

Høringsnotat

Dato: 28.09.2026

Saksnr: 26/5159

Høringsfrist: 20.11.2026

Forslag til endringer i utlendingsforskriften (utvikling og testing av IT-systemer i utlendingsforvaltningen mv.)

Innhold

1	Innledning.....	2
2	Bakgrunn	3
3	Utvikling og testing av informasjonssystemer (IT-systemer)	4
3.1	Gjeldende rett	4
3.1.1	Grunnloven og menneskerettighetene	4
3.1.2	Personvernforordningen	5
3.1.3	Forholdet mellom taushetsplikten og personvernforordningen	6
3.1.4	Politiregisterloven og personverndirektivet for politi og påtalemyndighet mv.	7
3.1.5	Europarådets personvernkonvensjon.....	8
3.1.6	Tilsvarende hjemler i annet regelverk.....	8
3.1.7	Utlendingsloven og -forskriften.....	10
3.2	Departementets forslag og vurdering	11
3.2.1	Terminologi	11
3.2.2	Behovet for en egen hjemmel om utvikling og testing av IT-systemer, herunder systemer basert på KI.....	13
3.2.3	Krav til nødvendighet og forholdsmessighet	15
3.2.4	Hvilke personopplysninger kan behandles til utvikling og testing av IT-systemer?	16
3.2.5	Konsekvenser for den enkeltes grunnleggende rettigheter, herunder personvernkonsekvenser	17
3.2.6	Behandlingsansvar mv.	19
3.2.7	Unntak fra taushetsplikten	19
3.2.8	Forholdet mellom forordningen om kunstig intelligens og utlendingsregelverket	24
3.2.9	Særlig om IT-systemer som behandler personopplysninger til delvis politimessige formål og delvis forvaltningsmessige formål	25

4	Kompetanse til å beslutte opptak av fingeravtrykk og ansiktsbilde etter Eurodac-forordningen 2024	25
4.1	Eurodac-forordningen 2024	25
4.2	Gjeldende rett	25
4.3	Departementets forslag og vurdering	26
5	Oppheving av den registrertes klageadgang etter Eurodac-forordningen 2024	27
5.1	Gjeldende rett	27
5.2	Departementets forslag og vurdering	29
6	Konsekvensjustering av aktuelle uttrykk i utlendingsforskriften	29
6.1	Gjeldende rett	29
6.2	Departementets forslag og vurdering	30
7	Økonomiske og administrative konsekvenser	30
8	Forslag til endringer i utlendingsforskriften	31

1 Innledning

Justis- og beredskapsdepartementet sender med dette på høring forslag til endringer i forskrift 15. oktober 2009 nr. 1286 (utlendingsforskriften, utf.). Endringsforslagene inngår i et større arbeid med å sikre en moderne, effektiv og fremtidsrettet utlendingsforvaltning.

Bakgrunnen for de enkelte forslagene er redegjort for i høringsnotatets punkt 2.

I punkt 3 foreslås det å innta i forskriften at utlendingsmyndighetene kan behandle innhentede personopplysninger til å *utvikle og teste* informasjonssystemer (IT-systemer), herunder systemer basert på kunstig intelligens (KI-systemer). Den nye hjemmelen vil ikke regulere den etterfølgende *bruken* av det aktuelle IT-systemet.

Punkt 4 omhandler kompetanse til å beslutte opptak av biometriske opplysninger etter Eurodac-forordningen 2024.¹ Det foreslås bl.a. endringer som skal tydeliggjøre at utlendingsmyndighetene har hjemmel til å oppta ansiktsbilde og fingeravtrykk til registrering i det felleseuropeiske systemet, Eurodac.

I punkt 5 foreslås det å oppheve den registrertes adgang til å klage på personvernrettslige avgjørelser etter Eurodac-forordningen, til *departementet* som overordnet forvaltningsorgan. Den registrerte må i stedet forholde seg til de klagemulighetene som fremgår av aktuelt personvernregelverk.

¹ Europaparlaments- og rådsforordning (EU) 2024/1358 av 14. mai 2024 om opprettelse av «Eurodac» for sammenligning av biometriske opplysninger for effektiv anvendelse av Europaparlaments- og rådsforordning (EU) 2024/1351 og (EU) 2024/1350 og rådsdirektiv 2001/55/EF og for å identifisere en tredjelandsborger eller statsløs med ulovlig opphold, og om anmodninger om sammenligning med Eurodac-opplysninger for medlemsstatenes rettshåndhevende myndigheter og Europol for rettshåndhevelsesformål, om endring av Europaparlaments- og rådsforordning (EU) 2018/1240 og (EU) 2019/818 og om oppheving av Europaparlaments- og rådsforordning (EU) nr. 603/2013 («Eurodac-forordningen»).

I punkt 6 foreslås det å justere ordlyden i aktuelle bestemmelser i utlendingsforskriften for å redusere risikoen for tolkningstvil.

Økonomiske og administrative konsekvenser av ovenstående forslag er nærmere behandlet i høringsnotatets punkt 7, mens konkrete forslag til endringer i aktuelt regelverk fremgår av punkt 8.

2 Bakgrunn

Norge er et av verdens mest digitaliserte land. I regjeringens nasjonale digitaliseringsstrategi for 2024–2030 er det uttalt at det overordnede målet med strategien er å gjøre Norge til det *mest digitaliserte landet* i verden innen 2030.² Dette skal oppnås gjennom flere ulike tiltak, herunder ved å utnytte mulighetene som ligger i kunstig intelligens (KI). Regjeringen har som mål at alle statlige virksomheter skal ta i bruk KI i sin oppgaveløsning i 2030.³ En viktig forutsetning for å nå målene i digitaliseringsstrategien, er at sektorregelverket oppdateres i tråd med den tekniske utviklingen i samfunnet.⁴

Utlendingsdirektoratet (UDI) anslår at de i 2026 vil motta om lag 194 000 saker.⁵ Et digitaliseringsvennlig regelverk vil kunne åpne for bruk av nye tekniske løsninger ved behandlingen av disse sakene; løsninger som kan effektivisere saksbehandlingen og på sikt føre til ressursbesparelser i utlendingsforvaltningen.

Forslaget om å forskriftsfeste adgangen til å behandle innhentede personopplysninger til å utvikle og teste IT-systemer, jf. høringsnotatets punkt 3, inngår i et større arbeid med forenkling av regelverket for utlendingsforvaltningen med formål å effektivisere og digitalisere saksbehandlingen. Det vises i denne sammenheng til høringsnotat 23. juni 2023⁶ og 19. januar d.å.⁷, og til forskrift om endring i utlendingsforskriften (oppholdstillatelse til studenter mv.) som trådte i kraft 1. september d.å.

I tillegg til å legge til rette for en digital transformasjon av utlendingsforvaltningen, er det viktig å sørge for at regelverket er klart og tilgjengelig for brukerne. Av denne grunn foreslås det flere mindre endringer i utlendingsforskriften, herunder endringer som skal tydeliggjøre utlendingsmyndighetenes kompetanse og myndighet til å beslutte og gjennomføre opptak av biometriske opplysninger etter Eurodac-forordningen 2024, samt justering av ordlyden i aktuelt regelverk for å redusere risikoen for tolkningstvil.

² [Nasjonal digitaliseringsstrategi 2024-2030 side 7.](#)

³ [Ibid side 8 flg.](#), se også [digitaliseringsrundskrivet D-2/25 punkt 1.3.](#)

⁴ Se også [Datatilsynets rapport om KI og personvern \(2018\) side 28](#), der tilsynet understreker viktigheten av at "lovgivningen holder følge med den teknologiske utviklingen".

⁵ [Anslag for saker til UDI i 2026 per juni 2026.](#)

⁶ [Høringsnotat 23. juni 2023 om forslag til endringer i utlendingsforskriften for et forenklet regelverk mv.](#)

⁷ [Høringsnotat 19. januar 2026 om forslag til endringer i utlendingsloven og utlendingsforskriften \(effektivisering og digitalisering av saksbehandlingen\).](#)

3 Utvikling og testing av informasjonssystemer (IT-systemer)

3.1 Gjeldende rett

3.1.1 Grunnloven og menneskerettighetene

Grunnloven § 102 verner om retten til respekt for privatliv, herunder retten til personvern. Regelen kom inn i Grunnloven i forbindelse med grunnlovsreformen i 2014. Kontroll- og konstitusjonskomitéen uttalte i sin innstilling⁸ at

«den teknologiske utviklingen gjør at behovet for å formulere kommunikasjon inn i Grunnloven er enda større nå enn tidligere. Teknologiutvikling er et gode, men krever mer av oss i henhold til å sikre personvern.»

Videre understreket komitéen at grunnlovsbestemmelsen skal

«leses som at systematisk innhenting, oppbevaring og bruk av opplysninger om andres personlige forhold bare kan finne sted i henhold til lov, benyttes i henhold til lov eller informert samtykke og slettes når formålet ikke lenger er til stede.»

Den europeiske menneskerettskonvensjon (EMK) artikkel 8 verner om retten til privatliv og familieliv. Den europeiske menneskerettsdomstol (EMD) har lagt til grunn at EMK artikkel 8 også omfatter vern av personopplysninger, jf. *Leander mot Sverige* (9248/81) avsnitt 48, og at begrepet «privatliv» skal tolkes vidt, jf. *Amann mot Sveits* (27798/95) avsnitt 65 og Europarådets personvernkonvensjon artikkel 1 og 2. Domstolen har videre i flere saker lagt til grunn at myndigheters innhenting og oppbevaring av personopplysninger utgjør et inngrep i retten til privatliv etter EMK artikkel 8, se som eksempel *S og Marper mot Storbritannia* (storkammer) nr. 3062/04 og 30566/04 avsnitt 121. Også en viderebehandling av personopplysninger vil kunne utgjøre et inngrep i retten til privatliv, idet opplysningene blir kjent for en større krets, se *M.S mot Sverige* (74/1996/693/885) avsnitt 33 til 35.

Det fremgår av EMK artikkel 8 nr. 2 at det kan gjøres inngrep i rettigheten etter nærmere angitte vilkår. Grunnloven § 102 åpner ikke etter sin ordlyd for å gjøre inngrep i retten til respekt for privatliv, men det følger av høyesterettspraksis at bestemmelsen må tolkes i lys av den tilsvarende rettigheten i EMK artikkel 8, se bl.a. HR-2020-2372-A avsnitt 38. Det vil dermed være adgang til å gjøre inngrep der vilkårene i EMK artikkel 8 nr. 2 er oppfylt. Av bestemmelsens andre ledd fremgår det at det kan gjøres inngrep i rettigheten dersom

«dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter»

Det første vilkåret er at inngrepet har hjemmel i lov eller i forskrift gitt med hjemmel i lov. Om det nærmere innholdet i lovskravet uttaler Høyesterett i Rt. 2014 s. 1105 avsnitt 30 at loven må «være tilgjengelig og så presis som forholdene tillater». Kravet til lovhemmel må videre nyanseres ut fra hvilket område en befinner seg på, arten av inngrepet, hvordan det rammer og hvor tyngende inngrepet er for enkeltindividet, se Rt. 1995 s. 530, s. 537.

⁸ Innst. 186 S (2013-2014) punkt 2.1.9 på side 27.

Det andre vilkåret som må være oppfylt for å kunne rettferdiggjøre et inngrep i retten til privatliv, er at inngrepet søker å oppnå et legitimt formål som nevnt i EMK artikkel 8 nr. 2. Det kan være flere grunner til at myndighetene ser behov for å behandle personopplysninger om den enkelte, f.eks. av hensyn til den offentlige trygghet, landets økonomiske velferd, for å forebygge uorden eller kriminalitet, jf. artikkel 8 nr. 2.

I tillegg til at inngrepet må ha tilstrekkelig hjemmel og være begrunnet i ett av de legitime formålene i artikkel 8 nr. 2, kreves det at inngrepet er forholdsmessig. I kravet om forholdsmessighet ligger at inngrepet må være i) egnet og ii) nødvendig for å oppnå det legitime formålet, samt at de legitime formålene som inngrepet er begrunnet i, veier tyngre enn de ulempene som inngrepet medfører for enkeltindividet (forholdsmessighet i snever forstand, *stricto sensu*). Høyesterett uttaler i HR-2015-206-A at forholdsmessighetsvurderingen «må ha for øye balansen mellom de beskyttede individuelle interessene på den ene siden og de legitime samfunnsbehovene som begrunner tiltaket på den andre», se avsnitt 60. I HR-2019-1226-A avsnitt 57 fremhever Høyesterett, under henvisning til S og Marper mot Storbritannia, at

«de nasjonale reglene må gi garantier – «appropriate safeguards» – mot bruk av personopplysninger som er uforenlig med artikkel 8. Lovgivningen må sikre at lagringen av slike opplysninger er «relevant and not excessive in relation to the purposes for which they are stored».»

I samme avgjørelse peker Høyesterett på at EMD gir uttrykk for at regelverket må gi effektiv beskyttelse mot misbruk av opplysningene.

3.1.2 Personvernforordningen

Personopplysningsloven (poppl.) gjennomfører i norsk rett personvernforordningen (EU) 2016/679⁹, jf. lovens § 1. Både loven og personvernforordningen kommer til anvendelse ved helt eller delvis automatisert behandling av personopplysninger og ved ikke-automatisert behandling av personopplysninger som inngår i eller skal inngå i et register, jf. poppl. § 2 første ledd første punktum. Regelverket gjelder også for utlendingsforvaltningens behandling av personopplysninger, se utlendingsloven (utl.) § 80.

Utlendingsmyndighetene behandler ofte sensitive personopplysninger om den enkelte, f.eks. biometriske opplysninger, opplysninger om seksuell orientering, religion og helse. Sensitive personopplysninger omtales i personvernforordningen som «særlige kategorier av personopplysninger», og er som den klare hovedregel forbudt å behandle, jf. artikkel 9 nr. 1. Forordningen åpner likevel for behandling av særlige kategorier av personopplysninger dersom ett av vilkårene i artikkel 9 nr. 2 er oppfylt. For offentlige myndigheter, herunder aktører i utlendingsforvaltningen, er artikkel 9 nr. 2 bokstav g, behandling av hensyn til viktige allmenne interesser, et særlig relevant unntak. Bestemmelsen gir imidlertid ikke i seg selv adgang til å behandle særlige kategorier av personopplysninger. Det rettslige grunnlaget for behandlingen må fremgå av nasjonal rett; et såkalt supplerende rettsgrunnlag. Behandlingen må videre være *nødvendig* av hensyn til de viktige allmenne interessene, hvilket betyr at det må gjøres en vurdering av om

⁹ Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning).

det finnes mindre inngripende tiltak for å oppnå formålet. Videre oppstilles det enkelte krav til hjemmelen, herunder at den må sikre egnede og særlige tiltak for å verne om den registrertes grunnleggende rettigheter og interesser (personverngarantier).

I tillegg til å behandle særlige kategorier av personopplysninger, behandler utlendingsmyndighetene *store* mengder personopplysninger om den enkelte, f.eks. i forbindelse med behandling av søknad om oppholdstillatelse. For å kunne utvikle og teste nye IT-løsninger, vil det i de aller fleste tilfeller være behov for å gjenbruke (viderebehandle) disse personopplysningene. Slik viderebehandling må skje i tråd med grunnleggende personvernrettslige regler og prinsipper.

Personvernforordningen artikkel 5 nr. 1 angir prinsipper for behandling av personopplysninger. Etter artikkel 5 nr. 1 bokstav a skal behandlingen skje på en «lovlig, rettferdig og åpen måte». I dette ligger at behandlingen må ha tilstrekkelig hjemmel (behandlingsgrunnlag), jf. artikkel 6. Personopplysninger skal videre, som det klare utgangspunkt, kun samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene (prinsippet om formålsbegrensning), jf. artikkel 5 nr. 1 bokstav b. Dette er imidlertid ikke ensbetydende med at personopplysninger ikke kan behandles til nye formål. Det oppstilles kun en grense mot *uforenlige* formål, dvs. formål som ikke er i tråd med det opprinnelige innsamlingsformålet. Hvorvidt viderebehandling til et nytt formål er å anse som uforenlig med det opprinnelige innsamlingsformålet, må avgjøres gjennom en konkret vurdering, se personvernforordningen artikkel 6 nr. 4, især bokstav a til e.

Departementet har i Prop. 79 L (2024–2025) lagt til grunn at det ikke kreves et annet rettslig grunnlag enn det som ligger til grunn for innsamlingen for å kunne behandle opplysningene til et nytt og forenlig formål, se punkt 12.5.1.2 på s. 176, jf. også fortalepunkt 50 i personvernforordningen. Dersom det nye formålet derimot ikke er forenlig, men uforenlig med innsamlingsformålet, må behandlingen være basert på den registrertes samtykke, eller ha hjemmel i nasjonal rett som skal ivareta noen av formålene i artikkel 23 nr. 1.

Den som behandler personopplysninger pålegges videre en rekke plikter og ansvar. Av særlig interesse er personvernforordningen artikkel 24 som regulerer den behandlingsansvarliges, jf. artikkel 4 nr. 7, sitt ansvar for behandlingen. Det fremgår av artikkel 24 nr. 1 at den behandlingsansvarlige plikter å gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at enhver behandling skjer i tråd med personvernforordningens regler. Det er for øvrig gitt spesifikke regler i utlendingsloven og -forskriften om behandlingsansvar i utlendingsforvaltningen, se punkt 3.1.7 nedenfor.

3.1.3 Forholdet mellom taushetsplikten og personvernforordningen

Enhver som utfører tjeneste eller arbeid for utlendingsmyndighetene har taushetsplikt iht. forvaltningsloven (fvl.). Taushetsplikten innebærer en plikt for vedkommende til å hindre at andre får adgang eller kjennskap til det han eller hun i forbindelse med tjenesten eller arbeidet får vite om noens personlige forhold, jf. fvl. § 13. Plikten gjelder ikke bare utad, men også internt i ett og samme forvaltningsorgan, hvilket betyr at for eksempel en saksbehandler ikke står fritt til å dele taushetsbelagte opplysninger med andre kollegaer. Hvorvidt slik deling kan skje må vurderes opp mot bestemmelsene som fastsetter unntak fra

taushetsplikten, jf. fvl. §§ 13 a og 13 b. Reglene om taushetsplikt i den gjeldende forvaltningsloven er i hovedsak videreført i den nye forvaltningsloven 2025, som p.t. ikke er satt i kraft.

Dersom et forvaltningsorgan ønsker å behandle innhentede personopplysninger til utvikling og testing av IT-systemer, vil opplysningene nødvendigvis måtte gjøres kjent for en videre krets av personer innenfor forvaltningsorganet, eksempelvis utviklere og konsulenter i virksomhetens IT-avdeling. Så lenge personopplysningene ikke er taushetsbelagte, kan opplysningene uten hinder av taushetsplikt viderebehandles innenfor rammen av personopplysningsloven og personvernforordningen. I de tilfeller hvor personopplysningene er taushetsbelagte, noe som ofte er tilfellet i utlendingsforvaltningen, må adgangen til å viderebehandle opplysningene vurderes opp mot taushetspliktsreglene i forvaltningsloven, jf. fvl. §§ 13 flg. Taushetsplikten i forvaltningsloven gjelder uavhengig av om personopplysningene viderebehandles for forenlige eller uforenlige formål iht. personvernforordningen. I tilfeller der det følger av sektorlovgivningen at et forvaltningsorgan kan viderebehandle personopplysninger til et nytt formål, må det vurderes om den aktuelle lovgivningen begrenser den lovbestemte taushetsplikten. Det følger av fvl. § 13 f andre ledd at bestemmelser i annen lov om rett eller plikt til å gi opplysninger ikke begrenser lovbestemt taushetsplikt, med mindre det er fastsatt eller klart forutsatt at taushetsplikten ikke skal gjelde. Denne bestemmelsen er ikke videreført i ny forvaltningslov, men dette innebærer ingen realitetsendring, da det samme uansett må anses å følge av bestemmelsen i ny lov § 2 fjerde ledd om at forvaltningsloven gjelder når ikke annet er bestemt i eller i medhold av lov, se Prop. 79 L (2024-2025) punkt 12.1.4.

For å kunne viderebehandle personopplysninger til nye formål er det altså ikke tilstrekkelig å utelukkende se hen til de rammer som personvernforordningen setter. I noen tilfeller må det også ses hen til de rammer som følger av taushetsplikten, da personopplysningene også kan være belagt med lovbestemt taushetsplikt, jf. punkt 3.2.7 nedenfor.

3.1.4 Politiregisterloven og personverndirektivet for politi og påtalemyndighet mv.

Personopplysningsloven og personvernforordningen, jf. punkt 3.1.2 ovenfor, gjelder ikke når annet er bestemt i eller med hjemmel i lov, jf. poppl. § 2 første ledd annet punktum. Om poppl. § 2 første ledd uttaler departementet følgende i Prop. 56 LS (2016–2017) punkt 4.5.2:

«Departementet bemerker for ordens skyld at § 2 første ledd ikke er ment å avskjære muligheten til å gi nasjonale regler som gjennomfører direktiv (EU) 2016/680, slik det for eksempel er gjort gjennom politiregisterloven. Det følger av forslaget til § 2 første ledd annet punktum at loven og forordningen ikke gjelder der annet er bestemt i eller i medhold av lov. 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.»

Politiregisterloven gjennomfører direktiv (EU) 2016/680¹⁰ i norsk rett. Loven gjelder for politiets og påtalemyndighetens behandling av opplysninger, jf. § 3 første ledd. Det er imidlertid gjort unntak for behandling som er del av politiets forvaltningsvirksomhet eller sivile gjøremål, jf. første ledd nr. 2.

For personopplysninger som behandles i et sentralt register, er det gitt utfyllende regler om politiregisterlovens virkeområde, jf. politiregisterforskriften § 1-3 nr. 3, jf. politiregisterloven § 14. Det fremgår av forskriftsbestemmelsen at politiregisterloven vil komme til anvendelse på opplysninger som behandles delvis til politimessige og delvis til forvaltningsmessige formål.

3.1.5 Europarådets personvernkonvensjon

Norge har ratifisert Europarådets konvensjon nr. 108 av 28. januar 1981 om personvern i forbindelse med elektronisk databehandling av personopplysninger (Europarådets personvernkonvensjon). Formålet med rettsakten, jf. artikkel 1, er å

«sikre respekt for enhver enkeltpersons rettigheter og grunnleggende friheter og især retten til privatlivets fred på territoriet til enhver part, uten hensyn til statsborgerskap eller bopel, i forbindelse med elektronisk databehandling av personopplysninger som vedrører ham («datavern»)).».

Konvensjonen har flere likhetstrekk med personvernforordningen, og den kommer til anvendelse på enhver behandling av personopplysninger som utføres av både private og offentlige aktører, herunder utlendingsmyndighetene. Ved endringsprotokoll 10. oktober 2018 er det oppstilt mer detaljerte krav enn i gjeldende konvensjon. Endringsprotokollen har ikke trådt i kraft, men Norge har signert endringsprotokollen og avgitt en erklæring om midlertidig anvendelse av protokollen.

Etter gjeldende personvernkonvensjon plikter den enkelte avtalepart å treffe nødvendige tiltak i sin interne lovgivning for å gjennomføre hovedprinsippene for datavern. Dette inkluderer tiltak som skal sikre datakvalitet, herunder at personopplysninger i) innsamles og bearbeides på rettferdig og lovlig vis; ii) lagres for bestemte og lovlige formål og ikke nyttes på en måte som er uforenlig med disse formål; iii) er adekvate, relevante og ikke for omfattende i relasjon til de formål de lagres til; iv) er nøyaktige og, der det er nødvendig, holdt a jour; og v) oppbevares på en måte som begrenser identifikasjon av datasubjektene innenfor rammen av formålsangivelsen, jf. artikkel 5. Konvensjonen oppstiller et forbud mot behandling av «særkategorier av personopplysninger», med mindre intern lovgivning gir tilstrekkelig vern, jf. artikkel 6. Det kan for øvrig gjøres unntak fra enkelte konvensjonsrettigheter i tråd med reglene i artikkel 9.

3.1.6 Tilsvarende hjemler i annet regelverk

Det finnes i dag flere hjemler i sektorregelverket som åpner for at personopplysninger som en offentlig virksomhet behandler i sin lovregulerte

¹⁰ Europaparlaments- og rådsdirektiv (EU) 2016/680 av 27. april 2016 om fysiske personers vern i forbindelse med kompetente myndigheters behandling av personopplysninger med sikte på å forebygge, etterforske, avsløre eller rettsforfølge straffbare handlinger eller fullbyrde strafferettslige sanksjoner og om fri utveksling av slike opplysninger, og opphevelse av Rådets rammebeslutning 2008/977/JIS.

virksomhet, også skal kunne brukes til utvikling og testing av IT-systemer. Et eksempel er skatteforvaltningsloven § 5-12, som lyder:

«(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 bl.a. i vareførselsloven § 7-17, skattebetalingsloven § 3-6, folkeregisterloven § 9-5, lov om Statens pensjonskasse § 45 b sjette ledd, husbankloven § 12 tredje ledd, a-opplysningsloven § 6 a og valutaregisterforskriften § 2 a.

Om begrunnelsen for å fastsette hjemler for bruk av personopplysninger til utvikling og testing av IT-systemer, viser Finansdepartementet i Prop. 1 LS (2018–2019) til at det i en del tilfeller ikke er mulig å utvikle og teste IT-systemer uten å bruke personopplysninger, dvs. opplysninger om identifiserte eller identifiserbare subjekter. I andre tilfeller er det svært tid- og ressurskrevende å lage anonyme eller fiktive opplysninger. På denne bakgrunn konkluderte Finansdepartementet med at Skatteetaten og Tolletaten har et begrunnet behov for å behandle personopplysninger til utvikling og testing av IT-systemer.

Om bakgrunnen for å lovregulere adgangen til å gjenbruke personopplysninger til utvikling og testing, viser Finansdepartementet til at

«[p]ersonvern hensyn taler for at det bør være klart for de registrerte hvordan personopplysningene deres blir brukt. I personvernforordningen artikkel 5 bokstav a kommer dette til uttrykk ved at personopplysninger skal behandles på en «åpen måte med hensyn til den registrerte» (prinsippet om åpenhet). Lovregulering av adgangen til å bruke personopplysninger bidrar til å skape slik åpenhet».¹¹

Selv om det ikke fremkommer klart av ordlyden, gir ovenstående bestemmelser adgang til å behandle personopplysninger som nevnt i personvernforordningen artikkel 9 og 10. På side 306 i proposisjonen, uttaler Finansdepartementet at

«[d]e delene av IT-systemene som skal behandle opplysninger som omfattes av personvernforordningen artikkel 9 og artikkel 10, må utvikles og testes på samme måte som de andre delene av IT-systemene. I høringsnotatet foreslo departementet at det skal fremgå av lovbestemmelsene at Skatteetaten og Tolletaten kan bruke opplysninger etter personvernforordningen artikkel 9 og artikkel 10 ved utvikling og testing av IT-systemer. Departementet viderefører i proposisjonen her forslaget om at det skal være adgang til å bruke slike opplysninger. Etter departementets vurdering er det imidlertid ikke nødvendig at det fremgår direkte av lovteksten at det er en slik adgang, når det er klart forutsatt at opplysningene skal kunne brukes».

Stortinget har for øvrig, etter forslag fra Justis- og beredskapsdepartementet i Prop. 36 L (2025–2026), vedtatt en lignende regulering i grenseloven § 22 a. Bestemmelsen trådte i kraft 1. juli d.å.

¹¹ Prop. 1 LS (2018–2019) punkt 18.5 på s. 304.

3.1.7 Utlendingsloven og -forskriften

I utl. § 83 a er det inntatt en generell bestemmelse om behandling av personopplysninger. Bestemmelsen bygger på personvernforordningen artikkel 6 nr. 1 første ledd bokstav e og artikkel 9 nr. 2 bokstav g, og lyder:

«Utlendingsmyndighetene kan behandle personopplysninger, herunder personopplysninger som nevnt i personvernforordningen artikkel 9 og 10, når dette er nødvendig for å utøve myndighet eller utføre andre oppgaver etter loven her.

Utlendingsmyndighetene kan behandle personopplysninger som nevnt i første ledd når det er nødvendig i forbindelse med tildeling av økonomiske ytelser til en utlending som er innkvartert etter § 95, ved utøvelse av omsorgsansvaret for enslige, mindreårige asylsøkere eller i forbindelse med assistert retur eller tilbakevending.

Kongen kan gi forskrift om behandlingen, blant annet om formålet med behandlingen, behandlingsansvar, hvilke personopplysninger som kan behandles, hvem det kan behandles personopplysninger om, bruk av automatiserte avgjørelser, adgangen til viderebehandling, utlevering, registerføring og tilgang til registre».

Etter første ledd kan utlendingsmyndighetene behandle personopplysninger, herunder særlige kategorier av personopplysninger, når det er nødvendig for å utføre lovpålagte oppgaver. Bestemmelsen gir ikke i seg selv adgang til å behandle personopplysninger, men er ment å angi de overordnede rammene for behandlingen. Behandling av personopplysninger kan kun skje i forbindelse med utøvelse av myndighet eller utføring av oppgaver som er hjemlet i «loven her», dvs. at bestemmelsen må holdes opp mot øvrige bestemmelser som tillegger utlendingsmyndighetene en oppgave eller kompetanse til å utøve myndighet. Selv om det ikke fremgår direkte av ordlyden, gjelder dette også for utøvelse av myndighet eller utføring av oppgaver som er forankret i forskrift med hjemmel i lov. Dette er bl.a. understreket i forarbeidene, Prop. 59 L (2017–2018) på side 18, der departementet uttaler at

«(...) bestemmelsen ikke skal anvendes alene, men at den i det enkelte tilfelle må holdes opp mot øvrige bestemmelser i lov eller forskrift som tillegger myndighet eller pålegger oppgaver».

Tredje ledd inneholder en forskriftshjemmel, som gir Kongen kompetanse til å gi regler i forskrift om behandling av personopplysninger, herunder adgang til viderebehandling. Slike regler er gitt i utlf. §§ 17-7 a og 17-7 b, som regulerer formålet med behandlingen, adgangen til viderebehandling og behandlingsansvaret. Av særlig interesse for utvikling og testing av IT-systemer, er bestemmelsen i § 17-7 a andre ledd, som lyder:

«Utlendingsmyndighetene kan viderebehandle personopplysninger for nye formål når det er nødvendig av kontrollhensyn og sakene har en forbindelse. Begrensningene i første punktum gjelder ikke for viderebehandling for forenelige formål.»

Hovedregelen fremgår av andre punktum, som noe implisitt fastslår at utlendingsmyndighetene kan viderebehandle personopplysninger til nye formål som er forenlige med det opprinnelige innsamlingsformålet, jf. også personvernforordningen artikkel 5 nr. 1 bokstav b og forenlighetsvurderingen i

artikkel 6 nr. 4. Det kreves ikke et særskilt rettslig grunnlag for slik viderebehandling, jf. punkt 3.1.2 over.

Viderebehandling til *uforenlige* formål, jf. andre ledd første punktum, kan kun skje dersom det er nødvendig av kontrollhensyn, og sakene har en sammenheng. Det oppstilles altså et krav til nødvendighet og forholdsmessighet for å kunne viderebehandle personopplysninger til nye, uforenlige formål, jf. personvernforordningen artikkel 6 nr. 4, jf. også artikkel 23 nr. 1 bokstav e. Dersom disse vilkårene er oppfylt, trenger ikke utlendingsmyndighetene å foreta en forenlighetsvurdering for å kunne viderebehandle personopplysningene. Viderebehandling til uforenlige formål i andre tilfeller enn de som er nevnt i utlf. § 17-7 a andre ledd første punktum vil kreve et særskilt viderebehandlingsgrunnlag som oppfyller kravene i personvernforordningen artikkel 6 nr. 4.

Det er videre gitt regler om *behandlingsansvar* i utlendingsloven og -forskriften. For enkelte systemer er behandlingsansvaret fastsatt av lovgiver i lovs form, se som eksempel utl. § 102 d, som fastsetter at UDI er behandlingsansvarlig for NORVIS. For andre systemer er behandlingsansvaret fastsatt i forskrift. Av særlig interesse er utlf. § 17-7 b, som lyder:

«Utlendingsdirektoratet, Utlendingsnemnda, politiet, Sysselmesteren på Svalbard og utenriktjenesten er hver for seg behandlingsansvarlig for behandling av personopplysninger for egne formål, herunder opplysninger registrert i Utlendingsdatabasen. Behandlingsansvaret i utenriktjenesten utøves av Utenriksdepartementet.

Utlendingsdirektoratet er behandlingsansvarlig for Utlendingsdatabasen.»

Bestemmelsens første ledd gir anvisning på et formålsorientert behandlingsansvar, mens andre ledd fastsetter at UDI er behandlingsansvarlig for Utlendingsdatabasen. Bestemmelsens første ledd er generelt utformet, og vil gjelde i den grad det ikke finnes andre, særskilte regler om behandlingsansvar for konkrete systemer. At UDI er behandlingsansvarlig for Utlendingsdatabasen er for øvrig ikke til hinder for at de øvrige aktørene i utlendingsforvaltningen anses som behandlingsansvarlige for behandling i og fra databasen som skjer til eget formål, jf. også uttalelsene i Prop. 37 LS (2025–2026), især punkt 8.4.4.5.

3.2 Departementets forslag og vurdering

3.2.1 Terminologi

I høringsnotatet her foreslås det hjemler for viderebehandling av personopplysninger til «utvikling» og «testing» av «informasjonssystemer». I Prop. 36 L (2025–2026) punkt 2.1.2 på s. 7 uttalte departementet følgende om innholdet i disse uttrykkene:

«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.»

Uttalelsen over er særlig myntet på politiet, men har etter departementets vurdering overføringsverdi til forslaget om etablering av tilsvarende utviklings- og testhjemler i utlendingsregelverket.

Departementet foreslår videre at hjemmelen skal gjelde for *utlendingsmyndighetene*. Med «utlendingsmyndighetene» siktes det her til offentlige virksomheter som utfører oppgaver etter utlendingsloven eller -forskriften, som UDI, Utlendingsnemnda (UNE), politiet, Sysselmesteren på Svalbard og de enkelte utenriksstasjonene. Det bemerkes i denne sammenheng at departementet i høringsnotat 20. mars d.å. har foreslått å overføre driftsansvaret for utlendingsinternatet fra Politiets utlendingsenhet til kriminalomsorgen.¹² Selv om kriminalomsorgen nå potensielt vil få oppgaver etter utlendingsloven, bemerker departementet at adgangen til å behandle personopplysninger for å utvikle og teste IT-systemer ikke er ment å omfatte kriminalomsorgen i forbindelse med deres oppgaver etter utlendingsloven og ny utlendingsinternatforskrift. Departementet viser her til at det i nevnte høringsnotat foreslås en egen hjemmel for at kriminalomsorgen skal kunne behandle personopplysninger i forbindelse med driften av utlendingsinternatet. Hjemmelen for deres behandling av personopplysninger til dette formålet vil altså ikke være den generelle hjemmelen i utl. § 83 a, som forslaget til utvikling og testing av IT-systemer er hjemlet i, men i stedet være en særskilt bestemmelse om behandling av personopplysninger i forbindelse med internering mv., som i høringsnotat 20. mars. d.å. foreslås inntatt i utl. § 107 syvende ledd første punktum. Departementet mener det uansett er hensiktsmessig å avvente etableringen av en ev. tilsvarende utviklings- og testhjemmel for kriminalomsorgen til det foreligger endelig klarhet i hvilke systemer kriminalomsorgen selv skal ha ansvar for å vedlikeholde og drifte.

Departementet bemerker videre at forslaget til ny bestemmelse er ment å være teknologinøytralt, selv om det i ordlyden vises til systemer basert på «kunstig intelligens». Henvisningen til KI er inntatt av pedagogiske grunner og er ment å utgjøre et ikke-uttømmende eksempel på hva som ligger i begrepet «informasjonssystemer», jf. også Prop. 36 L (2025-2026) punkt 2.1.2 på s. 7. For ordens skyld bemerker departementet at uttrykket «kunstig intelligens» skal forstås på tilsvarende måte som i KI-forordningen. Departementet viser for øvrig til punkt 3.2.8 for en nærmere vurdering av forholdet mellom den kommende KI-loven og det sektorspesifikke regelverket om utvikling og testing av IT-systemer.¹³

¹² [Høringsnotat 20. mars 2026 om overføring av driftsansvar for utlendingsinternatet fra politiet til kriminalomsorgen.](#)

¹³ Høringsnotatets punkt 3.2.8 tar utgangspunkt i forholdet mellom det horisontale KI-rammeverket og *utlendingsregelverket*, og en ev. overføringsverdi til øvrig sektorregelverk må derfor vurderes konkret.

3.2.2 Behovet for en egen hjemmel om utvikling og testing av IT-systemer, herunder systemer basert på KI

Som nevnt i punkt 2 over, mottar utlendingsmyndighetene godt over 100 000 saker i året. Avgjørelsene har stor betydning for den enkelte, samtidig som flere i dag må vente lenge på å få saken sin avgjort, bl.a. fordi utlendingsforvaltningen p.t. er under et stort press som følge av flere ekstraordinære hendelser de siste årene, inkludert Russlands angrepskrig mot Ukraina. Et viktig tiltak for å kunne redusere saksbehandlingstidene, er å ta i bruk ny teknologi, herunder KI-systemer. Det er imidlertid viktig å sikre at bruken av digitale hjelpemidler ikke går på bekostning av hensynet til å sikre riktige avgjørelser i utlendingssaker. Derfor må utlendingsmyndighetene sørge for at ev. IT-systemer som tas i bruk i saksbehandlingen er grundig utviklet og nøye testet. En viktig forutsetning for å kunne sikre høy standard i systemutviklingen er at utlendingsmyndighetene gis tilgang til data av høy kvalitet.

Personvern hensyn, herunder prinsippet om formålsbegrensning og dataminimering, tilsier at offentlige myndigheter, som den klare hovedregel, kun forholder seg til anonyme, aidentifiserte eller fiktive opplysninger ved utvikling og testing av IT-systemer, jf. hhv. artikkel 5 nr. 1 bokstav b og c i personvernforordningen.

I en del tilfeller vil det imidlertid være umulig eller svært ressurskrevende å utvikle nye systemer uten å ta i bruk reelle personopplysninger. Som nevnt over er det viktig at systemutviklingen har høy standard, for å kunne hindre at digitaliseringen av utlendingsforvaltningen bidrar til uriktige avgjørelser i enkeltsaker. Hensynet til å sikre riktige avgjørelser, sammenholdt med ønsket om å ta i bruk digitale systemer som vil kunne redusere saksbehandlingstidene slik at den enkelte får avgjort saken sin innen rimelig tid, er vektige hensyn som taler for at utlendingsmyndighetene gis adgang til å behandle reelle personopplysninger i systemutviklingen av nye IT-systemer.

Utlendingsmyndighetene behandler i dag en rekke personopplysninger, herunder særlige kategorier av personopplysninger som nevnt i personvernforordningen artikkel 9 og 10, i forbindelse med sine lovpålagte oppgaver, jf. også utl. § 83 a. Det klare utgangspunktet er at disse opplysningene innhentes og brukes i forbindelse med den enkelte utlendings sak for utlendingsmyndighetene. Gjenbruk av disse opplysningene til systemutviklingen av nye IT-systemer vil imidlertid kunne bidra til at utlendingsmyndighetene utvikler nye, effektive og trygge systemer. Så lenge det er tilstrekkelig å gjenbruke disse opplysningene for å møte utlendingsforvaltningens behov for data av høy kvalitet, er det med andre ord ikke behov for en egen *innsamlingshjemmel*.

Det kan likevel spørres om hvorvidt det er behov for å eksplisitt regulere utlendingsmyndighetenes adgang til å viderebehandle personopplysninger til utvikling og testing av IT-systemer, herunder KI-systemer. Som nevnt ovenfor i punkt 3.1.7, slår utlf. § 17-7 a andre ledd andre punktum fast at utlendingsmyndighetene kan viderebehandle personopplysninger til nye, *forenlige* formål. Dette betyr at det strengt tatt ikke er nødvendig med en egen hjemmel, så lenge det nye formålet er forenlig med det opprinnelige, jf. også foralepunkt 50 i personvernforordningen, og redegjørelsen i punkt 3.1.2 over. Hvorvidt et nytt formål er forenlig med det opprinnelige, må vurderes i lys av forenlighetstesten i

personvernforordningen artikkel 6 nr. 4. Bestemmelsen inneholder en ikke-uttømmende liste over momenter som det skal legges vekt på:

- «a. enhver forbindelse mellom formålene som personopplysningene er blitt samlet inn for, og formålene med den tiltenkte viderebehandlingen,
- b. i hvilken sammenheng personopplysningene er blitt samlet inn, særlig med hensyn til forholdet mellom de registrerte og den behandlingsansvarlige,
- c. personopplysningenes art, især om særlige kategorier av personopplysninger behandles, i henhold til artikkel 9, eller om personopplysninger om straffedommer og lovovertridelser behandles, i henhold til artikkel 10,
- d. de mulige konsekvensene av den tiltenkte viderebehandlingen for de registrerte,
- e. om det foreligger nødvendige garantier, som kan omfatte kryptering eller pseudonymisering».

Etter departementets syn er det flere momenter som taler for at viderebehandling til utvikling og testing av IT-systemer er forenlig med det opprinnelige formålet. Det er f.eks. en nær sammenheng mellom personopplysninger som innhentes og brukes i forbindelse med saksbehandling og den videre bruken av disse til utvikling og testing av IT-systemer, ved at de digitale systemene skal brukes i tilknytning til utlendingsmyndighetenes lovpålagte oppgaver, herunder saksbehandling av enkeltsaker, jf. artikkel 6 nr. 4 bokstav a. Departementet mener videre at det ikke ligger utenfor det som med rimelighet kan forventes når opplysninger som gis til eller innhentes av utlendingsmyndighetene i forbindelse med behandling av enkeltsaker, også brukes til å forbedre prosesser knyttet til behandling av de samme sakene, herunder utvikling og testing av IT-systemer, jf. artikkel 6 nr. 4 bokstav b.

Til tross for at det er flere momenter som trekker i retning av at viderebehandling til utvikling og testing av IT-systemer er et forenlig formål, finner departementet grunn til å eksplisitt regulere adgangen til viderebehandling. Departementet viser til at i fravær av en særskilt regulering, vil utlendingsmyndighetene i hvert enkelt tilfelle måtte vurdere om viderebehandlingen av de aktuelle personopplysningene vil være forenlig med det opprinnelige formålet. Dette kan fort bli en ressurs- og tidkrevende øvelse, som vil kunne gå på bekostning av utlendingsmyndighetenes øvrige oppgaver. Det er således behov for en særskilt regulering som åpner for viderebehandling til utvikling og testing av IT-systemer, med den følge at utlendingsmyndighetene slipper å foreta en konkret forenlighetsvurdering i den enkelte sak.

Departementet viser videre til hjemmelskravet etter EMK, jf. punkt 3.1.1, og at forslaget åpner for behandling av *særlige kategorier* av personopplysninger, noe som taler for det etableres en egen, særskilt hjemmel for behandling av personopplysninger til utvikling og testing av IT-systemer, herunder systemer basert på KI. Det vises i denne sammenheng også til departementets uttalelser i Prop. 56 LS (2017–2018) pkt. 6.3.2:

«Dersom behandlingen av personopplysninger utgjør et inngrep i retten til privatliv etter Grunnloven § 102 eller EMK artikkel 8, kan det imidlertid være nødvendig med et mer spesifikt rettslig grunnlag for behandlingen enn det ordlyden i forordningen kan tilsi. Det følger også uttrykkelig av fortalepunkt 41 at et rettslig grunnlag bør være «tydelig og presist, og anvendelsen av det bør være forutsigbar for personer som omfattes av det, i samsvar med rettspraksisen til Den europeiske unions domstol («Domstolen») og Den europeiske

menneskerettighetsdomstol». Med andre ord må forordningens krav om supplerende rettsgrunnlag for behandlingen tolkes og anvendes i tråd med de menneskerettslige kravene til rettsgrunnlag for inngrep i retten til privatliv. Dette innebærer at det må foretas en nærmere vurdering av rettsgrunnlaget og behandlingen, hvor det blant annet må legges vekt på hvor inngripende behandlingen er. Etter omstendighetene kan utfallet av en slik vurdering bli at det kreves et mer spesifikt grunnlag enn det som kan synes å være minimumskravene etter ordlyden i forordningen.»

Med bakgrunn i ovenstående drøftelse mener departementet at utlendingsmyndighetene har et klart begrunnet behov for å kunne behandle *innhentede* personopplysninger til utvikling og testing av IT-systemer, herunder KI-systemer, og at det er tjenlig med en egen bestemmelse om dette i utlendingsforskriften, jf. forslag til ny § 17-7 c, se punkt 8 nedenfor.

3.2.3 Krav til nødvendighet og forholdsmessighet

Det fremgår av personvernforordningen artikkel 6 nr. 4 at behandling av personopplysninger til uforenlige formål må utgjøre et «nødvendig og forholdsmessig tiltak i et demokratisk samfunn for å sikre oppnåelse av målene nevnt i artikkel 23 nr. 1». Departementet nevner i denne sammenheng at forslaget om at utlendingsmyndighetene kan viderebehandle personopplysninger til utvikling og testing av IT-systemer, rammes inn av et nødvendighetskriterium og et forholdsmessighetskriterium.

Hva gjelder nødvendighetsvilkåret, understreker departementet at selv om det ikke fremgår direkte av teksten i forslaget til ny forskriftsbestemmelse at det gjelder et krav om nødvendighet, er det ingen tvil om at utlendingsmyndighetene kun kan behandle personopplysninger i den utstrekning dette er nødvendig for å kunne utvikle og teste IT-systemer. Et krav om nødvendighet fremgår dessuten implisitt i kravet om at det må være «umulig eller uforholdsmessig vanskelig å oppnå formålet ved å bruke anonyme eller fiktive opplysninger», jf. forslaget til ny § 17-7 c, se bestemmelsens første ledd. Forslaget til ny forskriftsbestemmelse må uansett tolkes innenfor rammen av den generelle bestemmelsen i utl. § 83 a, som også gir anvisning på et nødvendighetsvilkår.

Når det gjelder det nærmere innholdet i nødvendighetsvilkåret, bemerker departementet at det må gjøres en vurdering av hvilke typer personopplysninger, hvilke datamengder og hvilken grad av identifiserbare opplysninger som er nødvendig for å oppnå formålet, jf. også prinsippet om dataminimering. Dette innebærer bl.a. at det ikke vil være anledning til å behandle personopplysninger dersom det er mulig å utvikle og teste systemet med mindre inngripende virkemidler, herunder anonyme og fiktive opplysninger.

Hva gjelder vilkåret om forholdsmessighet, understreker departementet at det kun vil være adgang til å behandle personopplysninger så lenge det er umulig eller uforholdsmessig vanskelig å bruke anonyme eller fiktive opplysninger til å oppnå formålet. Departementet har i Prop. 36 L (2025–2026) gitt nærmere føringer for innholdet i forholdsmessighetsvilkåret i den tilsvarende bestemmelsen i grenseloven § 22 a. Fra spesialmotivene hitsettes følgende:

«(...) 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.»

Avslutningsvis bemerker departementet at viderebehandling til uforenlige formål må være begrunnet i ett av målene nevnt i artikkel 23 nr. 1 i personvernforordningen. Etter departementets syn vil viderebehandling av personopplysninger til utvikling og testing av IT-systemer falle inn under artikkel 23 nr. 1 bokstav e om viktige mål av generell samfunnsinteresse.

3.2.4 Hvilke personopplysninger kan behandles til utvikling og testing av IT-systemer?

De aller fleste opplysninger som utlendingsmyndighetene i dag behandler, faller inn under personvernforordningen artikkel 9 og 10. I utlendingsforvaltningen behandles det ofte biometriske opplysninger, i tillegg til andre sensitive personopplysninger som religion, helse og seksuell orientering. De deler av IT-systemet som skal behandle slike opplysninger, må testes og utvikles med samme typer opplysninger, hvilket nødvendigvis gjør et behov for å åpne for at utlendingsmyndighetene kan behandle særlige kategorier av personopplysninger i forbindelse med utvikling og testing av slike systemer. Videre bemerker departementet at utlendingsmyndighetene plikter å fremme likestilling og hindre diskriminering iht. likestillings- og diskrimineringsloven § 24. Pliktens innhold er nærmere redegjort for av Likestillings- og diskrimineringsombudet i veilederen om innebygd diskrimineringsvern. Veilederen er skrevet med utgangspunkt i maskinlæringssystemer (KI-systemer), men har også generell overføringsverdi til øvrige IT-systemer som offentlige myndigheter utvikler. På s. 10 i veilederen skriver ombudet at

«det må stilles særlige krav til maskinlæringssystemer som utvikles for eller tas i bruk av offentlig sektor, der systemene kan få betydning for personers rettsstilling. Av den grunn har offentlig sektor et særlig ansvar for å sikre at ML-systemer som utvikles eller tas i bruk, fremmer likestilling og forebygger diskriminering (...).»¹⁴

Utlendingsmyndighetenes avgjørelser har svært stor betydning for enkeltindividene, og det er derfor viktig at ev. IT-systemer som benyttes i saksbehandlingen (f.eks. beslutningsstøttesystemer) ikke fører til usaklig forskjellsbehandling av den som enkeltsaken gjelder. For å hindre slik forskjellsbehandling (bias/skjevheter), kan det i noen tilfeller være nødvendig å behandle særlige kategorier av personopplysninger i systemutviklingsfasen.¹⁵

Departementet har vurdert om det bør fremgå uttrykkelig av forslaget til ny forskriftsbestemmelse at utlendingsmyndighetene har adgang til å behandle

¹⁴ Veilederen er tilgjengelig på [ombudets nettsider](#).

¹⁵ Departementet bemerker i denne sammenheng at EUs forordning om kunstig intelligens ((EU) 2024/1689, KI-forordningen) artikkel 4a (tidligere artikkel 10 nr. 5) etter nærmere angitte vilkår åpner for innhenting av særlige kategorier av personopplysninger for å teste om KI-systemer inneholder skjevheter (bias) som kan føre til diskriminering. Rettsakten er p.t. ikke gjennomført i norsk rett. Forslag til gjennomføring av forordningen ble sendt på [høring 30. juni 2025](#). Som følge av EUs forenklingsprosess, er deler av KI-forordningen justert og den trinnvise innføringen noe utsatt. Digitaliserings- og forvaltningsdepartementet har derfor besluttet å sende ut en [tilleggshøring av KI-loven i høst](#).

personopplysninger som nevnt i personvernforordningen artikkel 9 og 10, jf. prinsippet om åpenhet i artikkel 5 nr. 1 bokstav a, men har kommet til at det ikke er nødvendig med en eksplisitt regulering av dette, da det er klart forutsatt at slike opplysninger vil kunne benyttes i utviklingen og testingen av systemene. Departementet viser i denne sammenheng også til den generelle bestemmelsen i utl. § 83 a, som fastsetter at utlendingsmyndighetene kan behandle særlige kategorier av personopplysninger i sin myndighetsutøvelse og oppgaveløsning. For ordens skyld bemerker departementet at forslaget ikke gir utlendingsmyndighetene *fri* tilgang til å behandle alle typer sensitive personopplysninger som nevnt i artikkel 9 og 10 i personvernforordningen. Kravet til dataminimering innebærer at man skal søke å oppnå formålet med færrest mulig personopplysninger, se også punkt 3.2.3 over.

Avslutningsvis understreker departementet at forslaget til ny forskriftsbestemmelse ikke skal tolkes som en *innhentingshjemmel*. Forslaget er utformet slik at utlendingsmyndighetene kan behandle *innhentede* personopplysninger, hvilket betyr at det kun er adgang til å bruke opplysninger som er blitt lovlig innhentet etter andre regler. Departementet bemerker i denne sammenheng at UDI, UNE og politiet har flere hjemler i ulike sektorlovgivninger, som gir virksomhetene direkte eller indirekte adgang til å innhente og bruke personopplysninger, herunder statsborgerloven, passloven, grenseloven mv. For å begrense personvernkonsekvensene for den enkelte, foreslår departementet at viderebehandlingen av personopplysninger begrenses til opplysninger som virksomhetene har innhentet i relasjon til myndighetsutøvelse eller oppgaver som det aktuelle organet er pålagt etter utlendingsloven og forskrifter gitt med hjemmel i loven. Den praktiske konsekvensen av dette er f.eks. at UDI ikke kan behandle personopplysninger som direktoratet har innhentet eller mottatt i kraft av sin rolle som statsborgermyndighet, jf. statsborgerloven. For ordens skyld presiserer departementet at denne begrensningen ikke er til hinder for at utlendingsmyndighetene behandler opplysninger som de innhenter eller mottar fra andre offentlige virksomheter, f.eks. Skatteetaten, så lenge opplysningene er innhentet eller mottatt i kraft av organets rolle som utlendingsmyndighet. Departementet mener at denne begrensningen av pedagogiske grunner bør fremkomme uttrykkelig i utlendingsregelverket, se forslag til ny § 17-7 c første ledd i punkt 8 nedenfor.

3.2.5 Konsekvenser for den enkeltes grunnleggende rettigheter, herunder personvernkonsekvenser

Forslaget om en egen hjemmel for utvikling og testing av IT-systemer gir, som nevnt over, utlendingsmyndighetene adgang til å viderebehandle særlige kategorier av personopplysninger til dette formålet. Personvernkonsekvensene ved en ev. uberettiget behandling av personopplysninger som nevnt i personvernforordningen artikkel 9 og 10 er generelt større sammenlignet med alminnelige personopplysninger, og risikoen for uberettiget behandling øker når opplysningene viderebehandles til nye formål.

For å kunne begrense de personvernmessige ulempene for de registrerte, foreslår departementet å fastsette i forskrift at tilgang til personopplysninger etter bestemmelsen kun skal gis til personer som er særskilt bemyndiget. Dette vil kunne hindre at flere personer enn nødvendig gis tilgang til sensitive personopplysninger. Bemyndigelse skal gis av den som er behandlingsansvarlig.

De nærmere vilkårene for når slik bemyndigelse kan gis, lar departementet være opp til de enkelte virksomhetene å avgjøre. Departementet vil likevel understreke at tilgang kun bør gis til personer som har et klart begrunnet behov for slik tilgang. Se forslaget til § 17-7 c tredje ledd i forskriften, jf. punkt 8 nedenfor.

Videre foreslår departementet å fastsette i forskrift at personopplysninger som behandles etter bestemmelsen, ikke skal oppbevares lenger enn det som er nødvendig for formålet, jf. også prinsippet om lagringsbegrensning i personvernforordningen artikkel 5 nr. 1 bokstav e. Dette innebærer at utlendingsmyndighetene plikter å slette personopplysningene når det ikke lenger er nødvendig å behandle disse til utvikling og testing av IT-systemer. For ordens skyld understreker departementet at sletteplikten ikke skal tolkes dithen at personopplysningene skal slettes dersom de fremdeles er nødvendige for og kan behandles til andre formål, for eksempel som ledd i behandlingen av utlendingssaken.¹⁶ Se forslaget til § 17-7 c andre ledd, jf. punkt 8 nedenfor.

Departementet har for øvrig vurdert om det bør gjøres begrensninger i hvilke sakstyper (saker om beskyttelse, tilbakekall mv.) som det kan viderebehandles personopplysninger fra, men har kommet til at det ikke er hensiktsmessig, ei heller praktisk mulig med en slik begrensning. Departementet ser at det er en risiko for at viderebehandling av personopplysninger som har direkte eller indirekte utspring fra intervju i sak om beskyttelse (asylintervju) vil kunne ha en nedkjølende effekt for asylsøkere, herunder at asylsøkere unnlater å forklare seg om beskyttelsesbehovet av frykt for at en større, og for dem ukjent, personkrets får tilgang til opplysningene. For å kunne utvikle og teste IT-systemer som skal brukes til gjennomføring av asylintervjuer, vil det imidlertid i noen tilfeller være nødvendig å nettopp behandle opplysninger fra asylintervjuer. Det er derfor ikke aktuelt å avskjære utlendingsmyndighetene fra å bruke personopplysninger fra asylintervjuer.

Selv om det ikke er aktuelt å avskjære utlendingsmyndighetene fra å viderebehandle personopplysninger fra asylintervjuer, har departementet vurdert om det kan fastsettes særlige tiltak som kan begrense inngrepet i rettssfæren, f.eks. et krav om at utlendingsmyndighetene må innhente samtykke fra den registrerte etter at saken der asylintervjuet ble gjennomført er endelig avgjort. Departementet har likevel kommet til at en slik begrensning i realiteten har liten effekt. Det vil være uforholdsmessig vanskelig, og i noen tilfeller umulig, å holde opplysninger som innhentes fra asylintervjuer adskilt fra øvrige opplysninger i samme sak. For eksempel kan det tenkes tilfeller der UDI velger å gjøre ytterligere undersøkelser på bakgrunn av det asylsøkeren har forklart seg om i intervjuet; dette er undersøkelser som trolig ikke hadde vært igangsatt uten et forutgående asylintervju. Opplysningene fra disse undersøkelsene vil lagres på saken i datasystemet for utlendings- og flyktningssaker (DUF), uten at det er åpenbart for andre enn saksbehandler selv at opplysningene har en kobling til et forutgående asylintervju. Dette innebærer at i tilfeller der den registrerte ikke samtykker til at personopplysninger fra asylintervjuet brukes til utvikling og testing av IT-systemer, vil det likevel være en ikke-ubetydelig risiko for at det indirekte benyttes personopplysninger fra asylintervjuet når utlendingsmyndighetene innhenter personopplysninger fra beskyttelsessakens øvrige dokumenter.

¹⁶ For eksempel er det ikke ment å gjøre unntak fra slettefristen for biometriske opplysninger i utlf. § 18-4.

Avslutningsvis legger departementet til grunn at utlendingsmyndighetene behandler samtlige personopplysninger iht. reglene i personvernforordningen artikkel 32, og at de behandlingsansvarlige i hver organisasjon gjennomfører egnede tekniske og organisatoriske tiltak for å sikre personvernet, jf. artikkel 24.

3.2.6 Behandlingsansvar mv.

Forslaget til ny bestemmelse om behandling av innhentede personopplysninger til utvikling og testing av IT-systemer, herunder systemer basert på KI, gjelder som nevnt i punkt 3.2.1 for «utlendingsmyndighetene», herunder UDI, UNE og politiet. Felles for aktørene i utlendingsforvaltningen er at de benytter mange av de samme systemene i sin oppgaveløsning etter utlendingsloven, herunder systemer som DUF og Passweb, hvilket aktualiserer spørsmål om behandlingsansvar.

Departementet foreslår ikke her egne regler om behandlingsansvar for personopplysninger som skal viderebehandles til utvikling og testing av IT-systemer. I stedet vil gjeldende regelverk for behandlingsansvar komme til anvendelse på utlendingsmyndighetenes behandling av personopplysninger til dette formålet. Dette betyr at ved uttak av personopplysninger i f.eks. Utlendingsdatabasen, vil behandlingsansvaret reguleres av utlf. § 17-7 b.

Når det gjelder de nærmere grensene for behandlingsansvaret, bemerker departementet at det at en virksomhet har behandlingsansvar for selve systemløsningen, ikke er til hinder for at andre aktører har et selvstendig, formålsoverordnet behandlingsansvar, så lenge den aktuelle bestemmelsen som regulerer behandlingsansvaret åpner for dette. Til illustrasjon vises det til utlf. § 17-7 b, som bl.a. regulerer behandlingsansvaret for Utlendingsdatabasen. Bestemmelsen må tolkes dithen at UDI er behandlingsansvarlig for registeret som sådan (systemansvarlig), jf. andre ledd, mens den enkelte aktør i utlendingsforvaltningen har et selvstendig behandlingsansvar for behandling som skjer for «egne formål», jf. første ledd. Som behandlingsansvarlig for Utlendingsdatabasen vil UDI ha ansvaret for den tekniske og praktiske forvaltningen og driften av databasen og systemet. Direktoratet har også et overordnet ansvar for at behandlingen av opplysningene i databasen skjer i samsvar med gjeldende regelverk. Politiet og UNE vil på sin side anses som behandlingsansvarlige for personopplysninger de behandler for *egne formål*. Et selvstendig, formålsoverordnet behandlingsansvar innebærer at den enkelte aktør har et ansvar for å sikre personvernet i egen organisasjon og for å sikre at behandling av personopplysninger i og fra databasen skjer på lovlig måte.

Avslutningsvis bemerker departementet at dersom et behandlingsansvarlig forvaltningsorgan benytter en ekstern databehandler, skal forholdet mellom de to virksomhetene reguleres i en avtale, jf. personvernforordningen artikkel 28 nr. 3 første punktum.

3.2.7 Unntak fra taushetsplikten

3.2.7.1 Taushetsplikten som skranke for deling av opplysninger til utvikling og testing av IT-systemer

Som nevnt i punkt 3.1.3 over, vil taushetsplikten kunne sette enkelte begrensninger i adgangen til å viderebehandle personopplysninger som er taushetsbelagte. Det følger av fvl. § 13 f andre ledd at bestemmelse i annen lov om

rett eller plikt til å gi opplysninger ikke begrenser lovbestemt taushetsplikt, med mindre vedkommende bestemmelse fastsetter eller klart forutsetter at taushetsplikten ikke skal gjelde.

Brorparten av de personopplysninger som utlendingsmyndighetene har innhentet i forbindelse med saksbehandling og annen myndighetsutøvelse, er taushetsbelagte opplysninger iht. fvl. §§ 13 flg. Taushetsplikten gjelder også internt i samme organ, hvilket betyr at det ikke er fritt frem å utveksle taushetsbelagte personopplysninger internt i samme virksomhet, til det formål å utvikle og teste IT-systemer.

Det er imidlertid fastsatt begrensninger i taushetsplikten, jf. fvl. §§ 13 a flg. Av særlig interesse i saker der forvaltningen ønsker å viderebehandle taushetsbelagte personopplysninger til utvikling og testing av IT-systemer, er unntaket i § 13 b første ledd nr. 3.¹⁷ Etter bestemmelsen er taushetsplikten ikke til hinder for at

«opplysningene er tilgjengelig for andre tjenestemenn innen organet eller etaten i den utstrekning som trengs for en hensiktsmessig arbeids- og arkivordning, bl.a. til bruk ved vegledning i andre saker.»

En alminnelig språklig forståelse av bestemmelsen tilsier at taushetsplikten ikke utgjør en skranke for at opplysninger gjøres tilgjengelig for andre tjenestepersoner i virksomheten så langt det er nødvendig for at forvaltningsorganet skal kunne arbeide funksjonelt og godt, herunder sikre alminnelig drift.

I litteraturen er det imidlertid gitt uttrykk for at bestemmelsens rekkevidde er noe uklar.¹⁸ På denne bakgrunn finner departementet grunn til å kommentere det nærmere innholdet i bestemmelsen, især bestemmelsens forhold til utvikling og testing av IT-systemer.

3.2.7.2 Er konsulenter «tjenestemenn»?

Et første usikkerhetsmoment ved bestemmelsen er personangivelsen; det er kun adgang til å dele opplysninger med andre «tjenestemenn». Det kan ved første øyekast oppfattes som noe uklart om det med «tjenestemenn» siktes til «offentlig tjenestemann» slik dette er definert i fvl. § 2 første ledd bokstav d, eller om uttrykket skal forstås videre enn legaldefinisjonen. Forvaltningsloven § 2 første ledd bokstav d definerer en «offentlig tjenestemann» som en «embetsmann eller annen som er ansatt i statens eller en kommunes tjeneste». Etter ordlyden omfattes altså enhver person i *offentlig tjeneste*, herunder utviklere ansatt i organets IT-avdeling, mens ekstern arbeidskraft, typisk innleide arbeidstakere og oppdragstakere, faller utenfor.

Departementet mener at uttrykket «tjenestemenn» i fvl. § 13 b første ledd nr. 3 må omfatte enhver som utfører tjeneste eller arbeid for et forvaltningsorgan, herunder innleide arbeidstakere og oppdragstakere, og viser til begrunnelsen nedenfor.

Det er for det første intet i forarbeidene til gjeldende forvaltningslov som tilsier at man med begrepet «tjenestemenn» hadde til hensikt å avgrense mot innleide arbeidstakere, oppdragstakere eller andre som utfører tjeneste eller arbeid for et forvaltningsorgan. Dersom uttrykket «tjenestemenn» forstås likt som «offentlig tjenestemann» i fvl. § 2 første ledd bokstav d, vil dette kunne begrense forvaltningens mulighet til å bruke innleid personell til hensiktsmessig drift av

¹⁷ Bestemmelsen videreføres i ny forvaltningslov, jf. ny forvaltningslov § 34 første ledd bokstav e.

¹⁸ Se til illustrasjon Ejfestad og Selman (2021).

organet. Departementet kan ikke se at en slik avgrensning har vært tiltenkt fra lovgivers side.

Ved fastleggelsen av innholdet i en bestemmelse vil det også være aktuelt å se hen til formålet med regelen og loven som sådan. Gjeldende forvaltningslov har ingen formålsbestemmelse. Forhistorien viser likevel at formålet med loven var å gi betryggende regler for forvaltningens virksomhet, og at hensynet til rettssikkerhet sto sentralt.¹⁹ Forvaltningslovens regler om taushetsplikt skal bidra til å sikre befolkningens tillit til forvaltningen, ved å bl.a. beskytte parts- eller klientinteresser, jf. Ot.prp. nr. 3 (1976-1977) punkt 3.2.1 s. 13. Departementet kan ikke se at rettssikkerhetshensyn, ei heller behovet for hemmelighold, taler mot at innleide arbeidstakere og oppdragstakere omfattes av unntaket i fvl. § 13 b første ledd nr. 3, og viser her til at enhver person som utfører tjeneste eller arbeid for et forvaltningsorgan uansett vil være underlagt den samme taushetsplikten som organets egne ansatte, jf. fvl. § 13 første ledd, jf. også Ot.prp. nr. 3 (1976-1977) der Justis- og politidepartementet uttaler at den vide personangivelsen i fvl. § 13 første ledd i

«det vesentlige dekker behovet for hemmelighold også når opplysningene er gitt videre i medhold av § 13 b».

Også systembetragtninger taler for at innleide arbeidstakere og oppdragstakere omfattes av uttrykket «tjenestemenn» i fvl. § 13 b første ledd nr. 3. Departementet viser her til at den vide personangivelsen i fvl. § 13 første ledd gjør at også innleide arbeidstakere og oppdragstakere omfattes av de samme regler om taushetsplikt som organets egne ansatte. Systembetragtninger taler for at når en gruppe først omfattes av reglene om taushetsplikt, må den samme gruppen følgelig kunne motta taushetsbelagte opplysninger. Noe annet vil medføre at den vide personangivelsen i fvl. § 13 b første ledd får liten praktisk betydning.

Med bakgrunn i ovenstående tolkning mener departementet at innleide arbeidstakere og oppdragstakere, herunder konsulenter, må omfattes av uttrykket «tjenestemenn» i fvl. § 13 første ledd nr. 3.

3.2.7.3 Inngår utvikling og testing av IT-systemer i forvaltningsorganets «arbeids- og arkivordning»?

En alminnelig språklig forståelse av «arbeids- og arkivordning» tilsier at delingen av opplysningene er nødvendig for å ivareta alminnelig drift av virksomheten. Det fremgår ikke av ordlyden om utvikling og testing av IT-systemer omfattes av unntaket.

Departementet bemerker at samtlige forvaltningsorganer i dag benytter IT-systemer som ledd i sin oppgaveløsning, og at teknologien i mange tilfeller er helt nødvendig for at organet skal kunne oppfylle sitt samfunnsmandat. For eksempel vil feil og nedetider i et forvaltningsorgans IT-system kunne påvirke organets evne til å opprettholde alminnelig drift. Når IT-systemer benyttes av et stort antall forvaltningsorganer og utgjør en helt grunnleggende del av infrastrukturen i offentlig sektor, er det etter departementets syn lite tvil om at et velfungerende IT-system er nødvendig for en hensiktsmessig «arbeids- og arkivordning». I den grad bruk av taushetsbelagte opplysninger er nødvendig for å utvikle og teste disse

¹⁹ Se her Prop. 79 L (2024-2025) punkt 4.4.1 på side 42.

systemene, må det etter departementets syn være riktig fortolkning at delingen omfattes av begrensningen i fvl. § 13 b første ledd nr. 3.²⁰

Departementet viser videre til at gjeldende forvaltningslov ble vedtatt på 1960-tallet, og at forvaltningens arbeidsform og organisering har endret seg betraktelig siden den gang. Etter departementets syn må det ved tolkningen av fvl. § 13 b første ledd nr. 3 legges vekt på samfunnsutviklingen, herunder endringer i arbeidsform og -metodikk i offentlig sektor. Departementet finner støtte for dette i forhistorien til gjeldende forvaltningslov, som understreker at saksbehandlingsreglene ikke bare skal ivareta rettssikkerhetssyn, men også fremme en *effektiv saksbehandling*.²¹ Etter hvert som tiden går vil forvaltningen få tilgang til nye og bedre virkemidler, som vil kunne bidra til en mer effektiv saksbehandling enn tidligere. Fremveksten av ny teknologi, herunder IT-systemer, er et eksempel på dette. Forvaltningsloven § 13 b første ledd nr. 3 kan ikke tolkes slik at den innskrenker forvaltningens mulighet til å ta i bruk nye, trygge og innovative hjelpemidler i sin oppgaveløsning.

Med bakgrunn i vurderingen i punkt 3.2.7.2 og 3.2.7.3, mener departementet at det er adgang til å dele taushetsbelagte opplysninger til det formål å utvikle og teste IT-systemer i forvaltningen, og at opplysningene også kan deles med innleide arbeidstakere og oppdragstakere, herunder konsulenter.

3.2.7.4 Forholdet til ny forvaltningslov

Forslaget om å behandle personopplysninger, inkludert taushetsbelagte opplysninger, til utvikling og testing av IT-systemer i utlendingsforvaltningen skal også gjelde når gjeldende forvaltningslov erstattes med lov 20. juni 2025 nr. 81 (ny forvaltningslov). Departementet bemerker i denne sammenheng at § 13 b første ledd nr. 3 i gjeldende lov i all hovedsak er videreført i ny lov i § 34 første ledd bokstav e. Sistnevnte bestemmelse lyder:

«§ 34. Unntak fra taushetsplikt og deling av personopplysninger

(1) Taushetsplikten etter §§ 31 og 32 er ikke til hinder for

[...]

e. at opplysninger deles innenfor forvaltningsorganet eller etaten så langt det er nødvendig for veiledning eller til bruk i saker innenfor samme eller tilknyttede fagfelt, eller til bruk ved arkivering, utsending av vedtak og tilsvarende praktiske gjøremål

[...]»

Etter departementets syn utgjør ny forvaltningslov § 34 første ledd bokstav e et tilstrekkelig unntak fra taushetsplikten hva gjelder behandling av taushetsbelagte opplysninger til utvikling og testing av IT-systemer, slik at det ikke er behov for endringer i regelverket når ny lov settes i kraft. Departementet viser i denne sammenheng til vurderingen nedenfor:

I motsetning til gjeldende forvaltningslov § 13 b første ledd nr. 3, er ikke ny forvaltningslov § 34 første ledd bokstav e begrenset til «tjenestemenn» i organet.

²⁰ For sammenhengens skyld bemerkes det at Lovavdelingen i Justis- og beredskapsdepartementet i en tolkningsuttalelse fra 2004 og 1995 har gitt uttrykk for en vid fortolkning av uttrykket, hvilket også underbygger at utvikling og testing av IT-systemer omfattes av fvl. § 13 b første ledd nr. 3.

²¹ Prop. 79 L (2024-2025) punkt 4.4.1 på side 42.

Det betyr at også innleide arbeidstakere og oppdragstakere omfattes av bestemmelsens virkeområde.

Selv om det ikke fremgår av ordlyden at utvikling og testing av IT-systemer dekkes av bestemmelsen, bemerker departementet at unntaket i § 34 første ledd bokstav e skal legges til rette for en hensiktsmessig oppgaveløsning innad i organer og mellom organer i samme etat, og at den derfor oppstiller en *vid* delingsadgang, jf. spesialmotivene til bestemmelsen. Ettersom bestemmelsen i all hovedsak er en videreføring av gjeldende forvaltningslov § 13 b første ledd nr. 3, vil også vurderingen gjort under punkt 3.2.7.3 være av overføringsverdi til den tilsvarende bestemmelsen, § 34 første ledd bokstav e, i ny lov. Departementet viser her til at gjennomgangen i nevnte punkt klart slår fast at utvikling og testing av IT-systemer dekkes av begrensningen inntatt i gjeldende lov § 13 b første ledd nr. 3, og dermed også av unntaket inntatt i ny lov § 34 første ledd bokstav e.

For øvrig bemerker departementet at ny forvaltningslov § 34 annet ledd fastsetter at taushetsbelagte opplysninger om noens personlige forhold ikke kan deles dersom delingen vil kunne utgjøre et uforholdsmessig inngrep overfor den opplysningene gjelder. Bestemmelsen er ment som en sikkerhetsventil for å fange opp særlige tilfeller der opplysningene likevel ikke bør deles i det konkrete tilfellet. Den praktiske konsekvensen av regelen er at det i det enkelte tilfellet må gjøres en konkret forholdsmessighetsvurdering av om de taushetsbelagte opplysningene kan deles, selv om ett eller flere av vilkårene i første ledd er oppfylt.

I likhet med ny forvaltningslov § 34 andre ledd inneholder også den foreslåtte hjemmelen om utvikling og testing av IT-systemer i utlendingsforvaltningen et krav om forholdsmessighet, hvilket aktualiserer et spørsmål om forholdet mellom de to. Når det gjelder forholdsmessighetsvurderingen etter ny forvaltningslov § 34 andre ledd, bemerker departementet at denne vurderingen har flere likhetstrekk med forenlighetsvurderingen som gjøres etter personvernforordningen, jf. også spesialmotivene til bestemmelsen, hvor det fremgår at det i forholdsmessighetsvurderingen blant annet kan legges vekt på «i hvilken grad delingen kan ha sammenheng med det opprinnelige innsamlingsformålet» og at det i første rekke er ved «deling til helt andre formål enn de opprinnelige innsamlingsformålene, hvor begrensningen [i § 34 annet ledd] kan tenkes å komme til anvendelse». Slik departementet ser det, vil deling av taushetsbelagte opplysninger til utvikling og testing av IT-systemer som det klare utgangspunkt være forholdsmessig, jf. også forenlighetsvurderingen i punkt 3.2.2 over. Departementet ser likevel ikke bort fra at det i noen få tilfeller kan være uforholdsmessig å dele taushetsbelagte opplysninger til det formål å utvikle og teste IT-systemer. Dette vil imidlertid i første rekke gjelde i situasjoner der det er praktisk og teknisk mulig å utvikle og teste IT-systemene uten bruk av taushetsbelagte opplysninger, for eksempel gjennom anonymiserte opplysninger. Slike tilfeller vil uansett fanges opp av det tilsvarende kravet til forholdsmessighet i den foreslåtte bestemmelsen i utlendingsforskriften, som fastsetter at det kun er adgang til å bruke personopplysninger i systemutviklingen dersom det vil være «umulig eller uforholdsmessig vanskelig» å oppnå formålet ved å bruke anonyme eller fiktive opplysninger. Forholdsmessighetsvilkåret i ny forvaltningslov § 34 andre ledd har således liten praktisk og selvstendig betydning ved siden av det tilsvarende vilkåret i utlendingsforskriften.

Departementet gjør videre oppmerksom på at § 34 tredje ledd i ny forvaltningslov fastsetter at bestemmelsene i første ledd, herunder § 34 første ledd bokstav e, gir hjemmel for deling av personopplysninger, inkludert personopplysninger omfattet av personvernforordningen artikkel 9 og 10, se også punkt 3.2.4 over.

Med bakgrunn i vurderingen her, mener departementet at ny forvaltningslov § 34 første ledd bokstav e utgjør en tilstrekkelig begrensning i taushetsplikten, med den følge at taushetsbelagte opplysninger kan benyttes til utvikling og testing av IT-systemer, også når ny forvaltningslov settes i kraft.

3.2.8 Forholdet mellom forordningen om kunstig intelligens og utlendingsregelverket

KI-forordningen ((EU) 2024/1689) er det første helhetlige regelverket for KI, og fastsetter bl.a. regler for utvikling og bruk av teknologien. Det pågår et arbeid med å innlemme rettsakten i EØS-avtalen, og det tas sikte på å gjennomføre forordningen i norsk rett gjennom den såkalte «KI-loven».

Den kommende KI-loven vil legge premisser for testing, risikoklassifisering og tilsyn med KI-systemer på tvers av forvaltningen, og med det utgjøre grunnpilaren for regelverket om KI. En naturlig følge av dette er at loven vil regulere KI-virksomhet i utlendingsforvaltningen. Dette er likevel ikke til hinder for at det fastsettes presiserende regler i nasjonal rett, f.eks. sektorspesifikke regler om utvikling og testing av KI-systemer. Det må likevel gjøres en konkret vurdering av det nasjonale handlingsrommet for de ulike delene av KI-forordningen; på enkelte felt er det lite tvil om at rettsakten åpner for et nasjonalt handlingsrom mens på andre felt er det ikke like åpenbart.²²

Forslaget til ny bestemmelse om utvikling og testing av IT-systemer, herunder systemer basert på KI, i utlendingsforskriften, vil utgjøre en del av det *sektorspesifikke* regelverket om KI. Bestemmelsen må leses i lys av KI-forordningen og den kommende KI-loven, og tolkes innenfor rammen av det horisontale rammeverket for KI. Ved ev. motstrid vil KI-lovens regler måtte gis forrang over den sektorspesifikke regelen.

Departementet bemerker videre at når KI-loven er på plass, vil KI-forordningens regler om *risikoklassifisering* kunne få direkte betydning for utlendingsforvaltningens utvikling og testing av KI-systemer.²³ Rettsakten har en risikobasert tilnærming til regulering av KI; jo høyere risikoen er for at KI-systemet griper inn i grunnleggende rettigheter og friheter, desto strengere er reglene. Av særlig interesse for utlendingssektoren, er KI-forordningens regulering av såkalte *høyrisikosystemer*, se bestemmelsene inntatt i KI-forordningen kapittel III. Departementet påpeker i denne sammenheng at KI-systemer som utvikles av utlendingsmyndighetene etter omstendighetene vil kunne omfattes av KI-forordningens definisjon av høyrisikosystem, jf. rettsaktens vedlegg III nr. 7, jf. artikkel 6 nr. 2. Hva gjelder forholdet mellom den foreslåtte bestemmelsen i utlendingsforskriften om utvikling og testing av IT-systemer og KI-forordningens

²² Det nærmere valget av markedstilsynsmyndighet og meldermyndighet, er et eksempel på et område der forordningen gir et nasjonalt handlingsrom. Valget av myndighet må tilpasses norsk forvaltningsstruktur og tilsvarende organisatoriske forhold.

²³ For ordens skyld bemerker departementet at selv om KI-forordningen p.t. ikke er gjennomført i norsk rett, vil eksisterende regelverk, herunder personvernregelverket, gjelde ved utvikling og testing av KI-systemer.

risikobaserte tilnærming til KI-systemer, bemerker departementet at den foreslåtte bestemmelsen i utlendingsforskriften ikke er ment å rokke ved de plikter som utlendingsmyndighetene har i kraft av rollen som operatør (leverandør eller idriftsetter) iht. KI-forordningen. Det betyr at utlendingsmyndighetene ved utviklingen og testingen av et KI-system, må vurdere om det aktuelle systemet faller inn under KI-forordningens definisjon av høyrisiko. Hvis systemet vurderes som høyrisiko, må utlendingsmyndighetene etterleve de krav som gjelder for slike systemer, jf. forordningens kapittel III, da forordningen gjelder på tvers av forvaltningen og utgjør en del av det horisontale rammeverket for utviklingen og testingen av KI-systemer.

3.2.9 Særlig om IT-systemer som behandler personopplysninger til delvis politimessige formål og delvis forvaltningsmessige formål

Det fremgår av politiregisterforskriften § 1-3 nr. 3 at politiregisterloven, jf. § 3, vil gjelde for personopplysninger som behandles i et sentralt register, jf. politiregisterloven § 14, all den tid behandlingen skjer delvis til politimessige og delvis til forvaltningsmessige formål.

Den foreslåtte bestemmelsen i utlf. ny § 17-7 c om utvikling og testing av IT-systemer omfatter ikke utvikling og testing av systemer som *utelukkende* har et politimessig formål. Utvikling og testing av slike systemer må følge aktuelle regler i politiregisterloven, ev. supplert av politiregisterforskriften. For systemer som behandler personopplysninger til delvis forvaltningsmessige og delvis politimessige formål vil den foreslåtte bestemmelsen i utlendingsforskriften kun gjelde for utvikling og testing av den delen av systemet som behandler personopplysninger til forvaltningsmessige formål. Implisitt innebærer dette at det må være mulig å skille utviklingen og testingen av den forvaltningsmessige delen av systemet klart fra den delen av systemet som behandler personopplysninger til politimessige formål.

4 Kompetanse til å beslutte opptak av fingeravtrykk og ansiktsbilde etter Eurodac-forordningen 2024

4.1 Eurodac-forordningen 2024

Eurodac (European Dactyloscopy System) er en database for EUs medlemsland, Sveits, Liechtenstein, Island og Norge, der det lagres fingeravtrykk og enkelte andre opplysninger om personer som søker internasjonal beskyttelse (asyl) eller som blir pågrepet for irregulær grensepassering til EU/Schengen-området. Hensikten er å tilrettelegge for sammenlikning av fingeravtrykk for å identifisere asylsøkere, og for å fastsette hvilken medlemsstat som er ansvarlig for å behandle en søknad om internasjonal beskyttelse etter Dublin-regelverket. Rettshåndhevende myndigheter har også på bestemte vilkår mulighet til å søke i databasen som ledd i å forebygge, avdekke eller etterforske terrorisme og andre alvorlige straffbare handlinger.

4.2 Gjeldende rett

Det fremgår ikke eksplisitt av gjeldende utlendingslov og -forskrift hvilke nasjonale myndigheter som har kompetanse til å oppta fingeravtrykk og

ansiktsbilde etter Eurodac-forordningen. Dette er i motsetning til utlf. § 18-1 tredje ledd, som fastsetter at det for *nasjonale formål* er «Utlendingsdirektoratet, politiet, norsk utenrikstjeneste eller ekstern tjenesteyter i henhold til avtale etter [utlendingsforskriften] § 10-2 fjerde ledd», som kan utføre opptak av ansiktsbilde og fingeravtrykk. I Prop. 37 LS (2025–2026) har departementet lagt til grunn at regler om opptak av biometriske opplysninger til nasjonale formål også vil gjelde ved behandling av tilsvarende opplysninger i Eurodac. Fra nevnte proposisjon punkt 6.14.4 siteres følgende fra side 40:

«Ved eventuell motstrid mellom Eurodac-forordningen 2024 og de generelle reglene i utlendingsloven § 100 med tilhørende forskriftsbestemmelser, vil reglene som fremgår av Eurodac-forordningen 2024, jf. utlendingsloven § 101 med tilhørende forskriftsbestemmelser, gå foran de øvrige og generelle reglene i utlendingsloven og -forskriften, jf. § 100 fjerde ledd, jf. også utlendingsforskriften § 18-1 niende ledd. Dette innebærer at i tilfeller der Eurodac-forordningen 2024 ikke gir tilstrekkelig veiledning om et spørsmål, for eksempel om nasjonale ansvarsforhold, vil de generelle reglene i utlendingsloven og -forskriften komme supplerende til anvendelse.»

Ettersom gjeldende utlendingslov og -forskrift er tause om hvilke nasjonale myndigheter som har kompetanse til å beslutte opptak av biometriske opplysninger etter Eurodac-forordningen, vil den generelle reguleringen i utlf. § 18-1 tredje ledd komme supplerende til anvendelse.

4.3 Departementets forslag og vurdering

I Prop. 37 LS (2025–2026) uttaler departementet at det kan bli aktuelt å vurdere en forskriftsfesting av hvilke nasjonale myndigheter som skal kunne beslutte samt gjennomføre opptak av biometriske opplysninger etter Eurodac-forordningen 2024.

Etter departementets syn er det ikke strengt nødvendig å uttrykkelig fastsette dette i forskrift, all den tid utlf. § 18-1 tredje ledd kommer supplerende til anvendelse. Likevel ser departementet at det av pedagogiske grunner kan være formålstjenlig med en tydelig og særskilt regulering i forskrift. Departementet viser også til at ny Eurodac-forordning 2024 utvider formålet med Eurodac, og at det derfor er en ikke-ubetydelig risiko for at reguleringen i utlf. § 18-1 tredje ledd er for generell til å dekke det behovet som nå gjør seg gjeldende. På denne bakgrunn foreslås det en egen bestemmelse for opptak av biometriske opplysninger etter Eurodac-forordningen, se forslaget til regulering i utlf. § 18-7 i punkt 8 nedenfor.

Videre vurderer departementet om også UNE bør gis adgang til å *beslutte* opptak av biometriske opplysninger etter Eurodac-forordningen 2024; nemnda har ikke slik kompetanse i dag. Departementet utelukker ikke at det kan oppstå enkelttilfeller der UNE konkluderer med at registreringen i Eurodac er feil eller av tvilsom karakter, og at det derfor er behov for nytt opptak. Av hensyn til nemndas særlige rolle som et uavhengig klageorgan i utlendingsforvaltningen, samt av praktiske og ressursmessige grunner, er det ikke tjenlig å gi UNE myndighet til å også *utføre* opptaket av biometri. Et ev. opptak bør i slike tilfeller gjennomføres av politiet, som har bred operativ erfaring med gjennomføringen av biometriopptak. UNEs beslutning om opptak vil derfor i praksis innebære at utlendingen må møte hos politiet, slik at det kan innhentes biometriske opplysninger fra vedkommende. For å sikre en hensiktsmessig prosess for alle involverte aktører, herunder

utlendingen, bør UNE og politiet etablere gode rutiner for hvordan nemndas beslutninger om opptak av biometri rent praktisk skal følges opp. Departementet viser ellers til forslaget til regulering i ny § 18-7 første ledd andre punktum, se punkt 8 nedenfor.

I tillegg til å forskriftsfeste en egen bestemmelse om opptak av biometriske opplysninger etter Eurodac-forordningen 2024, foreslår departementet enkelte mindre justeringer i den tilsvarende bestemmelsen for nasjonale formål, utlf. § 18-1 tredje ledd. Det fremgår ikke klart av bestemmelsens ordlyd at utlendingsmyndighetene har kompetanse til å *beslutte* opptak av ansiktsbilde og fingeravtrykk. Slik bestemmelsen lyder i dag, har utlendingsmyndighetene kun adgang til å *oppta* biometriske opplysninger, og ikke nødvendigvis å beslutte selve opptaket. Det er likevel klart forutsatt i bestemmelsen, og i praksis, at myndigheten til å oppta biometri også omfatter kompetanse til å beslutte selve opptaket. Departementet mener likevel at det av hensyn til et klart og tilgjengelig utlendingsregelverk bør komme tydeligere frem at utlendingsmyndighetene også har kompetanse til å beslutte opptak av ansiktsbilde og fingeravtrykk.

Et skille mellom kompetanse til å beslutte samt utføre opptak av biometriske opplysninger er også nødvendig for å synliggjøre at ekstern tjenesteyter, jf. utlf. § 10-2 fjerde ledd, ikke har kompetanse til å *beslutte* opptak av biometriske opplysninger. En ekstern tjenesteyter har kun myndighet til å *gjennomføre* opptak etter avtale med aktuell fagmyndighet. Departementet ser det som hensiktsmessig å tydeliggjøre i forskrift at eksterne tjenesteytere *ikke* har slik beslutningskompetanse. Forslaget om å justere utlf. § 18-1 tredje ledd er ikke ment å innebære noen realitetsendring. Se forslag til endring av forskriftsbestemmelsen i punkt 8 nedenfor.

5 Oppheving av den registrertes klageadgang etter Eurodac-forordningen 2024

5.1 Gjeldende rett

Utlendingsforskriften § 18-7 gir regler om klageadgang etter Eurodac-forordningen 2024, og lyder:

«Den registrerte kan påklage avgjørelse om innsyn, retting, sletting eller erstatning. Klage fremsettes for den behandlingsansvarlige, jf. § 18-5, som forbereder og oversender klagen til departementet for avgjørelse.»

Gjeldende utforming av utlf. § 18-7 ble tilføyd i endringsforskrift 12. juni d.å.²⁴ Bestemmelsen gir den registrerte adgang til å påklage avgjørelser om ovennevnte sakstyper og fastsetter at en ev. klage skal fremsettes for den behandlingsansvarlige, som sender denne videre til departementet for endelig avgjørelse.

Rett til innsyn, retting, sletting og erstatning følger av Eurodac-forordningen 2024 artikkel 43 og 52. I tillegg følger det av personvernforordningen artikkel 12 at den behandlingsansvarlige plikter å legge til rette for at den registrerte kan utøve sine

²⁴ [Forskrift om endringer i utlendingsforskriften \(gjennomføring av relevante deler av Eurodac-forordningen 2024, forordning om asyl- og migrasjonshåndtering og kriseforordningen\)](#).

Bestemmelsen ble i endringsforskriften flyttet fra utlf. § 18-11 til § 18-7, samtidig som det ble gjort noen mindre justeringer av hensyn til en hensiktsmessig klageordning.

rettigheter iht. artikkel 15 til 22, herunder retten til innsyn (artikkel 15), retting (artikkel 16) og sletting (artikkel 17). Rett til erstatning følger for øvrig av artikkel 82 i personvernforordningen.

Utlendingsforskriften § 18-7 er en videreføring av en tilsvarende bestemmelse, § 132 g, i den nå opphevede utlendingsforskriften av 1990.²⁵ Den registrerte kunne etter § 132 g påklage avgjørelser om innsyn, retting, sletting eller erstatning til *Politidirektoratet*. Direktoratet var klageinstans for disse sakene, frem til Arbeids- og inkluderingsdepartementet overtok denne rollen i 2008.²⁶ I dag er det Justis- og beredskapsdepartementet som innehar rollen som klageorgan.²⁷

Bakgrunnen for å innføre en egen nasjonal regulering av klageadgangen fremstår noe uklar, men skyldes trolig at Eurodac-forordningen 2000 ga tydelige føringer om at den registrerte skulle ha rett til å utøve sine rettigheter etter EUs personvern direktiv²⁸, herunder også en rett til å påklage bestemte personvernrettslige avgjørelser tatt av den behandlingsansvarlige, til medlemsstatenes «kompetente myndigheter», jf. artikkel 18 i Eurodac-forordningen 2000 nr. 11 og 12.²⁹

I Ot.prp. nr. 96 (2000–2001) uttaler Kommunal- og regionaldepartementet at det likevel er Datatilsynet som vil være nasjonal tilsynsmyndighet for så vidt gjelder den norske deltakelsen i Eurodac-samarbeidet. I rollen som tilsynsmyndighet er Datatilsynet ansvarlig for å overvåke at norske myndigheters behandling av personopplysninger skjer på lovlig måte i samsvar med bestemmelsene i Eurodac-forordningen 2000 og personvern direktivet.

I likhet med Eurodac-forordningen 2000 og Eurodac-forordningen 2013, er Datatilsynet nasjonal tilsynsmyndighet etter Eurodac-forordningen 2024, jf. artikkel 44, som fastsetter at tilsynsmyndigheten i artikkel 51 nr. 1 i personvernforordningen skal overvåke lovligheten av behandling av personopplysninger. I Norge er det Datatilsynet som har rollen som tilsynsmyndighet iht. artikkel 51 nr. 1, jf. poppl. § 20.

Den registrerte har rett til å klage til Datatilsynet dersom vedkommende mener at personopplysninger om hen er behandlet i strid med personvernforordningen, jf. personvernforordningen artikkel 77. Bestemmelsen gjelder også for urettmessig behandling av personopplysninger i Eurodac-registeret.³⁰

²⁵ Se [høringsnotat 24. mars 2009](#), der departementet i punkt 18.2 på side 45 foreslår å videreføre bestemmelsen i ny utlendingsforskrift av 2010.

²⁶ Se endringsforskrift 20. januar 2008 nr. 56.

²⁷ Se delegeringsvedtak 9. oktober 2009 nr. 1260, jf. omorganiseringsvedtak 18. desember 2009 nr. 1582.

²⁸ Europaparlaments og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger.

²⁹ Se også Ot.prp. nr. 96 (2000–2001) punkt 2.2.2 på side 20.

³⁰ Datatilsynet har en egen [samlingside](#) for spørsmål knyttet til behandling av personopplysninger i Eurodac. På siden fremgår det at urettmessig behandling av personopplysninger kan påklages til tilsynet. I saker som gjelder Eurodac vil tilsynet bl.a. ta stilling til om vedtak om avslag på innsyn, retting eller sletting er i samsvar med regelverket. Departementet bemerker, for ordens skyld, at nettsiden p.t. ikke er oppdatert ifm. gjennomføring av ny Eurodac-forordning 2024.

Klageadgangen etter utlf. § 18-7 er med andre ord en *parallel* klageordning, der departementet er klageinstans for avgjørelser som tas av underliggende virksomheter, herunder UDI.

5.2 Departementets forslag og vurdering

Departementet kan ikke se at Eurodac-forordningen 2024 krever at medlemsstatene har eller oppretter en egen parallel klageordning ved siden av den som allerede gjelder etter personvernforordningens bestemmelser. Personvernforordningen gjelder for behandling av personopplysninger etter Eurodac-forordningen 2024, hvilket betyr at en ev. urettmessig behandling kan påklages til Datatilsynet av den registrerte. Etter departementets syn vil en parallel klageordning føre til uklarheter hva gjelder ansvarsforhold mellom de ulike virksomhetene som behandler klagen. Hensynet til en forutsigbar, effektiv og klar klageordning taler for å oppheve den nasjonale klageordningen i utlf. § 18-7. En parallel klageordning er etter departementets vurdering også avvikende mht. systematikken for klager etter personvernforordningen, som skal gå til Datatilsynet, jf. personvernforordningen artikkel 77. Departementet viser også til at andre felleseuropeiske systemer, f.eks. SIS-registeret³¹, ikke inneholder en tilsvarende klageordning for avgjørelser om innsyn, retting og sletting; ordningen her er at klagen sendes til Datatilsynet. Med dette som bakgrunn foreslår departementet å oppheve klageadgangen i gjeldende utlf. § 18-7, se forslaget i punkt 8 under.

Som nevnt i punkt 5.1 over, gir utlf. § 18-7 den registrerte rett til å påklage avgjørelser om *erstatning* til departementet som overordnet forvaltningsorgan. Datatilsynet har ikke myndighet til å vurdere om det skal tilkjennes erstatning for ev. brudd på personvernregelverket. Den registrerte kan imidlertid bringe utlendingsmyndighetenes avgjørelse inn for domstolene, jf. artikkel 82 nr. 6, jf. artikkel 79 nr. 2. Forslaget om å oppheve klageordningen etter gjeldende § 18-7 omfatter også retten til å klage på avgjørelser om erstatning. Den registrertes rettssikkerhet anses ivaretatt ved at vedkommende kan bringe saken inn for domstolene.

For sammenhengens skyld bemerker departementet at rettshåndhevende myndigheter, herunder politiet og Politiets sikkerhetstjeneste (PST), kan etter nærmere angitte vilkår søke i Eurodac som ledd i å forebygge, avdekke eller etterforske terrorisme og andre alvorlige straffbare handlinger. Behandling av personopplysninger til dette formålet reguleres av politiregisterloven. Etter politiregisterloven § 55 kan den registrerte eller den som antar å være registrert, påklage avgjørelser truffet i medhold av loven til overordnet organ, herunder avgjørelser om innsyn, retting, sperring og sletting.

6 Konsekvensjustering av aktuelle uttrykk i utlendingsforskriften

6.1 Gjeldende rett

Utlendingsloven og -forskriften benytter i dag «fotografi» og «ansiktsfoto». Av hensyn til et klart og tilgjengelig regelverk, foreslo departementet i Prop. 73 LS

³¹ Schengen informasjonssystem (SIS) er et digitalt register der myndighetene i Schengen-landene kan utveksle informasjon.

(2025–2026) å endre utlendingsloven og grenseloven ved å erstatte termene over med hhv. «bilde» og «ansiktsbilde». Endringene er ment å være av rent terminologisk art.

6.2 Departementets forslag og vurdering

Utlendingsloven og -forskriften har som følge av vedtakelsen av forslagene i Prop. 73 LS (2025–2026) to ulike termer for samme begrep. For å minimere risikoen for tolkningstvil, foreslår derfor departementet å gjøre tilsvarende justeringer i utlendingsforskriften. I likhet med forslaget i nevnte proposisjon, vil også forslaget her være av rent terminologisk art og ikke medføre materielle endringer sammenliknet med dagens rettstilstand. Se punkt 8 nedenfor.

7 Økonomiske og administrative konsekvenser

Forslaget om å eksplisitt regulere utlendingsmyndighetenes adgang til å behandle innhentede personopplysninger til utvikling og testing av IT-systemer, herunder systemer basert på KI, antas ikke å medføre vesentlige økonomiske eller administrative konsekvenser i seg selv. Dersom virksomhetene tar i bruk hjemlene for å utvikle og teste IT-systemer, må de imidlertid gjennomføre egnede tekniske og organisatoriske tiltak for å sikre at personopplysningene behandles i tråd med personvernforordningen, herunder sørge for god tilgangsstyring slik at det kun er personer med tjenstlig behov som får tilgang til personopplysningene. De økonomiske og administrative konsekvensene av slike tiltak er usikre, og noe man ev. må komme tilbake til i de ordinære budsjettprosessene med forslag til inndekning av ev. merkostnader.

Forslaget om å forskriftsfeste utlendingsmyndighetenes adgang til å beslutte og utføre opptak av biometriske opplysninger etter Eurodac-forordningen 2024 antas ikke å medføre økonomiske og administrative konsekvenser, da dette er oppgaver som virksomhetene allerede har i dag. Dersom det besluttes at også UNE skal gis kompetanse til å beslutte opptak av biometri etter Eurodac-forordningen 2024, vil det likevel kunne medføre enkelte økonomiske og administrative konsekvenser for politiet ifm. gjennomføring av biometriopptaket. Departementet bemerker imidlertid at det bare i et svært begrenset antall saker vil være aktuelt at UNE beslutter opptak av biometri. Eventuelle økonomiske og administrative konsekvenser for politiet antas derfor å være marginale, og antas å kunne dekkes innenfor gjeldende budsjettammer.

Når det gjelder forslaget om å oppheve klageordningen i utlf. § 18-7, legger departementet til grunn at opphevelsen ikke vil medføre kostnader for utlendingsmyndighetene. Det kan imidlertid tenkes at Datatilsynet vil kunne få noen flere klager enn tidligere, fordi klageadgangen til departementet oppheves. Departementet vil likevel bemerke at selv om det ikke finnes tall på antall klager som er behandlet av departementet etter tidligere og gjeldende Eurodac-forordning, er det grunn til å tro at ordningen med å kunne påklage avgjørelser om innsyn, retting, og sletting i Eurodac til departementet blir svært lite brukt, og at ev. økonomiske og administrative konsekvenser for Datatilsynet vil være ubetydelige og dermed kunne dekkes innenfor gjeldende budsjettammer. Behov for endringer i ressursbruk til tilsynsoppgaver må ev. evalueres og tas hensyn til etter at Eurodac-forordningen 2024 har fått tid til å virke og man har vunnet tilstrekkelige erfaringer.

8 Forslag til endringer i utlendingsforskriften

Ny § 17-7 c skal lyde:

§ 17-7 c *Utvikling og testing av informasjonssystemer, herunder systemer basert på kunstig intelligens*

Utlendingsmyndighetene kan behandle personopplysninger innhentet etter andre bestemmelser i utlendingsloven eller i forskrifter gitt i medhold av utlendingsloven til utvikling og testing av utlendingsforvaltningens informasjonssystemer, herunder systemer basert på kunstig intelligens, dersom det vil være umulig eller uforholdsmessig vanskelig å oppnå formålet ved å bruke anonyme eller fiktive opplysninger.

Personopplysningene skal ikke brukes til utvikling og testing lenger enn nødvendig.

Tilgang til personopplysningene skal bare gis til personer som er særskilt bemyndiget. Bemyndigelse gis av den behandlingsansvarlige.

Gjeldende § 17-7 c, § 17-7 d, § 17-7 e, § 17-7 f, § 17-7 g, § 17-7 h, § 17-7 i, § 17-7 j og § 17-7 k blir henholdsvis § 17-7 d, § 17-7 e, § 17-7 f, § 17-7 g, § 17-7 h, § 17-7 i, § 17-7 j, § 17-7 k og ny § 17-7 l.

§ 18-1 tredje ledd skal lyde:

Opptak av *ansiktsbilde* eller fingeravtrykk etter første ledd kan *beslattes* og utføres av Utlendingsdirektoratet, politiet *eller* norsk utenriktjeneste. *En ekstern tjenesteyter kan i henhold til avtale etter § 10-2 fjerde ledd utføre opptak av ansiktsbilde eller fingeravtrykk.*

§ 18-1 niende ledd skal lyde:

For behandling av fingeravtrykk og *ansiktsbilde* i henhold til Eurodac-forordningen, jf. lovens § 101, gjelder reglene i § 18-5 til § 18-7.

Gjeldende § 18-7 oppheves.

Ny § 18-7 skal lyde:

§ 18-7 *Opptak av biometriske opplysninger etter Eurodac-forordningen*

Opptak av ansiktsbilde eller fingeravtrykk etter Eurodac-forordningen kan beslattes og utføres av Utlendingsdirektoratet, politiet eller norsk utenriktjeneste. Utlendingsnemnda kan beslutte opptak av ansiktsbilde eller fingeravtrykk. En ekstern tjenesteyter kan i henhold til avtale etter § 10-2 fjerde ledd utføre opptak av ansiktsbilde eller fingeravtrykk.

I følgende bestemmelser og overskrift endres «fotografi» til «bilde»:

- Utlendingsforskriften § 1-7
- Utlendingsforskriften § 2-4
- Utlendingsforskriften § 2-7
- Utlendingsforskriften § 2-9
- Utlendingsforskriften § 3-16
- Utlendingsforskriften § 12-4
- Mellomoverskrift til utlendingsforskriften §§ 18-1, 18-2, 18-3 og 18-4

I følgende bestemmelser og overskrift endres «ansiktsfoto» til «ansiktsbilde»:

- Utlendingsforskriften § 10-2
- Utlendingsforskriften § 12-11
- Overskrift til utlendingsforskriften § 18-1
- Utlendingsforskriften § 18-1
- Overskrift til utlendingsforskriften § 18-2
- Utlendingsforskriften § 18-2
- Overskrift til utlendingsforskriften § 18-4
- Utlendingsforskriften § 18-4
- Mellomoverskrift til utlendingsforskriften § 18-4 a