tilsvarende krav om plettfriandel og fremleggelse av utvidet og uttømmende politiattest i bestemmelsens annet ledd om opptak til videreutdanning og høyere grads studier ved Politihøgskolen.

13.2 Forslaget i høringsnotatet

Departementet mente i høringsnotatet at det må være samme strenge krav til andel for opptak til det nye etterforskningsstudiet som for opptak til bachelorstudiet, for å sikre at det ikke opptas studenter som ikke får jobb i etaten.

I høringsnotatet ble det derfor foreslått en hjemmel for å kunne kreve fremlagt uttømmende og utvidet politiattest etter politiregisterloven § 41 også for søkere til videreutdanning eller høyere grads studier, i tillegg til at det ble foreslått inntatt et krav om plettfriandel for søkere til slike studier. Det ble påpekt at det ikke alltid vil være nødvendig å kreve fremlagt slik attest, for eksempel i tilfeller hvor søkeren har grunnutdanning fra Politihøgskolen og allerede er ansatt i politiet.

13.3 Høringsinstansenes syn

Politidirektoratet, Politihøgskolen, Politiets Fellesforbund, Norges Politilederlag, Parat Politiet og Tekna har uttalt seg om forslaget. Alle instansene støtter at det innføres en hjemmel for å kreve uttømmende og utvidet politiattest. De fleste instansene støtter også at det innføres et lovfestet krav om plettfriandel.

Politidirektoratet uttaler at de har vurdert om det også bør inntas et krav om skikkethet, men har kommet til at det ikke foreslås nå.

Politidirektoratet mener at det fremstår som noe uklart om forslaget er ment å gjelde for alle videreutdanninger ved Politihøgskolen, og at det bør presiseres dersom dette ikke er tilfelle. Politidirektoratet mener at Politihøgskolen bør gis fullmakt til å vurdere for hvilke videreutdannings-tilbud og høyere grads studier det bør stilles krav om plettfriandel.

Politihøgskolen mener at den foreslåtte endringen i stor grad tilfredsstiller behovet for å kunne gjennomføre andelssjekk på etter- og videreutdanninger samt høyere grads utdanninger. Politihøgskolen foreslår at et krav om plettfriandel skal kunne fastsettes for nærmere bestemte studier etter en konkret vurdering av om det er nødvendig ut fra det enkelte studiets innhold og karakter. Høgskolen mener kravet om politiattest bør gjelde for alle søkere, også de som allerede er ansatt i politiet.

Politihøgskolen foreslår følgende alternative formuleringer til § 24 b nytt annet ledd, annet og tredje punktum:

Det kan fastsettes krav om plettfriandel til videreutdanninger og høyere grads studier ved Politihøgskolen. Søkere til studier med krav om plettfriandel, må fremlegge utvidet og uttømmende politiattest, jf. politiregisterloven § 41.

Politihøgskolen mener at det synes lite tjenlig å innføre en opptaksprosess der man også skal vurdere studentenes skikkethet for tjeneste i politiet. Det vises til at en slik ordning vil medføre omfattende praktiske konsekvenser og merarbeid, også underveis i utdanningen dersom det oppstår nye forhold.

Etter Politihøgskolens skjønn vil kravet om plettfriandel ved opptak og det at utdannede studenter vil bli skikkethetsvurdert før ansettelse i politiet, være tilstrekkelig.

Politiets Fellesforbund uttaler at det må stilles strenge krav om plettfriandel og skikkethet ved opptak til årsstudiet, på linje med det som gjelder ved opptak til bachelor i politiutdanning. Dette må reguleres tydelig og praktiseres for alle søkere.

Tekna uttaler at kravet om plettfriandel må konkretiseres i forskrift, slik at det ikke oppstår tvil om hvilke kriterier som gjelder. Dette vil etter Teknas vurdering skape trygghet for etaten og for studentene.

13.4 Departementets vurderinger

Departementet registrerer at høringsinstansene som har uttalt seg gir bred støtte til forslaget om en hjemmel for å kunne kreve fremlagt utvidet og uttømmende politiattest fra søkere til etterutdanning og høyere grads studier ved Politihøgskolen og innføring av krav om plettfriandel.

Departementet foreslår ikke å innføre et skikethetskrav for opptak til etterutdanninger og høyere grads studier ved Politihøgskolen. Spørsmålet har ikke vært på høring og er ikke utredet nærmere. En hjemmel til å kunne kreve fremlagt uttømmende og utvidet politiattest ved opptak vil etter departementets oppfatning være tilstrekkelig for å sile ut de som åpenbart ikke vil kvalifisere for tilsetning i politiet.

Politihøgskolen foreslår, med støtte fra Politidirektoratet, å åpne for at skolen selv skal kunne avgjøre om det skal stilles krav om plettfriandel for opptak til bestemte videreutdanninger og høyere grads studier. I dag er det 137 ulike studietilbud knyttet til etterutdanning eller videreutdanning ved Politihøgskolen av kortere og lengre varighet. Hovedtyngden av studietilbudene retter seg mot ansatte i politiet og påtalemyndigheten, men det er også flere studier som retter seg mot andre målgrupper, både i privat og offentlig sektor. Eksempler på dette er kurs og etterutdanning om økonomisk kriminalitet, som retter seg mot

bankansatte og tilsatte i andre kontrolltater. Departementet er enig i at Politihøgskolen selv bør vurdere behovet for et krav om plettfriandel, på bakgrunn av innholdet i og målgruppen for de konkrete studietilbudene. Forslaget til endringer i politiloven § 24 b annet ledd er justert i tråd med dette.

Politihøgskolen har også foreslått at det for søkere til studier hvor det vurderes at et krav om plettfriandel er nødvendig, skal være obligatorisk å fremlegge uttømmende og utvidet politiattest. Departementets hensikt med forslaget om å lovfeste at det «kan» kreves fremlagt uttømmende og utvidet politiattest, var å synliggjøre at det bør foretas en konkret vurdering av når krav om fremleggelse av politiattest for opptak er nødvendig. Dette kan i stor grad ivaretas ved at Politihøgskolen gis myndighet til å vurdere for hvilke studietilbud et krav om plettfriandel er nødvendig. Departementet har derfor kommet til at det bør være et obligatorisk krav om fremleggelse av politiattest dersom Politihøgskolen har besluttet å stille krav om plettfriandel. En slik regel vil være enkel å praktisere, og vil i tillegg sikre at alle søkere likebehandles.

Til Teknas innspill om at det er behov for å konkretisere kravet til plettfriandel, bemerker departementet at kravet vil tilsvare det som gjelder for opptak til bachelorstudiet ved Politihøgskolen. Innholdet i begrepet er nærmere redegjort for i Ot.prp. nr. 22 (1994–95) *Om lov om politiet (politiloven)* punkt V, merknaden til § 18. Plettfriandel er et strengt vandelskrav, som innebærer at også forseelser som i andre sammenhenger regnes som mindre alvorlige, kan være tilstrekkelig til å avslå søknaden om opptak.

14 Økonomiske og administrative konsekvenser

Forslagene vil ikke i seg selv medføre økonomiske eller administrative konsekvenser av betydning. Forslagene pålegger ingen testing eller utvikling. Eventuell bruk av hjemmelen vil imidlertid innebære at regelverkets krav må følges, herunder må det sikres tilstrekkelig sporbarhet av opplysningene. Departementet legger til grunn at slike konsekvenser må håndteres innenfor de til enhver tid gjeldende budsjettammer.

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. Omfanget vil avhenge av i hvilket omfang adgangen til å benytte opplysningene til testing og utvikling tas i bruk. Statens sivilrettsforvaltning fikk i 2024 bevilget midler til å ansette en teknolog i utvalgets sekretariat, noe som ventes å bidra til å lette utvalgets kontroll på dette området.

Departementet har løpende dialog med KK-utvalget om den til enhver tid gjeldende ressurs-situasjonen. Gjennomføringen av de nye oppgavene vil inngå i dialogen og departementets kontinuerlige vurderinger av det eventuelle behovet for økte bevilgninger.

Økt bruk av opplysninger til testing og utvikling vil også kunne medføre behov for forhåndsdrøftinger med Datatilsynet i noen flere tilfeller enn i dag. Omfanget er usikkert, men antas å være begrenset i lys av at politiregisterforskriften § 41-2 allerede stiller krav om forhåndsdrøftelser i flere tilfeller.

Endringsforslagene om databehandlere, politiattest og taushetsplikten til Tilsynsrådet for tvangsreturer og utlendingsinternatet vil ikke ha økonomiske eller administrative konsekvenser av betydning. Eventuelle merkostnader dekkes innenfor de til enhver tid gjeldende budsjettammer.

15 Merknader til bestemmelsene

15.1 Straffeprosessloven

Til § 216 i

Første ledd tredje punktum *ny bokstav l* klargjør at opplysninger innhentet ved kommunikasjonskontroll, romavlytting og dataavlesning kan benyttes til testing og utvikling av informasjonssystemer innenfor politiregisterlovens virkeområde. Bruk til dette formålet må skje internt i politiet og påtalemyndigheten, og opplysningene vil ikke kunne utleveres i forbindelse med testing og utvikling. Begrepene testing, utvikling og informasjonssystemer skal forstås på samme måte som i politiregisterloven § 3. Bestemmelsen er nærmere omtalt i punkt 7.4 i proposisjonen.

15.2 Politiloven

Til § 17 f

Annet ledd *ny bokstav g* åpner for at opplysninger innhentet ved PSTs forebyggende tvangsmiddelbruk kan benyttes til testing og utvikling av informasjonssystemer innenfor politiregisterlovens virkeområde. Begrepene testing, utvikling og informasjonssystemer skal forstås på samme måte som i politiregisterloven § 3. Se nærmere omtale i punkt 7.4 i proposisjonen.

Til § 24 b

Endringen i *annet ledd nytt annet punktum* innebærer at Politihøgskolen kan fastsette krav om plettfriandel for opptak til videreutdanninger og høyere grads studier. Om et slikt krav skal stilles vil særlig bero på studiets innhold og karakter, formålet med studiet og hvilken målgruppe det retter seg mot. Etter annet ledd *nytt tredje punktum* skal det kreves fremlagt uttømmende og utvidet politiattest fra søkerne dersom det er fastsatt krav om plettfriandel.

Plettfriandel innebærer et strengt vandelskrav, og skal forstås på samme måte som i politiloven §§ 18 og 24 b første ledd. Se nærmere omtale i punkt 13.4 i proposisjonen.

15.3 Utlendingsloven

Til § 107 a

Nytt *annet ledd* regulerer tilsynsrådets taushetsplikt. Etter *første punktum* gjelder taushetsplikten i forvaltningsloven for enhver som utfører tjeneste eller arbeid for tilsynsrådet. *Annet punktum* utvider taushetsplikten til også å omfatte forhold av betydning for sikkerheten ved utlendingsinternatet og særskilt tilrettelagte innkvarteringssteder, opplysninger knyttet til forestående tvangsreturer og opplysninger som det av hensyn til politiets operative virksomhet eller arbeid med tvangsreturer er behov for å holde hemmelig. Opplysninger om politiets arbeid med tvangsreturer som omfattes av taushetsplikten kan for eksempel være knyttet til dialogen og samhandlingen med myndighetene i land personer blir returnert til. Se nærmere omtale i punkt 12.3 i proposisjonen.

15.4 Politiregisterloven

Til § 3

Fjerde ledd *nytt annet punktum* klargjør at politiregisterlovens virkeområde også omfatter behandling av opplysninger i forbindelse med testing og utvikling av informasjonssystemer som skal brukes innenfor politiregisterlovens virkeområde. Behandling av opplysninger til testing og utvikling vil bli nærmere regulert i forskrift, jf. forslaget til nytt nr. 27 i politiregisterloven § 69 første ledd.

Med informasjonssystemer menes systemer for innsamling, lagring, bearbeiding, overføring og presentasjon av opplysninger, basert på informasjons- og kommunikasjonsteknologi. Eksempler på dette er saksbehandlingssystemer, modeller for beslutningsstøtte og analysesystemer. Det omfatter også systemer som benytter maskinlæring og kunstig intelligens.

Begrepene testing og utvikling dekker hele utviklingsfasen og alle steg i denne, samt ulike former for testing av informasjonssystemer. Utvikling omfatter både videreutvikling av eksisterende systemer og at helt nye systemer lages. Det

omfatter også endring av ferdig utviklede systemer for å tilpasse dem til politiets behov. Testing omfatter blant annet feilretting og analyse av testresultater, for eksempel for å avdekke årsaken til at systemene ikke gir det resultat eller den kvaliteten som er forventet. Det omfatter også testing og kvalitetssikring av verktøy og modeller som er utviklet eller trent av andre, samt trening av modeller politiet selv utvikler.

Endringen er nærmere omtalt i punkt 6.5 i proposisjonen.

Til § 18

Endringene i *tredje ledd* åpner for større fleksibilitet i utformingen av databehandleravtalen, ved at omfanget av taushetsplikten for den som er ansatt hos eller utfører tjeneste eller arbeid for databehandler, og som får tilgang til opplysninger som er underlagt taushetsplikt i henhold til politiregisterloven, skal fremgå av avtalen fremfor å pålegges etter politiregisterloven § 35. Videre skal databehandlers plikt til å opplyse om hvem som får tilgang til de taushetsbelagte opplysningene først inntre på forespørsel. Endringene innebærer ellers kun presiseringer av gjeldende rett. Se nærmere omtale i punkt 10.4 i proposisjonen.

Til § 40

Nr. 3 bokstav f oppheves som følge av at overføringer til barneverntjenesten ikke lenger registreres i reaksjonsregisteret og dermed uansett ikke vil fremkomme på en politiattest. Det vises til nærmere omtale i punkt 11.4 i proposisjonen.

Til § 65 a

Annet ledd *nytt nr. 4* åpner for at åpent tilgjengelig informasjon som antas å være nødvendig for utarbeidelse av analyser og etterretningsvurderinger, også kan brukes til testing og utvikling. Muligheten for slik bruk er begrenset til testing og utvikling av informasjonssystemer som skal brukes til behandling av åpent tilgjengelig informasjon til etterretningsformål, jf. bestemmelsens første ledd. Dette innebærer blant annet at opplysningene kan brukes til å teste og utvikle automatiserte analyseverktøy som bestemmelsen åpner for at kan benyttes til behandlingen. Bestemmelsen åpner ikke for å bruke opplysningene til å teste og utvikle systemer med rene forebyggings- eller etterforskningsformål. Se nærmere omtale i punkt 8.4 i proposisjonen.

Til § 69

Første ledd *nytt nr. 27* gir hjemmel for å gi nærmere regler i forskrift om behandling av opplysninger i forbindelse med testing og utvikling av informasjonssystemer som skal brukes innenfor politiregisterlovens virkeområde. Det tas blant annet sikte på å gi forskriftsbestemmelser om at opplysninger bare kan brukes til testing og utvikling dersom det er umulig eller uforholdsmessig vanskelig å oppnå formålet ved å bruke anonyme eller fiktive opplysninger, krav om den behandlingsansvarliges godkjenning og mulighet til å stille vilkår for behandlingen, samt om forhåndsdrøftelser med Datatilsynet. Se nærmere omtale i punkt 6.5 i proposisjonen.

15.5 Grenseloven

Til § 22

Endringene i *tredje ledd første punktum* er kun en språklig justering som ikke er ment å innebære noen realitetsendring.

Tredje ledd *nytt annet punktum* viderefører annet ledd i den nå opphevede § 6 a i passloven, og lovfester plikten til å tilintetgjøre ansiktsbilder og fingeravtrykk som innhentes ved grensepassering når identiteten er fastslått. Det gjøres unntak fra plikten til tilintetgjøring av de biometriske opplysningene dersom de er nødvendige for testing og utvikling etter § 22 a, jf. denne bestemmelsens annet ledd. Bestemmelsen er nærmere omtalt i punkt 9.5.2 i proposisjonen.

Til § 22 a

Bestemmelsen er ny.

Første ledd gir hjemmel for at personopplysninger kan brukes til testing og utvikling av informasjonssystemer som skal brukes for grensekontrollformål, på nærmere vilkår.

Med anonyme og fiktive opplysninger menes henholdsvis reelle opplysninger som ikke kan knyttes til bestemte personer, og opplysninger som er laget for test- og utviklingsformål. At det er «umulig» å oppnå formålet omfatter både tilfeller der testingen eller utviklingen faktisk ikke lar seg gjennomføre, og der bruk av anonyme eller fiktive 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.

Annet ledd *første punktum* åpner for lagring av ansiktsbilder og fingeravtrykk innhentet ved grensepassering i inntil seks måneder dersom det er nødvendig for å teste og utvikle informasjonssystemer. Vilkåret er også her at det må være umulig eller uforholdsmessig vanskelig å oppnå formålet ved bruk av anonyme eller fiktive opplysninger. Annet ledd *annet punktum* inneholder en formålsbegrensning slik at ansiktsbilder og fingeravtrykk bare kan behandles til testing og utvikling av informasjonssystemer, og ikke til andre formål eller i andre sammenhenger.

Kravet i *tredje ledd første punktum* om at opplysningene skal holdes atskilt, kan ivaretas enten ved at opplysningene lagres i et eget system eller ved at det etableres et logisk skille mellom disse opplysningene og andre opplysninger som behandles.

Kravet i *tredje ledd annet punktum* om særskilt bemyndigelse skal forstås på samme måte som tilsvarende krav etter politiregisterlov-givningen, og innebærer at personene må ha tjenestemessig behov for tilgang, være kvalifisert og ha gjennomgått opplæring. Bemyndigelse gis

av den behandlingsansvarlige, jf. annet ledd *tredje punktum*.

Etter *fjerde ledd* skal ansiktsbilder og fingeravtrykk slettes i form av tilintetgjøring. Henvisningen til arkivlova § 13 annet ledd har først og fremst pedagogisk betydning.

Bestemmelsen er nærmere omtalt i punkt 9.5 i proposisjonen.

Til § 25

Endringen i *nr. 10* tydeliggjør at muligheten til å gi nærmere regler i forskrift om behandling av opplysninger også omfatter behandling i forbindelse med testing og utvikling av informasjonssystemer. Se nærmere omtale i punkt 9.5.1 i proposisjonen.

Justis- og beredskapsdepartementet

t i l r å r :

At Deres Majestet godkjenner og skriver under et framlagt forslag til proposisjon til Stortinget om endringer i politiregisterloven og grenseloven mv. (testing og utvikling av informasjonssystemer).

Vi **HARALD**, Norges Konge,

s t a d f e s t e r :

Stortinget blir bedt om å gjøre vedtak til lov om endringer i politiregisterloven og grenseloven mv. (testing og utvikling av informasjonssystemer) i samsvar med et vedlagt forslag.

Forslag

til lov om endringer i politiregisterloven og grenseloven mv. (testing og utvikling av informasjonssystemer)

I

I lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker skal § 216 i første ledd tredje punktum bokstav k og ny bokstav l lyde:

- 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.*

II

I lov 4. august 1995 nr. 53 om politiet gjøres følgende endringer:

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

- 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.*

§ 24 b annet ledd skal lyde:

Opptak til videreutdanning og høyere grads studier foretas av Politihøgskolen. *Politihøgskolen kan fastsette krav om plettfri vandel for opptak til videreutdanninger og studier som nevnt i første punktum. Dersom det er fastsatt krav om plettfri vandel for opptak, skal det kreves fremlagt uttømmende og utvidet politiattest fra søkeren, jf. politiregisterloven § 41.* Departementet gir nærmere regler om saksbehandling og opptakskrav, herunder dokumentasjon av kompetanse.

III

I lov 15. mai 2008 nr. 35 om utlendingers adgang til riket og deres opphold her gjøres følgende endringer:

§ 107 a annet ledd skal lyde:

Enhver som utfører tjeneste eller arbeid for tilsynsrådet, har taushetsplikt etter forvaltningsloven. Taushetsplikten omfatter også forhold av betydning for sikkerheten ved utlendingsinternatet og ved særskilt tilrettelagte innkvarteringssteder, opplysninger knyttet til forestående tvangsreturer og opplysninger som det av hensyn til politiets operative virksomhet eller arbeid med tvangsreturer er behov for å holde hemmelig.

Nåværende annet ledd blir nytt tredje ledd.

IV

I lov 28. mai 2010 nr. 16 om behandling av opplysninger i politiet og påtalemyndigheten gjøres følgende endringer:

§ 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.

§ 18 tredje ledd skal lyde:

Den som er ansatt hos, eller utfører tjeneste eller arbeid for databehandler, og som får tilgang til opplysninger som er *taushetsbelagt* i henhold til denne loven, skal *være underlagt taushetsplikt. Omfanget av taushetsplikten skal fremgå av den behandlingsansvarliges avtale med databehandler.* Det kan kreves uttømmende og utvidet politiattest av enhver som er ansatt hos eller utfører tjeneste eller arbeid for databehandler. Databehandler plikter *på forespørsel* å oppgi hvem som får tilgang til de taushetsbelagte opplysningene.

§ 40 nr. 3 bokstav f oppheves.

Nåværende bokstav g til i blir bokstav f til h.

§ 65 a annet ledd nr. 3 og nytt nr. 4 skal lyde:

3. etterforskning av lovbrudd som nevnt i politiloven § 17 b, jf. straffeprosessloven § 224
4. *testing og utvikling av informasjonssystemer som skal brukes til behandling av åpent tilgjengelig informasjon til etterretningsformål, jf. denne bestemmelsens første ledd.*

§ 69 første ledd nr. 26 og nytt nr. 27 skal lyde:

26. særregler for militærpolitiets behandling av opplysninger,
27. *behandling av opplysninger i forbindelse med testing og utvikling av informasjonssystemer.*

V

I lov 20. april 2018 nr. 8 om grensetilsyn og grensekontroll av personer gjøres følgende endringer:

§ 22 tredje ledd skal lyde:

Biometriske opplysninger (ansiktsbilde og fingeravtrykk) kan innhentes 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 kan behandles for å utvikle og

teste 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 også lagre ansiktsbilder og fingeravtrykk innhentet i medhold av § 22 tredje ledd i inntil seks måneder dersom det er nødvendig for å teste og utvikle informasjonssystemer til bruk for grensekontrollformål dersom det vil være umulig eller uforholdsmessig vanskelig å oppnå formålet ved å bruke anonyme eller fiktive opplysninger. Opplysninger som lagres etter dette leddet, kan bare behandles til dette formålet.

Opplysninger som behandles etter annet ledd i bestemmelsen her skal holdes atskilt. Tilgang skal bare gis til personer som er særskilt bemyndiget. Bemyndigelse gis av den behandlingsansvarlige.

Ansiktsbilder og fingeravtrykk skal slettes i form av tilintetgjøring, jf. arkivlova § 13 annet ledd.

§ 25 nr. 10 skal lyde:

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

VI

1. Loven gjelder fra den tid Kongen bestemmer. Kongen kan sette i kraft de enkelte bestemmelsene til forskjellig tid.
2. Kongen kan gi nærmere overgangsregler.

