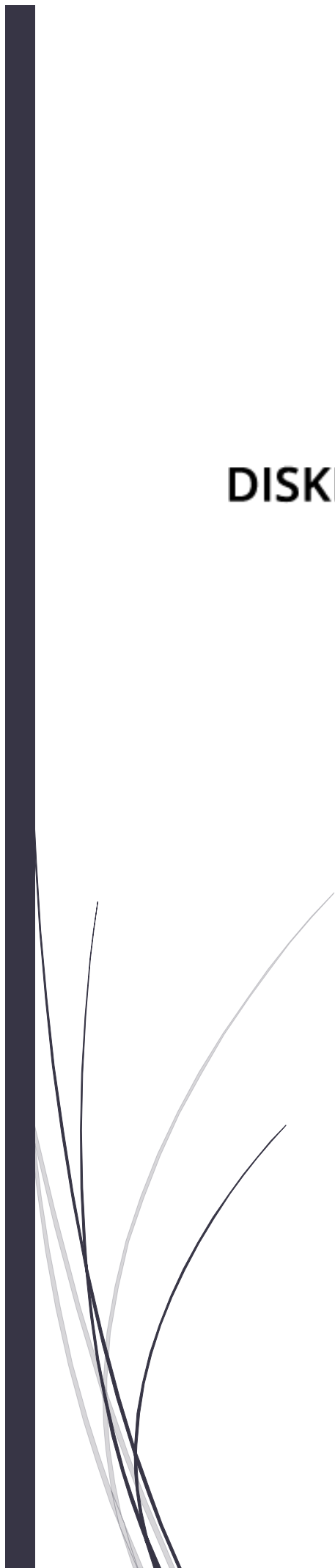




DISKRIMINERINGSNEMNDA

Årsrapport 2022

13.03.2023



Innhold

I. Leiarens fråsegn.....	3
II. Introduksjon til verksemda og hovudtal	4
Omtale av verksemda og samfunnsoppdraget.....	4
Omtale av organisasjon og leiing	8
Sekretariatet	9
Nemnda.....	9
Presentasjon av utvalde hovudtal	10
III. Aktivitetar og resultat i 2022.....	12
Samla vurdering av prioriteringar, ressursbruk, resultat og måloppnåing 2022	12
Resultat og måloppnåing i 2022	13
Rapporteringskrav: Gjennomsnittleg saksbehandlingstid	13
Rapporteringskrav: Etablera eit godt og effektivt lågterskeltilbod for saker om gjengjelding etter varsling	14
Nærare om behandla klagesaker	14
Saker avgjort i forsterka nemnd.....	18
Andre oppgåver	18
Arkiv og kjøp av nytt saksbehandlingssystem.....	18
Nettstaden	19
Promoteringskampanje.....	20
Fagleg kompetanseutvikling	20
Høyringssvar	21
IV. Styling og kontroll i verksemda	21
Tryggleik og beredskap	22
Personvern.....	22
Konsulentbruk	23
Lærlingar	23
Klima- og miljø	23
Korleis Diskrimineringsnemnda oppfyller aktivitetsplikta i likestillings- og diskrimineringslova §§ 24 og 26	24
Del 1: Tilstand for kjønnslikestilling	24
Del 2: Arbeidet vårt for likestilling og mot diskriminering	25
Likestillingsarbeid for Diskrimineringsnemnda som myndigheitsorgan	29

V. Vurdering av framtidsutsikter	32
VI. Årsrekneskap	34

I. Leiarens fråsegn

Året 2022 har vore nok eit produktivt år for Diskrimineringsnemnda med totalt 416 avvikla saker. Samstundes har året vore eit av dei mest krevjande åra sidan oppstarten i 2018.

Årsaka til at året har vore krevjande, er at arbeidspresset har blitt markant større, samstundes som at bemanninga i sekretariatet ikkje er auka tilsvarande. Diskrimineringsnemnda opplever endå ei stor auke i talet på mottekne klagesaker og det ser ut til å vera ei varig trend. I 2022 fekk Diskrimineringsnemnda totalt 574 nye klagesaker. Til samanlikning fekk me 513 saker i 2021, og 304 saker i 2020. Det vil seia at talet på mottekne klagesaker i 2022 nærast er dubla samanlikna med 2020.

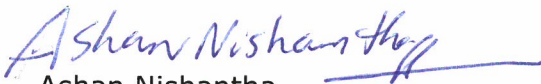
Auken i talet på saker fører til at fleire saker vert avgjort i nemnd, og at det vert gjennomført munnlege forhandlingar i fleire saker. Me ser også at me no mottek meir krevjande saker, dels som fylgje av at myndigheitsområdet til nemnda er utvida på fleire felt på kort tid. Samla inneber desse tilhøva ei auke i ressursbruken og lengre saksbehandlingstid per sak, og me har no den største restansen me nokosinne har hatt.

Ressursane i 2022 er brukt til å oppfylle målkrava for året om at Diskrimineringsnemnda skal vera eit godt og effektivt handhevingsapparat og ha ei gjennomsnittleg saksbehandlingstid på maks 7 månadar. I tillegg skulle me etablera ferdig lågterskeltilbodet for saker om gjengjelding etter varsling. Me har også mellom anna måtta bruka mykje tid og ressursar på å skifta saksbehandlingssystem, samt oppgradera nettsidene våre i tråd med dei nye krava i WCAG 2.1.

Den samla ressursbruken vart halde innanfor godkjent løyving. For nærare detaljar visar eg til Del 6 Årsrekneskap.

Eg ynskjer å avslutta her med å rosa sekretariatet og nemnda for det solide arbeidet dei gjer kvar einaste dag for at Diskrimineringsnemnda skal levera så godt som mogleg på samfunnsoppdraget vårt og oppfylle krava departementet stiller til oss. Både resultatene for 2022, og opplevinga eg har som direktør, vitnar om at Diskrimineringsnemnda har ein arbeidsstyrke der både arbeidsviljen og arbeidskapasiteten er stor.

Bergen, 13.03.2023


Ashan Nishantha
direktør

II. Introduksjon til verksemda og hovudtal

Omtale av verksemda og samfunnsoppdraget

Diskrimineringsnemnda er eit domstolsliknande og uavhengig forvaltningsorgan som avgjer saker om diskriminering, trakassering og gjengjelding, inkludert seksuell trakassering og gjengjelding etter varslings i arbeidsmiljølova. Ein part, ombudet eller andre med rettsleg klageinteresse kan ta ein sak inn for nemnda. Nemnda fører ikkje tilsyn og kan ikkje ta opp saker på eige initiativ.

Diskrimineringsnemnda er administrativt underlagt Kultur- og likestillingsdepartementet og Arbeids- og inkluderingsdepartementet (saker om gjengjelding etter varslings i arbeidsmiljølova).

Beviskravet i saker om diskriminering, trakassering og gjengjelding er det same, uavhengig av om saka vert teke inn for nemnda, eller dei ordinære domstolane. Men nemnda er eit lågterskeltilbod og eit alternativ til domstolsbehandling i desse sakene. I tillegg spelar nemnda ei viktig rolle i rettsutviklinga både på likestillings- og antidiskrimineringsfeltet og innanfor feltet for gjengjelding etter varslings.

Det er gratis å få saka behandla, og partane vel sjølv om dei vil bruka advokat. Heile prosessen kan gjennomførast digitalt med nemnda sine skjema som er tilgjengelege på nettstaden, og dei som vil kommunisera per vanleg post kan gjera det. Det er difor ikkje naudsynt å møte motparten fysisk.

Det er ikkje mogleg å klaga anonymt. Prosessen i nemnda er lagt opp som ein kontradiktorisk to-partsprosess. Det betyr at partane som hovudregel får sjå alt motparten sender inn av informasjon og dokumentasjon, og får høve til å ta til motmæle. Nemnda gjev rettleiing om prosessen på vakttelefonen, som er open kvar dagar mellom klokka 10 og 14, og har også ei ordning for skrivehjelp for partar som ikkje kan skriva norsk eller få hjelp av andre. I tillegg har nemnda informative nettsider, der det mellom anna er lagt ut informasjon om prosessen, statistikk, avgjerder i anonymisert form og samandrag av sentral informasjon på totalt 10 ulike språk. Nemnda har vitnestøtteordning via Røde kors og kan tilby tolk i tråd med tolkelova. Me kan derimot ikkje gje råd eller annan partshjelp, fordi nemnda skal vera upartisk.

Til skilnad frå dei ordinære domstolane, har nemnda ei sjølvstendig undersøkingsplikt for å få saka tilstrekkeleg opplyst før den vert avgjort. Dei som førebur sakene i sekretariatet er alle juristar. Kvar sak vert avgjort av ein erfaren dommar. Dersom saka vert behandla i nemnd, vert saka avgjort av ein erfaren dommar i tillegg til to andre juristar. Alle i nemnda har spesialkompetanse innan rettsfelte nemnda handhevar.

Nemnda kan treffa vedtak eller gje fråsegner om at det føreligg brot på lovane nemnda handhevar:

Likestillings- og diskrimineringsloven (lov nr. 51/2017)
Arbeidsmiljøloven kapittel 13, med unntak av § 13-1 tredje ledd (lov nr. 62/2005)
Eierseksjonsloven § 6 (lov nr. 65/2017)
Husleieloven § 1-8 (lov nr. 17/1999)
Bustadbyggjelagslova § 1-4 (lov nr. 38/2003)
Burettslagslova § 1-5 (lov nr. 39/2003)
Skipsarbeiderloven kapittel 10, med unntak av § 10-1 (lov nr. 102/2013)

Nemnda behandlar også saker om gjengjelding etter arbeidsmiljølova § 2 A-4 og oppreisning og erstatning etter § 2 A-5, med unntak av saker om oppseiing eller avskjed.

Diskrimineringsnemnda si verksemd er regulert av lov om Likestillings- og diskrimineringsombudet og Diskrimineringsnemnda (diskrimineringsombodslova nr. 50/2017) og forskrift om organisasjon, oppgaver og saksbehandling for Diskrimineringsnemnda (FOR-2017-12-20-2260). I tillegg gjeld enkelte av forvaltningslova og tvistelova sine reglar for saksbehandlinga.

Nemnda skal fyrst og fremst avgjera om eit tilhøve som er klaga inn for nemnda er i strid med likestillings- og diskrimineringsregelverket, eventuelt forbodet mot gjengjelding etter varsling. Nemnda kan i tillegg påleggja stans, retting og andre tiltak som er naudsynte for å sikra at diskriminering, trakassering, instruks eller gjengjelding sluttar, og for å hindra gjentakning jf. diskrimineringsombodslova § 11. Vidare kan Diskrimineringsnemnda treffa vedtak om tvangsmulkt for å sikra gjennomføring av eit pålegg, dersom fristen for å retta seg etter pålegget er broten.

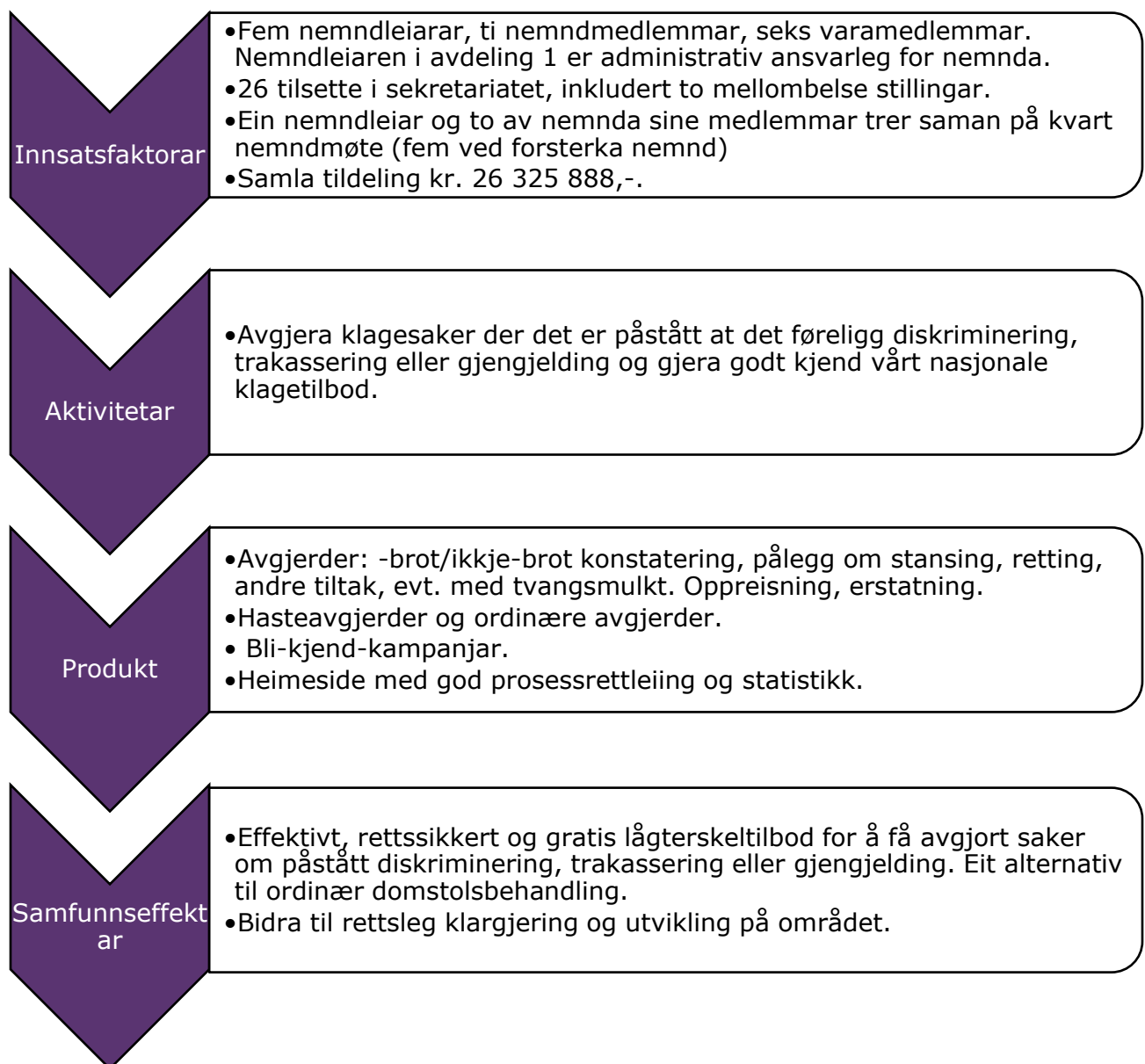
Diskrimineringsnemnda kan tilkjenna oppreisning i arbeidstilhøve og erstatning i enkle sakstilhøve, dersom klagaren krev det. Nemndleiaren kan gje hastepålegg om retting, stans eller andre tiltak når ein sak ikkje kan venta på vanleg nemndbehandling.

Saksbehandlinga i Diskrimineringsnemnda er som hovudregel skriftleg, med moglegheit for munnlege forhandlingar avslutningsvis dersom nemndleiaren meiner at bevissituasjonen krev det. Partane kan på si side krevja munnlege forhandlingar i saker der det er kravd oppreisning og i saker om seksuell trakassering.

Nemnda behandlar alle klagesaker i ein instans. Det betyr at nemnda sine vedtak er endelege forvaltningsvedtak som ikkje kan overprøvast gjennom

forvaltningsklage. Vedtaka kan derimot takast inn for domstolane til full prøving av saka. Det same gjeld avgjerder om tvangsmulkt. Dersom eit vedtak eller ei avgjerd om tvangsmulkt ikkje vert teken inn for domstolane innan søksmålsfristen på 3 månadar, får avgjerda verknad som ein rettskraftig dom. Nemnda sine ikkje-bindande fråsegner kan derimot ikkje takast inn for domstolane. Dersom ein part ynskjer å få prøvd saka for domstolane, må parten i so fall ta ut søksmål mot motparten. Det kan parten gjera uavhengig av nemnda si fråsegn.

Diskrimineringsnemnda si resultatkjede:

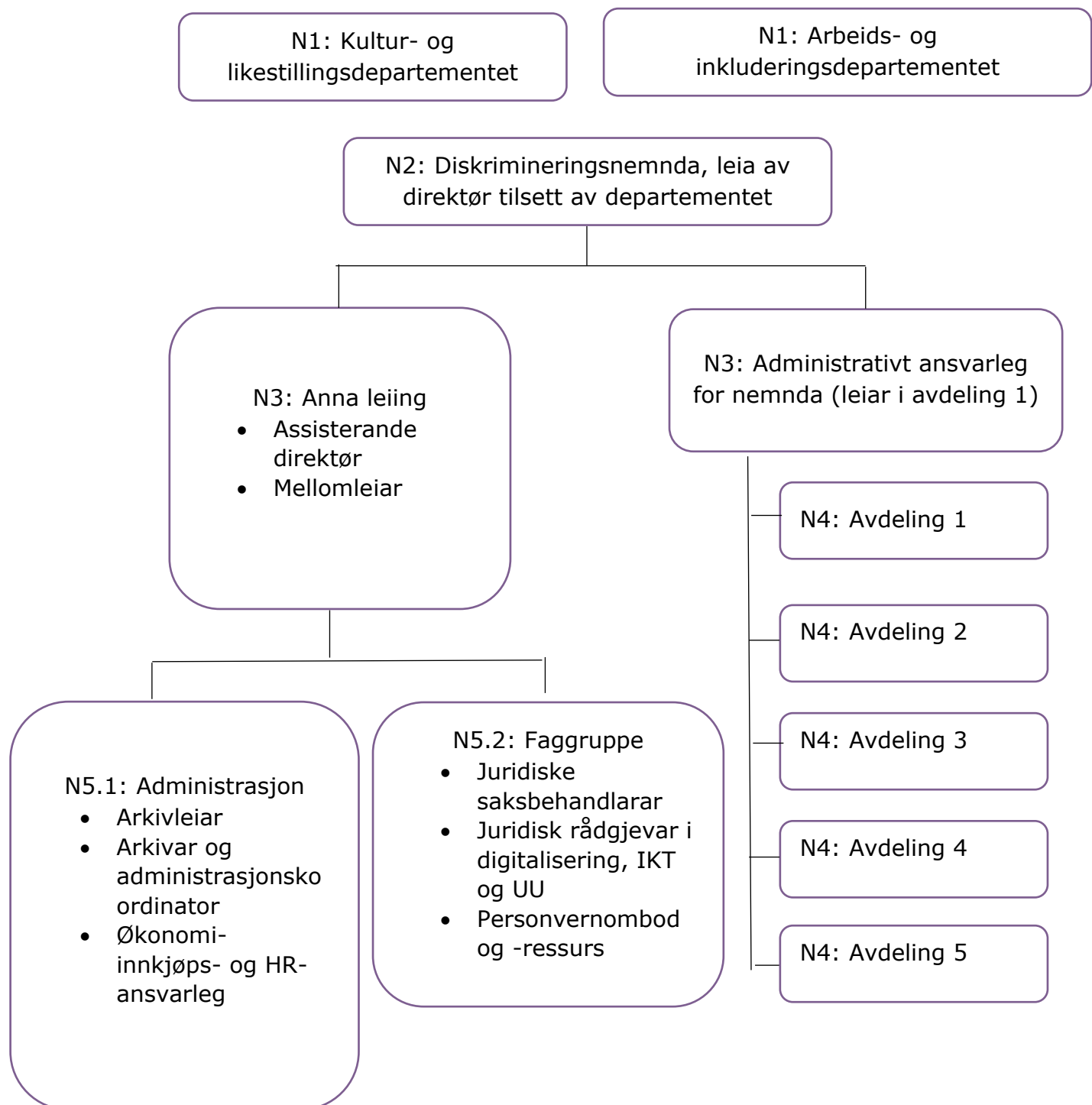


Diskrimineringsnemnda har ein samarbeidsavtale med Digitaliseringsdirektoratet som inneber at direktoratet gjev ei IKT-fagleg fråsegn i klagesakene nemnda behandlar der det er påstand om brot på regelverket for universell utforming av IKT (typisk i appar og på nettsider). Diskrimineringsnemnda sin samarbeidsavtale med Digitaliseringsdirektoratet er ein tilsvarande avtale som det Likestillings- og diskrimineringsombudet hadde tidlegare med Difi. Bakgrunnen for samarbeidsavtalen er at det vert lagt til grunn i førearbeida til likestillings- og diskrimineringslova, Prop. 81 L (2016-2017) på side 214 og 325, at Diskrimineringsnemnda hentar inn slike rådgjevande fråsegner frå sektorbestemte handhevingsorgan og tilsynsmyndigheiter, dersom det er tvil om sektorbestemte lovar og forskrifter er fylgt.

Nemnda har også eit godt samarbeid med Likestillings- og diskrimineringsombodet for å ivareta god koordinering av rollane våre og sikra en fortløpande informasjons- og erfaringsutveksling oss imellom, slik at me utfyller kvarandre godt. Me har også etablert ein god kontakt med Barne-, ungdoms- og familiedirektoratet, samt Arbeidstilsynet med tanke på at me behandlar av saker om gjengjelding etter arbeidsmiljølova.

Omtale av organisasjon og leing

Figur 1: Organisasjonskart for Diskrimineringsnemnda



Diskrimineringsnemnda vert leia av direktør Ashan Nishantha. Kristine F. Sandven er assisterande direktør og Ingelin Gammersvik er mellomleiar. Arkivleiar er Helene Reksten.

Diskrimineringsnemnda er delt i ei nemnd og eit sekretariat. Sekretariatet førebur sakene, medan nemnda avgjer dei. I tillegg til å førebu sakene, inkludert å ha kontakt med partane, arrangerer sekretariatet møta i nemnda, lagar utkast til nemnda sine avgjerder og sørgjer elles for den daglege drifta av Diskrimineringsnemnda. Diskrimineringsnemnda har kontor i Statens hus i Bergen.

Sekretariatet

I 2022 har sekretariatet hatt totalt 26 tilsette (21 planlagde) fordelt på 19,15 utførte årsverk. Seks av dei tilsette jobba i leiinga/administrasjonen og resten var juridiske saksbehandlarar, faste og mellombelse. Ein juridisk saksbehandlar vart lånt ut til Norsk Kulturråd i ein periode på tre månader, i samband med forvaltninga av stimuleringsordninga for kultursektoren.

Fem tilsette, inkludert fire faste juridiske saksbehandlarar, slutta i løpet av 2022. Det vart ikkje gjennomført ordinære tilsettingsprosessar i 2022. Ein person vart tilsett av direktøren i ei mellombels stilling med varigheit på eitt år, som ledd i eit prosjekt etter initiativ av Kultur- og likestillingsdepartementet, knytt til kortare saksbehandlingstid innan saker om universell utforming av IKT. Våren 2022 hadde me ei seks månaders prøveordning med ei stilling som juridisk rådgjevar innan digitalisering, IKT og universell utforming frå og med 1. januar 2022. Det nye WCAG 2.1-regelverket utløyste eit ekstra behov for denne typen stilling. Stillinga vart forlenga ut 2022 på grunn av arbeidet vårt for å få nettsidene i tråd med WCAG 2.1, samt eit generelt behov for intern IKT- og digitaliseringskompetanse.

Våren 2022 hadde me ein masterstipendiat med skriveplass, medan me i månadsskiftet august/september hadde ein studentpraktikant. Praktikantane jobbar tilnærma likt som ein juridisk saksbehandlar, medan masterstipendiatane skriv masteroppgåva si med kontorplass hjå oss.

Nemnda

Nemnda var i 2022 delt inn i fem avdelingar. Kvar avdeling har ein nemndleiar. Alle nemndleiarar er dommarar eller har dommarkompetanse. Nemndleiar i avdeling 1, Ivar Danielsen, var administrativ ansvarleg for nemnda fram til han slutta i juni 2022. Reidun Wallevik overtok då som nemndleiar for avdeling 1, og som administrativ ansvarleg for nemnda.

Nemnda hadde i 2022 ti medlemmar og seks varamedlemmar. Dei fleste medlemmane og varamedlemmane er dommarar, advokatar eller juridiske professorar. Medlemmane vert normalt oppnemnd av departementet for ein periode på fire år, og for maksimalt to periodar.

Nemnda hadde i 2022 fylgjande faste medlemmar:

Nemndleiarar: Ivar Danielsen (leiar av nemnda og avdeling 1 fram til juni 2022), Elisabeth Deinboll (leiar avdeling 2), Torstein Frantzen (leiar avdeling 3) Reidun Wallevik (leiar av avdeling 4 fram til juni 2022, deretter leiar avdeling 1), Bjørnar Borvik (leiar av avdeling 4 frå juni 2022) og Anniken Mellegaard Douglass (leiar av avdeling 5).

Nemndmedlemmar: Gislaug Øygarden, Andreas Skoe Cederkvist, Jens Kristian Johansen, Usman Ivar Shakar, Møyfrid Eggebø, Thorkil H. Aschehough, Kirsti Coward, Lars Magnus Bergh, Tine Eidsvaag og May Britt Erstad.

Varamedlemmar: Henriette Nazarian, Marte T. Strand Sinkerud, Lola Magnussen, Eirik Eldjarn, Magne Strandberg og Maria Torvund.

Presentasjon av utvalde hovudtal

Tabell 1: Presentasjon av utvalde volumtal for 2020-2022

Volumtal 2020-2022	2020	2021	2022
Innkomne saker til behandling	304	513	574
Ferdigbehandla saker	313	430	417
Saker bortlagt og avvist	123	171	140
Saker der nemnda har fatta eit vedtak i saka	31	45	71
Saker der nemnda har gjeve ei fråsegn i saka	76	82	75
Avgjorte saker med pålegg	3	1	17
Avgjorte saker med tilkjent oppreisning og/eller erstatning	9	11	14
Hastevedtak	2	0	0
Gjennomsnittleg saksbehandlingstid	216 dagar (7, 1 månader)	133 dagar (4 månader)	182 dagar (6 månader)
Saker behandla i forsterka nemnd	1	2	4
Søksmål	0	0	0

Tabell 2: Nøkkeltal fra årsrekneskapen 2020-2022

Nøkkeltall fra årsregnskapet 2022	2020	2021	2022¹
Tilsette	26	23	25
Avtalte årsverk	19,10	21	21
Utførte årsverk	17,69	20,11	19,15
Samla tildeling post 01-99 inkludert overføring av mindreforbruk året før	23 286 000	23 402 000	26 325 888
Samla tildeling post 01-99 Stimuleringsmidlar til kultur, frivilligheit og idrett ism. Covid-19			232 000,00
Samla tildeling post 01-99 budsjettfullmakta frå Arbeids- og inkluderingsdepartementet	3 000 000	3 000 000	
Totalt samla tildeling post 01-99	26 286 000	26 402 000	26 557 888, 00
Utnyttingsgrad post 01-29	90,48	96,35	95
Brukte midlar post 01-29 eks offentlig refusjonar løn	24 388 587,95	25 992 085,54	25 192 345,00
Tilgjengelege midlar post 01-29 + offentlig refusjon løn	26 954 203,00	26 975 337,00	27 068 538,00
Driftsutgifter Sum utbetalningar til drift inkludert investerings- og finansutgifter	23 720 384,95	25 418 749,32	25 470 994,00
Lønsandel av driftsutgifter i %	63,67	69,75	72
Utbetalningar til løn	15 103 465,50	17 730 025,96	18 260 218,92
Lønskostnadar per årsverk	925 838,76	948 132,62	953 536,24

¹ Det er ved ein feil brukt lønsutbetalningar (note 2 i årsrekneskapen) i utrekning av lønsandel av driftsutgifter og ikkje lønsutgifter unnateke konto 530-534 slik fotnote 10 i rettleiaren visar til. Det er difor noko feil i utrekningar av utnyttingsgrad for 2020 og 2021. Korrigert for «unntatt konto 530-533» er utnyttingsgrad for 2020 64 og utnyttingsgrad for 2021 70.

III. Aktivitetar og resultat i 2022

Samla vurdering av prioriteringar, ressursbruk, resultat og måloppnåing 2022

Diskrimineringsnemnda sitt overordna samfunnsoppdrag er å vera eit effektivt handhevingsapparat som avgjer dei diskriminerings-, trakasserings- og gjengjeldingssakene som vert tekne inn for organet, med kvalitet på ekspertnivå. Kultur- og likestillingsdepartementet sette fylgjande overordna mål for Diskrimineringsnemnda i 2022:

«Effektivt håndhevingsapparat på likestillings- og ikke-diskrimineringsområdet».

Diskrimineringsnemnda sitt hovudfokus er difor å tilby ei effektiv og god klagesaksbehandling. Det meste av nemnda sin samla ressursbruk er løns- og honorarutgifter til tilsette og nemndmedlemmar, som gjev grunnlaget for å oppfylle dei to styringsmåla for nemnda i 2022:

- Maks 7 månadar gjennomsnittleg saksbehandlingstid
- Etablera eit godt og effektivt lågterskeltilbod for saker om gjengjelding etter varsling.

Diskrimineringsnemnda hadde ei stor auke i talet på innkomne klagesaker i 2021, noko som skapte ein nesten dobbelt så stor restanse ved årsskiftet 2021/2022 samanlikna med året før. I 2022 har i tillegg innkomne klagesaker halde fram med å stige, samstundes som talet på tilsette i sekretariatet har blitt redusert av budsjettmessige grunnar. Det har difor vore ei utfordring å halda saksbehandlingstida nede, og samstundes avvikla like mange klagesaker som tidlegare. Dette har ført til at andre prosjekt og sideoppgåver har måtta bli nedprioritert og utsett.

I 2022 måtte Diskrimineringsnemnda i tillegg kjøpa nytt saksbehandlingssystem, fordi avtalen for det tidlegare saksbehandlingssystemet gjekk ut. Dette var eit arbeid som var heilt naudsynt, men som det vart brukt mykje tid og ressursar på. Det vart også lagt ned eit større arbeid med nettstaden til Diskrimineringsnemnda i 2022, for å få nettsidene i tråd med dei komande krava i WCAG 2.1.

Samla sett er Diskrimineringsnemnda nøgd med årsresultata, oppfylt måloppnåing og ressursbruk. Me har etablert eit lågterskeltilbod for saker om gjengjelding etter varsling, og samstundes klart å halda saksbehandlingstida under målkravet på sju månader. Det heile på trass av stort arbeidspress i sekretariatet og nemnda, og stigande tal på klagesaker inn.

Resultat og måloppnåing i 2022

Tabell 3 viser ei oppstilling av mål, styringsparameter og resultatkrav gjeve av Kultur- og likestillingsdepartementet, og Diskrimineringsnemnda sitt resultat i 2022.

Tabell 3: Oversikt over mål, styringsparametere, resultatkrav og resultat i 2022.

Hovudmål, styringsparametre og resultatkrav bestemt av Kulturdepartementet

Diskrimineringsnemnda sine resultat

Hovudmål: Effektivt handhevingsapparat på likestillings- og ikkje-diskrimineringsområdet			
#	Styringsparameter	Resultatkrav	Resultat
S1.1	Gjennomsnittleg saksbehandlingstid	Maks 7 månader gjennomsnittleg saksbehandlingstid	Oppfylt (182 dagar, dvs. 6 månader).
S1.2	Etablera eit godt og effektivt lågterskeltilbod for saker om gjengjelding etter varsling	Sørgja for effektiv handheving av saker om gjengjelding etter varsling. Det skal rapporterast på den samla oppfølginga og resultat av innsatsen for gjengjeldingssakene etter varsling, inkludert talet på innkomne saker, talet på realitetsbehandla saker og talet på saker der nemnda konkluderer med at det har skjedd eit brot på forbodet mot gjengjelding etter varsling.	Oppfylt (sjå rapportering nedanfor).

Rapporteringskrav: Gjennomsnittleg saksbehandlingstid

Gjennomsnittleg saksbehandlingstid i 2022 var 6 månader (182 dagar), noko som inneber at resultatkravet er oppfylt. Saksbehandlingstida har derimot gått opp med to månader sidan 2021, dvs. auka med 50%. Alle saker, både saker som vert behandla i ordinær nemnd, lagt bort, avvist og avslutta utan avgjerd, har auka saksbehandlingstid samanlikna med fjoråret.

I tillegg ser me ein tendens til at fleire saker vert behandla i ordinær nemnd enn tidlegare. Dette er svært positivt, fordi det er eit teikn på at

Diskrimineringsnemnda stadig mottek meir relevante klagesaker. Desse sakene er samstundes normalt meir ressurskrevjande og tek lengre tid å behandla enn saker som vert lagt bort, avvist eller avslutta utan avgjerd. Det er også eit aukande tal på saker som vert behandla med munnleg forhandling.

Det er ynskjeleg at saksbehandlingstida på saker som vert behandla i ordinær nemnd er kortast mogleg. Dette er viktig for rettstryggleiken til partane som har saker hjå oss og for nemnda sin legitimitet meir generelt. Me jobbar difor for å redusera saksbehandlingstida. Utviklinga no går diverre i motsett retning. Saksbehandlingstida for saker som vart behandla på nemndmøter har auka frå 248 dagar i 2021 til 286 dagar i 2022. Dette er framleis langt under eitt år (350 dagar), som var talet for 2020, men me skulle gjerne sett at utviklinga gjekk motsett veg. Dersom innkomne saker fortset å liggja på same nivå framover, og nemnda ikkje vert styrka med ei auke i talet på tilsette i sekretariatet, er det ikkje tvil om at saksbehandlingstida vil halda fram med å auka vidare i 2023.

Rapporteringskrav: Etablera eit godt og effektivt lågterskeltilbod for saker om gjengjelding etter varsling

Diskrimineringsnemnda fekk myndigheit til å behandla saker om gjengjelding etter varsling i arbeidslivet 1. juli 2021. Sekretariatet jobbar aktivt med kompetanseoppbygging på området, og har gjennomført fleire kurs og seminar om emnet både i førebuingssfasen til me fekk myndigheita og etter. Det er etablert ei faggruppe internt i sekretariatet som behandlar desse sakene, og på den måten skapar me eit fora for erfaringsutveksling og spisskompetanse. Ved utgangen av 2022 har Diskrimineringsnemnda motteke totalt 63 saker der gjengjelding etter varsling er ført opp som grunnlag. 42 av desse sakene fekk nemnda i 2022, mot 21 saker året før. Dette visar at tilfanget av saker er stabilt, ettersom nemnda berre hadde myndigheit til å behandla desse sakene halve året i 2021.

I 2022 avgjorde Diskrimineringsnemnda 16 saker om gjengjelding etter varsling. Tre av desse vart behandla i nemnd. To av dei nemndbehandla sakene resulterte i ei fråsegn om at det ikkje hadde funne stad brot på regelverket. Den siste saka vart dels avvist og dels gjeve ei fråsegn i om at det ikkje hadde funne stad brot. Av dei andre 13 sakene vart fire avvist, tre vart lagt bort, to vart avslutta utan at det vart teke avgjerd i dei fordi klagaren ikkje svarte på spørsmål frå nemnda om opplysningar som var naudsynte for å behandla saka, og dei fire siste vart trekt av klagaren. Diskrimineringsnemnda har i 2022 ikkje behandla saker om gjengjelding etter varsling der nemnda har konkludert med at det har funne stad brot på regelverket.

Nærare om behandla klagesaker

Me hadde 28 møter i nemnda i 2022. Til samanlikning hadde me 23 møter i

2021, og 21 møter i 2020. Det vert normalt halde to nemndmøter i månaden, med unnatak av juli. På grunn av overgangen til nytt saksbehandlingssystem hadde me ikkje nemndmøte i verken juni, juli eller august i 2022. I staden hadde me tre nemndmøte i månaden gjennom hausten.

Fire saker vart behandla i forsterka nemnd. Det vart tilkjent oppreisning og/eller erstatning i 14 saker.

Diskrimineringsnemnda hadde ved årsskiftet 2022/2023 ein restanse på 359 saker. Til samanlikning var restansen i 2021/2022 på 202 saker, medan restansen ved årsskiftet 2020/2021 var på 119 saker.

Tabell 4 nedanfor visar ein oversikt over talet på avgjorte saker og resultat i sakene for 2022.

Tabell 4: Oversikt over avgjorte saker i 2022, 2021 og 2020.

Oversikt over avgjorte saker i 2022, 2021 og 2020²

Kategori	Tal for 2022	Tal for 2021	Tal for 2020
Totalt avgjorte klagesaker	417	430	313
Saker med regelbrot	71	45	31
Saker utan regelbrot	75	82	76
Saker som er bortlagt	95	121	94
Saker som er avvist	45	50	29
Saker som er trekt eller avslutta pga. manglande oppfølging frå klagar	131	132	83
Hasteavgjerder	0	0	2
Avgjorte saker med tilkjent oppreisning og/eller erstatning	14	11	9
Saker avgjort med munnleg forhandling	34	33	15
Saker avgjort av forsterka nemnd	4	2	1
Avgjorte saker med pålegg	17	1	3
Avgjorte saker med tvangsmulkt	10	1	1

² Merk at enkelte saker tel fleire stadar. Resultatet i saka vert berre telt ein gong, men dersom saka til dømes har blitt hastebehandla, avgjort med munnleg forhandling, forsterka nemnd eller det har blitt tilkjent oppreisning og erstatning, vert saka registrert der også. Tala for dei to tidlegare åra i tabellen er endra i tråd med oppdatert statistikk på nettsidene våre.

Tabell 5 nedanfor visar statistikk over talet på avgjorte klagesaker sortert etter grunnlag i 2022. Også i 2022 behandla Diskrimineringsnemnda flest saker om diskrimineringsgrunnlaget funksjonsnedsetting.

Tabell 5: Statistikk over talet på avgjorte klagesaker sortert etter grunnlag i 2022, 2021 og 2020.

Talet på avgjorte klagesaker sortert etter grunnlag	Tal for 2022	Tal for 2021	Tal for 2020
Funksjonsnedsetting	111	124	96
Etnisitet	97	95	97
Alder	93	46	59
Kjønn	43	77	51
Individuell tilrettelegging for funksjonsnedsette	29	26	9
Seksuell trakassering	23	25	10
Omsorgsoppgåver	18	21	12
Politisk syn	18	17	4
Universell utforming – IKT	17	12	3
Ikkje opplyst om/ikkje verna	15	39	5
Graviditet	15	12	16
Gjengjelding etter varslings	16	8	-
Permisjon ved fødsel eller adopsjon	14	21	25
Livssyn	13	23	8
Religion	11	21	14
Kjønnsidentitet	10	15	6
Universell utforming - fysisk	9	11	13
Medlem i arbeidstakarorganisasjon	8	4	3
Kjønnsuttrykk	7	10	5
Seksuell orientering	7	5	4
Innhenting av opplysningar i tilsettingsprosessar	6	1	1
Lik lønn for arbeid av lik verdi	3	14	5
Arbeidsgjevar si utgreiingsplikt	2	1	1
Arbeidstakar sine rettar ved foreldrepermisjon	1	5	3
Arbeidsgjevar si opplysningsplikt ovanfor arbeidstakar	1	1	0
Individuell tilrettelegging for gravide	1	3	0
Innhald i læremiddel og undervisning	1	2	1
Arbeidsgjevar si opplysningsplikt ovanfor arbeidssøkjjar	1	2	0
Universell utforming – aktivitetsplikt	0	0	1

Me ser ei klar auke i saker som gjeld diskrimineringsgrunnlaget alder. Dei fleste av desse sakene er enten innanfor arbeidslivet, eller varer og tenester. Dei fleste av sakene innanfor samfunnsområdet varer og tenester, er saker mot utestadar med påstand om diskriminerande aldersgrenser.

Saker som gjeld universell utforming av IKT heldt også fram med å auka. Sakene gjeld i stor grad ulike appar og nettsider for varer og tenester og læremiddel i skulen som ikkje er universelt utforma. Dette er saker som krev både teknologisk og juridisk kompetanse. I behandlinga av klagesaker om universell utforming av IKT, er nemnda avhengig av Digitaliseringsdirektoratet sin kompetanse på dette området, der de tekniske sidene vert testa. På bakgrunn av testane, gjev direktoratet ei IKT-fagleg fråsegn til nemnda, som nemnda brukar i si juridiske vurdering av saka.

Som regel må det gjerast fleire testar og re-testar i den enkelte sak. Fyrst må ein klarleggja kva som ikkje er universelt utforma og deretter må ein gjera ein eller fleire re-testar for å verifisera om feilane er retta slik innklaga hevdar. I 2022 sendte Diskrimineringsnemnda 47 IKT-løysingar for testing og fråsegn til Digitaliseringsdirektoratet. Direktoratet har opplyst at arbeidet kravde 5,5 årsverk hjå dei. Saksbehandlingstida i denne typen saker er difor avhengig av kapasiteten i både Diskrimineringsnemnda og Digitaliseringsdirektoratet.

Dei fleste sakene som Diskrimineringsnemnda behandlar er innanfor arbeidslivet. Av 416 ferdigbehandla saker i 2022, gjaldt 177 av desse spørsmål om diskriminering/trakassering/gjengjelding i arbeidslivet. Heile 125 saker var innanfor samfunnsområdet varer og tenester i 2022. Til samanlikning var det berre 73 saker innanfor dette området i 2021.

Tabell 6: Statistikk over avgjorte klagesaker sortert etter samfunnsområde i 2022, 2021 og 2020.

Avgjorte klagesaker sortert etter samfunnsområde	Tal for 2022	Tal for 2021	Tal for 2020
Arbeidsliv	177	180	128
Varer og tenester	125	73	44
Offentleg forvaltning	47	68	59
Samfunnsliv	12	28	16
Utdanning	21	24	23
Bustad	15	24	18
Politi, rettsvesen mv.	6	13	16
Kombinasjon	3	10	4
Anna	10	9	3
Frivillig arbeid	1	0	2

Ingen av Diskrimineringsnemnda sine vedtak vart tekne inn for domstolane i 2022.

Me publiserer som nærast alle avgjerder som vert tekne av nemnda på heimesida vår, www.diskrimineringsnemnda.no og på Lovdata. Nokre få vert ikkje publisert på grunn av personvernomsyn eller fortrulegheit (gradering). Me publiserer [nyheitsartiklar](#) som omhandlar viktige avgjerder, og me har ei [abonnementsordning](#). Ved å melda seg på her, får ein tilsendt avgjerder og nyheitsartiklar frå den siste månaden.

Saker avgjort i forsterka nemnd

Forskrifta til diskrimineringsombudslova § 6 gjev nemndleiaren myndigheit til å avgjera at ei sak skal verta behandla i forsterka nemnd dersom særlege grunnar tilseier slik behandling. I 2022 vart fire saker behandla i forsterka nemnd.

Ei av sakene (sak 21/544) gjaldt spørsmålet om ein blomsterbutikk-kjede handla i strid med forbodet mot diskriminering på grunn av alder som følgje av lønssystemet til verksemda. Nemnda konkluderte med at systemet braut med lova, og tilkjente klagar kr 57 836 i erstatning for økonomiske tap. Nemnda tolka i den samanheng førearbeida til diskrimineringsombudslova, Prop. 80 L (2016-2017) side 106, som seier noko om den summen nemnda maksimalt skal kunne tilkjenne i erstatning (kr 10 000), opp mot innhaldet i den lovfastsette erstatningsheimelen i diskrimineringsombudslova § 12. På grunnlag av den totale rettskjeldesituasjonen, konkluderte nemnda med at lova sin klare ordlyd ikkje kunne setjast til sides. Nemnda kom soleis til at nemnda sin kompetanse difor ikkje er avgrensa til summen som var gjeven i førearbeida. [Avgjerda i sak 21/544 kan lesast på heimesida vår.](#)

Andre oppgåver

Arkiv og kjøp av nytt saksbehandlingssystem

Diskrimineringsnemnda har vore full-elektroniske sidan november 2018. I juni 2022 gjekk avtalen med Acos ut. Me skifta då sak- og arkivsystem frå Websak Basis til Elements Cloud levert av Sikri, etter ein offentlig kunngjort anskaffingsprosess. Diskrimineringsnemnda fekk hjelp frå Odin Prosjekt AS i prosessen, etter ein minikonkurranse om dette oppdraget.

Implementeringa og overgangen til det nye systemet tok mykje tid og ressursar internt. Det vart gjennomført ein risikoanalyse og ei vurdering av personvernkonsekvensar i forkant av implementeringa. I etterkant opplevde me mykje problem, både generelt med å få alle tilsette og nemnda over i det nye systemet, og problem knytt til mottak av post gjennom dei elektroniske skjemaane samt statistikken på nettsidene våre. Dette var eit arbeid som strekte seg over fleire månadar og involverte fleire av dei tilsette i sekretariatet. Me måtte også avlysa nemndmøta i juni og august som følgje av overgangen.

Ved overgangen vart det oppretta ein historisk base der dei pågåande sakene vart migrert over. På eit seinare tidspunkt, når uttrekk frå Elements Cloud skal avleverast til Arkivverket, vil historisk base avleverast på same måte.

I tillegg vart det oppretta ein eigen arkivdel i produksjonsbasen i Elements Cloud, der me skal digitalisera arkivet etter Likestillings- og diskrimineringsnemnda. Dette arkivet er allereie ordna av ASTA, men fordi digital pliktavlevering står på trappene til å bli vedteke, og me er samde i at dette arbeidet både er samfunnsøkonomisk og bedriftsøkonomisk lønsamt, startar me arbeidet no. Dette er eit prosjekt me vil jobba med over tid. Oppgraderinga er i tråd med den nasjonale strategien for bruk av skytenester, og me vonar at dette, saman med dei integrerte applikasjonane våre, vil gjera saksbehandlinga og kommunikasjonen med partane våre meir tilgjengeleg og effektiv.

Nettstaden

Arbeidet med nettstaden i 2022 har i all hovudsak dreidd seg om å få nettsidene i tråd med dei komande krava i WCAG 2.1. Dette har vore svært viktig for oss med omsyn til at alle skal kunna bruka dei og all den tid det er me som skal ta imot klagesaker på tilgjengelegheitsfråsegner. Året har difor vore prega av fleire hendingar som me ikkje hadde føresett omfanget av på førehand.

Som planlagt, vart fyrste kvartal brukt til å jobba med utvikling av nettsidene, der målet var å få dei i tråd med dei komande krava for universell utforming. Vår mellombelse IKT-ansvarlege i 2022, hadde fagleg bakgrunn frå Digitaliseringsdirektoratet, og gjennom dette fyrste hands kunnskap om kva som juridisk sett ligg i krava til tilgjengelegheitsfråsegna. IKT-ansvarleg stod soleis for mykje av arbeidet med klårgjering mellom oss og nettsideleverandøren. Endringane vart sette i produksjon fyrst seint på hausten, då me laut prioritera andre gjeremål fyrst.

På nettsidene våre har me ein søkefunksjon opp mot klagesaker, samt levande statistikk. Data som kjem opp her, vert direkte overført frå saksbehandlingssystemet vårt. Skifte av saksbehandlingssystem gjorde difor at me laut setja opp koplinga mellom saksbehandlingssystemet og nettsidene på nytt, og både nettsideleverandør og ny leverandør av saksbehandlingssystem måtte vera involverte. Overgangen baud på større utfordringar enn me hadde føresett og me jobba mykje med testing og feilsøking. Trass i førebuande møter med alle involverte, og ein plan for gjennomføring, var me ikkje i mål med denne delen av overgangen før seinhaustes 2022.

Kontrakten med nettsideleverandøren gjekk ut ved utgangen av 2022, slik at resten av hausten gjekk med til å offentlig kunngjera konkurranse og velgje leverandør for desse tenestene frå og med 2023. I prosjektgruppa sat

innkjøpsansvarleg, nettsideansvarleg, direktør og IKT-ansvarleg. Før sjølve overgangen jobba me med planlegging samt kompetanseoverføring mellom gamal og ny leverandør. IKT-ansvarleg og nettsideansvarleg hadde ansvaret for sjølve overgangen frå Diskrimineringsnemnda si side. Overgangen starta i desember, og var ferdig tidleg på nyåret 2023.

Promoteringskampanje

I 2022 gjennomførte Diskrimineringsnemnda ein kampanje retta mot «Pride»-markeringane i Bergen og Oslo i høve 50-års jubileet for opphevinga av den sokalla «homoparagrafen». Kampanjane var digitale og vart promotert via sosiale medium. I Bergen deltok også Diskrimineringsnemnda i Pride-markeringa ved å ha stand, og direktøren heldt eit føredrag om Diskrimineringsnemnda si myndigheit, og om kvifor ein skal bruka Diskrimineringsnemnda når ein opplever diskriminering og trakassering basert på seksuell orientering, kjønnsidentitet og kjønnsuttrykk.

Fagleg kompetanseutvikling

For å vera eit effektivt handhevingsapparat med høg kvalitet på avgjerdene som vert fatta, er det svært viktig at både nemnda og sekretariatet heldt seg fagleg oppdatert og vert sikra fagleg utvikling. Året 2022 var eit spanande år på fagfronten innanfor likestillings- og diskrimineringsfeltet og det vart gjennomført ei rekkje føredrag i nemnda våren 2022.

I februar 2022 hadde Sivilombodet v/seniorrådgjevar Aronsen eit føredrag for sekretariatet om korleis Sivilombodet behandlar tilsettingssaker. I april 2022 heldt professor Magne Strandberg ved Universitetet i Bergen eit føredrag for sekretariatet om bevisbyrderregelen i likestillings- og diskrimineringslova § 37. Bevisbyrderregelen og beviskravet i likestillings- og diskrimineringsretten har vore gjenstand for debatt det siste året, særleg etter Høgsterett sin dom i den sokalla «Mekanikarsaka» (HR-2020-2476-A). I ljøs av dette var Strandberg sitt føredrag særleg aktuelt for nemnda, og Strandberg heldt difor føredraget på nytt for nemnda og sekretariatet under sommarseminaret i juni 2022. I mai 2022 heldt professor Anne Marie Frøseth ved UiB eit føredrag for sekretariatet om diskrimineringsansvar ved trakassering på digitale medium.

I juni 2022 vart det gjennomført eit to-dagars sommarseminar for sekretariatet og nemnda. Hovudtemaet for seminaret var kjønns- og seksualitetsmangfald, der mellom anna FRI og Trantastisk heldt to lærerike føredrag for oss. Likestillings- og diskrimineringsombodet heldt også ein presentasjon av rettleiingstenesta si, samt eit føredrag om refleksjonar rundt konvensjonane som rettskjelde og døme frå diskrimineringsrapporten for 2021. Me hadde også føredrag om gjengjelding etter varsling og universell utforming av IKT, særleg sett opp mot dei nye krava i WCAG 2.1.

Sekretariatet fekk i tillegg våren 2022 presentert masteroppgåvene til to masterstipendiatar som hadde hatt skriveplass hjå Diskrimineringsnemnda hausten 2021. Begge stipendiatane hadde skrive oppgåver om seksuell trakassering, med noko ulik vinkling: ein av stipendiatane skreiv om den nedre grensa for seksuell trakassering i ljøs av «Mekanikardommen», medan den andre skreiv om dei materielle vilkåra og handhevinga av forbodet, med fokus på Diskrimineringsnemnda sin kompetanse til å handheva forbodet.

Våren 2022 prioriterte også sekretariatet kontakt med nokre av dei andre offentlege organa innanfor likestillings- og diskrimineringsfeltet: Likestillings- og diskrimineringsombodet og Barne-, ungdoms-, og familiedirektoratet. Me jobba mellom anna med korleis organa best mogleg kan utfylla kvarandre, innanfor dei rammene som regulerer det enkelte organ sine oppgåver. Me hadde også gode møte med Arbeidstilsynet om saker om gjengjelding etter varslingsfor å læra meir om kvarandre slik at me kan utfylla kvarandre best mogleg i slike saker.

Hausten 2022 var preget av eit stort arbeidspress og ressursutfordringar hjå sekretariatet. Dette påverka også det faglege opplegget. Dei resterande midlane på fagbudsjettet måtte omprioriterast, og det faglege opplegget hausten 2022 vart difor avgrensa. Det vart gjennomført eit internt føredrag av fagansvarleg hausten 2022, om skiljet mellom direkte og indirekte forskjellsbehandling.

Høyringsssvar

I 2022 gav Diskrimineringsnemnda seks høyringsssvar. Høyringsssvara omhandla forslag til ny arkivlov, forslag om forlenging av reglane om koronasertifikat, mellombelse endringar i lovverket som følgje av fordrivne frå Ukraina med rett til mellombels kollektivt vern, nytt lovforslag om forbod mot konverteringsterapi, utgreiing om gjennomføring av varslingsdirektivet i norsk rett og ratifikasjon av ILO-konvensjon nr. 190 om avskaffelse av vold og trakassering i arbeidslivet, og om endringar i arbeidsmiljølova sitt regelverk om trakassering. [Høyringsssvara våre kan lesast på nettsidene våre.](#)

IV. Styring og kontroll i verksemda

Vår overordna vurdering er at verksemda tilfredsstiller dei krava som vert stilt til styring og kontroll i ulike regelverk. Me har gode system, rutinar og arbeidsmetodar i verksemda.

Verksemda sine løns- og rekneskapstenester vert levert av Direktoratet for økonomiservice (DFØ) der me er fullservicekunde, og tenestene oppfyller krava som fylgjer av økonomiregelverket og økonomiinstruksen. I tillegg er økonomi-, innkjøp- og HR-ansvarleg hjå oss controller. Riksrevisjonen reviderer

rekneskapen vår. Innkjøp vert gjort i tråd med regelverket for offentlege anskaffingar og vår interne rutine for innkjøp.

Tryggleik og beredskap

Diskrimineringsnemnda jobbar jamt med tryggleik, beredskap og kontinuitet for å oppfylle gjeldande krav og føringar til digital tryggleik, informasjonstryggleik og personvern. I den samanheng visar me til vedlagte rapport om det konkrete arbeidet på området for tryggleik, kontinuitet og beredskap i løpet av året.

Personvern

Diskrimineringsnemnda har gode system for å ivareta personvernprinsippa og informasjonstryggleiken ved behandlinga av personopplysningar. I internkontrollsystemet vårt har me ei samling dokument som skildrar rutinar og emne på personvernfeltet. Denne samlinga er ei viktig kjelde til oversikt og felles kunnskap for alle i verksemda, og ho vert oppdatert jamleg. I løpet av 2022 har det blitt lagt til ei rutine for sletting av personopplysningar og behandlingsoversikten har blitt oppdatert.

Ordninga med personvernombod har i 2022 vore organisert ved at to juridiske saksbehandlarar har blitt utpeika til oppgåva som personvernombod og fungerande personvernombod. Arbeidet er organisert som ei sideoppgåve til ordinær klagesaksbehandling for eit år om gangen.

Personvernombodet har eit fast punkt på dei månadlege verksemdsmøta, der meldte avvik i internkontrollsystemet vert gjennomgått, i tillegg til andre aktuelle saker på personvernfeltet.

I 2022 vart fråsegna for informasjonsskapslar på nettsida gjennomgått og oppdatert. I mars, i samband med skiftet av saksbehandlingssystem, gjennomførte personverngruppa og arkivleiar ein risiko- og sårbarheitsanalyse (ROS) av dei to systema det hadde komme tilbod på (Websak og Elements). Begge systema var NOARK-godkjende og vart vurdert til å oppfylle krava til informasjonstryggleik.

Etter at leverandør var valt, vart det gjennomført ei nærare vurdering av personvernkonsekvensar (DPIA). Dette arbeidet føregjekk i forkant av og parallelt med at systemet vart sett i drift.

Om hausten gjennomførte tilsette i sekretariatet medarbeidarundersøkinga MIST. Før medarbeidarundersøkinga, gjekk fungerande personvernombod og personvernombodet gjennom konsekvensar undersøkinga kunne ha for personvernet. Ved kjøp av ny leverandør for drift av nettsida, kom personvernombodet med innspel om mellom anna statistikkverktøy for nettsida.

Konsulentbruk

Sekretariatet for Diskrimineringsnemnda skal i fylgje tildelingsbrevet arbeida for å redusera konsulentbruken på områder der det ligg til rette for å bruka interne ressursar og kompetanse.

Diskrimineringsnemnda brukar konsulenttenester i svært lita grad. Så langt fagkompetansen er til stades i verksemda, freistar me alltid å få dekkja behova våre internt ved å frigjera kapasitet til gjennomføring av prosjekt.

I 2022 brukte me tenester frå Odin Prosjekt AS for å gjennomføra to offentlege anskaffingar over terskelverdi, hovudsakeleg på grunn av manglande kapasitet til å gjennomføra oppgåva sjølv, i tillegg til manglande tilgang på utlysingsverktøy i samband med kunngjering av konkurransar.

Lærlingar

I 2022 starta Diskrimineringsnemnda arbeidet med å knyta oss til Direktoratet for forvaltning og økonomistyring, OK Stat som opplæringskontor og faget service og administrasjon.

I prosessen fram mot å bli godkjend lærebedrift har Diskrimineringsnemnda utpekt to faglege leiarar. For å bli godkjend som lærebedrift, måtte faglege leiarar, og verksemda elles, godkjennast av fylkeskommunen. Dei faglege leiarane har delteke på kurs i regi av Vestland fylkeskommune for å fullføra ei todelt obligatorisk opplæring.

Diskrimineringsnemnda fekk godkjenning som lærebedrift i service og administrasjonsfaget 7. juni 2022. Dei faglege leiarane vart godkjende 18. oktober 2022. Fordi verksemda og faglege leiarar vart godkjent så seint på året, har me ikkje hatt moglegheita til å vurdere å ta inn lærlingar i 2022. Diskrimineringsnemnda har derimot fullført kravet om å knyta seg til eit opplæringskontor. Kravet i årets tildelingsbrev er soleis oppfylt.

Klima- og miljø

Diskrimineringsnemnda jobbar for å ha klima- og miljøomsyn med i vurderingane av korleis kontorkvardagen for dei tilsette skal vera, ved mellom anna bruk av meir heimekontor og digitale nemndmøter, mindre papirutskrift og resirkulering av boss. Verksemda undersøkte i 2021 om det var tiltak som kunne setjast i verk for å medverka til å nå dei nasjonale klima- og miljømåla. Dei aktuelle tiltaka vart iverksett via HMS-handboka vår. Det vart ikkje planlagt eller påbegynt ytterlegare tiltak i 2022 fordi me meinte det var tilstrekkeleg å vidareføra eksisterande tiltak.

Korleis Diskrimineringsnemnda oppfyller aktivitetsplikta i likestillings- og diskrimineringslova §§ 24 og 26

Del 1: Tilstand for kjønnslikestilling

Plikta til å kartleggja lønstilhøve fordelt etter kjønn og bruk av ufrivillig deltidsarbeid skal skje annakvart år. Kultur- og likestillingsdepartementet la til grunn at kartlegginga skulle skje fyrste gong for årsrapporten 2021. Neste rapportering på dette blir då i årsrapporten for 2023.

Lønsskartlegginga vert gjort i samarbeid mellom direktør og tillitsvalt. For 2022 vart det bestemt at kartlegginga skulle skje i gruppa for aktivitets- og utgreiingsplikta (ARP-gruppa), der også assisterande direktør, verneombod og ein juridisk saksbehandlar deltek.

Tabell 7: Kartlegging av kjønnsbalansen fordelt på stillingar og leiarstillingar i 2022. Studentengasjement er ikkje rekna med.

	Alle stillingar			Leiarstillingar		
	Talet på menn	Talet på kvinner	Totalt	Talet på menn	Talet på kvinner	Totalt
2022	6	18	24	1	3	4
2021	5	18	23	1	3	4
2020	5	16	21	1	2	3

Kartlegginga visar at kjønnsbalansen er ganske lik som tidlegare, med unntak av at me har fått ein ytterlegare mannleg tilsett. Dette er ein juridisk saksbehandlar i ei mellombels stilling på eit år. Kjønnsbalansen for dei faste tilsette er dermed den same som fjoråret.

Tabell 8: Kartlegging av kjønnsbalansen i sekretariatet for mellombelse tilsette, personar i foreldrepermisjon og deltidsarbeid. Tala refererer seg til alle som har vore tilsett i verksemda i løpet av 2022. Studentengasjement er ikkje rekna med.

	Mellombelse tilsette		Foreldre- permisjon		Faktisk deltid	
	Kvinner	Menn	Kvinner	Menn	Kvinner	Menn
2022:	0 %	100 %	3,1 %	0%	0	0
2021:	50%	50%	0,2%	0	6,3 %	0
2020:	50%	50%	1,7%	0	2 stk	0

Ingen tilsette jobba ufrivillig deltid. Dei mellombelse stillingane i 2022 var ei stilling som juridisk saksbehandlar, og ei stilling som juridisk rådgjevar i digitalisering, IKT og UU.

Del 2: Arbeidet vårt for likestilling og mot diskriminering

Diskrimineringsnemnda har som mål å vera eit førebilete for likestilling og ikkje-diskriminering i alt me gjer. Arbeidsplassen vår skal vera ein tilgjengeleg og god stad å arbeida for alle, og skal fremja likestilling og mangfald. Me ynskjer å ha ein jamn kjønnsbalanse og ha eit mangfald som speglar folkesetnaden elles. Dette står tydeleg i personalpolitikken vår.

Prinsipp, prosedyrar og standardar for likestilling og mot diskriminering

Likestillingsarbeidet vårt er forankra i personalpolitikken, ein eigen strategi for likestilling og mangfald, samt retningslinjer og rutinar elles i verksemda. Det står tydeleg i det skriftlege verdigrunnlaget vårt at Diskrimineringsnemnda verdsett mangfald og at likestilling er eit element me er medvitne om i alt me gjer.

I strategien vår for likestilling og mangfald skildrar me langsiktige og overordna mål som Diskrimineringsnemnda har som arbeidsgjevar, fordelt på dei ulike diskrimineringsgrunnlaga. Det vert også presisert kva overordna strategi Diskrimineringsnemnda har sett seg for å nå desse måla. Kvart år utarbeidar me handlingsplanar som ligg ved strategien, som vert fylgt aktivt opp gjennom året.

Slik jobbar me for å sikra likestilling og ikkje-diskriminering i praksis

Diskrimineringsnemnda jobbar aktivt, målretta og planmessig for å fremja likestilling og hindra diskriminering. Arbeidet er strukturert i ei eiga ARP-gruppe som er sett saman av direktøren, assisterande direktør, tillitsvalt, verneombod og ein juridisk saksbehandlar som prosjektleiar.

For å fylgje opp arbeidsgjevar si aktivitetsplikt etter likestillings- og diskrimineringslova § 26, gjennomførte Diskrimineringsnemnda ei risikokartlegging av dei ulike diskrimineringsgrunnlaga på ulike personalområder våren 2022.

Risikokartlegginga vart gjennomført av ARP-gruppa i form av ein workshop i mars 2022. Rettleiingane og malane frå Barne- ungdoms- og familiedirektoratet vart brukt som utgangspunkt for kartlegginga, i tillegg til risikokartlegginga som vart gjennomført året før.

Statistikk, medarbeidarsamtalar, medarbeidarundersøkingar og erfaringar vart brukt som grunnlag for risikovurderinga. Basert på risikovurderinga, vart det fastsett nye mål og tiltak som verksemda jobba vidare med gjennom året. Tiltaka vert presisert i ein handlingsplan med tilhøyrande fristar, og teke inn i verksemda sine verktøy for prosjektstyring.

Endringar som vert innført i verksemda sin personalpolitikk og andre skriftlege rutinar og retningslinjer som fylgje av ARP-arbeidet, vert presentert for dei tilsette i fellesmøte.

I desember 2022 gjennomførte ARP-gruppa ei evaluering av arbeidet med arbeidsgjevar si aktivitetsplikt. Her undersøkte me om me hadde gjennomført dei planlagde tiltaka for året og om tiltaka hadde den effekten me ynskte. I tillegg føretok me ei evaluering av korleis arbeidsprosessane rundt arbeidet og involveringa av dei tillitsvalte og tilsette fungerte, og om risikoundersøkingane me gjennomførte i år var tilstrekkelege, eller om me burde gjera andre typar undersøkingar.

Me oppdaga fylgjande risikoar for diskriminering og hindre for likestilling i 2022:

Under risikokartlegginga vert alle dei ulike grunnlaga på dei ulike områda som er nemnt i likestillings- og diskrimineringslova vurdert. ARP-gruppa tok utgangspunkt i risikovurderinga me gjennomførte i 2021, og vurderte om det var endringar i risikobilete eller om nye tiltak som burde setjast i verk. Gruppa var samde om at risikovurderinga frå fjoråret endå gav eit dekkande bilete. Samstundes vart det avgjort at me skulle gjennomføra nokre ytterlegare tiltak, spesielt på området for rekruttering. Dette fordi dette var eit område der me oppnådde minst resultat.

Oppfatninga vår er at Diskrimineringsnemnda generelt har gode rutinar, system og haldningar i verksemda som er eigna til å fremja likestilling og hindra diskriminering på ulike personalområder. Diskrimineringsnemnda har medarbeidarar med god kjennskap til, og interesse for, likestillings- og diskrimineringsregelverket. Det dannar eit godt grunnlag for ein arbeidsplass som fremjar likestilling og hindrar diskriminering. Nedanfor gjennomgår me dei funna som vart gjort på ulike personalområde, og kva tiltak som vart planlagt og iverksett i 2022.

Rekruttering

Diskrimineringsnemnda har ei målsetting om at våre tilsette skal spegla det faktiske mangfaldet i folkesetnaden. Me har endå ikkje fått det mangfaldet me ynskjer i tilsettegruppa, sjølv om det har blitt betra sidan etableringa i 2018. Me bestemte difor å setja inn nye tiltak på området i 2022.

Me ser det er lite mangfald i søkjarmassen vår. Difor vart mellom anna stillingsutlysingane som me har brukt tidlegare, nøyte gjennomgått i ARP-workshopen, og det vart føreslått fleire forbetringar. Det var semje om at det skulle utarbeidast eit nytt forslag til utlysingstekst for juridiske saksbehandlarar, der me mellom anna er ekstra nøyte på om me stiller for strenge kvalifikasjonar som gjer at søkjarmassen vår vert for snever. På grunn av manglande kapasitet, og fordi det ikkje var aktuelt å tilsette nokon i 2022, er tiltaket vidareført til 2023.

For å auke den interne kompetansen, deltok tilsetterepresentanten og tillitsvalt hausten 2022 på eit informasjonskurs om samarbeid med NAV i tilsettingsprosessar. Det vart i ettertid avgjort at Diskrimineringsnemnda skal vurdera deltaking i Traineeordninga for alle stillingar som vert lyst ut framover, og at Diskrimineringsnemnda så langt som mogleg skal freista å delta i ordninga. Dette vart teke inn og presisert i tilsettingsrutinen for Diskrimineringsnemnda. Det vart også avgjort at me ved neste rekruttering tek kontakt for å inngå eit samarbeid med NAV.

I juni 2022 oppdaterte me rutinen for tilsetting, og tok inn verkemiddel ein kan bruka i rekrutteringsprosessen, slik at me skal vera meir medvitne på dette i neste tilsettingsprosess.

Det vart ikkje gjennomført ordinære tilsettingsprosessar i 2022. En juridisk mann vart tilsett av direktøren i ei mellombels stilling som varar i eit år. Me har difor ikkje hatt moglegheit til å vurdera effekten av dei nye tiltaka endå.

Opprykk og utviklingsmoglegheiter

Personalpolitikken vår har tydelege kriterium for å sikra at stillingsopprykk vert gjeve på grunn av evner, prestasjonar, arbeidsoppgåver, kvalifikasjonar, erfaringar mv. Desse krava er like for alle. Det vart ikkje vurdert at det føreligg nokon risiko for diskriminering eller hindre for likestilling for nokre av diskrimineringsgrunnlag under dette personalområdet. Det vart difor heller ikkje planlagt tiltak for dette feltet i 2022.

I 2021 vart det gjort ei presisering av utviklingsmoglegheiter for alle i personalpolitikken, samt rettar for gravide og foreldre som er i permisjon. Det var for tidleg å måla resultatet av tiltaka i fjor. Det vart difor bestemt å måla effekten av desse tiltaka ved å undersøkje det i medarbeidarundersøkinga for 2022.

I medarbeidarundersøkinga som vart brukt i 2022, var det ikkje mogleg å leggja til eigne spørsmål. Undersøkinga var difor ikkje eigna til å måla effekten av tiltaka me sette i verk i 2021. Til neste år har me difor bestemt at me skal vurdere om det er andre måtar som eignar seg til å måla effekten av tiltaka på.

Tilrettelegging for mangfald og moglegheit for å kombinera arbeid og familieliv
Diskrimineringsnemnda har ein tydeleg og uttalt ambisjon om å leggja til rette for tilsette som treng det, både som fylgje av til dømes funksjonsnedsetting, omsorgsoppgåver eller etnisitet. Fleksibel arbeidstid er med på å løysa nokre av dei praktiske utfordringane det er å kombinera arbeid og familieliv. I tillegg startar me aldri dei faste møta våre tidlegare enn kl. 09.00 og sluttar seinast kl. 14.30. Me har ei eiga allergi-liste for dei tilsette, og sørgjer for at det vert tilbydt likeverdige alternativ.

Etter risikokartlegginga i 2021, vart det gjennomført fleire tiltak på dette området, sjølv om risikoen vart vurdert som låg. Det vart ikkje avdekka ytterlegare risikoar eller hinder for likestilling etter gjennomgangen i 2022. Det har soleis ikkje blitt sett i gang nye tiltak på dette området i 2022.

Eit tiltak som vart vidareført frå 2021 til 2022 var å undersøkje moglegheita for eit universelt utforma saksbehandlingssystem. Dette tiltaket vart gjennomført i 2022. Arkivforskrifta § 11 stiller derimot krav til at offentlege organ skal bruka Noark-godkjende system ved elektronisk journalføring og arkivering. Av dei systema som er Noark-godkjende, tilfredstilte ingen krava til universell utforming. Det var difor ikkje mogleg å kjøpa eit universelt utforma saksbehandlingssystem.

Løn og arbeidstilhøve

Personalpolitikken inneheldt tydelege vilkår for fastsetting av løn på ulike stillingsnivå, lønsutvikling og individuelle lønsforhandlingar. Ved risikovurderinga avdekka me ingen risiko for diskriminering eller hinder for likestilling på dette området, og det vart difor heller ikkje planlagt tiltak.

Diskrimineringsnemnda har sjølv sagt som mål at tilsette skal ha lik løn for arbeid av lik verdi. I medarbeidarundersøkinga hausten 2022 rapporterte to personar at dei opplevde at tilsette var blitt ulikt behandla på grunn av kjønn, og ein person rapporterte om forskjellsbehandling på grunn av alder. Me har grunn til å tru at rapporteringa rettar seg mot området løn. Dette skal verksemda undersøkje og arbeida vidare med i 2023.

Hindra trakassering, seksuell trakassering og kjønnsbasert vald

Diskrimineringsnemnda har nulltoleranse for mobbing, diskriminering, trakassering og vald. Dette går tydeleg fram av personalpolitikken og strategien for likestilling og mangfald. Me har ei eiga retningslinje for konflikthandtering.

Verksemda har tydelege rutinar for varsling og handtering av saker om trakassering, og desse er gjort kjend og er lett tilgjengeleg for dei tilsette i verksemda. Me vurderer at risikoen for at tilsette kan bli utsett for nokon form for trakassering eller vald er veldig låg.

Ingen tilsette meldte om trakassering, seksuell trakassering eller mobbing i medarbeidarundersøkinga for 2022.

Resultat av arbeidet og forventningar framover

Me er godt nøgde med gjennomførte tiltak og resultat så langt, men vil samstundes fortsetja å jobba med dette. Arbeidet i år har vore noko prega av det store arbeidspresset, der enkelte tiltak har blitt utsett av omsyn til kapasitet. Me tek likevel med oss evalueringa og tiltaka som står att vidare inn i arbeidet i 2023.

Likestillingsarbeid for Diskrimineringsnemnda som myndigheitsorgan

Diskrimineringsnemnda sitt samfunnsoppdrag er å jobba for eit Noreg med stadig mindre diskriminering og trakassering. Diskrimineringsnemnda har som mål å medverka til auka likestilling, mindre diskriminering og motarbeiding av stereotypisering gjennom utøvinga av samfunnsoppdraget. Dette jobbar verksemda med kvar dag gjennom å avgjera dei konkrete enkeltsakene som vert tekne inn for oss på ein effektiv måte og med høg kvalitet.

Diskrimineringsnemnda brukar heile det tildelte budsjettet til å medverka til redusert diskriminering og trakassering i Noreg. Dette gjer verksemda konkret både gjennom avgjerdene, skrivehjelp i klageprosessen for dei som treng det og gjennom oppdaterte nettsider med gode søkjeverktøy som for avgjerder og statistikk.

Vår oppfatning er at den beste måten Diskrimineringsnemnda som offentlig myndigheitsorgan kan gjera sitt for å fremja likestilling og hindra diskriminering, er å sikra kvalitetsmessig gode avgjerder innan kortast mogleg saksbehandlingstid. Samstundes må Diskrimineringsnemnda sitt samfunnsoppdrag, tenestetilbod og avgjerder bli gjort godt kjent blant folk flest. Dette vert gjort gjennom våre promoteringskampanjar, nettstaden vår, månadlege nyheitsbrev og gjennom informasjon om avgjerdene til media og relevante interesseorganisasjonar.

Offentlege myndigheiter si aktivitetsplikt inneber i tillegg ei plikt til å ivareta omsynet til likestilling og mangfald ved verksemda sitt offentlege tenestetilbod. Tenestetilbodet vårt, både klagesaksbehandlinga og nettstaden, skal være eit tilgjengeleg og likeverdig tilbod for alle.

Strategien for likestilling- og mangfald som me utarbeidde i 2021, skildrar langsiktige og overordna mål og strategiar for Diskrimineringsnemnda som offentleg myndigheitsorgan. Strategien skal vera eit styringsverktøy i dette arbeidet, og vert konkretisert i verksemda sitt årshjul og i årlege handlingsplanar.

Me får i hovudsak kunnskap om likestillingssituasjonen på alle diskrimineringsgrunnlag gjennom klagesaksbehandlinga, gjennom vår daglege medievarsling frå fysiske og sosiale medium og ved å samarbeida og utveksla erfaringar med andre aktørar, særleg i likestillingsfamilien.

I 2022 gjennomførte me møter med både Bufdir og LDO, både for å utveksla informasjon om samfunnsoppdraga våre, og i samband med Bufdir sin planlagde kampanje for mindre diskriminering basert på religion, livssyn og etnisitet. Me hadde også møter med Arbeidstilsynet, knytt til Diskrimineringsnemnda si myndigheit til å behandla klager på gjengjelding etter arbeidsmiljølov. Eit viktig tema i møta med Arbeidstilsynet var korleis organa kan utfylla kvarandre best mogleg innanfor dette feltet.

Korleis arbeidde verksemda med å omsetta prinsipp, prosedyrar og standardar for likestilling og ikkje-diskriminering til handling?

For å sørgja for at Diskrimineringsnemnda sitt samfunnsoppdrag og tenestetilbod vert godt kjent i samfunnet, er promoteringsarbeidet vårt ein viktig faktor. I 2022 gjennomførte Diskrimineringsnemnda ein kampanje retta mot «Pride»-markeringane i Bergen og Oslo i høve 50-års jubileet for opphevinga av den sokalla «homoparagrafen». I Bergen deltok også Diskrimineringsnemnda i Pride-markering ved å ha stand, og direktøren heldt eit føredrag om Diskrimineringsnemnda sin myndigheit og kvifor ein skal klaga til nemnda dersom ein opplever diskriminering eller trakassering.

Diskrimineringsnemnda er opptatt av å møta partane med respekt uavhengig av diskrimineringsgrunnlag, og bruka kjønnsnøytrale ord og uttrykk i all vår kommunikasjon ut, både skriftleg og munnleg. I juni 2022 vart de gjennomført eit to-dagars sommarseminar for sekretariatet og nemnda. Hovudtemaet for samlinga var kjønns- og seksualitetsmangfald, der mellom anna FRI og Trantastisk heldt føredrag. Me hadde også føredrag om gjengjelding etter varsling og universell utforming av IKT, særleg sett opp mot dei nye krava i WCAG 2.1.

I 2022 arbeidde me vidare med å sikra universell utforming av tenestetilbodet på nettsidene våre, hovudsakeleg for å få nettsidene i tråd med krava i WCAG 2.1. Dette er veldig viktig for oss fordi me vil at alle skal kunne bruka nettsidene våre på like vilkår.

Me har også jobba med universell utforming av dei elektroniske nettskjemaa våre, særleg i samband med at me fekk nye skjema sommaren 2022. Mykje av arbeidet til no har gått på tilgjengeliggjering for skjermopplesar. Dette arbeidet strekkjer seg inn i 2023. I samband med at me fekk nye elektroniske skjema, vart klageskjemaet oppdatert slik at det no er mogleg å velgje pronomen.

Resultata som vart nådd og forventningar framover:

Vi er godt nøgde med arbeidet me har lagt ned på dette området så langt. Me fekk diverre ikkje gjennomført den planlagde brukarundersøkinga av tenestene våre, fordi det verken var økonomi eller kapasitet til å gjennomføre dette i 2022. Tiltaket vert difor vidareført til neste år. Me ser også føre oss for at me i 2023 vil fortsetja å prioritera arbeidet med universell utforming av nettsidene våre.

V. Vurdering av framtidsutsikter

Stortinget etablerte Diskrimineringsnemnda med føremål om å sikra eit godt og effektivt lågterskeltilbod, og eit alternativ til dei ordinære domstolane, i saker om diskriminering og trakassering. Grepet var viktig for å redusera diskriminering og trakassering i Noreg og for å oppfylle Noreg sine folkerettslege plikter. Sidan oppstarten i 2018, har nemnda ferdigbehandla 1556 saker innanfor sitt felt.

Frå og med 1. januar 2020 vart nemnda gjeve myndigheit til sivilrettsleg behandling av saker om seksuell trakassering. Frå og med 1. juli 2021 vart nemnda gjeve myndigheit til å behandla saker om gjengjelding etter varslings. Begge desse myndigheitstildelingane er eit supplement til slik behandling i dei ordinære domstolane og vart gjort for å senka terskelen for å ta slike saker inn til rettsleg avgjerd. Praksis og ei rekkje undersøkingar viste nemleg at svært få slike saker vart tekne inn for dei ordinære domstolane. Vidare er nemnda si myndigheit også utvida knytt til EU si skjerping av reglane om universell utforming. Nemnda er no også føreslått som handhevingsorgan for EU si neste skjerping (Tilgjengelighetsdirektivet) på dette området. Ein reknar med at direktivet får verknad frå og med 2025. Nemnda er i tillegg gjeven handhevingsmyndigheita knytt til arbeidsgjevar si skjerpa aktivitets- og utgreiingsplikt.

Talet på saker inn i nemnda er nærast dubla samanlikna med 2020. Diskrimineringsnemnda ser positivt på, og er nøgde med, at fleire brukar klageetilbodet. Dette vitnar både om at tilbodet som nemnda leverer vert meir kjend, men også at Diskrimineringsnemnda kan spela ei sentral rolle for å løysa dei utfordringane Noreg endå har med omsyn til diskriminering og manglande likestilling. Diskrimineringsnemnda står no i eit skjeringspunkt. Talet på tilsette har ikkje auka i takt med auken i saksmengda. Me har heller aldri hatt så store restansar som me har no, og saksbehandlingstida har diverre vore aukande sidan 2021.

I tillegg opplever nemnda kritikk frå ulike hald. Noko av kritikken skuldast nok diverre at feil eller unyansert faktum vert lagt til grunn for vurderingane som ligg bak kritikken, medan andre tilhøve er noko me absolutt lyt sjå nærare på og finna gode løysingar på. Me ser difor fram til evalueringa av nemnda som skal finna stad i 2023 og meiner ei slik evaluering er ein god måte å gripa fat i dette på.

Eit kvalitetsmessig godt og effektivt handhevingsorgan, er ein kostnadseffektiv og avgjerande enkeltfaktor i eit samla system for å redusera diskriminering, trakassering og gjengjelding. Det gjeld særleg dersom ein samanliknar driftskostnadane med dei samfunnskostnadane dagens tilstand har. Diskrimineringsnemnda treng ei vesentleg og varig økonomisk styrking framover.

Me treng også å sjå nærare på om andre delar at nemnda sine rammevilkår bør justerast noko slik at me kan møte dei som brukar nemnda på ein betre måte.

Ved å rusta og dimensjonera Diskrimineringsnemnda for framtida, vil nemnda kunne utføra samfunnsoppdraget sitt slik meininga har vore frå starten, og kunna fortsetja arbeidet på same nivå som fram til no. Det gjeld både med omsyn til å levera eit godt og trygt alternativ på feltet, med avgjerder av høg kvalitet, men også å vera ein sentral aktør innan Noreg sitt system for arbeidet mot diskriminering og for likestilling. Det skal ikkje vera tvil om at Diskrimineringsnemnda ynskjer at folk skal kjenna til tilbodet vårt, bruka det når dei har behov for det, og oppleve nemnda som eit effektivt og godt lågterskelalternativ til dei ordinære domstolane.

VI. Årsrekneskap

Kommentar frå leiaren om årsrekneskapen 2022

Nemnda fører rerekneskapen i tråd til kontantprinsippet.

Stadfesting

Årsrekneskapen er avlagt i tråd med føresegner om økonomistyring i staten, rundskriv R-115 frå Finansdepartementet og krav frå Kultur- og likestillingsdepartementet i instruks om økonomistyring. Rekneskapen gjev eit dekkjande bilete av nemnda sine tilgjengelege løysingar, samt rekneskapsførte utgifter og inntekter.

Vurderingar av vesentlege tilhøve

Diskrimineringsnemnda hadde ei samla tildeling på 26 325 888 i 2022 samt 232 000 i refusjonar frå Norsk kulturråd på utlånt personell frå våren 2022. Artskontorrapporteringa visar at rapporterte utgifter til drift (eksklusiv løn) utgjorde 6 229 671 kroner. Utbetalingar til løn og sosiale utgifter var på 19 473 324 kroner.

Riksrevisjonen er ekstern revisor, og stadfestar rekneskapen for Diskrimineringsnemnda. Årsregnskapet er per i dag ikkje ferdig revidert, men me forventar at revisjonsrapporten kjem i løpet av våren 2023, seinast 1. mai. Rapporten vil bli publisert på heimesida Diskrimineringsnemnda.

Bergen, 13.03.2023


Ashan Nishantha
direktør

Prinsippnote til årsrekneskapen

Årsrekneskapen til Diskrimineringsnemnda er utarbeidd og avlagt etter nærare retningslinjer fastsett i føresegnar om økonomistyring i staten («føresegnene»). Årsrekneskapen er i tråd med krava i føresegnene punkt 3.4.1, Finansdepartementet sitt rundskriv R-115 og eventuelle krav slått fast at overordna departement. Oppstillinga av løyvingsrapporteringa og artskontorrapporteringa er utarbeidd med utgangspunkt i føresegnene punkt 3.4.2 – dei grunnleggande prinsippa for årsrekneskapen:

- a) Rekneskapen fylgjer kalenderåret
 - b) Rekneskapen inneheldt alle rapporterte utgifter og inntekter for rekneskapesåret
 - c) Utgifter og inntekter er ført i rekneskapen med brutto beløp
 - d) Rekneskapen er utarbeidd i tråd med kontantprinsippet
- Oppstillingane av løyvings- og artskontorrapportering er utarbeidd etter dei same prinsippa, men gruppert etter ulike kontoplanar. Prinsippa samsvarar med krav i føresegnene punkt 3.5 til korleis verksemdene skal rapportera til statsrekneskapen. Sumlinja «*Netto rapportert til løyvingsrekneskapen*» er lik i båe oppstillingar.

Verksemda er knytt til staten si konsernkontoordning i Norges Bank i tråd med krav i føresegnene punkt 3.7.1. Bruttobudsjetterte verksemdar får ikkje tilført likviditet gjennom året, men har ein rett til trekk på konsernkontoen sin. Ved årsslutt vert saldoen nullstilt på den enkelte oppgjerskonto ved overgang til nytt år.

Oppstilling av løyvingsrapportering

Oppstillinga av løysingsrapportering omfattar ein øvre del med løysingsrapporteringa, og ein nedre del som visar behaldningar verksemda står oppført med i kapitalrekneskapen. Løysingsrapporteringa visar rekneskapstal som verksemda har rapportert til statsrekneskapen. Det vert stilt opp etter dei kapitela og postar i løysingsrekneskapen som verksemda har fullmakt til å disponera. Kolonna «*samla tildeling*» visar kva verksemda har fått stilt til disposisjon i tildelingsbrev for kvar statskonto (kapittel/post). Oppstillinga visar i tillegg alle finansielle eigendelar og plikter verksemda står oppført med i staten sitt kapitalrekneskap.

Oppstilling av artskontorapportering

Oppstillinga av artskontorapporteringa har ein øvre del som visar kva som er rapportert til statsrekneskapen etter standard kontoplan for statlege verksemder og en nedre del som visar eigendelar og gjeld som inngår i mellomverande med statskassa. Artskontorapporteringa visar rekneskapstal verksemda har rapportert til statsrekneskapen etter standard kontoplan for statlege verksemder.

Verksemder har ein rett til trekk på konsernkonto i Norges Bank. Tildelingane er ikkje inntektsført og difor ikkje vist som inntekt i oppstillinga.

Oppstilling av løyvingrapportering 31.12.2022

Utgiftskapittel	Kapittelnamn	Post	Posttekst	Note	Samla tildeling *	Rekneskap 2022	Meirutgift (-) og mindretgift
0350	Sekretariatet for Diskrimineringsnemnda	01	Driftsutgifter	A,B	26 325 888	25 470 994	854 894
325	Stimuleringsmidlar til kultur, frivilligheit og idrett ism. Covid-19	77	Driftsutgifter		232 000	232 000	
1633	Nettoordning, statleg betalt meirverdiavgift	01	Driftsutgifter			766 831	
Sum utgiftsført					26 557 888	25 702 994	854 894

Inntektskapittel	Kapittelnamn	Post	Posttekst	Note	Samla tildeling *	Rekneskap 2022	Meirutgift (-) og mindretgift
5309	Tilfeldige inntekter	29	Tilfeldige inntekter	Ymse	0	26 176	
5700	Tilfeldige inntekter Folketrygda sine inntekter	72	Arbeidsgjevaravgift - Folketrygda	Arbeidsgjevaravgift	0	2 386 286	
Sum utgiftsført						2 412 462	
	Netto rapportert til løyvingrekneskapen					23 290 532	
	Kapitalkontoar						
60089201			Norges Bank KK /innbetalingar			519 600	
60089202			Norges Bank KK/utbetalingar			-24 012 685	
708049			Endring i mellomverande med statskassen			-564 279	

Sum rapportert				-766 831	
----------------	--	--	--	----------	--

Behaldningar rapportert til kapitalrekneskapet (31.12)				
Konto	Tekst	31.12.20 21	31.12.20 22	Endring
708049	Mellomverande med statskassen	-914 520	-1 478 799	-564 279

Note A Forklaring av samla tildeling utgifter			
Kapittel og post	Overført frå i fjor	Årets tildelingar	Samla tildeling
350-01	905 888	25 420 000	26 325 888
325-77		232 000	232 000

Note B Forklaring til brukte fullmakter og berekning av mogleg overførbart beløp til neste år				
Kapittel og post	Stikkord	Meirutgift (-)/ mindre utgift	Sum grunnlag for overføring	Mogleg overførbart beløp berekna av verksemda
350-01		854 894	854 894	854 894

Forklaring til bruk av budsjettfullmakter

Diskrimineringsnemnda sitt sekretariat vart gjeven ei fullmakt til å belasta statsbudsjettet, kap. 325-77 i samband med at me lånte ut ein av våre juridiske saksbehandlarar til Norsk kulturråd i ein 3-månaders periode etter spørsmål frå departementet.

Det vart ført totalt kr. 232 000 på belastningsfullmakta på kap. 325-77, som tilsvara utgifttapet vårt i samband med utlånet.

Oppstilling av artskontorrapporteringa 31.12.2022 inkl. utgiftskapittel 325-77			
	Note	2021	2022
Driftsutgifter rapportert til løyvingsrekneskapen			
Utbetalingar til løn	2	19 066 947	19 473 324
Andre utbetalingar til drift	3	5 919 068	6 229 671
<i>Sum utbetalingar til drift</i>		<i>24 986 015</i>	<i>25 702 995</i>
Netto rapporterte driftsutgifter		24 986 015	25 702 995
Investerings- og finansutgifter rapportert til løyvingsrekneskapen			
Utbetaling til investeringar/ datamaskiner	5	432 735	
<i>Sum investerings- og finansutgifter</i>		<i>432 735</i>	
Netto rapporterte investerings- og finansutgifter		432 735	
Innkrevingsverksemd og andre overføringer til staten			
Innbetaling av skattar, avgifter, gebyr m.m.	6	-1 945	0
<i>Sum innkrevingsverksemd og andre overføringer til staten</i>		<i>-1 945</i>	<i>0</i>
Inntekter og utgifter rapportert på felleskapittel *			
Gruppelivsforsikring konto 1985 (ref. kap. 5309, inntekt)		-26 483	26 176
Arbeidsgjevaravgift konto 1986 (ref. kap. 5700, inntekt)		-2 349 288	2 386 286
Nettoføringsordning for meirverdiavgift konto 1987 (ref. kap. 1633, utgift)		813 367	766 831
<i>Netto rapporterte utgifter på felleskapittel</i>		<i>-1 562 404</i>	<i>-1 645 631</i>
Netto rapportert til løyvingsrekneskapen		23 854 400	24 057 363

Oversikt over mellomverande med statskassen	Note	2021	2022
Fordringar på tilsette		0	0
Kontantar		0	0
Bankkontoar med statlege middel utanfor Norges Bank		0	0
Skuldig skattetrekk og andre trekk		-917 930	-1 041 436
Skuldige offentlege avgifter		0	0
Pensjonspremie sett av til Statens pensjonskasse		0	-437 363
Mottatte forskotsbetalingar		0	0
Løn (negativ netto, for mykje utbetalt løn m.m.)		3 410	0
Differansar på bank og uidentifiserte innbetalingar		0	0
Sum mellomverande med statskassen	8	-914 520	-1 478 799
Kontrollsum netto rapportert til løyvingsrekneskapen			
Artskontorrapportering		23 854 400	24 057 363
Løyvingsrapportering		23 854 400	23 290 532
Kontrollsum mellomverande med statskassen			
Artskontorrapportering		-914 520	-1 478 799

Løyvingsrapportering		-914 520	-1 478 799
----------------------	--	----------	------------

Note 2 Utbetalinger til løn		
	31.12.2021	31.12.2022
Løn	14 233 450	14 758 328
Arbeidsgjevaravgift	2 349 288	2 386 286
Pensjonsutgifter	1 607 023	976 168
Sjukepengar og andre refusjonar (-)	-573 337	-510 650
Andre ytingar	1 450 523	1 863 192
Sum utbetalinger til løn	19 066 947	19 473 324

Note 3 Andre utbetalinger til drift		
	31.12.2021	31.12.2022
Husleige	2 041 281	2 106 652
Vedlikehald egne bygg og anlegg	0	0
Vedlikehald og ombygging av leigde lokale	39 864	
Andre utgifter til drift av eigedom og lokale	623 361	786 107
Reparasjon og vedlikehald av maskiner, utstyr mv.	0	1 857
Mindre utstyrskjøp	19 450	-503
Leige av maskiner, inventar og liknande	577 972	285 535
Kjøp av konsulenttenester	18 835	138 167
Kjøp av andre framande tenester	1 504 874	2 145 731
Reiser og diett	115 575	131 317
Andre driftsutgifter	977 855	634 808
Sum andre utbetalinger til drift	5 919 068	6 229 671

Note 5 Utbetaling til investeringar og kjøp av aksjar		
	31.12.2021	31.12.2022
<i>Utbetaling til investeringar</i>		
Immaterielle eigedelar og liknande	0	0
Tomter, bygningar og annan fast eigedom	0	0
Infrastruktureigedelar	0	0
Maskiner og transportmiddel	0	0
Driftslausøyre, inventar, verktøy og liknande	432 735	0
Sum utbetaling til investeringar	432 735	

Note 6 Innkreivingsverksemd og andre overføringer til staten		
	31.12.2021	31.12.2022
Gruppelivsforsikring	-26 483	0
Tilfeldige inntekter	-1 945	
Sum innkreivingsverksemd og andre overføringer til staten	-28 428	0

Note 9 Samanheng mellom avrekning med statskassa og mellomverande med statskassa			
Del A Skilnaden mellom avrekning med statskassa og mellomverande med statskassa	31.12.2022	31.12.2022	
	Spesifisering av <u>bokført</u> avrekning med statskassa	Spesifisering av <u>rapportert</u> mellomverande med statskassa	Skilnad
Finansielle anleggsmiddel			
Investeringar i aksjar og andelar*	0	0	0
Obligasjonar	0	0	0
Sum	0	0	0
Omløpsmiddel			
Kundefordringar	0	0	0
Andre fordringar	0	0	0
Bankinnskot, kontantar og liknande	0	0	0
Sum	0	0	0
Langsiktig gjeld			
Anna langsiktig gjeld	0	0	0
Sum	0	0	0
Kortsiktig gjeld			
Leverandørgjeld	-1 017 919	0	-1 017 919
Skuldig skattetrekk	-1 041 436	-1 041 436	0
Skuldige offentlege avgifter	0	0	0
Anna kortsiktig gjeld	-183 655	-437 363	253 708
Sum	-2 243 011	-1 478 799	-764 212
Sum	-2 243 011	-1 478 799	-764 212
Kontrollsum rapportert mellomverande med statskassen			
Rapportert mellomverande med statskassen note 9		-1 478 799	

Løyvingsrapportering		-1 478 799	
----------------------	--	------------	--

Table of Contents

Vedlegg 1 til årsrapporten	2
ROS-vurdering ny nettsideleverandør	4
ROS-rapport ny nettsideleverandør	17
ROS-vurdering nytt saksbehandlingssystem - Elements	27
ROS-rapport nytt saksbehandlingssystem - Elements	33
ROS-vurdering nytt saksbehandlingssystem - Websak	43
ROS-rapport nytt saksbehandlingssystem - Websak	49
DPIA nytt saksbehandlingssystem	59

Vedlegg 1 til årsrapporten til Diskrimineringsnemnda

Unnateke offentlegheit, jf. offl. § 24, tredje ledd

Diskrimineringsnemnda jobbar jamt med tryggleik, beredskap og kontinuitet for å oppfylle gjeldande krav og føringar til digital tryggleik, informasjonstryggleik og personvern.

Diskrimineringsnemnda organiserer arbeidet i ei eiga tryggleiksgruppe, kalla «sikkerhetsgruppen». I 2022 har sikkerhetsgruppen vore sett saman av assisterande direktør (leiar av gruppa), rådgjevar innan digitalisering, IKT og UU, personvernombodet og ein ekstra personvernressurs. Gruppa møtest jamleg og jobbar med utgangspunkt i *NSMs grunnprinsipp for IKT-sikkerhet* og *Nasjonal strategi for digital sikkerhet*. Sikkerhetsgruppen er i tillegg med i *Nettverk for informasjonssikkerhet* i regi av Digitaliseringsdirektoratet, og deltek jamleg på dei gratis kursa som vert tilbydt der. Vidare kjem det viktige arbeidet som arkivtenesta vår gjer, som også har stor betydning for det samla tryggleiksarbeidet vårt. Endeleg har me eit løpande og godt samarbeid med IT-driftsleverandøren vår, der me har strenge krav til både informasjonstryggleik og personvern i avtalen mellom oss. Også dette er viktige aspekt i tryggleiksarbeidet vårt.

I 2021 gjennomførte KPMG ei temperaturmåling i Diskrimineringsnemnda, for å kartleggja status på informasjonstryggleik. Dette vart gjort på oppdrag frå Kultur- og likestillingsdepartementet og Digitaliseringsutvalet. Denne målinga viste at Diskrimineringsnemnda hadde tilfredsstillande kontroll innan dei aller fleste av NSM sine grunnprinsipp, og sikkerhetsgruppen jobba hausten 2021 med å fylgja opp og gjennomføra dei tilrådde tiltaka som kom fram i temperaturmålinga. Alle tiltak vart gjennomført hausten 2021, med unntak av eitt, altså å gjennomføra ein årleg, overordna risiko- og sårbarheitsanalyse (ROS) for informasjonstryggleik.

Trass i eit utfordrande tryggleiksbudsjett, vart det likevel gjennomført fleire aktivitetar i 2022, i tillegg til jamlege møte i sikkerhetsgruppen. I den samanheng er det verdt å trekkja fram kriseøvinga vår i april, der HMS stod sentralt. Kriseøvinga var eit fyrstehjelpskurs i regi av Bergen brannvesen. I tillegg tok alle dei tilsette i sekretariatet kurs i NSM sine grunnprinsipp i 2022, og informasjonstryggleik vart gjennomgått saman med nemnda i samband med sommarseminaret i juni. Under den nasjonale tryggleiksmånaden i oktober, gjennomførte sekretariatet i Diskrimineringsnemnda eit eigeprodusert opplegg som mellom anna inkluderte diskusjonsoppgåver. Det er viktig med ein slik årleg tryggleiksmånad for å styrka det daglege fokuset på informasjonstryggleik, kva trugslar me kan bli utsett for og korleis me kan avverja dei ulike trugslane. Krise-, kontinuitets- og beredskapsplanen vår vert oppdatert årleg i ljøs av

utviklinga på dette feltet. Våren og sommaren 2022 gjennomførte personverngruppa vår ROS og DPIA i samband med overgangen til nytt saksbehandlingssystem. Hausten 2022 vart det gjennomført ROS før kjøp av ny nettsideleverandør. Risikovurderingane fylgjer nedanfor. Risikovurderingane har ei sterk side til informasjonstryggleiksarbeidet vårt fordi personvern og informasjonstryggleik er tett samanvevd. Risikovurderingane vert i stor grad overlappende og ein del av vårt samla HMS-arbeid. Endeleg vart det gjennomført ei oppdatering av personvernfråsegnene våre på nettsida og innstillingane for informasjonsskapslar (cookies) der.

At 2022 har vore eit krevjande år med omsyn til kapasitet, visar seg også innanfor arbeidet med tryggleik og beredskap. Det siste tiltaket frå temperaturmålinga, vart opphæveleg skyvd på frå 2021 til 2022. ROSen var heller ikkje mogleg å gjennomføra i 2022, fordi ein slik ROS krev hjelp frå IT-driftsleverandøren vår. Det vart det diverre ikkje funne rom for på budsjettet for 2022. Diskrimineringsnemnda har halde overordna departement løpande orientert om utsettinga gjennom budsjettdialogen og i etatsstyringsmøta og planlegg å få utført denne i 2023.

ID	Risikobeskrivelse Stikkord om: (1) innledende hendelse(r) (2) informasjonssikkerhetsbruddet (3) de uønskede konsekvensene som kan oppstå	Begrunnelse for konsekvensvurdering
R1	Manglende/mangelfull vaktordning hos ny leverandør, som gjør at vi ikke får tilstrekkelig bistand ved avvikshåndtering (dvs. av-indeksering og fjerning feilpubliserte avgjørelser fra nettet på en rask og grundig måte). Kan innebære brudd på konfidensialitet.	Kan få konsekvens for DN's omdømme og tillit, parter og lovkrav dersom opplysningene spres. Settes til høy pga eventuelle konsekvenser for partenes rettssikkerhet.
R2	Leverandøren sletter ikke personopplysninger som de får som følge av avvikshåndteringen (fjerning og av-indeksering av avgjørelser). Kan innebære brudd på konfidensialitet.	Kan få konsekvenser for DN's omdømme og tillit, parter og lovkrav dersom opplysningene spres. Settes til høy pga eventuelle konsekvenser for partenes rettssikkerhet.
R3	I leverandørens avvikshåndtering (fjerning og av-indeksering av avgjørelser) behandler de personopplysninger for DN. Ansatte hos leverandøren med tilgang kan lekke personopplysninger som gjør at utenforstående kan få tilgang på personopplysninger i strid med vår taushetsplikt. Vil innebære brudd på konfidensialitet.	Kan få konsekvens for DN's omdømme og tillit, parter og lovkrav. Settes til høy pga eventuelle konsekvenser for partenes rettssikkerhet.
R4	Utsiktede personer hos nettsideleverandøren får tilgang til personopplysninger. Vil føre til brudd på konfidensialitet.	Kan få konsekvens for DN's omdømme og tillit, parter og lovkrav dersom opplysningene spres. Kan medføre at avvik må meldes til Datatilsynet. Konsekvensen derfor til høy.

R5	Ansatte hos leverandøren endrer innholdet eller oppbyggingen på nettsiden uautorisert. Dersom de endrer informasjon om personer som har sine opplysninger på nettstedet (nemnda, PVO, direktør), kan dette medføre brudd på integritet. Eksempelvis kan dette gjelde opplysninger som privat adresse. Eller at de legger ut meninger vi ikke kan stå inne for etc.	Kan få konsekvens for DN's omdømme og tillit. Kan medføre brudd på personregelverket. Kan måtte melde avvik til Datatilsynet.
R6	Rettighet og tilgang til løsningen kan gå tapt ved overgang til ny leverandør fordi tidligere leverandør motsetter seg skiftet. Brudd på tilgjengelighet.	Rettstvist (økonomi) og omdømme og tillit (manglende hjemmeside over lang tid). Merarbeid for sekretariatet.
R7	Løsningen eller data går tapt ved overgangen. Nettsiden bryter sammen eller deler mister funksjonalitet. Brudd på tilgjengelighet.	Konsekvensen er nedetid og ressursbruk med rekonstruksjon. Kan få konsekvenser for DN's omdømme dersom lang nedetid. Skjemaene er publisert på nettsidene, vil ikke være tilgjengelige dersom nettsiden er nede.
R8	Leverandøren går konkurs før avtaleperioden er over.	Må sette i gang ny prosess for å finne ny leverandør og overføre løsningen. Vil dermed gi økonomiske konsekvenser, men ikke i et svært stort omfang.

R9	Manglende IT-kompetanse i sekretariatet. Vi har liten kunnskap om hva som kan gjøres for å unngå risiko som teknisk svikt, og har derfor begrensede muligheter til å forebygge mot det	Konsekvensen er nedetid og ressursbruk med rekonstruksjon. Kan få konsekvenser for DN's omdømme dersom lang nedetid. Skjemaene er publisert på nettsidene, vil ikke være tilgjengelige dersom nettsiden er nede.
R10	De løsningene som Advenio har laget til oss spesifikt (API, nyhetsbrev, cookie-oppsett, kontaktskjema) er muligens satt opp på en ustandardisert måte. Vi risikerer at ny leverandør mangler kompetanse til å ivareta og videreutvikle en eller flere av disse løsningene.	Konsekvensen er ressursbruk med testing hos sekretariatet og potensielt at feil data eller andre feil i løsningen kan forekomme (feil søk og statistikk, manglende mottak av e-post via kontaktskjema, utkast til nyhetsbrev blir sendt ut). Særlig ved nedetid/feil på publisering av data fra rest-API fra Elements, vil kunne kreve svært høy ressursbruk for rekonstruksjon. Manglende avgjørelser ut på nett, fører til flere innsyns krav og det vil være krevende for den enkelte saksbehandler som ikke får ut saker. Vi har krav på oss fra departement og samfunn om å ha statistikk og avgjørelser tilgjengelig, men det er ikke lovfestet hvor hurtig slik tilgjengeliggjøring
R11	Nåværende leverandør er samarbeidspartner med IT-driftsleverandør Braathe. Vil en overgang innebære kontraktsbrudd med Braathe, evt. sikkerhetsbrudd da ny leverandør må ha tilgang til server hos Braathe?	Omdømme og eventuelt økonomi (rettstvist) dersom presmissene for å lyse ut vedlikehold er uklare
R12	Vi er avhengige av bistand for å løse endringsbehov vi måtte ha i fremtiden, ved endrede regelverk innen personvern (analyseverktøy og informasjonskapsler). Vi har derfor behov for å få gode opplysninger når vi spør, samt bistand til tekniske løsninger, i tråd med til enhver tids gjeldende regelverk. Manglende teknisk kompetanse og kjennskap til personvernlovgivningen hos en evt. ny leverandør innebærer at DN ikke klarer å oppfylle sine rettslige forpliktelser etter regelverket.	Kan få konsekvens for DN's omdømme og tillit, parter og lovkrav. DN klarer ikke oppfylle sine rettslige forpliktelser etter personvernregelverket.
R13	Nettstedet vårt bryter reglene om universell utforming fordi ny leverandør ikke har tilstrekkelig kompetanse på regelverket og de tekniske løsningene.	Kan få konsekvens for DN's omdømme og tillit, parter og lovkrav dersom vi ikke overholder regelverket. Særlig med tanke på at vi har en del brukere med funksjonsnedsettelse, og at det er vi som skal håndheve regelverket.

Konsekvens		Begrunnelse for vurdering av tilhørende sannsynlighet	Risikonivå
Tilhørende sannsynlighet			
Høy	Moderat	Vi har liten kunnskap om hvorvidt leverandører av vedlikehold av nettsider normalt innehar kompetanse om av-indeksering, men vi legger til grunn at de fleste har teknikere med nødvendig kompetanse, og en supportordning som kan strekke seg utenfor normal arbeidstid ved behov.	Moderat
Høy	Moderat	Risikoen avhenger av at leverandørens ansatte går ut over det som er avtalt bruk av opplysningen. Dersom de mangler rutiner, vil det like være en viss sannsynlighet for at opplysningene blir værende hos leverandøren.	Moderat
Høy	Lav	Sannsynlighet avhenger av at leverandørens ansatte går ut over det som er avtalt bruk av opplysningene i henhold til databehandleravtalen. I tillegg har vi få slike avvikssaker i året, da vi har gode interne rutiner. I tillegg er det lite sannsynlig at et av de få avvikene vi har i året, skal gjelde en sak som leverandøren kjenner til og kan misbruke.	Moderat
Moderat	Lav	Sannsynlighet avhenger av at leverandørens ansatte går ut over det som er avtalt bruk av opplysningene i henhold til databehandleravtalen. I tillegg har vi få slike avvikssaker i året, da vi har gode interne rutiner, og det er lite sannsynlig at et av de få avvikene vi har i året, skal gjelde en sak som leverandøren kjenner til og kan misbruke. Endelig er det slik at leverandøren ikke har behov for å lese avgjørelsen for å fjerne den/av-indeksere den	Lav

Moderat	Lav	Risikoen avhenger av at leverandørens ansatte opptrer med forsett og har en viss kunnskap om interne forhold. Videre avhenger risikoen av at leverandørens ansatte går ut over det som er avtalt.	Lav
Moderat	Lav	Løsningen ligger på servere driftet av Braathe Gruppen, som fortsatt vil være vår IT-driftslevernadør. Sannsynlighet for at tilgang til løsningen går tapt, vurderes derfor som meget lav.	Lav
Moderat	Lav	Teknisk svikt forekommer, men sjelden i omfang som fører til lang tids nedetid eller at data går tapt. Braathe tar back up og driften vil fortsatt ligge hos Braathe. I realiteten er overgangen, så vidt vi vet, at en ny leverandør får tilgang og adm.rettigheter.	Lav
Lav	Lav	I anbudsdokumentene (krav til leverandør) krever vi skatteattest.	Lav

Moderat	Lav	Braathe Gruppen har nettsiden på sin server (inkl.backup) og en gjenoppretting etter en eventuell teknisk svikt vil derfor være mulig. Vi har bistand inn i prosessen fra Odin, samt at det er kontraktsfestet at Advenio skal bistå.	Lav
Moderat	Høy	Mellom moderat og høy. Vi er usikre på hvor store deler av løsningen som er utenfor standard, men vi vet at APlet er noe utdatert, noe som kan føre til at ny leverandør ikke klarer å håndtere det (fort nok/uten startvansker). Samtidig skal alle store endringer gjøres i testløsning først. Utfordringen er dersom vi ikke oppdager feil i testingen, og vi sender ut/publiserer med feil.	Moderat
Moderat	Lav	Finnes ikke spor i kontrakten med Braathe som tilsier at Advenio skal ha eksklusiv tilgang. Det er forholdsvis vanlig at en ekstern leverandør må samarbeide med IT-driftsleverandør for tilgang og annet.	Lav
Høy	Moderat	Vi er usikre på hvor mye personvernaglig kompetanse som finnes i IT-bransjen. Vår erfaring så langt tyder på at denne er noe lav. Samtidig har vi selv både PVO og personvernressurs	Moderat
Høy	Høy	Vår erfaring så langt tilsier at det er lite kunnskap om UU i bransjen. Dette både pga vår erfaring med nåværende leverandør, og konkrete, enkle tester på andre leverandørers egne nettsider.	Høy

Vurdering av risikohåndtering	Konsekvens etter tiltak	Sannsynlighet etter tiltak	Gjenværende risiko
I konkurransedokumentene har vi beskrevet vårt behov, både hva gjelder fjerning og avindeksering, og tilgjengelighet på support, se krav 6. Ny leverandør beskriver overordnet sin løsning til krav 6 i bilag 2 hvor de presiserer at "personell får opplæring i hvordan de publiserte avgjørelsene skal fjernes, enten dette skjer i publiseringsverktøy eller på et mer teknisk nivå (database og lignende)". Dette vil også være tema når vi setter	Høy	Lav	Moderat
Det følger av databehandleravtalen punkt 6 at databehandler skal slette eller tilbakelevere alle personopplysninger til behandlingsansvarlig etter at tjenestene knyttet til behandlingen er levert, og slette eksisterende kopier inkludert eventuelle sikkerhetskopier, med mindre det er et lovmessig krav at personopplysningene fortsatt skal	Høy	Lav	Moderat
Leverandøren er profesjonell. Det følger av databehandleravtalen punkt 2 at databehandler har taushetsplikt om personopplysninger som vedkommende får tilgang til som en følge av avtalen med oss og behandling av personopplysningene, og at databehandler skal sikre at personer som er autorisert til å	Høy	Lav	Moderat
behandle personopplysningene har Leverandøren er profesjonell. Det følger av databehandleravtalen punkt 2 at databehandler har taushetsplikt om personopplysninger som vedkommende får tilgang til som en følge av avtalen med oss og behandling av personopplysningene, og at databehandler skal sikre at personer som er autorisert til å behandle personopplysningene har	Høy	Lav	Moderat
forpliktet seg til å behandle			

Avtalen mellom partene regulerer skriftliggjøring av hva som skal endres på nettsidene, og tilgang gis til et begrenset antall personer. Det følger av avtalen at partene skal holde hverandre oppdatert, at det skal føres protoll fra samarbeidsmøter. Logg i Umbraco synliggjør hvilken bruker som har endret hva.	Lav	Lav	Lav
Det følger av inneværende vedlikeholdsavtalen bilag 1 at leverandør skal overlevere teknisk dokumentasjon og kildekode ved opphør og at leverandør skal bistå i overgangen til ny leverandør.	Moderat	Lav	Lav
Vedlikeholdsavtalen med nåværende leverandør regulerer at de skal samarbeide ved overgangen. Vi har tatt kontakt med Braathe Gruppen og fått en fast person å forholde oss til samt sikre god kommunikasjon. Vi har avtalt med ny og nåværende leverandør at de skal samarbeide frem til ny leverandør er i stand til å håndtere løsningen, slik at alle parter får tilstrekkelig med tid til å gjøre overgangen god nok.	Moderat	Lav	Lav
Det følger av vedlikeholdsavtalen at vi kan heve avtalen med umiddelbar virkning ved konkurs.	Lav	Lav	Lav

Vi bør vurdere å skaffe oss kompetanse innen IT, som blant annet kan bistå i lignende prosesser i fremtiden.	Moderat	Lav	Lav
Advenio har gitt en skriftlig beskrivelse av løsningen vår, som går ut sammen med anbudsdokumentene, samt sendt ny leverandør dokumentasjon på løsningen. Vi vil kjøre backup på tilleggsattributter før overgang. Etter gjennomgangen av tilbudene og ved valget, antar vi at ny leverandør har korrekt kompetanse. Vi har satt av tid til over nyttår for overgangen, for å sikre god teknisk kompetanseoverføring fra Advenio til ny leverandør.	Lav	Moderat	Lav
Braathe Gruppen har skriftlig stadfestet at de ikke har utfordringer med at vi skifter leverandør, og at de vil bistå oss med å gi de tilgang til servere.	Moderat	Lav	Lav
Punkt 2 i databehandleravtalen regulerer blant annet databehandler skal sørge for at behandlingen av personopplysninger er i samsvar med gjeldende lov (personvernloven), hovedavtalen, avtalen samt eventuelle instruksjoner som er gitt av oss. Videre skal databehandler bistå oss i å svare på anmodninger fra de registrerte osv.. Det følger videre av avtalen at leverandør skal ha kompetanse på	Høy	Lav	Moderat
Det følger av avtalen bilag 2 krav 7 at leverandørens sentrale konsulenter har inngående kjennskap til WCAG-standarden og erfaring med universell utforming av både nettsteder og webapplikasjoner. De har god erfaring med testverktøy og å gjøre egne manuelle analyser for å finne og fikse feil relatert til universell utforming. Avtalen forplikter også leverandør å ta opp feil på eget initiativ. Dersom vi skal kunne verifisere løsningene som vi får tilhvdrt av leverandør som i tråd	Høy	Lav	Moderat

Deltakere

Navn	Rolle/funksjon
Ingelin Gammersvik	Prosjektleder
Kristian Skjeldal	Personvernombud
Ingrid Teistung	Personvernressurs
Simon Eika	UU- og ikt-ansvarlig

Konsekvens-matrise	Lav		Moderat		Høy		Svært høy	
	1		2		3		4	
Virksomhet Omdømme og tillit	Kun mindre diskusjon i organisasjonen		Avsender må forklare seg for partene om saken. Enkeltstående presseoppslag.		Offentlig debatt, ledelsen må forklare seg for myndigheter. Midlertidig endret oppfatning av DN's profesjonalitet. Ekstern gransking.		Politisk debatt, betydelig økonomisk erstatning/tap. Varig endret oppfatning av DN's profesjonalitet.	
Virksomhet Økonomisk	Ubetydelige økonomiske tap		Mange små kostnader. Reduserte besparelser.		Stort økonomisk tap. Stor engangskostnad		Betydelig økonomisk erstatning/tap	
Virksomhet Lovkrav, mål og rettssikkerhet	Mindre lovbrudd oppdages før det får virkning utenfor organisasjonen. Kun kortere overskridelse av saksbehandlingstid.		Overholder ikke kravene til saksbehandlingstid, får påpekning fra departementet.		Overtredelsesgebyr, erstatningssøksmål. Pålegg. Klarer ikke ivareta partenes rettssikkerhet.		Alvorlige brudd på lover, regler og avtaler. Ikke formålseffektiv og kostnadseffektiv realisering av DN's samlede mandat og mål. Klarer ikke overholde kravene i Tildelingsbrevet. Straffansvar. Betydelige overtredelsesgebyr og store erstatningssummer. Pålegg.	
Partene	En mindre uleilighet, økonomisk tap som kan gjenopprettes eller tap av anseelse eller integritet gjennom kompromittering av personopplysninger		Gjenopprettbart økonomisk tap eller tap av anseelse og integritet gjennom kompromittering av særlige kategorier av personopplysninger. Fare for skade eller helsetap.		Helsetap, uopprettelig økonomisk tap eller alvorlig tap av anseelse og integritet		Tap av liv, vedvarende helsetap, betydelig og uopprettelig økonomisk tap eller alvorlig tap av anseelse /integritet.	

Vurdering	Frekvens	Motivasjon	Letthetsbetraktninger
-----------	----------	------------	-----------------------

Sannsynlig at hendelsen inntreffer og får den beskrevne konsekvensen	Hendelsen inntreffer ukentlig eller oftere og får den beskrevne konsekvensen	Sikkerhetsbrudd kan skje ved uaktsomhet (ubevisst eller uten forsett) av egne medarbeidere eller utenforstående. Det er ikke nødvendig med spesielle kunnskaper om interne forhold.	sikkerhetstiltak er ikke etablert - krever små til normale ressurser av egne medarbeidere eller eksterne for å brytes - ikke nødvendig med kjennskap til tiltakene
4			
Mulig at hendelsen inntreffer og får den beskrevne konsekvensen	Hendelsen inntreffer en gang i måneden og får den beskrevne konsekvensen	Sikkerhetsbrudd kan skje ved uaktsomhet av egne medarbeidere. Utenforstående må ha noe kompetanse, og forsettlig (bevisst eller aktivt) gå inn for å bryte sikkerhetstiltakene.	- sikkerhetstiltak er ikke fullt etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer ikke etter hensikten - egne medarbeidere trenger kun små til normale ressurser for å bryte tiltakene
3			
Mindre sannsynlig at hendelsen inntreffer og får den beskrevne konsekvensen	Hendelsen inntreffer årlig og får den beskrevne konsekvensen	Sikkerhetsbrudd kan skje ved at egne medarbeidere opptrer med forsett og har en viss kompetanse. Utenforstående må opptre med overlegg og noe kunnskap om interne forhold	- sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer etter hensikten

2		Kunnskap om internt sikkerhetsnett (med hensikt og plan, eksempelvis ved at flere tiltak brytes i riktig rekkefølge) for å omgå/bryte sikkerhetstiltakene.	- egne medarbeidere trenger små til normale ressurser og normal kjennskap til tiltakene for å bryte disse - eksterne trenger gode ressurser og god kjennskap til tiltakene for å bryte disse
Sjelden at hendelsen inntreffer og får den beskrevne konsekvensen 1	Hendelsen inntreffer omkring hvert 3. år eller sjeldnere og får den beskrevne konsekvensen	Sikkerhetsbrudd kan kun skje ved at egne medarbeidere opptre med overlegg og har spesiell kompetanse eller kunnskap. Utenforstående må ha spisskompetanse og et samarbeid med personer i virksomheten.	- sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer etter hensikten - krever gode ressurser og godt kjennskap av egne medarbeidere for å brytes - eksterne kan ikke omgå tiltakene

Lav risiko	Ingen tiltak nødvendig
Moderat risiko	Hendelsene skal vurderes nærmere og eventuelle tiltak implementeres eller risiko aksepteres
Høy risiko	Tiltak skal iverksettes

**Risikovurdering for anskaffelse av
leverandør av vedlikehold på nettstedet
fra Netpower Web Solutions AS**

20. desember 2022

1 Innhold

1. Hva skal anskaffes?	3
2. Omfang.....	3
2.1. Avgrensninger	3
2.2. Oversikt over verdier.....	3
3. Konsekvens	4
4. Sannsynlighet	5
5. Risikovurdering	7
6. Tiltak	8
7. Restrisiko etter tiltak – konklusjon	10

1. Hva skal anskaffes?

Fordi vår avtale med nåværende leverandør av vedlikehold og oppdateringer på nettstedet vårt, Advenio AS, går ut 31. desember 2022, har vi behov for å få en ny avtale om dette. Det går frem av konkurransedokumentene at tjenesten innebærer vedlikehold av nettstedet www.diskrimineringsnemnda.no, samt utviklingsbehov som måtte forekomme i fremtiden. Ansvar for drift av nettstedet ligger i dag hos vår IT-driftsleverandør Braathe Gruppen AS. Før vi kunngjorde konkurransen, gjennomførte vi en foreløpig ROS. Vedlagte ROS bygger videre på den foreløpige.

Denne rapporten redegjør for risikobildet knyttet til Diskrimineringsnemndas anskaffelse av ny leverandør av vedlikehold m.m av nettstedet og gir vurderingen av hvilke sikkerhetstiltak som bør iverksettes ved overgangen til ny leverandør. Den er gjennomført etter kontraktsigneringen med Netpower Web Solutions AS.

2. Omfang

Denne rapporten omfatter ROS-analyse for risikobildet ved overgangen fra nåværende leverandør til ny leverandør, angir aksepter risiko og gir anbefalinger på hvilke sikkerhetstiltak som bør iverksettes for å styre et gitt risikoscenario til akseptabelt nivå. Analysen går inn på deler av Diskrimineringsnemndas bruk av leverandørens tjenester, men er ikke uttømmende om bruk.

2.1. Avgrensninger

Analysen bygger på Diskrimineringsnemndas nivå for akseptabel risiko. Analysen omfatter selve overgangen, og er avgrenset mot Diskrimineringsnemndas bruk av Netpower Web Solutions tjenester. Analysen er gjort før Diskrimineringsnemnda har tatt i bruk Netpower Web Solutions sine tjenester, men etter at kontrakten er signert. Noe kommunikasjon i form av Workshops er gjennomført med ny leverandør.

2.2. Oversikt over verdier

En verdi er alt som anses som verdifullt for en virksomhet eller en innbygger, eksempelvis tap av omdømme, brudd på lov eller forskrift eller brudd på ønsket/pålegg om konfidensialitet.

Den verdien som Diskrimineringsnemnda hovedsakelig behandler er særlige kategorier personopplysninger knyttet til diskrimineringsgrunnlag i konkrete klagesaker, personalsaker og personopplysninger i generelle saker. Oversikt over personopplysninger som Diskrimineringsnemnda behandler finnes i vår behandlingsoversikt, jf. GDPR artikkel 30.

3. Konsekvens

Vurderingen tar utgangspunkt i listen av de identifiserte uønskede hendelsene, og skal gi svar på spørsmål av typen «hva er konsekvensen hvis det som kan gå galt går galt».

At verdiene i systemet er korrekt fastsatt er kritisk for en riktig vurdering av konsekvenser.

Konsekvens kan uttrykkes som økonomiske tap, tap av liv og helse, tap av omdømme, straffeansvar for virksomheten osv.

Behovet for å fastsette kriterier for konsekvens følger av ISO/IEC 27005:2011 kapittel 7.2.3. Det benyttes fire graderinger på konsekvens:

1. Lav
2. Moderat
3. Høy
4. Svært høy

Nedenfor er kriteriene som vil bli benyttet videre:

Konsekvens- matrise	Lav	Moderat	Høy	Svært høy
	1	2	3	4
Virksomhet Omdømme	Kun mindre diskusjon i organisasjonen	Avsender må forklare seg for kundene om saken. Enkeltstående presseoppslag.	Offentlig debatt, ledelsen må forklare seg for myndigheter. Midlertidig endret oppfatning av DN's profesjonalitet. Ekstern gransking.	Politisk debatt, betydelig økonomisk erstatning/tap. Varig endret oppfatning av DN's profesjonalitet
Virksomhet Økonomisk	Ubetydelige økonomiske tap	Mange små kostnader. Reduserte besparelser.	Stort økonomisk tap. Stor engangskostnad	Betydelig økonomisk erstatning/tap
Virksomhet Lovkrav, mål og rettssikkerhet.	Mindre lovbrudd oppdages før det får virkning utenfor DN. Kun kortere overskridelse av saksbehandlingstid.	Overholder ikke kravene til saksbehandlingstid, får påpekning fra departementet.	Overtredelsesgebyr, erstatnings-søksmål. Pålegg. Klarer ikke ivareta partenenes rettssikkerhet.	Alvorlige brudd på lover, regler og avtaler. Ikke formåls effektiv og kostnadseffektiv realisering av DN's samlede mandat og mål. Klarer ikke overholde kravene i tildelingsbrevet. Straffansvar. Betydelige overtredelses-

Konsekvens- matrise	Lav	Moderat	Høy	Svært høy
	1	2	3	4
				gebyr og store erstatnings-summer.
Partene	En mindre uleilighet, økonomisk tap som kan gjenopprettes eller tap av anseelse eller integritet gjennom kompromittering av personopplysninger	Gjenopprettbart økonomisk tap eller tap av anseelse og integritet gjennom kompromittering av særlige kategorier av personopplysninger. Fare for skade eller helsetap.	Helsetap, uopprettelig økonomisk tap eller alvorlig tap av anseelse og integritet	Tap av liv, vedvarende helsetap, betydelig og uopprettelig økonomisk tap eller alvorlig tap av anseelse /integritet.

Kriteriene er hentet fra Norsk Helsenetts veileder for risikovurdering¹ og deretter modifisert i møte om risikovurderinger i Diskrimineringsnemnda i oktober 2018.

4. Sannsynlighet

Vurdering av sannsynligheten har som mål å finne svar på «hva er sannsynligheten for at det som kan gå galt går galt og får den beskrevne konsekvensen». Svaret angis kvantitativt, og sannsynlighetsskalaen ble fastsatt under kontekstetableringen.

For hver av de uønskede hendelser som er identifisert skal man gjøre en vurdering av sannsynligheten for at hendelsen inntreffer og at den får det utfallet/konsekvensen som er beskrevet. I mange tilfeller kan det være vanskelig å si noe om frekvens, da det ikke finnes noe godt statistisk materiale. I disse situasjonene kan man ta med en aktørs motivasjon for å gjennomføre en handling, eller hvor lett det vil være for en aktør å gjennomføre handlingen.

En integrert del av risikoaksept er å fastsette nivåer for sannsynlighet:

Vurdering	Frekvens	Motivasjon	Letthetsbetraktninger
Sannsynlig at hendelsen inntreffer og får den beskrevne konsekvensen	Hendelsen inntreffer ukentlig eller oftere og får den beskrevne konsekvensen	Sikkerhetsbrudd kan skje ved uaktsomhet (ubevisst eller uten forsett) av egne medarbeidere eller utenforstående.	- sikkerhetstiltak er ikke etablert - krever små til normale ressurser av egne medarbeidere eller eksterne for å brytes

¹ <http://www.nhn.no/informasjonnssikkerhet/risikovurdering>

Vurdering	Frekvens	Motivasjon	Letthetsbetraktninger
4		Det er ikke nødvendig med spesielle kunnskaper om interne forhold.	- ikke nødvendig med kjennskap til tiltakene
Mulig at hendelsen inntreffer og får den beskrevne konsekvensen 3	Hendelsen inntreffer en gang i måneden og får den beskrevne konsekvensen	Sikkerhetsbrudd kan skje ved uaktsomhet av egne medarbeidere. Utenforstående må ha noe kompetanse, og forsettlig (bevisst eller aktivt) gå inn for å bryte sikkerhetstiltakene.	- sikkerhetstiltak er ikke fullt etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer ikke etter hensikten - egne medarbeidere trenger kun små til normale ressurser for å bryte tiltakene
Mindre sannsynlig at hendelsen inntreffer og får den beskrevne konsekvensen 2	Hendelsen inntreffer årlig og får den beskrevne konsekvensen	Sikkerhetsbrudd kan skje ved at egne medarbeidere opptrer med forsett og har en viss kompetanse. Utenforstående må opptre med overlegg og noe kunnskap om interne forhold (med hensikt og plan, eksempelvis ved at flere tiltak brytes i riktig rekkefølge) for å omgå/bryte sikkerhetstiltakene.	- sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer etter hensikten - egne medarbeidere trenger små til normale ressurser og normal kjennskap til tiltakene for å bryte disse - eksterne trenger gode ressurser og god kjennskap til tiltakene for å bryte disse
Sjelden at hendelsen inntreffer og får den beskrevne konsekvensen 1	Hendelsen inntreffer omkring hvert 3. år eller sjeldnere og får den beskrevne konsekvensen	Sikkerhetsbrudd kan kun skje ved at egne medarbeidere opptrer med overlegg og har spesiell kompetanse eller kunnskap. Utenforstående må ha	- sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer etter hensikten - krever gode ressurser og godt kjennskap av egne medarbeidere for å brytes

Vurdering	Frekvens	Motivasjon	Letthetsbetraktninger
		spisskompetanse og et samarbeid med personer i virksomheten.	- eksterne kan ikke omgå tiltakene

Der erfaringstall foreligger, gir disse en indikasjon på framtidig frekvens. På bakgrunn av letthets- og motivasjonsvurderingen gjengitt over, kan også forventet frekvens anslås. Til hjelp for vurderingen er det utarbeidet kriterier for letthetsbetraktninger, se over.

Trusselaktører er ikke like, og det finnes mange metoder for å kategorisere ulike trusselaktører. Her er det tatt utgangspunkt i de samme egenskapene som i risikohåndterings-guiden til NIST, SP 800-302, og lagt til utholdenhet:

- Evne - En aktørs tilgang på kompetanse og ressurser.
- Vilje - En aktørs grad av motivasjon for å angripe.
- Måltrettethet - En aktørs grad av måltrettethet mot brukere eller brukergrupper. Måltrettethet vil øke risikoen for individene angrepet rettes mot, pga økt frekvens og tilpasning av angrepene.
- Utholdenhet - En aktørs evne til å opprettholde et angrep over tid og evnen til å utføre flere angrepsforsøk over tid.

Det er imidlertid også verdt å være oppmerksom på at trusselaktørers gevinst av vellykket sikkerhetsbrudd vil påvirke frekvensvurderingen, jf. at verdien vil være styrende for motivasjonen.

Det kan således være nødvendig å knytte et anslag over gevinsten for trusselaktøren til opplysningene som inngår i løsningen – i tillegg til taps- og skadepotensialet for virksomheten selv, innbyggeren mv., jf. konsekvenskategoriene. For motivasjonsvurderingen vises til omtalen i Datatilsynets veileder kapittel 7.3.

Diskrimineringsnemnda har per dags dato ikke systematiserte og skriftlige erfaringstall. Der vi vet at enkelte hendelser har skjedd, eller at samme type hendelse har skjedd flere ganger, er dette tatt med i sannsynlighetsvurderingen. Det bemerkes at dette medfører noe usikkerhet ved vurderingen. Der historiske erfaringstall mangler har vi hovedsakelig brukt motivasjons- og letthetsbetraktninger.

5. Risikovurdering

I risikoregisteret evaluerer vi risikoene ved å trekke frem relevante scenarier og knytte disse til verdier for sannsynlighet og konsekvens. Produktet av disse gir en verdi for risiko. Ved vurdering av risiko er eksisterende og planlagte tiltak og

² <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

effekten av disse på sannsynlighet og konsekvens gjenspeilet i verdiene.

Hva som er akseptabel risiko for Diskrimineringsnemnda er fastsatt i Policy for informasjonssikkerhet versjon 1.1 pr. 31.10.2018.

6. Tiltak

I dette kapittelet er beskrevet en oppsummering av anbefalte tiltak som er detaljert i risikoregisteret:

- 1. I konkurransedokumentene har vi beskrevet vårt behov, både hva gjelder fjerning og avindeksering, og tilgjengelighet på support, se krav 6. Ny leverandør beskriver overordnet sin løsning til krav 6 i bilag 2 hvor de presiserer at «personell får opplæring i hvordan de publiserte avgjørelsene skal fjernes, enten dette skjer i publiseringsverktøy eller på et mer teknisk nivå (database og lignende)». Dette vil også være tema når vi setter opp rammene for hvordan våre konkrete kontaktpunkt med ny leverandør skal være.*
- 2. Det følger av databehandleravtalen punkt 6 at databehandler skal slette eller tilbakelevere alle personopplysninger til behandlingsansvarlig etter at tjenestene knyttet til behandlingen er levert, og slette eksisterende kopier inkludert eventuelle sikkerhetskopier, med mindre det er et lovmessig krav at personopplysningene fortsatt skal lagres. Vi skal motta skriftlig bekreftelse på at dette er gjort. Dette følger også av personvernforordningen. I forbindelse med oppstart og oppsett av samhandlingsplanen vil vi også be om å få oversendt deres rutiner ved håndteringen, slik at vi kan sikre disse.*
- 3. Leverandøren er profesjonell. Det følger av databehandleravtalen punkt 2 at databehandler har taushetsplikt om personopplysninger som vedkommende får tilgang til som en følge av avtalen med oss og behandling av personopplysningene, og at databehandler skal sikre at personer som er autorisert til å behandle personopplysningene har forpliktet seg til å behandle opplysningene fortrolig eller er underlagt en egnet lovfestet taushetsplikt som skal kunne dokumenteres. Se også databehandleravtalen punkt 4. Dette vil vi presisere når vi setter opp samhandlingsplanen med ny leverandør. Gjennomgang av tilgang når arbeidsforhold avsluttes.*
- 4. Leverandøren er profesjonell. Det følger av databehandleravtalen punkt 2 at databehandler har taushetsplikt om personopplysninger som vedkommende får tilgang til som en følge av avtalen med oss og behandling av personopplysningene, og at databehandler skal sikre at personer som er autorisert til å behandle personopplysningene har forpliktet seg til å behandle opplysningene fortrolig eller er underlagt en egnet lovfestet taushetsplikt som skal kunne dokumenteres. Se også databehandleravtalen punkt 4. Dette vil vi presisere når vi setter opp*

samhandlingsplanen med ny leverandør. Gjennomgang av tilgang når arbeidsforhold avsluttes.

- 5. Avtalen mellom partene regulerer skriftliggjøring av hva som skal endres på nettsidene, og tilgang gis til et begrenset antall personer. Det følger av avtalen at partene skal holde hverandre oppdatert, at det skal føres protoll fra samarbeidsmøter. Logg i Umbraco synliggjør hvilken bruker som har endret hva.*
- 6. Det følger av inneværende vedlikeholdsavtalen bilag 1 at leverandør skal overlevere teknisk dokumentasjon og kildekode ved opphør og at leverandør skal bistå i overgangen til ny leverandør.*
- 7. Vedlikeholdsavtalen med nåværende leverandør regulerer at de skal samarbeide ved overgangen. Vi har tatt kontakt med Braathe Gruppen og fått en fast person å forholde oss til samt sikre god kommunikasjon. Vi har avtalt med ny og nåværende leverandør at de skal samarbeide frem til ny leverandør er i stand til å håndtere løsningen, slik at alle parter får tilstrekkelig med tid til å gjøre overgangen god nok.*
- 8. Det følge av vedlikeholdsavtalen at vi kan heve avtalen med umiddelbar virkning ved konkurs.*
- 9. Vi bør vurdere å skaffe oss kompetanse innen IT, som blant annet kan bistå i lignende prosesser i fremtiden.*
- 10. Advenio har gitt en skriftlig beskrivelse av løsningen vår, som går ut sammen med anbudsdokumentene, samt sendt ny leverandør dokumentasjon på løsningen. Vi vil kjøre backup på tilleggsattributter før overgang. Etter gjennomgangen av tilbudene og ved valget, antar vi at ny leverandør har korrekt kompetanse. Vi har satt av tid til over nyttår for overgangen, for å sikre god teknisk kompetanseoverføring fra Advenio til ny leverandør.*
- 11. Braathe Gruppen har skriftlig stadfestet at de ikke har utfordringer med at vi skifter leverandør, og at de vil bistå oss med å gi de tilgang til servere.*
- 12. Punkt 2 i databehandleravtalen regulerer blant annet at databehandler skal sørge for at behandlingen av personopplysninger er i samsvar med gjeldende lov (personvernloven), hovedavtalen, avtalen samt eventuelle instruksjoner som er gitt av oss. Videre skal databehandler bistå oss i å svare på anmodninger fra de registrerte osv.. Det følger videre av avtalen at leverandør skal ha kompetanse på håndtering av informasjonskapsler, innebygd personvern samt styring av ordning for samtykker fra de registrerte og at innstillinger for informasjonskapsler skal til enhver tid være i tråd med gjeldende regelverk, se bilag 2 krav 11. Vi har også stilt krav om at leverandøren skal kunne veilede om personvernvennlige webanalyseverktøy, se bilag 2 krav 13.*
- 13. Det følger av avtalen bilag 2 krav 7 at leverandørens sentrale konsulenter har inngående kjennskap til WCAG-standard og erfaring med universell utforming av både nettsteder og webapplikasjoner. De har god erfaring med testverktøy og å gjøre egne manuelle analyser for å finne og fikse feil relatert til universell utforming. Avtalen forplikter også leverandør å ta opp*

feil på eget initiativ. Dersom vi skal kunne verifisere løsningene som vi får tilbudt av leverandør som i tråd med reglene for universell utforming, bør vi ha ansatt personell for dette internt.

7. Restrisiko etter tiltak – konklusjon

Sannsynlighet		Gjenstående risiko				
		Svært høy				
		Høy				
		Moderat	R10			
		Lav	R5,R8	R6,R7,R9,R11	R1,R2,R3,R4,R12,R13	
			Lav	Moderat	Høy	Svært høy
		Konsekvens				

ID	Risiko beskrivelse Stikkord om: (1) innledende hendelse(r) (2) informasjons sikkerhetsbruddet (3) de uønskede konsekvensene som kan oppstå	Konsekvens		Tilhørende sannsynlighet		Risikovalv		Konsekvens etter tiltak	
		Begrunnelse for konsekvensvurdering		begrunnelse for vurdering av tilhørende sannsynlighet		Vurdering av risiko/håndtering		Sannsynlighet etter tiltak	
									Gjennvendende risiko
R1	Data går tapt i omleggingsfasen. Brudd på integritet og tilgjengelighet på data.	Skrift vil være en ny leverandør for diskrimineringsnemda, som medfører at data må konverteres og migreres til et historisk arkiv. Alle metadata med tilhørende elektroniske dokumenter må følge med (i hvilken arkivdel de er skapt, tilgang osv.). Etter gjennomført migrering vil det være fullt mulig å ta utvalgte data fra databasen.	Svært høy	Moderat	På grunn av dataomfanget og at en del av arbeidet må gjøres manuelt, er det sannsynlig at ulikhet i feil av ansatte vil øke.	Høy	Det må utarbeides lister over alle saker som må opprettes på nytt i Elements, hvor sakbehandlere og arkivert samarbeider om oppretting og mulige kryssreferanser. Gjensidig sjekk og kontroll.	Lav	Moderat
R2	Data i gjennett system blir slettet etter at det er tatt sikkerhetsskopi og overføring til nytt system har skjedd. Med flere kopier øker faren for at data skal komme på avveie. Brudd på prinsippet om dataminimering. Risiko for brudd på konfidensialitet.	Daten blir evt. liggende hos AcoS som vi har databehandlingsavtale med, derfor ikke brudd på konfidensialitet. Brudd på prinsippet om dataminimering - mindre lovbrudd oppdages før det får virkning utenfor DN.	Lav	Lav	Sletting requires av avtalen vi allerede har med AcoS. Siden dette er avtaleregulert og vil følges opp av DN vurderes sannsynligheten som lav.	Lav	Tiltak: Forsikre oss om at sletting fra gammelt system blir gjennomført.	Lav	Lav
R3	Manglende styring og forvaltning av skytjenesten. DN har ikke et bevisst forhold til hvordan skytjenesten styres og forvaltes. Risiko for brudd på blant annet konfidensialitet og at data kommer på avveie.	Ansvar for behandlingens ansvarlig kan ikke ivaretas forsvarlig. Kan medføre at ledelsen må forklare seg for offentlige myndigheter. Midlertidig endret opplåning av DNS profesjonallitet. Lovbrudd som kan medføre overtredelsesgebyr fra Dataatbyret.	Høy	Moderat	DN mottar ikke tilstrekkelig intern teknisk kompetanse som er nødvendig for å forstå alle de tekniske aspektene bak skytjenester for å ivareta behandlingsansvaret. DN er bevisst på egen forvaltning, men uten god informasjon, avtaleregulering og leverandører som gir DN stand til å forstå sikkerhetsaspektene ved bruk av skytjenester.	Moderat	Tilbudet fra Sikri gir en god beskrivelse av skytjenesten og aksepterer DNS databehandlingsavtale. Tilbyr abonnementsordning og varsling. Sikri er litt vagere i sin beskrivelse av løsningen enn AcoS, og har litt mer generelle henvisninger til gode leverandører som gir DN stand til å forstå sikkerhetsaspektene ved bruk av skytjenester.	Lav	Lav
R4	Manglende/lang responstid fra leverandør. Det tar lang tid å rette opp feil/gjøre sikkerhetsoppdateringer. Risiko for nedetid. Brudd på tilgjengelighet.	Kan medføre at DN ikke overholder kravene til saksbehandlingstid. Kan medføre manglende mulighet til å behandle innviskrav og avvismeldinger innen angitte tidsfrister.	Moderat	Moderat	Prisliggt leverandøren i langt større grad enn ved en lokal løsning. Det kan innebære lang responstid når det gjelder feilrettinger og etablering av sikkerhetstiltak. Uten avtaleregulering øker sannsynligheten for feil.	Moderat	innenfor 07.00-17.00 mandag til fredag, ref. tilbudet SSA-L s. 7. Tjenesten oppgraderes hver 2. uke med minimal eller ingen nedetid, vanligvis på søndag ettermiddag. Responstid på uønskete kritisk nivå vurderes i henhold til SSA-L kap. 6.	Lav	Lav
R5	Manglende sikkerhetskopiering i den nye løsningen medfører at data går tapt. Brudd på tilgjengelighet og integritet.	Manglende sikkerhetskopiering kan medføre at enkelt-filer eller data som er slettet eller endret utslisket. Ikke kan gjenskapes. Tap av data vil kunne gå utover saksbehandlingstiden, og medføre midlertidig endret opplåning av DNS profesjonallitet. Brudd på personvernegehevet.	Moderat	Moderat	Noen skytjenestandører tar ikke sikkerhetskopier, men benytter muligheten for å gjenskape data innenfor et gitt tidspunkt. Dersom dette ikke reguleres i avtale, vurderes det som moderat sannsynlig at risikoen kan øke.	Moderat	Sikri har rutiner for sikkerhetskopiering og gjennoppretting, ref. tilbudet bilag 2 vedlegg 1 s. 32. Dette må følges opp ved implementering.	Lav	Lav
R6	Manglende brukeropplæring i saksbehandlingssystemet. Ved overgang til skytjening, blir risikoen for at ansatte gir eksterne brukere tilgang til data større (enkeltre å dele utenfor organisasjonen - flere kunder på samme system). Data blir utlevert utslisket og uvidkommende får tilgang til personopplysninger. Brudd på konfidensialitet.	Uvidkommende får tilgang til enkeltsaker. Lovbrudd som kan medføre overtredelsesgebyr fra Dataatbyret. Midlertidig endret opplåning av DNS profesjonallitet.	Moderat	Høy	Uten tilfredsstillende opplæring i nye systemer er det en høy sannsynlighet for at utsliskede feil kan øke.	Moderat	God brukeropplæring skissert i tilbudet. Tiltak: Det må settes av tilstrekkelig tid og ressurser internt for å få til god brukeropplæring internt.	Lav	Lav
R7	Manglende/feil dataisolasjon. Feil i konfigurasjon/administrasjonsensitivitet (hypervisor)/menneskelig feil fører til at det oppstår datalekkasje mellom kunder (tenanter). Brudd på konfidensialitet.	Lovbrudd - Fare for at en større mengde personensensitive opplysninger kommer på avveie.	Høy	Lav	En skytjening innebærer at flere kunder anvender samme lagringsløsning. Selv om disse er adskilt logisk ved hjelp av virtuelle maskiner, kan feil føre til at det oppstår datalekkasje mellom ulike kunder i løsningen.	Moderat	ELEMENTS BENYTER AZURE OG MICROSOFT, slik som vi har det hos Braathe i dag. Tiltak: Skaffe oss nærmere informasjon om hvordan leverandørene håndterer dette, og om det er ytterligere tiltak som kan iverksettes (eksempelvis overgang til ES).	Lav	Moderat
R8	Det skjer organisatoriske endringer hos skytjenestegiver (kjøpt opp, fusjonert, økonomiske utfordringer). Kvaliteten på tjenesten reduseres, f.eks. nedbemanning, redusert arbeidskapasitet eller manglende sikkerhetsoppfølging.	Kan skape utfordringer for DNS drift, og gå utover saksbehandlingstiden.	Moderat	Lav	Sikri er forholdsvis nyoppstartet. Derfor kjenner vi ikke til om det er noen spesielle tiltak som kan iverksettes for å sikre kvaliteten og sikkerhetsoppfølgingen er god uavhengig av organisatoriske endringer. Responstid og kvalitet er avtalt. Tiltak: Sjekk referanser og reguler muligheten for å avslutte avtalen..	Lav	Avtaleregulering skal sørge for at kvaliteten og sikkerhetsoppfølgingen er god uavhengig av organisatoriske endringer. Responstid og kvalitet er avtalt. Tiltak: Sjekk referanser og reguler muligheten for å avslutte avtalen..	Lav	Lav
R9	Manglende sletting av data i skytjeningen.	Brudd på prinsippet om dataminimering. Mindre lovbrudd oppdages før det får virkning utenfor DN.	Moderat	Høy	Multitenant miljø (mange kunder på samme server) kan føre til at data som skal slettes ikke blir slettet tilstrekkelig.	Moderat	Tilbudet garanterer for at de ivaretar skytjeningen på en god måte, og følger opp personvernegehevet. Tiltak: følges opp ved implementering. Utarbeide interne rutiner for sletting.	Lav	Lav

R10	Hele skydingen blir utlignelig i lengre tid på grunn av fire påføring, brann, naturkatastrofe mv. Brudd på tilgjengelighet.	Risiko for nedetid over en lengre periode (deler). Ikke formålseffektiv og kostnads effektiv realisering av DNS mandat og mål. Klarer ikke overholde kravene i tildelingsbrevet.	Høy	Lav	Samsynligheten vurderes som lav, ettersom det aldri har skjedd i Norge at en skytsløyning har blitt utlignelig på grunn av brann/naturkatastrofe.	Moderat	Slik har to dataentere og backup. Gode garantier for oppetid.	Høy	Lav	Moderat
R12	Fal tilgangsstyring til data i historisk base. Brudd på konfidensialitet.	Ved migrering av data til historisk base tapos tilgangsstyring fra produksjonsmiljøet og alle ansatte får tilgang til alle saker og dokumenter ved sak. De fleste ansatte har uansett tilgang til alle klagesaker, men ikke personalmapper. Vil kun få virkning internt.	Moderat	Høy	Manglende planlegging og bevissthet om dette, gir en høy samsynlighet for uriktig tilgangsstyring i historisk base ved overgang til Sikri sin løsning. Krever en aktiv handling fra ansatte, men enkelt å få tilgang til opplysningene. Må aktiv gå inn å søke på sakene for å lese opplysningene.	Moderat	Slik presenterer i beskrivelsen av migreringen til historisk base at alle metadata modifiserer, også tilgangsstyringen m.m.	Moderat	Lav	Lav
R13	Daaangrep mot løsningen blir ikke stoppet i tide. Skytvevarenderen gir ikke motfall dersom man blir utsatt for DDOS-angrep (distribuert tjenestektangrep) eller "phishing".	Uvedkommende får tilgang til en større mengde tautshetbelagte opplysninger. Kan i tillegg medføre lengre nedetid. Ikke formålseffektiv og kostnads effektiv realisering av DNS smiede mandat og mål. Klarer ikke overholde kravene i tildelingsbrevet. Varig svekkelse av DNS tillit.	Svært høy	Høy	Vurderes samsynligheten for dataangrep som høy. Truselaktene viser stor kapasitet til å gjennomføre cyberangrep. Siden 2019 har NSM sett en tredobling i antall cyberhendelser som får alvorlige konsekvenser for virksomheter i Norge. Phishing har blitt svært vanlig blant samarbeidspartnere.	Høy	Slike teknisk oppsett mot overbelastning gjennom foderert (m) logging eller via SAML sertifiserte (m) logginger.	Svært høy	Lav	Moderat
R14	Data blir ikke tilfredsstillende sikret på grunn av manglende mulighet for tilgangsstyring. Data blir lagt i mapper hvor brukere uten tjenstlig behov har tilgang, kan endre og slette. Brudd på konfidensialitet, tilgjengelighet og integritet.	Selv ved feil, vil det ikke gi store konsekvenser. Alle har tilgang til alle klagesaker, det er bare personaldelen i arkivet enkelte ikke har tilgang til.	Moderat	Lav	Normalt at det tilrettelegges for tilgangsstyring ved bruk av NOARK godkjent sakbehandlingsystem.	Lav	Slik viser til at de har gode løsninger for dette. Interne tiltak: Tilgangsstyring. Oppklaring. Etablere rutiner for håndtering av data, og hvor ulike typer data skal lagres.	Moderat	Lav	Lav
R15	Skytsløyningen utsettes for dataangrep. Brudd på tilgjengelighet og konfidensialitet.	Bege skytsløyninger benytter Microsoft Exchange i bunn. DN har i dag microsoft E3-lisens, og behandler sensitive personopplysninger i skytsløyningen. Ved overgang til saksbehandlingsystem i skyen, vil mengden sensitive personopplysninger og tautshetbelagte opplysninger øke (alle saksbehandlingsopplysninger blir tilgjengelige der).	Svært høy	Høy	Basert på NSMs rapport "Risiko 2022", vurderes samsynligheten for dataangrep som høy. Truselaktene viser stor kapasitet til å gjennomføre cyberangrep. Siden 2019 har NSM sett en tredobling i antall cyberhendelser som får alvorlige konsekvenser for virksomheter i Norge.	Høy	Tilbudet redigerer godt for løsningen sikkerhet og risikoreduerende tiltak. Sikri er sertifisert etter ISO 27001 standarden. Tiltak: Ettersom begge skytsløyningene benytter Microsoft Exchange bunn (som vi har hos Braathe i dag), har vi trolig på vår side redusert risikoen for sikkerhetssvikt.	Svært høy	Lav	Moderat
R16	Data blir lagret på sikre lokasjoner, for eksempel på servere i land hvor man ikke har kontroll på sikkerheten. Data kan komme på awele. Brudd på konfidensialitet.	Store mengder tautshetbelagte opplysninger kan komme på awele. Alvorlig regelbrudd. Offentlig debatt, ledelsen må forlate seg for myndigheter. Midlertidig endret oppfatning av DNS profesjonalitet.	Høy	Lav	Bege løsningene er NOARK godkjent som forutsatt lagring av data i Norge.	Moderat	Noark godkjent løsning som forutsatt lagring av data i Norge. Reguleres også i databehandlingsloven.	Høy	Lav	Moderat
R17	Data er utlignelig fordi det nye systemet virker ikke som forutsatt, på grunn av forhold hos leverandør eller DN. Brudd på tilgjengelighet.	Risiko for nedetid over en lengre periode (deler). Ikke formålseffektiv og kostnads effektiv realisering av DNS mandat og mål. Klarer ikke overholde kravene i tildelingsbrevet.	Høy	Moderat	Law ICT-kompetanse internt. Avhengig av Braathe og at leverandøren gir god og forståelig informasjon, med klare bestillinger på hva som er nødvendig for at løsningen skal fungere som forutsatt.	Moderat	Tilbudt 1. Forordningene for tilbudet må forelegges Braathe til kontroll. 2. Sjekk oppgitte referanser i tilbudet. 3. God planlegging og evt. bistand fra Braathe ved overgang til ny løsning. Sekretariatet arbeider på PC-er fra nemnda, der Braathe sørger for at sikkerheten opprettholdes ved at alle oppgaver knyttet til drift og vedlikehold. Er ansvarlig for sikkerhet knyttet til angrep og uønsket inntrengning utenfra, ref. tilbudet del 2 vedleggs SSA-L. Tiltak: Tydelig avtale hvem som har ansvar for hva. Slaffe på leverandøren.	Høy	Lav	Moderat
R18	Nødvendige sikkerhetsoppdateringer blir ikke gjort og sårbarheter i systemet utrykkes. Skytsløyningen kan bli utsatt for dataangrep. Brudd på tilgjengelighet, integritet og konfidensialitet.	Uvedkommende får tilgang til en større mengde tautshetbelagte opplysninger. Kan i tillegg medføre lengre nedetid. Ikke formålseffektiv og kostnads effektiv realisering av DNS smiede mandat og mål. Klarer ikke overholde kravene i tildelingsbrevet. Varig svekkelse av DNS tillit.	Høy	Lav	Samsynligheten for dette vurderes i utgangspunktet som lav. Tilbydene er profesjonelle aktører og ruinene for sikkerhetsoppdatering fremstår gode.	Moderat	Alle oppgaver knyttet til drift og vedlikehold. Er ansvarlig for sikkerhet knyttet til angrep og uønsket inntrengning utenfra, ref. tilbudet del 2 vedleggs SSA-L. Tiltak: Tydelig avtale hvem som har ansvar for hva. Slaffe på leverandøren.	Høy	Lav	Moderat
R19	Sikkerhetsbrudd blir ikke oppdaget. Responsmiljøet lokalt avdekker ikke mistenkelig trafikk eller angrep på nettverksnivå.	Uvedkommende får tilgang til en større mengde tautshetbelagte opplysninger. Data på awele. Varig svekkelse av DNS tillit.	Høy	Lav	Samsynligheten for dette vurderes i utgangspunktet som lav. Tilbydene er profesjonelle aktører med gode sikkerhetsrutiner for å oppdage sikkerhetsbrudd.	Moderat	Tilnærming til informasjonsikkerhet, med gode rutiner. Tiltak: Forsikre oss om at skytvevarenderen har løsninger som effektivt overvåker og kan håndtere dataangrep. Kreve at leverandøren har kontinuitetsplaner.	Høy	Lav	Moderat
R20	Utro tjener hos leverandøren. Benytter seg av sine tilganger for å selge data, personlister, e-poster eller annen informasjon for egen vinnings skyld. Brudd på konfidensialitet.	Uvedkommende får tilgang til større mengder tautshetbelagte og personensitive opplysninger. Lovbrudd. Må melde avvik til Datatilsynet.	Høy	Lav	Tilbydene er profesjonelle aktører. Begge tilbudene legger opp til at det er få ansatte som har tilgang. Dette er også avtalerregulert. Risikoen vurderes derfor som lav.	Moderat	Oppklaring, tilgangsstyring og tautshetsklæringer er tatt høyde for i tilbudet. Reguleres i databehandlingsloven.	Høy	Lav	Moderat

R21	Treg/utfredstillende datailgang. Netverkskapasiteten vår eller andre interne forhold er ikke tilstrekkelig for behovet i skyeningen. Brudd på tilgjengelighet.	Data kan bli delvis utligengeligg. Frustrasjon blant de ansatte.	Lav	Moderat	Vanskelig å vurdere sannsynligheten. Erfaringen vi har med bruk av Teams innenfor Citrix er dårlig. Etter som vi muligens fortsatt skal benytte Citrix til dette, vurderer vi det som moderat sannsynlig.	Lav	Tilbak: God planlegging og bistand av Braathe ved implementering. Braathe må involveres tidlig i prosessen. Vurder i samarbeid med Braathe om det er mulig at sekretariatet/nemnda arbeider i skyeningen utenfor Citrix.	Moderat	Lav	Lav
R22	Data blir avlyttet under transport til/fra skyleverandør. Brudd på konfidensialitet.	Uvedkommende får tilgang til tusenvis av sensitive opplysninger. Data på avveie. Lovbrudd som må meldes til Dataatilsynet.	Høy	Lav	Begge tilbyderne er profesjonelle aktører med oppsett for autentiseringsmekanismer og kryptering.	Moderat	Data krypteres med AES256 for både strukturerte og ustrukturerte data. TLS sørger for at kommunikasjonen mellom tjenester er kryptert, ref. tilbudet fra Skri bilag 2 vedlegg 1.	Høy	Lav	Moderat
R23	Manglende styring av brukertilgang. Brukertilgang blir ikke endret eller avsluttet når personer (interne eller eksterne) skifter rolle, slutter eller av andre årsaker ikke lenger skal ha tilgang til data. Brudd på konfidensialitet.	Begrenset konsekvens. Kan få tilgang til nye dokumenter som man ikke har et tjenestlig behov for å se. Begrenset hvor mange dokumenter det er snakk om, men muligheter for at opplysninger om kollegaer blir kjent.	Moderat	Moderat	Krever aktiv handling fra den som har tilgang, men samtidig enkelt å få tilgang til dataen. Enkelt å glipe på sletting (manuell jobb).	Moderat	Databehandleravtalen gir tilgang ved behov. Elements har muligheter for tilgangstyring/ulike brukertilganger. Tilbak: Regulere dette i interne rutiner.	Moderat	Lav	Lav
R24	Uautorisert tilgang til data via felles PC. Brudd på konfidensialitet. Neste bruker får tilgang til data ved å trykke "tillbake" på nettleieren.	Uvedkommende får tilgang til person sensitive opplysninger.	Høy	Moderat	Ved test av internkontrollsystemet var det mulig å få tilgang til IKS ved å trykke "tillbake" på nettleieren. Nemnda har ikke egen DN-PC, og vi er kjent med at det hender at famillemedlemmer benytter samme PC'er.	Moderat	Tilbak: To-faktor pålogging. Oppklaring og rutiner. IKT-rutinen må oppdateres. Vurder om nemnda fortsatt må arbeide innefor Citrix.	Høy	Lav	Moderat
R25	Tap av data på nettsiden	Statistikk over klagesaker på diskrimineringsnemnda.no er koblet opp mot saksbehandlersystemet og går tapt ved omlegging uten særlige tiltak.	Høy	Moderat	Viktig å finne en løsning på dette før omlegging. Dagens system er basert på en direkte kobling til saksbehandlersystemet	Moderat	Viktig å sørge for plan for å ivareta dette.	Moderat	Lav	Lav
R26						#N/A				#N/A
R27						#N/A				#N/A
R28						#N/A				#N/A
R29						#N/A				#N/A
R30						#N/A				#N/A

Deltakere	
Navn	Rolle/funksjon
Helene A. Reksten	Arkivleder
Kristian Skjeldal	Personvernombud
Ingrid Teistung	fung.personvernombud

Konsekvens- matrise	Lav 1		Moderat 2		Høy 3		Svært høy 4	
Virksomhet Omdømme og tillit	Kun mindre diskusjon i organisasjonen		Avsender må forklare seg for partene om saken. Enkeltstående presseoppslag.		Offentlig debatt, ledelsen må forklare seg for myndigheter. Midlertidig endret oppfatning av DN's profesjonalitet. Ekstern gransking.		Politisk debatt, betydelig økonomisk erstatning/tap. Varig endret oppfatning av DN's profesjonalitet.	
Virksomhet Økonomisk	Ubetydelige økonomiske tap		Mange små kostnader. Reduserte besparelser.		Stort økonomisk tap. Stor engangskostnad		Betydelig økonomisk erstatning/tap	
Virksomhet Lovkrav, mål og rettssikkerhet	Mindre lovbrudd oppdages før det får virkning utenfor organisasjonen. Kun kortere overskridelse av saksbehandlingstid.		Overholder ikke kravene til saksbehandlingstid, får påpekning fra departementet.		Overtredelsesgebyr, erstatningssøksmål. Pålegg. Klarer ikke ivareta partenes rettssikkerhet.		Alvorlige brudd på lover, regler og avtaler. Ikke formålseffektiv og kostnadseffektiv realisering av DN's samlede mandat og mål. Klarer ikke overholde kravene i Tildelingsbrevet. Straffansvar. Betydelige overtredelsesgebyr og store erstatningssummer. Pålegg.	
Partene	En mindre uleilighet, økonomisk tap som kan gjenopprettes eller tap av anseelse eller integritet gjennom kompromittering av personopplysninger		Gjenopprettbart økonomisk tap eller tap av anseelse og integritet gjennom kompromittering av særlige kategorier av personopplysninger. Fare for skade eller helsetap.		Helsetap, uopprettelig økonomisk tap eller alvorlig tap av anseelse og integritet		Tap av liv, vedvarende helsetap, betydelig og uopprettelig økonomisk tap eller alvorlig tap av anseelse /integritet.	

Vurdering	Frekvens	Motivasjon	Letthetsbetraktninger
-----------	----------	------------	-----------------------

Sannsynlig at hendelsen inntreffer og får den beskrevne konsekvensen	Hendelsen inntreffer ukentlig eller oftere og får den beskrevne konsekvensen	Sikkerhetsbrudd kan skje ved uaktsomhet (ubevisst eller uten forsett) av egne medarbeidere eller utenforstående. Det er ikke nødvendig med spesielle kunnskaper om interne forhold.	sikkerhetstiltak er ikke etablert - krever små til normale ressurser av egne medarbeidere eller eksterne for å brytes - ikke nødvendig med kjennskap til tiltakene
Mulig at hendelsen inntreffer og får den beskrevne konsekvensen	Hendelsen inntreffer en gang i måneden og får den beskrevne konsekvensen	Sikkerhetsbrudd kan skje ved uaktsomhet av egne medarbeidere. Utenforstående må ha noe kompetanse, og forsettlig (bevisst eller aktivt) gå inn for å bryte sikkerhetstiltakene.	- sikkerhetstiltak er ikke fullt etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer ikke etter hensikten - egne medarbeidere trenger kun små til normale ressurser for å bryte tiltakene
Mindre sannsynlig at hendelsen inntreffer og får den beskrevne konsekvensen	Hendelsen inntreffer årlig og får den beskrevne konsekvensen	Sikkerhetsbrudd kan skje ved at egne medarbeidere opptrer med forsett og har en viss kompetanse. Utenforstående må opptre med overlegg og noe kompetanse.	- sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer etter hensikten

Risikovurdering for anskaffelse av sak- og arkivsystem fra SIKRI

25. mars 2022

1 Innhold

1.	Hva skal anskaffes?	3
2.	Omfang	3
2.1.	Avgrensninger	3
2.2.	Oversikt over verdier	3
3.	Konsekvens	3
4.	Sannsynlighet	5
5.	Risikovurdering	7
6.	Tiltak	7
7.	Restrisiko etter tiltak – konklusjon	9

1. Hva skal anskaffes?

Diskrimineringsnemnda skal anskaffe et velfungerende elektronisk sak- og arkivsystem for å oppfylle sine oppgaver. Løsningen skal være en ferdigutviklet standardløsning levert som SaaS (Software as a Service). Det skal være tilstrekkelig sikkerhet for personopplysninger og prinsippene for personvern skal ivaretas, blant annet innebygget personvern, jf. GDPR art. 32, 25 og 5.

2. Omfang

Denne rapporten omfatter ROS-analyse for risikobildet dersom Diskrimineringsnemnda anskaffer sak- og arkivsystem fra SIKRI, angir akseptert risiko og gir anbefalinger på hvilke tiltak som bør iverksettes for å styre et gitt risikoscenario til akseptabelt nivå. Analysen går inn på deler av Diskrimineringsnemndas bruk av programvaren, men er ikke uttømmende om bruk.

Rapporten fokuserer på

2.1. Avgrensninger

Analysen bygger på Diskrimineringsnemndas nivå for akseptabel risiko. Analysen omfatter selve programvaren, og er avgrenset mot Diskrimineringsnemndas bruk av programvaren. Analysen er gjort før Diskrimineringsnemnda har avgjort hvilken programvare vi ønsker å kjøpe, og er en del av anskaffelsesprosessen.

2.2. Oversikt over verdier

En verdi er alt som anses som verdifullt for en virksomhet eller en innbygger, eksempelvis tap av omdømme, brudd på lov eller forskrift eller brudd på ønsket/pålegg om konfidensialitet.

Den verdien som Diskrimineringsnemnda hovedsakelig behandler er særlige kategorier personopplysninger knyttet til diskrimineringsgrunnlag i konkrete klagesaker, personalsaker og personopplysninger i generelle saker. Oversikt over personopplysninger som Diskrimineringsnemnda behandler finnes i vår behandlingsoversikt, jf. GDPR artikkel 30.

3. Konsekvens

Vurderingen tar utgangspunkt i listen av de identifiserte uønskede hendelsene, og skal gi svar på spørsmål av typen «hva er konsekvensen hvis det som kan gå galt går galt».

At verdiene i systemet er korrekt fastsatt er kritisk for en riktig vurdering av konsekvenser.

Konsekvens kan uttrykkes som økonomiske tap, tap av liv og helse, tap av omdømme, straffeansvar for virksomheten osv.

Behovet for å fastsette kriterier for konsekvens følger av ISO/IEC 27005:2011 kapittel 7.2.3. Det benyttes fire graderinger på konsekvens:

1. Lav
2. Moderat
3. Høy
4. Svært høy

Nedenfor er kriteriene som vil bli benyttet videre:

Konsekvens- matrise	Lav	Moderat	Høy	Svært høy
	1	2	3	4
Virksomhet Omdømme	Kun mindre diskusjon i organisasjonen	Avsender må forklare seg for kundene om saken. Enkeltstående presseoppslag.	Offentlig debatt, ledelsen må forklare seg for myndigheter. Midlertidig endret oppfatning av DNS profesjonalitet. Ekstern gransking.	Politisk debatt, betydelig økonomisk erstatning/tap. Varig endret oppfatning av DNS profesjonalitet
Virksomhet Økonomisk	Ubetydelige økonomiske tap	Mange små kostnader. Reduserte besparelser.	Stort økonomisk tap. Stor engangs-kostnad	Betydelig økonomisk erstatning/tap
Virksomhet Lovkrav, mål og rettssikkerhet.	Mindre lovbrudd oppdages før det får virkning utenfor DN. Kun kortere overskridelse av saks-behandlings-tid.	Overholder ikke kravene til saks-behandlingstid, får påpekning fra departementet.	Overtredelses-gebyr, erstatnings-søksmål. Pålegg. Klarer ikke ivareta partenes rettssikkerhet.	Alvorlige brudd på lover, regler og avtaler. Ikke formåls effektiv og kostnadseffektiv realisering av DNS samlede mandat og mål. Klarer ikke overholde kravene i tildelingsbrevet. Straffansvar. Betydelige overtredelses-gebyr og store erstatnings-sommer.
Partene	En mindre uleilighet, økonomisk tap som kan gjenopprettes eller tap av anseelse eller integritet gjennom	Gjenopprettbart økonomisk tap eller tap av anseelse og integritet gjennom kompromittering av særlige kategorier av	Helsetap, uopprettelig økonomisk tap eller alvorlig tap av anseelse og integritet	Tap av liv, vedvarende helsetap, betydelig og uopprettelig økonomisk tap eller alvorlig tap

Konsekvens- matrise	Lav	Moderat	Høy	Svært høy
	1	2	3	4
	kompromittering av personopplysninger	personopplysninger. Fare for skade eller helsetap.		av anseelse /integritet.

Kriteriene er hentet fra Norsk Helsenetts veileder for risikovurdering¹ og deretter modifisert i møte om risikovurderinger i Diskrimineringsnemnda i oktober 2018.

4. Sannsynlighet

Vurdering av sannsynligheten har som mål å finne svar på «hva er sannsynligheten for at det som kan gå galt går galt og får den beskrevne konsekvensen». Svaret angis kvantitativt, og sannsynlighetsskalaen ble fastsatt under kontekstetableringen.

For hver av de uønskede hendelser som er identifisert skal man gjøre en vurdering av sannsynligheten for at hendelsen inntreffer og at den får det utfallet/konsekvensen som er beskrevet. I mange tilfeller kan det være vanskelig å si noe om frekvens, da det ikke finnes noe godt statistisk materiale. I disse situasjonene kan man ta med en aktørs motivasjon for å gjennomføre en handling, eller hvor lett det vil være for en aktør å gjennomføre handlingen.

En integrert del av risikoaksept er å fastsette nivåer for sannsynlighet:

Vurdering	Frekvens	Motivasjon	Letthetsbetraktninger
Sannsynlig at hendelsen inntreffer og får den beskrevne konsekvensen 4	Hendelsen inntreffer ukentlig eller oftere og får den beskrevne konsekvensen	Sikkerhetsbrudd kan skje ved uaktsomhet (ubevisst eller uten forsett) av egne medarbeidere eller utenforstående. Det er ikke nødvendig med spesielle kunnskaper om interne forhold.	- sikkerhetstiltak er ikke etablert - krever små til normale ressurser av egne medarbeidere eller eksterne for å brytes - ikke nødvendig med kjennskap til tiltakene
Mulig at hendelsen inntreffer og får den	Hendelsen inntreffer en gang i måneden og får den	Sikkerhetsbrudd kan skje ved uaktsomhet av egne medarbeidere.	- sikkerhetstiltak er ikke fullt etablert i forhold til sikkerhetsbehovet

¹ <http://www.nhn.no/informasjssikkerhet/risikovurdering>

Vurdering	Frekvens	Motivasjon	Letthetsbetraktninger
beskrevne konsekvensen 3	beskrevne konsekvensen	Utenforstående må ha noe kompetanse, og forsettlig (bevisst eller aktivt) gå inn for å bryte sikkerhetstiltakene.	- sikkerhetstiltak fungerer ikke etter hensikten - egne medarbeidere trenger kun små til normale ressurser for å bryte tiltakene
Mindre sannsynlig at hendelsen inntreffer og får den beskrevne konsekvensen 2	Hendelsen inntreffer årlig og får den beskrevne konsekvensen	Sikkerhetsbrudd kan skje ved at egne medarbeidere opptrer med forsett og har en viss kompetanse. Utenforstående må opptre med overlegg og noe kunnskap om interne forhold (med hensikt og plan, eksempelvis ved at flere tiltak brytes i riktig rekkefølge) for å omgå/bryte sikkerhetstiltakene.	- sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer etter hensikten - egne medarbeidere trenger små til normale ressurser og normal kjennskap til tiltakene for å bryte disse - eksterne trenger gode ressurser og god kjennskap til tiltakene for å bryte disse
Sjelden at hendelsen inntreffer og får den beskrevne konsekvensen 1	Hendelsen inntreffer omkring hvert 3. år eller sjeldnere og får den beskrevne konsekvensen	Sikkerhetsbrudd kan kun skje ved at egne medarbeidere opptrer med overlegg og har spesiell kompetanse eller kunnskap. Utenforstående må ha spisskompetanse og et samarbeid med personer i virksomheten.	- sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer etter hensikten - krever gode ressurser og godt kjennskap av egne medarbeidere for å brytes - eksterne kan ikke omgå tiltakene

Der erfaringstall foreligger, gir disse en indikasjon på framtidig frekvens. På bakgrunn av letthets- og motivasjonsvurderingen gjengitt over, kan også forventet frekvens anslås. Til hjelp for vurderingen er det utarbeidet kriterier for letthetsbetraktninger, se over.

Trusselaktører er ikke like, og det finnes mange metoder for å kategorisere ulike trusselaktører. Her er det tatt utgangspunkt i de samme egenskapene som i risikohåndterings-guiden til NIST, SP 800-302, og lagt til utholdenhet:

- Evne - En aktørs tilgang på kompetanse og ressurser.
- Vilje - En aktørs grad av motivasjon for å angripe.
- Måltrettethet - En aktørs grad av måltrettethet mot brukere eller brukergrupper. Måltrettethet vil øke risikoen for individene angrepet rettes mot, pga økt frekvens og tilpasning av angrepene.
- Utholdenhet - En aktørs evne til å opprettholde et angrep over tid og evnen til å utføre flere angrepsforsøk over tid.

Det er imidlertid også verdt å være oppmerksom på at trusselaktørers gevinst av vellykket sikkerhetsbrudd vil påvirke frekvensvurderingen, jf. at verdien vil være styrende for motivasjonen.

Det kan således være nødvendig å knytte et anslag over gevinsten for trusselaktøren til opplysningene som inngår i løsningen – i tillegg til taps- og skadepotensialet for virksomheten selv, innbyggeren mv., jf. konsekvenskategoriene. For motivasjonsvurderingen vises til omtalen i Datatilsynets veileder kapittel 7.3.

Diskrimineringsnemnda har per dags dato ikke systematiserte og skriftlige erfaringstall. Der vi vet at enkelte hendelser har skjedd, eller at samme type hendelse har skjedd flere ganger, er dette tatt med i sannsynlighetsvurderingen. Det bemerkes at dette medfører noe usikkerhet ved vurderingen. Der historiske erfaringstall mangler har vi hovedsakelig brukt motivasjons- og letthetsbetraktninger.

5. Risikovurdering

I risikoregisteret evaluerer vi risikoene ved å trekke frem relevante scenarier og knytte disse til verdier for sannsynlighet og konsekvens. Produktet av disse gir en verdi for risiko. Ved vurdering av risiko er eksisterende og planlagte tiltak og effekten av disse på sannsynlighet og konsekvens gjenspeilet i verdiene.

Hva som er akseptabel risiko for Diskrimineringsnemnda er fastsatt i Policy for informasjonssikkerhet versjon 3 pr. 13.01.2022.

6. Tiltak

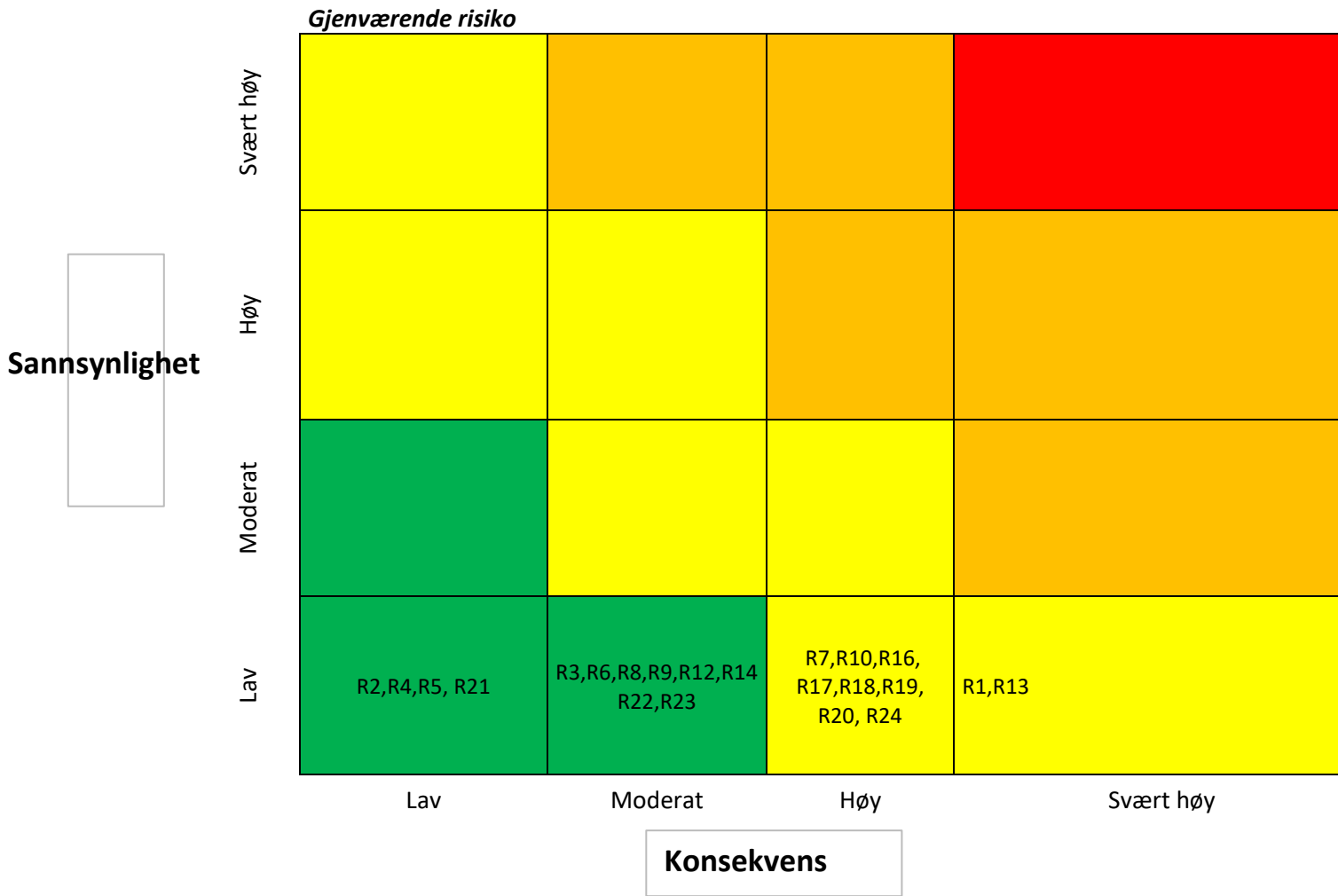
I dette kapittelet er beskrevet en oppsummering av anbefalte tiltak som er detaljert i risikoregisteret:

1. *Lage liste over alle saker som må opprettes på nytt i Elements, hvor saksbehandler og arkivet samarbeider om oppretting og mulige kryssreferanser. Gjensidig sjekk og kontroll.*

² <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

2. Avklare gjennomføring av sletting i gammelt system.
3. Avklare leverandørens plikt iht databehandleravtalen at databehandler skal bistå den behandlingsansvalige til å oppfylle sine plikter som behandlingsansvarlig, herunder i forhold til skytjenesten.
4. Avklare implementering av sikkerhetskopi og jevnlig backup.
5. Avklare brukeropplæring, herunder tid og ressurser internt.
6. Gjøre avklaringer opp mot Braathe mht forutsetninger for systemet, brukervennlighet og sikkerhet, herunder vurdere E5 som sikkerhetsløsning hos Microsoft (i motsetning til E3 som er dagens løsning) og bruk av Citrix.
7. Sjekke referanser og muligheter for å komme seg ut av avtalen ved ev. organisatoriske endringer hos leverandør/skyleverandør i fremtiden.
8. Avklare/sørge for gode sletterutiner (multitenant miljø kan føre til at data som skal slettes ikke blir slettet tilstrekkelig).
9. Sikre teknisk oppsett mot overbelastning (ved DDOS-angrep) gjennom føderert innlogging eller via SAML-sertifiserte innlogginger.
10. Avklare tilrettelegging for tilgangsstyring, herunder klassifisering av data, tilgangsstyring og brukeropplæring.
11. Tydelig avtale hvem som har ansvar for hva når det gjelder sikkerhetsoppdateringer.
12. Forsikre oss om at skyleverandøren har løsninger som effektivt overvåker og kan håndtere dataangrep. Kreve at leverandøren har kontinuitetsplaner og vurdere skyleverandørens løsning for å håndtere dataangrep.

7. Restrisiko etter tiltak – konklusjon



2		kunnskap om interne forhold (med hensikt og plan, eksempelvis ved at flere tiltak brytes i riktig rekkefølge) for å omgå/bryte sikkerhetstiltakene.	- egne medarbeidere trenger små til normale ressurser og normal kjennskap til tiltakene for å bryte disse - eksterne trenger gode ressurser og god kjennskap til tiltakene for å bryte disse
Sjelden at hendelsen inntreffer og får den beskrevne konsekvensen 1	Hendelsen inntreffer omkring hvert 3. år eller sjeldnere og får den beskrevne konsekvensen	Sikkerhetsbrudd kan kun skje ved at egne medarbeidere opptrer med overlegg og har spesiell kompetanse eller kunnskap. Utenforstående må ha spisskompetanse og et samarbeid med personer i virksomheten.	- sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer etter hensikten - krever gode ressurser og godt kjennskap av egne medarbeidere for å brytes - eksterne kan ikke omgå tiltakene

Lav risiko	Ingen tiltak nødvendig
Moderat risiko	Hendelsene skal vurderes nærmere og eventuelle tiltak implementeres eller risiko aksepteres
Høy risiko	Tiltak skal iverksettes

R10	Hele skydingen blir utlignelig i lengre tid på grunn av fire pårking, brann, naturkatastrofe mv. Brudd på tilgjengelighet.	Risiko for nedetid over en lengre periode (deler). Ikke formålseffektiv og kostnadsineffektiv realisering av DNS mandat og mål. Klarer ikke overholde kravene i tildelingsbrevet.	Høy	Lav	Samsynligheten vurderes som lav, ettersom det aldri har skjedd i Norge at en skyldning har blitt utlignelig på grunn av brann/naturkatastrofe.	Moderat	Moderat	Acos har tre uavhengige datastener og backup. Gode garantier for oppsett.	Høy	Lav	Moderat
R12	Fel tilgangsstyring til data i historisk base. Brudd på konfidensialitet.	Ved migrering av data til historisk base tapes tilgangsstyring fra produksjonsmiljøet og alle ansatte får tilgang til alle saker og dokumenter ved sak. De fleste ansatte har usensert tilgang til alle klagesaker, men ikke personalmapper. Vil kun få virkning internt.	Moderat	Lav	Ved overgang til Acos sin løsning forsetter produktproben i skyen. Alle metadataene vurderes derfor som lav.	Lav	Lav	Ingen tiltak nødvendig.	Moderat	Lav	Lav
R13	Dataangrep mot løsningen blir ikke stoppet i tide. Skyleverandøren gir ikke motfall dersom man blir utsatt for DDOS-angrep (distribuert tjenestektangrep) eller "phishing".	Uvedkommende får tilgang til en større mengde taushetsbelagte opplysninger. Kan i tillegg medføre lengre nedetid. Ikke formålseffektiv og kostnadsineffektiv realisering av DNS smiede mandat og mål. Klarer ikke overholde kravene i tildelingsbrevet. Varig svekkelse av DNS tillit.	Svært høy	Høy	Basert på NSM's rapport "Risiko 2022", vurderes samsynligheten for dataangrep som høy. Trusleaktene viser stor kapasitet til å gjennomføre cyberangrep. Siden 2019 har NSM sett en tendens til åntall cyberhendelser som får alvorlige konsekvenser for virksomheter i Norge. Phishing har blitt svært vanlig blant samarbeidspartnere.	Høy	#N/A	Slike teknisk oppsett mot overbelastning gjennom føderert (m logging eller via SAML sertifiserte m logginger..	Svært høy		
R14	Data blir ikke tilfredsstillende sikret på grunn av manglende mulighet for tilgangsstyring. Data blir lagt i mapper hvor brukere uten tjenstlig behov har tilgang, kan endre og slette. Brudd på konfidensialitet, tilgjengelighet og integritet.	Selv ved feil, vil det ikke gi store konsekvenser. Alle har tilgang til alle klagesaker, det er bare personaldelen i arkivet enkelte ikke har tilgang til.	Moderat	Lav	Normalt at det tilrettelegges for tilgangsstyring ved bruk av NOARK-godkjent sakbehandlingssystem.	Lav	Lav	Acos viser til at de har gode løsninger for dette, interne tiltak, klassifisere data. Tilgangsstyring. Oppfølging. Etablere rutiner for håndtering av data, og hvor ulike typer data skal lagres.		Lav	Lav
R15	Skydsynligheten utsettes for dataangrep. Brudd på tilgjengelighet og konfidensialitet.	Store mengder taushetsbelagte opplysninger kan komme på avveie. Avorlig regelbrudd. Offentlig debatt, ledelsen må forlate seg for myndigheter. Midlertidig endret oppfatning av DNS profesjonalitet.	Svært høy	Høy	Basert på NSM's rapport "Risiko 2022", vurderes samsynligheten for dataangrep som høy. Trusleaktene viser stor kapasitet til å gjennomføre cyberangrep. Siden 2019 har NSM sett en tendens til åntall cyberhendelser som får alvorlige konsekvenser for virksomheter i Norge.	Høy	Moderat	Tilbudet redager godt for løsnings sikkerhet og risikoreduerende tiltak. Acos er sertifisert etter ISO 27001 standarden. Tiltak: Ettersom begge skydsynene benytter Microsoft Exchange bunn (som vi har hos Braathe i dag), har vi trolig på vår side sikkerhet til å sikre sikkerheten ved å...	Svært høy	Lav	Moderat
R16	Data blir lagret på sikre lokasjoner, for eksempel på servere i land hvor man ikke har kontroll på sikkerheten. Data kan komme på avveie. Brudd på konfidensialitet.	Store mengder taushetsbelagte opplysninger kan komme på avveie. Avorlig regelbrudd. Offentlig debatt, ledelsen må forlate seg for myndigheter. Midlertidig endret oppfatning av DNS profesjonalitet.	Høy	Lav	Begge løsningene er NOARK-godkjent som forutsatt lagring av data i Norge. Samsynligheten vurderes derfor som lav.	Moderat	Moderat	Noark-godkjent løsning som forutsatt lagring av data i Norge. Reguleres også i databehandlingsloven.	Høy	Lav	Moderat
R17	Data er utlignelig fordi det nye systemet virker ikke som forutsatt, på grunn av forhold hos leverandør eller DN. Brudd på tilgjengelighet.	Risiko for nedetid over en lengre periode (deler). Ikke formålseffektiv og kostnadsineffektiv realisering av DNS mandat og mål. Klarer ikke overholde kravene i tildelingsbrevet.	Høy	Moderat	Law ICT-kompetanse internt. Avhengig av Braathe og at leverandøren gir god og forståelig informasjon, med klare bestillinger på hva som er nødvendig for at løsningen skal fungere som forutsatt.	Moderat	Moderat	Tilbud 1. Forordningene for tilbudet må forelegges Braathe til kontroll. 2. Sjekk oppgitte referanser i tilbudet. 3. God planlegging og evt. bistand fra Braathe ved overgang til ny løsning. Sekretariatet arbeider på PC-er fra nemnda, der Braathe sørger for at ved behov for informasjon om dette, kan de få tilgang til informasjonen som er nødvendig for å gjennomføre oppdraget.	Høy	Lav	Moderat
R18	Nødvendige sikkerhetsoppdateringer blir ikke gjort og sårbarheter i systemet utnyttes. Skydsynen kan bli utsatt for dataangrep. Brudd på tilgjengelighet, integritet og konfidensialitet.	Uvedkommende får tilgang til en større mengde taushetsbelagte opplysninger. Kan i tillegg medføre lengre nedetid. Ikke formålseffektiv og kostnadsineffektiv realisering av DNS smiede mandat og mål. Klarer ikke overholde kravene i tildelingsbrevet. Varig svekkelse av DNS tillit.	Høy	Lav	Samsynligheten for dette vurderes i utgangspunktet som lav. Tilbydene er profesjonelle aktører og ruinene for sikkerhetsoppdatering fremstår gode.	Moderat	Moderat	ACOS sitt eget skriptor. Drifter programvare på en Azure plattform. Acos tar ansvar for alle oppgaver knyttet til drift og vedlikehold av tjenesten. På den måten sikres en tilgjengelig og stabil programvare som kan håndtere dataangrep. Kree at leverandøren har kontinuitetsplaner.	Høy	Lav	Moderat
R19	Sikkerhetsbrudd blir ikke oppdaget. Responsmiljøet lokalt avdekker ikke mistenkelig trafikk eller angrep på nettverksnivå.	Uvedkommende får tilgang til en større mengde taushetsbelagte opplysninger. Data på avveie. Varig svekkelse av DNS tillit.	Høy	Lav	Samsynligheten for dette vurderes i utgangspunktet som lav. Tilbydene er profesjonelle aktører med gode sikkerhetsrutiner for å oppdage sikkerhetsbrudd.	Moderat	Moderat	tilnærming til informasjonsikkerhet, med gode rutiner. Tiltak: Forsikre oss om at skyleverandøren har løsninger som effektivt overvåker og kan håndtere dataangrep. Kree at leverandøren har kontinuitetsplaner.	Høy	Lav	Moderat
R20	Utro tjener hos leverandøren. Benytter seg av sine tilganger for å selge data, personlister, e-poster eller annen informasjon for egen vinnings skyld. Brudd på konfidensialitet.	Uvedkommende får tilgang til større mengder taushetsbelagte og personensitive opplysninger. Lovbrudd. Må melde avvik til Datatilsynet.	Høy	Lav	Tilbydene er profesjonelle aktører. Begge tilbudene legger opp til at det er få ansatte som har tilgang. Dette er også avaregulert. Risikoen vurderes derfor som lav.	Moderat	Moderat	Oppfølging, tilgangsstyring og taushetsdeklarerer er tatt høyde for i tilbudet. Reguleres i databehandlingsloven.	Høy	Lav	Moderat

R21	Treg/utfredstillende datainngang. Netverkskapasiteten vår eller andre interne forhold er ikke tilstrekkelig for behovet i skyeningen. Brudd på tilgjengelighet.	Data kan bli delvis utliggeligg. Frustrasjon blant de ansatte.	Lav	Moderat	Vanskelig å vurdere sannsynligheten. Erfaringen vi har med bruk av Teams innefor Citrix er dårlig. Etter som vi muligens fortsatt skal benytte Citrix til dette, vurderer vi det som moderat sannsynlig.	Lav	Tiltak: God planlegging og bistand av Braathe ved implementering. Braathe må involveres tidlig i prosessen. Vurder i samarbeid med Braathe om det er mulig å sekretariet/nemnda arbeider i skyningen utenfor Citrix.	Lav	Lav
R22	Data blir avlyttet under transport til/fra skyleverandør. Brudd på konfidensialitet.	Uvedkommende får tilgang til tusenvis av dokumenter og personlige opplysninger. Data på avveie. Lovbrudd som må meldes til Datainsynet.	Høy	Lav	Bagge tilbyderne er profesjonelle aktører med oppsett for autentiseringsmekanismer og kryptering.	Moderat	redigjenter som sender data autentiseres seg mot integrasjonsgressenittet via OAuth2-prosessen eller maskinier med tilgjengelige sikkerhet, ref. tilbuddet fra Xcos. Der dette ikke er mulig, tilbys oppsett av andre felleksjoner. Koudesione	Moderat	Modrat
R23	Manglende styring av brukertilganger. Brukertilganger blir ikke endret eller avsluttet når personer (interne eller eksterne) skifter rolle, slutter eller av andre årsaker ikke lenger skal ha tilgang til data. Brudd på konfidensialitet.	Begrenset konsekvens. Kan få tilgang til nye dokumenter som man ikke har et tjenestlig behov for å se. Begrenset hvor mange dokumenter det er snakk om, men muligheter for at opplysninger om kollegaer blir kjent.	Moderat	Moderat	Krever aktiv handling fra den som har tilgang, men samtidig enkelt å få tilgang til dataen. Enkelt å glipe på sletting (manuell jobb).	Moderat	Databehandlevaren gir tilgang ved behov. Websak har mulighet for tilgangstyring/ulike brukertilganger. Tiltak: Regulere dette i interne rutiner.	Lav	Modrat
R24	Uautorisert tilgang til data via felles PC. Brudd på konfidensialitet. Neste bruker får tilgang til data ved å trykke "tilbake" på nettleieren.	Uvedkommende får tilgang til personensitive opplysninger.	Høy	Moderat	Ved test av internkontrollsystemet var det mulig å få tilgang til IKS ved å trykke "tilbake" på nettleieren. Nemnda har like egen DN-pc.	Moderat	Tiltak: To-faktor pålogging. Oppklaring og rutiner. IKT-rutinen må oppdateres. Vurdere om nemnda fortsatt må arbeide innefor Citrix. .	Modrat	Modrat
R25	Tap av data på nettsiden	Statistikk over klagesaker på diskrimineringsnemnda.no er koblet opp mot saksbehandlersystemet og går tapt ved omlegging uten særlige tiltak.	Høy	Moderat	Viktig å finne en løsning på dette før omlegging. Dagens system er basert på en direkte kobling til saksbehandlersystemet	Moderat	Viktig å sørge for plan for å ivareta dette	Lav	Lav
R26						#N/A		#N/A	#N/A
R27						#N/A		#N/A	#N/A
R28						#N/A		#N/A	#N/A
R29						#N/A		#N/A	#N/A
R30						#N/A		#N/A	#N/A

Deltakere	
Navn	Rolle/funksjon
Helene A. Reksten	Arkivleder
Kristian Skjeldal	personvernombud
Ingrid Teistung	fung.personvernombud

Konsekvens- matrise	Lav 1		Moderat 2		Høy 3		Svært høy 4	
Virksomhet Omdømme og tillit	Kun mindre diskusjon i organisasjonen		Avsender må forklare seg for partene om saken. Enkeltstående presseoppslag.		Offentlig debatt, ledelsen må forklare seg for myndigheter. Midlertidig endret oppfatning av DN's profesjonalitet. Ekstern gransking.		Politisk debatt, betydelig økonomisk erstatning/tap. Varig endret oppfatning av DN's profesjonalitet.	
Virksomhet Økonomisk	Ubetydelige økonomiske tap		Mange små kostnader. Reduserte besparelser.		Stort økonomisk tap. Stor engangskostnad		Betydelig økonomisk erstatning/tap	
Virksomhet Lovkrav, mål og rettssikkerhet	Mindre lovbrudd oppdages før det får virkning utenfor organisasjonen. Kun kortere overskridelse av saksbehandlingstid.		Overholder ikke kravene til saksbehandlingstid, får påpekning fra departementet.		Overtredelsesgebyr, erstatningssøksmål. Pålegg. Klarer ikke ivareta partenes rettssikkerhet.		Alvorlige brudd på lover, regler og avtaler. Ikke formålseffektiv og kostnadseffektiv realisering av DN's samlede mandat og mål. Klarer ikke overholde kravene i Tildelingsbrevet. Straffansvar. Betydelige overtredelsesgebyr og store erstatningssummer. Pålegg.	
Partene	En mindre uleilighet, økonomisk tap som kan gjenopprettes eller tap av anseelse eller integritet gjennom kompromittering av personopplysninger		Gjenopprettbart økonomisk tap eller tap av anseelse og integritet gjennom kompromittering av særlige kategorier av personopplysninger. Fare for skade eller helsetap.		Helsetap, uopprettelig økonomisk tap eller alvorlig tap av anseelse og integritet		Tap av liv, vedvarende helsetap, betydelig og uopprettelig økonomisk tap eller alvorlig tap av anseelse /integritet.	

Vurdering	Frekvens	Motivasjon	Letthetsbetraktninger
-----------	----------	------------	-----------------------

Sannsynlig at hendelsen inntreffer og får den beskrevne konsekvensen	Hendelsen inntreffer ukentlig eller oftere og får den beskrevne konsekvensen	Sikkerhetsbrudd kan skje ved uaktsomhet (ubevisst eller uten forsett) av egne medarbeidere eller utenforstående. Det er ikke nødvendig med spesielle kunnskaper om interne forhold.	sikkerhetstiltak er ikke etablert - krever små til normale ressurser av egne medarbeidere eller eksterne for å brytes - ikke nødvendig med kjennskap til tiltakene
4			
Mulig at hendelsen inntreffer og får den beskrevne konsekvensen	Hendelsen inntreffer en gang i måneden og får den beskrevne konsekvensen	Sikkerhetsbrudd kan skje ved uaktsomhet av egne medarbeidere. Utenforstående må ha noe kompetanse, og forsettlig (bevisst eller aktivt) gå inn for å bryte sikkerhetstiltakene.	- sikkerhetstiltak er ikke fullt etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer ikke etter hensikten - egne medarbeidere trenger kun små til normale ressurser for å bryte tiltakene
3			
Mindre sannsynlig at hendelsen inntreffer og får den beskrevne konsekvensen	Hendelsen inntreffer årlig og får den beskrevne konsekvensen	Sikkerhetsbrudd kan skje ved at egne medarbeidere opptrer med forsett og har en viss kompetanse. Utenforstående må opptre med overlegg og noe kompetanse.	- sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer etter hensikten

Risikovurdering for anskaffelse av sak- og arkivsystem fra ACOS

25. mars 2022

1 Innhold

1.	Hva skal anskaffes?	3
2.	Omfang	3
2.1.	Avgrensninger	3
2.2.	Oversikt over verdier	3
3.	Konsekvens	3
4.	Sannsynlighet	5
5.	Risikovurdering	7
6.	Tiltak	7
7.	Restrisiko etter tiltak – konklusjon	9

1. Hva skal anskaffes?

Diskrimineringsnemnda skal anskaffe et velfungerende elektronisk sak- og arkivsystem for å oppfylle sine oppgaver. Løsningen skal være en ferdigutviklet standardløsning levert som SaaS (Software as a Service). Det skal være tilstrekkelig sikkerhet for personopplysninger og prinsippene for personvern skal ivaretas, blant annet innebygget personvern, jf. GDPR art. 32, 25 og 5.

2. Omfang

Denne rapporten omfatter ROS-analyse for risikobildet dersom Diskrimineringsnemnda anskaffer sak- og arkivsystem fra ACOS, angir akseptert risiko og gir anbefalinger på hvilke tiltak som bør iverksettes for å styre et gitt risikoscenario til akseptabelt nivå. Analysen går inn på deler av Diskrimineringsnemndas bruk av programvaren, men er ikke uttømmende om bruk.

Rapporten fokuserer på

2.1. Avgrensninger

Analysen bygger på Diskrimineringsnemndas nivå for akseptabel risiko. Analysen omfatter selve programvaren, og er avgrenset mot Diskrimineringsnemndas bruk av programvaren. Analysen er gjort før Diskrimineringsnemnda har avgjort hvilken programvare vi ønsker å kjøpe, og er en del av anskaffelsesprosessen.

2.2. Oversikt over verdier

En verdi er alt som anses som verdifullt for en virksomhet eller en innbygger, eksempelvis tap av omdømme, brudd på lov eller forskrift eller brudd på ønsket/pålegg om konfidensialitet.

Den verdien som Diskrimineringsnemnda hovedsakelig behandler er særlige kategorier personopplysninger knyttet til diskrimineringsgrunnlag i konkrete klagesaker, personalsaker og personopplysninger i generelle saker. Oversikt over personopplysninger som Diskrimineringsnemnda behandler finnes i vår behandlingsoversikt, jf. GDPR artikkel 30.

3. Konsekvens

Vurderingen tar utgangspunkt i listen av de identifiserte uønskede hendelsene, og skal gi svar på spørsmål av typen «hva er konsekvensen hvis det som kan gå galt går galt».

At verdiene i systemet er korrekt fastsatt er kritisk for en riktig vurdering av konsekvenser.

Konsekvens kan uttrykkes som økonomiske tap, tap av liv og helse, tap av omdømme, straffeansvar for virksomheten osv.

Behovet for å fastsette kriterier for konsekvens følger av ISO/IEC 27005:2011 kapittel 7.2.3. Det benyttes fire graderinger på konsekvens:

1. Lav
2. Moderat
3. Høy
4. Svært høy

Nedenfor er kriteriene som vil bli benyttet videre:

Konsekvens- matrise	Lav	Moderat	Høy	Svært høy
	1	2	3	4
Virksomhet Omdømme	Kun mindre diskusjon i organisasjonen	Avsender må forklare seg for kundene om saken. Enkeltstående presseoppslag.	Offentlig debatt, ledelsen må forklare seg for myndigheter. Midlertidig endret oppfatning av DNS profesjonalitet. Ekstern gransking.	Politisk debatt, betydelig økonomisk erstatning/tap. Varig endret oppfatning av DNS profesjonalitet
Virksomhet Økonomisk	Ubetydelige økonomiske tap	Mange små kostnader. Reduserte besparelser.	Stort økonomisk tap. Stor engangs-kostnad	Betydelig økonomisk erstatning/tap
Virksomhet Lovkrav, mål og rettssikkerhet.	Mindre lovbrudd oppdages før det får virkning utenfor DN. Kun kortere overskridelse av saks-behandlings-tid.	Overholder ikke kravene til saks-behandlingstid, får påpekning fra departementet.	Overtredelses-gebyr, erstatnings-søksmål. Pålegg. Klarer ikke ivareta partenes rettssikkerhet.	Alvorlige brudd på lover, regler og avtaler. Ikke formåls effektiv og kostnadseffektiv realisering av DNS samlede mandat og mål. Klarer ikke overholde kravene i tildelingsbrevet. Straffansvar. Betydelige overtredelses-gebyr og store erstatnings-sommer.
Partene	En mindre uleilighet, økonomisk tap som kan gjenopprettes eller tap av anseelse eller integritet gjennom	Gjenopprettbart økonomisk tap eller tap av anseelse og integritet gjennom kompromittering av særlige kategorier av	Helsetap, uopprettelig økonomisk tap eller alvorlig tap av anseelse og integritet	Tap av liv, vedvarende helsetap, betydelig og uopprettelig økonomisk tap eller alvorlig tap

Konsekvens- matrise	Lav	Moderat	Høy	Svært høy
	1	2	3	4
	kompromittering av personopplysninger	personopplysninger. Fare for skade eller helsetap.		av anseelse /integritet.

Kriteriene er hentet fra Norsk Helsenetts veileder for risikovurdering¹ og deretter modifisert i møte om risikovurderinger i Diskrimineringsnemnda i oktober 2018.

4. Sannsynlighet

Vurdering av sannsynligheten har som mål å finne svar på «hva er sannsynligheten for at det som kan gå galt går galt og får den beskrevne konsekvensen». Svaret angis kvantitativt, og sannsynlighetsskalaen ble fastsatt under kontekstetableringen.

For hver av de uønskede hendelser som er identifisert skal man gjøre en vurdering av sannsynligheten for at hendelsen inntreffer og at den får det utfallet/konsekvensen som er beskrevet. I mange tilfeller kan det være vanskelig å si noe om frekvens, da det ikke finnes noe godt statistisk materiale. I disse situasjonene kan man ta med en aktørs motivasjon for å gjennomføre en handling, eller hvor lett det vil være for en aktør å gjennomføre handlingen.

En integrert del av risikoaksept er å fastsette nivåer for sannsynlighet:

Vurdering	Frekvens	Motivasjon	Letthetsbetraktninger
Sannsynlig at hendelsen inntreffer og får den beskrevne konsekvensen 4	Hendelsen inntreffer ukentlig eller oftere og får den beskrevne konsekvensen	Sikkerhetsbrudd kan skje ved uaktsomhet (ubevisst eller uten forsett) av egne medarbeidere eller utenforstående. Det er ikke nødvendig med spesielle kunnskaper om interne forhold.	- sikkerhetstiltak er ikke etablert - krever små til normale ressurser av egne medarbeidere eller eksterne for å brytes - ikke nødvendig med kjennskap til tiltakene
Mulig at hendelsen inntreffer og får den	Hendelsen inntreffer en gang i måneden og får den	Sikkerhetsbrudd kan skje ved uaktsomhet av egne medarbeidere.	- sikkerhetstiltak er ikke fullt etablert i forhold til sikkerhetsbehovet

¹ <http://www.nhn.no/informasjonsikkerhet/risikovurdering>

Vurdering	Frekvens	Motivasjon	Letthetsbetraktninger
beskrevne konsekvensen 3	beskrevne konsekvensen	Utenforstående må ha noe kompetanse, og forsettlig (bevisst eller aktivt) gå inn for å bryte sikkerhetstiltakene.	- sikkerhetstiltak fungerer ikke etter hensikten - egne medarbeidere trenger kun små til normale ressurser for å bryte tiltakene
Mindre sannsynlig at hendelsen inntreffer og får den beskrevne konsekvensen 2	Hendelsen inntreffer årlig og får den beskrevne konsekvensen	Sikkerhetsbrudd kan skje ved at egne medarbeidere opptrer med forsett og har en viss kompetanse. Utenforstående må opptre med overlegg og noe kunnskap om interne forhold (med hensikt og plan, eksempelvis ved at flere tiltak brytes i riktig rekkefølge) for å omgå/bryte sikkerhetstiltakene.	- sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer etter hensikten - egne medarbeidere trenger små til normale ressurser og normal kjennskap til tiltakene for å bryte disse - eksterne trenger gode ressurser og god kjennskap til tiltakene for å bryte disse
Sjelden at hendelsen inntreffer og får den beskrevne konsekvensen 1	Hendelsen inntreffer omkring hvert 3. år eller sjeldnere og får den beskrevne konsekvensen	Sikkerhetsbrudd kan kun skje ved at egne medarbeidere opptrer med overlegg og har spesiell kompetanse eller kunnskap. Utenforstående må ha spisskompetanse og et samarbeid med personer i virksomheten.	- sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer etter hensikten - krever gode ressurser og godt kjennskap av egne medarbeidere for å brytes - eksterne kan ikke omgå tiltakene

Der erfaringstall foreligger, gir disse en indikasjon på framtidig frekvens. På bakgrunn av letthets- og motivasjonsvurderingen gjengitt over, kan også forventet frekvens anslås. Til hjelp for vurderingen er det utarbeidet kriterier for letthetsbetraktninger, se over.

Trusselaktører er ikke like, og det finnes mange metoder for å kategorisere ulike trusselaktører. Her er det tatt utgangspunkt i de samme egenskapene som i risikohåndterings-guiden til NIST, SP 800-302, og lagt til utholdenhet:

- Evne - En aktørs tilgang på kompetanse og ressurser.
- Vilje - En aktørs grad av motivasjon for å angripe.
- Måltrettethet - En aktørs grad av måltrettethet mot brukere eller brukergrupper. Måltrettethet vil øke risikoen for individene angrepet rettes mot, pga økt frekvens og tilpasning av angrepene.
- Utholdenhet - En aktørs evne til å opprettholde et angrep over tid og evnen til å utføre flere angrepsforsøk over tid.

Det er imidlertid også verdt å være oppmerksom på at trusselaktørers gevinst av vellykket sikkerhetsbrudd vil påvirke frekvensvurderingen, jf. at verdien vil være styrende for motivasjonen.

Det kan således være nødvendig å knytte et anslag over gevinsten for trusselaktøren til opplysningene som inngår i løsningen – i tillegg til taps- og skadepotensialet for virksomheten selv, innbyggeren mv., jf. konsekvenskategoriene. For motivasjonsvurderingen vises til omtalen i Datatilsynets veileder kapittel 7.3.

Diskrimineringsnemnda har per dags dato ikke systematiserte og skriftlige erfaringstall. Der vi vet at enkelte hendelser har skjedd, eller at samme type hendelse har skjedd flere ganger, er dette tatt med i sannsynlighetsvurderingen. Det bemerkes at dette medfører noe usikkerhet ved vurderingen. Der historiske erfaringstall mangler har vi hovedsakelig brukt motivasjons- og letthetsbetraktninger.

5. Risikovurdering

I risikoregisteret evaluerer vi risikoene ved å trekke frem relevante scenarier og knytte disse til verdier for sannsynlighet og konsekvens. Produktet av disse gir en verdi for risiko. Ved vurdering av risiko er eksisterende og planlagte tiltak og effekten av disse på sannsynlighet og konsekvens gjenspeilet i verdiene.

Hva som er akseptabel risiko for Diskrimineringsnemnda er fastsatt i Policy for informasjonssikkerhet versjon 3 pr. 13.01.2022.

6. Tiltak

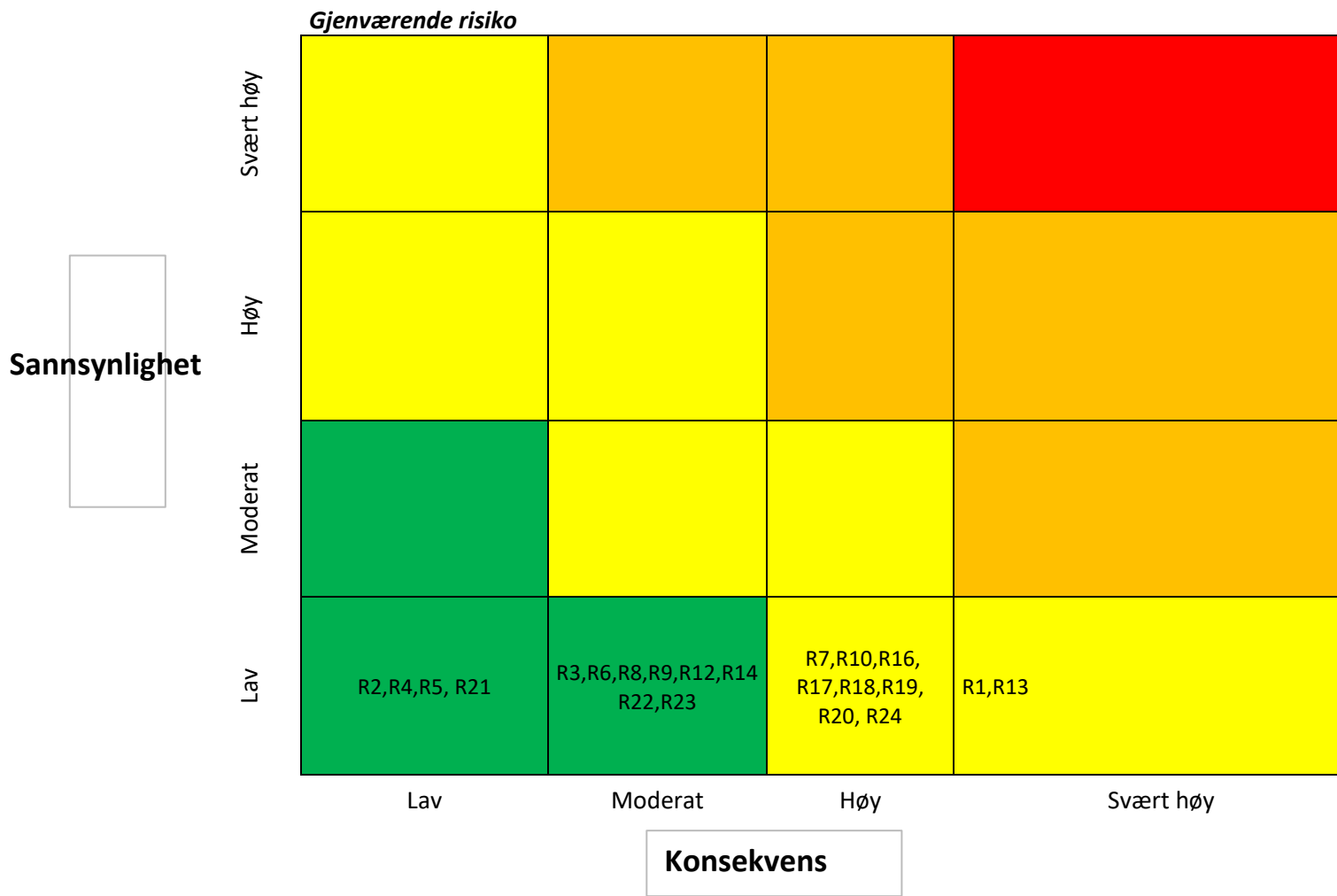
I dette kapittelet er beskrevet en oppsummering av anbefalte tiltak som er detaljert i risikoregisteret:

1. *Sørge for tilstrekkelig garanti i avtalen for at omleggingsfasen blir ivarettatt, slik at data ikke går tapt. Krav om sikkerhetskopi*

² <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

2. Avklare leverandørens plikt iht databehandleravtalen at databehandler skal bistå den behandlingsansvalige til å oppfylle sine plikter som behandlingsansvarlig, herunder i forhold til skytjenesten.
3. Avklare implementering av sikkerhetskopi og jevnlig backup.
4. Avklare brukeropplæring, herunder tid og ressurser internt.
5. Gjøre avklaringer opp mot Braathe mht forutsetninger for systemet, brukervennlighet og sikkerhet, herunder vurdere E5 som sikkerhetsløsning hos Microsoft (i motsetning til E3 som er dagens løsning) og bruk av Citrix.
6. Sjekke referanser og muligheter for å komme seg ut av avtalen ved ev. organisatoriske endringer hos leverandør/skyleverandør i fremtiden.
7. Avklare/sørge for gode sletterutiner (multitenant miljø kan føre til at data som skal slettes ikke blir slettet tilstrekkelig).
8. Sikre teknisk oppsett mot overbelastning (ved DDOS-angrep) gjennom føderert innlogging eller via SAML-sertifiserte innlogginger.
9. Avklare tilrettelegging for tilgangsstyring, herunder klassifisering av data, tilgangsstyring og brukeropplæring.
10. Tydelig avtale hvem som har ansvar for hva når det gjelder sikkerhetsoppdateringer.
11. Forsikre oss om at skyleverandøren har løsninger som effektivt overvåker og kan håndtere dataangrep. Kreve at leverandøren har kontinuitetsplaner og vurdere skyleverandørens løsning for å håndtere dataangrep.

7. Restrisiko etter tiltak – konklusjon



2		kunnskap om interne forhold (med hensikt og plan, eksempelvis ved at flere tiltak brytes i riktig rekkefølge) for å omgå/bryte sikkerhetstiltakene.	- egne medarbeidere trenger små til normale ressurser og normal kjennskap til tiltakene for å bryte disse - eksterne trenger gode ressurser og god kjennskap til tiltakene for å bryte disse
Sjelden at hendelsen inntreffer og får den beskrevne konsekvensen 1	Hendelsen inntreffer omkring hvert 3. år eller sjeldnere og får den beskrevne konsekvensen	Sikkerhetsbrudd kan kun skje ved at egne medarbeidere opptrer med overlegg og har spesiell kompetanse eller kunnskap. Utenforstående må ha spisskompetanse og et samarbeid med personer i virksomheten.	- sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer etter hensikten - krever gode ressurser og godt kjennskap av egne medarbeidere for å brytes - eksterne kan ikke omgå tiltakene

Lav risiko	Ingen tiltak nødvendig
Moderat risiko	Hendelsene skal vurderes nærmere og eventuelle tiltak implementeres eller risiko aksepteres
Høy risiko	Tiltak skal iverksettes

VURDERING AV PERSONVERNKONSEKVENSER (DPIA)¹ NYTT SAKSBEHANDLINGSSYSTEM

1. Vurdering av nytt saksbehandlingssystem

Diskrimineringsnemnda (DN) innfører nytt sak- og arkivsystem - Elements Cloud («Systemet»). Dette innebærer at Websak (WS) avvikles som sak- og arkivsystem. Systemet omfatter behandling av personopplysninger, og blant annet når det gjelder klagesaksbehandlingen omfattes også særlige kategorier (sensitive) personopplysninger. Behandlingen er en videreføring fra WS, og det er ikke nye typer personopplysninger eller andre formål som skal oppnås.

Vurderingen tar utgangspunkt i personvernforordningen (GDPR) artikkel 35 for å vurdere hvilke konsekvenser Behandlingen i Systemet vil ha for personopplysningsvernet for de personer det behandles personopplysninger om («Registrerte»).

I likhet med WS er Elements Cloud et NOARK-godkjent system for saksbehandling og arkiv, og det er høye krav til personvern og informasjonssikkerhet som er bygget inn i løsningen. Elements Cloud leveres som en tjeneste (SaaS) som både omfatter programvare og lagring av data i en skyløsning (i Norge).

2. Om vurdering av personvernkonsekvenser skal gjennomføres

Personvernforordningen artikkel 35 slår fast at en vurdering av personvernkonsekvenser skal gjennomføres når det er sannsynlig at en viss type behandling av personopplysninger medfører høy risiko for at de registrertes rettigheter og friheter etter forordningen ikke ivaretas.

De registrertes rettigheter omfatter rett til innsyn, retting, sletting, begrensning av behandling, rett til å protestere, retter ved automatiserte avgjørelser, rett til dataportabilitet og rett til informasjon.

De registrertes friheter omfatter grunnleggende menneskerettigheter som retten til privatliv og kommunikasjonsvern, retten til ikke å bli diskriminert, tanke, tros- og livssynsfrihet samt ytrings- og informasjonsfrihet.

Ved en DPIA skal risikoen vurderes med utgangspunkt i de registrertes perspektiv. Aktuelle risikofaktorer er brudd på konfidensialitet, integritet og tilgjengelighet. Det gjelder også graden av risiko for manglende medbestemmelse/mulighet til å gripe inn, åpenhet og forutsigbarhet for de registrerte.

¹ Se også Datatilsynets veileder om vurdering av personvernkonsekvenser: .

Overgangen til et nytt saksbehandlingssystem innebærer at det vil behandles store mengder særlige kategorier personopplysninger i et helt nytt system. Uten tilpasninger medfører dette i utgangspunktet en høy risiko for at de registrertes rettigheter og friheter etter forordningen ikke ivaretas, og tilsier at DPIA skal gjennomføres. Det har også blitt vurdert nødvendig å gjennomføre en intern ROS-analyse for Elements Cloud, jf. rapport 25. mars 2022.

3. Grunnleggende utgangspunkter og beskrivelser

«Behandling» av personopplysninger omfatter enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring. Behandlingen av ulike personopplysninger i Elements Cloud omfatter først og fremst mottak, lagring og utsendelse av slike opplysninger i forbindelse med den saksbehandlingen som foregår i DN.

Konsekvensvurderingen er gjennomført ved en gjennomgang av saken i en arbeidsgruppe bestående av personverngruppen (personvernombud og personvernressurs) og arkivleder. Hensynet til tid og ressurser har ikke gjort det mulig med en mer omfattende behandling og bredere medvirkning.

4. Opplysningene som skal behandles

Opplysningene som skal behandles i Systemet gjelder klagesakssaksbehandlingen i DN, personalforvaltning og generelle forvaltningssaker.

Klagesakene i DN, som utgjør den vesentligste delen av saksbehandlingen i Systemet, inneholder opplysninger om ulike diskrimineringsgrunnlag, som i stor grad overlapper med det som defineres som særlige kategorier (sensitive) personopplysninger, jf. personvernforordningen art. 9 nr. 1. Volumet av opplysninger som behandles varierer fra sak til sak og omfatter relativt detaljerte opplysninger om den enkelte.

5. De registrerte

De registrerte er parter i klagesaker og andre, slik som vitner, sakkyndige, journalister mv. I tillegg omfattes ansatte, nemndmedlemmer og varamedlemmer, studentpraktikanter og jobbsøkere.

6. Behandlingens lovlighet

All behandling av personopplysninger skal skje med et lovlig grunnlag. Systemet

skal legge til rette for at DN kan oppfylle sine plikter etter diskrimineringsombudsloven som forvaltningsorgan og plikten til å holde arkiv etter arkivloven. Saksbehandlingen gjelder utøving av offentlig myndighet som DN er pålagt, jf. personvernforordningen art. 6 nr. 1 bokstav e. Personalforvaltningen skjer på grunnlag av arbeidsavtalen, jf. personvernforordningen art. 6 nr. 1 bokstav b. I noen tilfeller vil behandlingsgrunnlaget kunne være rettslig forpliktelse, jf. personvernforordningen art. 6 nr. 1 bokstav c, jf. for eksempel arbeidsmiljøloven, bokføringsregelverket og arkivregelverket.

Klagesaksbehandlingen omfatter i stor grad særlige kategorier (sensitive) personopplysninger. Behandlingen har tilleggsgrunnlag i personvernforordningen art. 9, jf. 2. ledd nr. 1 bokstav g «viktige allmenne interesser...på grunnlag av...medlemsstatenes nasjonale rett.».

De registrerte informeres om behandlingen i personvernerklæring på diskrimineringsnemnda.no og i en egen personvernerklæring for ansatte i IKS. Det er også en personvernerklæring som er knyttet til bruk av skjemaløsningen. I klagesaksbehandlingen informeres partene i et eget informasjonsskriv.

7. Beskrivelse av behandlingen

Behandlingen i Systemet kan beskrives på følgende måte:

Skjemaløsningen:

Det er etablert ny skjemaløsning i tilknytning til Systemet. Utformingen av skjemaene videreføres som før. I klageskjemaet er det tatt inn en rubrikk for fødselsnummer.

Digital post via SvarUt/inn:

Løsning for sikkert mottak og sending av digital post er integrert i Systemet.

Integrasjon med Folkeregisteret/Kontakt- og reservasjonsregisteret/Enhetsregisteret

Systemet har integrasjon med Folkeregisteret/Kontakt- og reservasjonsregisteret/Enhetsregisteret. Oppslag gjøres mot Folkeregisteret og Enhetsregisteret for å registrere saksparter. Kontakt- og reservasjonsregisteret fanger opp hvem som har reservert seg mot digitale postforsendelser.

Integrasjon med Teams:

Systemet har integrasjon med Teams

Lagring i skyløsning:

Data lagres i skyløsningen til SIKRI, som er en del av leveransen for Elements Cloud (SaaS-avtale). Datalagringen skjer i Norge. Det er gitt garanti for sikker lagring bl.a. i ht ISO 27001 som standard for informasjonssikkerhet. Arkivsystemet er NOARK-godkjent standard. Back up (sikkerhetskopi) lagres i 30 dager.

Tilgang til data:

Systemet har tilgangsbegrensninger internt for ulike brukergrupper. Det vil si saksbehandlere, administrasjon, ledelse og nemndmedlemmer. Hvem som gis tilgang til hva er avgjort ut fra en vurdering av rolle og tjenstlig behov, basert på prinsippet om dataspredningsminimering og personvern.

Pålogging skjer via Citrix og har to-faktor autentisering.

Viderebehandling for arkivformål:

Data som er lagret i arkivsystemet viderebehandles for arkivformål i henhold til arkivloven og slettes iht. vår kassasjonsplan. Data i klagesaker skal bevares for alltid.

8. Innebygd personvern

Elements Cloud ivaretar prinsipper for innebygd personvern. Dette innebærer blant annet utvikling av mulighet for loggføring av oppslag og forbedring av søkemuligheter for å kunne finne ut hvilke opplysninger som er registrert om en person.

9. Personvernprinsippene

Personvernprinsippene (personvernforordningen artikkel 5) innebærer at all behandling av personopplysninger skal skje på en lovlig, rettferdig og åpen måte, at de skal benyttes til bestemte formål («formålsbegrensning»), omfanget personopplysninger skal være begrenset til det som er nødvendig («dataminimering»), de skal være korrekte og oppdaterte («riktighet»), ikke lagres lenger enn nødvendig («lagringsbegrensning») og ha tilstrekkelig sikkerhet mot uautorisert eller ulovlig behandling og mot utilsiktet tap («integritet og konfidensialitet»).

Den behandlingsansvarlige skal kunne påvise at personvernprinsippene følges («ansvar»). Ved å ivareta de registrertes rettigheter og friheter gjennomføres personvernprinsippene.

10. Ivaretagelse av de registrertes rettigheter

Risikoen for de registrertes rettigheter vurderes ikke som større enn normal ved det nye Systemet. Det vises i denne sammenheng til risikovurderingen som er foretatt.

11. Ivaretagelse av de registrertes friheter

Risikoen for de registrertes friheter iht. EMK vurderes på samme måte som for de registrertes rettigheter.

12. Sikkerhet ved behandlingen

Det er gjennomført en risikovurdering av Systemet, jf. ROS-rapport 25. mars

2022. Det ble foreslått følgende tiltak for å redusere risiko:

- Lage liste over alle saker som må opprettes på nytt i Elements, hvor saksbehandler og arkivet samarbeider om oppretting og mulige kryssreferanser. Gjensidig sjekk og kontroll.
- Avklare gjennomføring av sletting i gammelt system.
- Avklare leverandørens plikt iht. databehandleravtalen at databehandler skal bistå den behandlingsansvarlige til å oppfylle sine plikter som behandlingsansvarlig, herunder i forhold til skytjenesten.
- Avklare implementering av sikkerhetskopi og jevnlig backup.
- Avklare brukeropplæring, herunder tid og ressurser internt.
- Gjøre avklaringer opp mot Braathe mht. forutsetninger for systemet, brukervennlighet og sikkerhet, herunder vurdere E5 som sikkerhetsløsning hos Microsoft (i motsetning til E3 som er dagens løsning) og bruk av Citrix.
- Sjekke referanser og muligheter for å komme seg ut av avtalen ved ev. organisatoriske endringer hos leverandør/skyleverandør i fremtiden.
- Avklare/sørge for gode sletterutiner (multitenant miljø kan føre til at data som skal slettes ikke blir slettet tilstrekkelig).
- Sikre teknisk oppsett mot overbelastning (ved DDOS-angrep) gjennom føderert innlogging eller via SAML-sertifiserte innlogginger.
- Avklare tilrettelegging for tilgangsstyring, herunder klassifisering av data, tilgangsstyring og brukeropplæring.
- Tydelig avtale hvem som har ansvar for hva når det gjelder sikkerhetsoppdateringer.
- Forsikre oss om at skyleverandøren har løsninger som effektivt overvåker og kan håndtere dataangrep. Kreve at leverandøren har kontinuitetsplaner og vurdere skyleverandørens løsning for å håndtere dataangrep.

Tiltakene er gjennomført og restrisiko etter dette vurderes som håndterbar og akseptabel.

13. Personopplysningsvern ved behandlingen

I forbindelse med konfigurasjon av Systemet for bruk i DN har det blitt gjort flere tilpasninger for å ivareta personvern – særlig med tanke på at saksbehandlingen omhandler særlige kategorier (sensitive) personopplysninger:

- Det er etablert en trygg vei inn for digital post gjennom skjemaløsningen som er integrert med Systemet via SvarInn.
- Ved bruk av skjemaløsningen blir avsenderen låst til innlogget MinID bruker, og det innebærer en endring i forhold til tidligere. Ved å få sikker identitet på innsenderen unngår vi at klageskjema blir sendt inn i andres navn uten at det fremgår tydelig.
- Folkeregisteret, Kontakt- og reservasjonsregisteret og Enhetsregisteret er integrert i Systemet og rutinen beskriver at saksparter skal søkes opp i Folkeregisteret eller Enhetsregisteret. Dette bidrar til korrekte og oppdaterte personopplysninger – herunder om hvem som har reservert seg mot å få digital post.
- Ved ekspedering blir forsendelser som ikke skal sendes til mottakerens digitale postkasse umiddelbart sendt til print. Integrasjon med Kontakt- og reservasjonsregisteret skal sørge for oppdaterte opplysninger.
- Det er lagt til rette for at lyd/videofiler kan lastes opp på et fildelingsområde ved innsending av skjema. På denne måten sørges det for sikker digital kommunikasjon også når det gjelder denne typen medium.
- Det er opprettet tilgangsgrupper internt som skal begrense tilgangen til Systemet utfra tjenstlig behov. Det er tilgangsgrupper for personal, saksbehandlere og for nemndmedlemmer. Integrasjon med Webcruiter og hvem som inngår databehandleravtale må avklares.
- Oppretting av saker foretas av arkivet og arkivleder avslutter saker. Dette skal sikre at det ikke skjer feil ved at opplysninger blir endret utilsiktet.
- Journalføring skjer fortløpende og det er sperre på endringer som skal hindre feil.
- Det er sperre på avsluttede saker slik at nye journalposter ikke kan legges til. Det reduserer faren for at journalposter ikke når frem til saksansvarlig.
- Tittel 2 finnes ikke i Elements i motsetning til i WS. Navn tas derfor ikke med i tittelfeltet på journalposten.
- Det er ikke mulig å slette journalposter ved en feil. Arkivet har mulighet til å sette en journalpost til utgått.
- Funksjonen for offentlig journal er deaktivert ettersom sakene i utgangspunktet er skjermet u.off. pga. personlige forhold som de fleste sakene gjelder.
- Saker som er klassifisert UO er ikke mulig å ekspedere via e-post.
- Godkjenninger fra ledelse eller nemndleder må dokumenteres og saksbehandlingsrutinene må justeres for å sikre at denne

dokumentasjonen blir lagret på saken.

- Graderte dokumenter skal fortsatt ikke lagres i Systemet for saksbehandling, og rutinen for behandlingen av denne typen saker videreføres.
- Fildeling og samtaler utenfor systemet som i Teams må lagres på sak i Systemet, og rutine for dette videreføres.

14. Medvirkning fra berørte parter

Det har ikke blitt vurdert som aktuelt å ha med andre berørte parter ved vurderingen, slik som representanter fra de registrerte eller databehandlerne.

15. Involvering av personvernombudet

Personvernombudet er med i personverngruppen og kjenner ut ifra gjennomgangen i arbeidsgruppen godt til saken.

16. Ledelsens godkjenning

Vurderingen av personvernkonsekvenser må behandles av ledelsen i virksomheten, som må tilslutte seg vurderingen, beslutte ytterligere risikoreduserende tiltak eller akseptere restrisikoen. Dersom restrisikoen medfører en høy risiko for behandlingen, skal ledelsen beslutte forhåndsdrøftelse med Datatilsynet.

17. Konklusjon

Risikoen anses innenfor det akseptable, og behandlingen kan videreføres i tråd med de forutsetningene som det er lagt opp til under risikoreduserende tiltak, jf. ovenfor under avsnittene 12 og 13.