ØKONOMISTYRELSEN

Analyse af systemunderstøttelse af whistleblowerordninger i staten (uddrag)

November 2020

Introduktion

Om rapporten

Nærværende rapport er udarbejdet på grundlag af regeringens beslutning om at indføre whistleblowerordninger i staten senest den 1. november 2020 og er udarbejdet af Økonomistyrelsen med inddragelse af alle ministerier.

Rapporten undersøger om de kommende whistleblowerordninger i staten med fordel kan understøttes af et fælles it-system. Rapporten kortlægger regler, behov og krav til statslige whistleblowerordninger og undersøger, om ordningerne helt eller delvist kan systemunderstøttes, samt hvorvidt dette med fordel kan være en fælles løsning for staten.

Rapporten er færdiggjort ultimo oktober 2020, dvs. inden regeringen i november 2020 traf beslutning om, at Statens It skulle forestå anskaffelse og udrulning af et obligatorisk, fællesstatsligt whistleblowersystem, og skal derfor læses i lyset heraf. Analysen dannede baggrund for beslutningen, og analysens afdækning af faktuelle forhold, fx kortlægning af eksisterende ordninger mv., er ikke efterfølgende tilpasset.

Indholdsfortegnelse

ØKONOMISTYRELSEN

Ledelsesresumé (1/2)

Hovedkonklusioner

- **Analysen undersøger hensigtsmæssigheden af eventuel fælles systemunderstøttelse af de statslige whistleblowerordninger.** Undersøgelsen besvarer således, om ordningerne meningsfuldt kan systemunderstøttes, og hvordan systemunderstøttelse mest hensigtsmæssigt anskaffes.
- **Analysen er afgrænset til statslige whistleblowerordninger:** Analysen omhandler de statslige whistleblowerordninger, der etableres i overensstemmelse med Justitsministeriets vejledning. Ordninger i regi af andre offentlige virksomheder, regioner og kommuner er uden for scope. Ordningerne er tiltænkt de statslige myndigheders arbejdstagere, samarbejdspartnere samt personer med nære relationer til indberetter. Borgere er som udgangspunkt ikke omfattet.
- **Der er foretaget en kortlægning af eksisterende whistleblowerordninger i staten, der viser en begrænset udbredelse:** 3 ud 18 ministerier har etableret indberetningsordninger for hele deres område, mens 10 har etableret ordninger i nogle underliggende myndigheder.
- **Der er stor variation i ministeriernes nuværende ordninger:** Der er stor variation i ordningernes udformning og kompleksitet inden for og på tværs af de enkelte ministerområder, herunder ift. omfattede typer henvendelser, omfattede indberettere samt indberetningskanaler, der spænder over e-mails, breve, formularløsninger og egentlige it-systemer. Kun fire ministerier har deres ordninger understøttet af et specialiseret whistleblowersystem.
- **Der er foretaget en behovsafdækning, der viser stor ensartethed på tværs af staten:** Analysen viser, at de typiske procestrin i indberetningen og behandlingen af whistleblowersager med fordel kan systemunderstøttes. Ministeriernes systembehov er meget ensartede, da ordningerne skal etableres inden for den samme ramme (Justitsministeriets vejledning). Det gælder design, vejledning, indberetning, sagsbehandling, kommunikation og non-funktionelle krav.
- **Der er foretaget en markedskortlægning, der viser flere kvalitative gevinster ved at understøtte behovene med standardløsninger i markedet:** Specialiseret whistleblowersoftware er den mest relevante softwaretype, og der findes flere standardløsninger, som nemt kan tilpasses myndighedernes behov. Løsningerne kan medføre en række kvalitative gevinster, fx brugervenlighed, kontrol og sikkerhed for både indberetter og myndighed.

ØKONOMISTYRELSEN

Ledelsesresumé (2/2)

Hovedkonklusioner

- **Statslige myndigheder er blevet hørt i processen:** For at sikre en anbefaling, der tager højde for erfaringer, ønsker og behov på tværs af staten, er der i arbejdet med analysen indsamlet input og erfaringer fra alle ministerier, herunder vedr. tidsforbrug og udgifter ifm. tidligere lignende systemanskaffelser.
- **Der er foretaget en vurdering af kvalitative og økonomiske fordele ved forskellige løsningsscenarier:** Der er opstillet tre mulige løsningsscenarier for anskaffelse. Disse er vurderet ud fra fire kriterier med relevans for indberetter, myndighed og statens økonomi: 1) tillid og retssikkerhed, 2) kvalitet i sagsbehandlingen, 3) fleksibilitet i lokal tilpasning, 4) lavere omkostninger. Anbefalingen er baseret på en samlet afvejning af scenariernes fordele og ulemper.
- **Det anbefales, at der anskaffes ét fælles it-system til understøttelse af ordningerne:** En fælles løsning, der er forpligtende for et større antal statslige myndigheder, vurderes at være den mest hensigtsmæssige måde at udbrede systemunderstøttelse.
- **Valget af løsningsscenarie har indflydelse på omkostninger ved en fælles løsning:** En indhentning af priseksempler fra leverandører viser, at der tilbydes bedre licens- og anskaffelsespriser desto flere ministerier, der er med på en kontrakt. Dertil kan der være betragtelige tidsbesparelser for myndigheder, hvis anskaffelsen af en løsning gennemføres ét sted.
- **Et fællesstatsligt whistleblowersystem skal anskaffes via et udbud:** Uanset den endelig kontraktværdi, skal et statsligt whistleblowersystem anskaffes i et udbud, grundet klar grænseroverskridende interesse og en kontraktværdi på over 1 mio. kr.
- **Det anbefales, at driften af løsningen varetages af én enhed:** Der er være flere fordele ved at anskaffe systemet via Statens It og drifte det som en applikationsservice. Her vil det skulle afklares, hvad der vil være den mest hensigtsmæssige udbudsproces, og om løsningen skal driftes on-premise.
- **En it-system forventes at kunne udrulles i løbet af [sommeren 2021]:** Hvis det besluttes at anskaffe et fælles it-system, skal der gennemføres et udbud, etableres drift og den valgte løsning udrulles. Den endelige tidsplan herfor skal dog kvalificeres i det videre arbejde.

ØKONOMISTYRELSEN

Kapitel 1:
Baggrund og opdrag

ØKONOMISTYRELSEN

Whistleblowerordninger skal bidrage til åbenhed, gennemsigtighed og tillid i den offentlige sektor

Formål og baggrund for statens whisteblowerordninger

Formålet med whistleblowerordninger i staten er at bidrage til åbenhed, gennemsigtighed og tillid i den offentlige sektor, da whistleblowere kan afdække og afsløre fejl, forsømmelser og andre kritisable forhold. Ordningerne skal sikre en sikker, fortrolig og tryg indgang til at indberette om alvorlige forhold af betydning for myndigheders opgavevaretagelse, uden at whistleblowere skal frygte negative konsekvenser. Samtidigt kan ordningerne forhøje niveauet i myndighedsudøvelsen.

Flere statslige myndigheder har allerede etableret whistleblowerrordninger, og regeringen har besluttet, at der den 1. november 2020 skal være indført whistleblowerordninger på hele statens område. Justitsministeriet har med inddragelse af de øvrige ministerier udarbejdet en fællesstatslig vejledning, som udmøntes i interne vejledninger og ordninger i de enkelte omfattede myndigheder på samtlige ministerområder.

Etableringen af whistleblowerordninger på hele statens området kan ses i sammenhæng med regeringens forståelsespapir vedr. styrkelsen af offentligt ansattes ytringsfrihed. Dertil kommer, at EU's whistleblowerdirektiv skal være implementeret senest i december 2021. Et forslag til whistleblowerlov forventes fremsat i første halvår af 2021. Der vil som følge af implementeringen af direktivet være behov for at tilpasse de statslige whistleblowerordninger. Foranalysen har på den baggrund taget højde for de væsentligste tilpasninger, der umiddelbart må forventes i den anledning.

Baggrund og kontekst

Fælles vejledning for whistleblowerordninger på statens område
Justitsministeriet (2020)

Europaparlamentets og rådets direktiv 2019/1937
Om beskyttelse af personer, der indberetter overtrædelser af EU-retten (2019)

Retfærdig retning for Danmark
Politisk forståelse mellem S, R, SF og Ø (2019)

ØKONOMISTYRELSEN

Etablering af whistleblowerordninger i staten følger to spor

EU-direktivet stiller særskilte krav til ordningerne

Den fælles vejledning stiller krav til etablering af indberetningskanaler. Implementeringen af whistleblowerdirektivet i dansk ret vil dog som nævnt medføre behov for ændringer. Særligt følgende har indflydelse på evt. fællesstatslig systemanskaffelse:

- *Anonymitet*: Direktivet lader det være op til medlemsstaterne om anonym whistleblowing skal være et lovkrav. Det er således indtil videre uvist, om de statslige whistleblowerordninger skal være forpligtet til at modtage, behandle og følge op på anonyme indberetninger[1]. Analysen baserer sig derfor på en antagelse om, at anonym tovejskommunikation skal være muligt, således at det senere kan tilvælges og eventuelt gøres obligatorisk.
- *Omfattede myndigheder*: Den fælles vejledning lægger op til, at der kan etableres én whistleblowerordning for et helt ministerområde, herunder departementer og underliggende myndigheder. Direktivet forpligter *alle* juridiske enheder med 50 eller flere beskæftigede i den offentlige sektor (dvs. inkl. uafhængige, fx selvejende institutioner, råd, nævn mv.) til at oprette interne kanaler. Direktivet giver endvidere ikke mulighed for, at flere juridiske enheder i staten kan deles om en fælles indberetningskanal, f.eks. på et ministerområde. Dermed bør systemunderstøttelse pr. den 17. december 2021 kunne omfatte flere myndigheder end dem, som efter den fælles vejledning skal oprette en whistleblowerordning.

Illustration af overordnet tidsforløb i de to spor

		Dansk spor	EU-spor
2019	Marts	Justitsministeriets ordning etableres	
	Oktober		EU-direktiv 2019/1937 vedtaget
2020	Juli	KU-beslutning om ordninger i staten	
	Oktober	Fællesstatslig vejledning færdig	
	November	Implementering af ordninger i staten	
	November	**Analyse og anbefaling om systemunderstøttelse færdig**	
2021	1. halvår	(Evt.) anskaffelse af systemunderstøttelse	Fremsættelse af forslag til whistleblowerlov
	December	Sidste frist for etablering af indberetningskanaler	Implementeringsfrist for EU-direktiv

[1] Direktivet definerer endvidere ikke, hvad der skal forstås ved anonymitet.

ØKONOMISTYRELSEN

Systemunderstøttelse vedrører den interne indberetningskanal

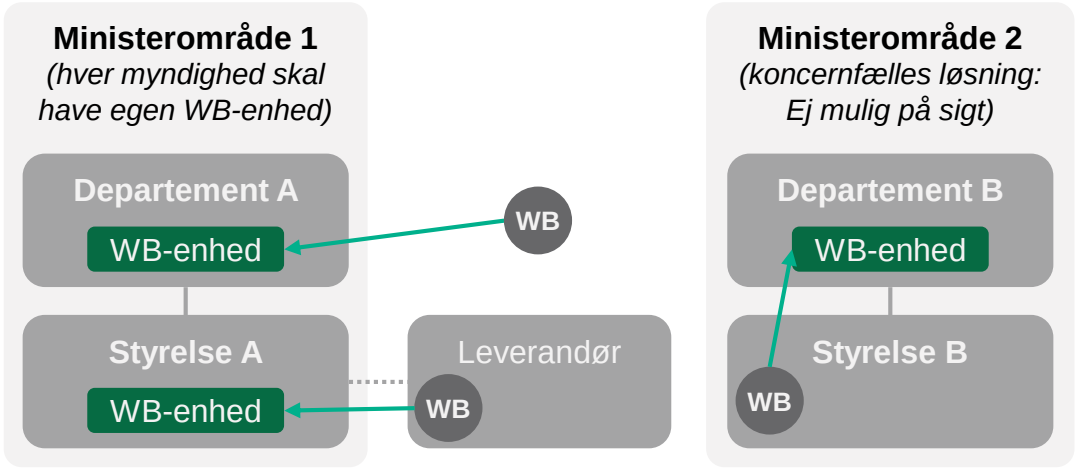
Systemunderstøttelse skal supplere ordningernes struktur

Etablering af whistleblowerordninger indebærer, at de enkelte ministerområder senest pr. 1. november 2020 i overensstemmelse med den fælles vejledning skal etablere nødvendig organisering og procedurer for håndtering af whistleblowersager, herunder udpege en whistleblowerenhed til behandling af indberetninger.

Der skal efter whistleblowerdirektivet etableres én intern indberetningskanal pr. juridisk enhed (dvs. pr. selvstændigt CVR-nr.). Koncernfælles indberetningskanaler vil således ikke være tilstrækkelige, når den kommende whistleblowerlov træder i kraft (senest december 2021). Whistleblowerenhederne skal være afgrænset fra den øvrige organisation. De udpegede enheder har bl.a. ansvaret for at vurdere, om de indkomne indberetninger falder inden for ordningens anvendelsesområde, jf. næste side.

Analysen omhandler ikke den substantielle vurdering og sagsbehandling ifm. indberetninger, men snarere hvordan et system kan understøtte modtagelse af indberetninger og opfølgende kommunikation med indberetteren (whistlebloweren). Systemunderstøttelse skal således fungere som de enkelte myndigheders interne kanaler, hvorigennem sagerne tilgår whistleblowerenheden, jf. figuren til højre. Analysen undersøger, om de statslige ordninger bør systemunderstøttes, og hvordan dette gøres mest hensigtsmæssigt efter de krav, der følger af den fælles vejledning, og på sigt den kommende whistleblowerlov, som implementerer direktivet i dansk ret. Analysen vedrører alene de krav, der har implikationer for systemunderstøttelsen.

It-systemet er kun ét ud af flere elementer i ordningerne



De valgte kanaler skal understøtte sikker indberetning direkte til whistleblowerenhederne, der er etableret inden for ministerområdernes organisationer. Dette uanset hvordan ministeriet har organiseret sin ordning og uanset om whistleblowerenen er ansat i ministeriet, hos en samarbejdspartner eller andetsteds.

Forklaring

- Whistleblower (WB)
- Kanal
- WB-enhed
- Arbejdsplads

ØKONOMISTYRELSEN

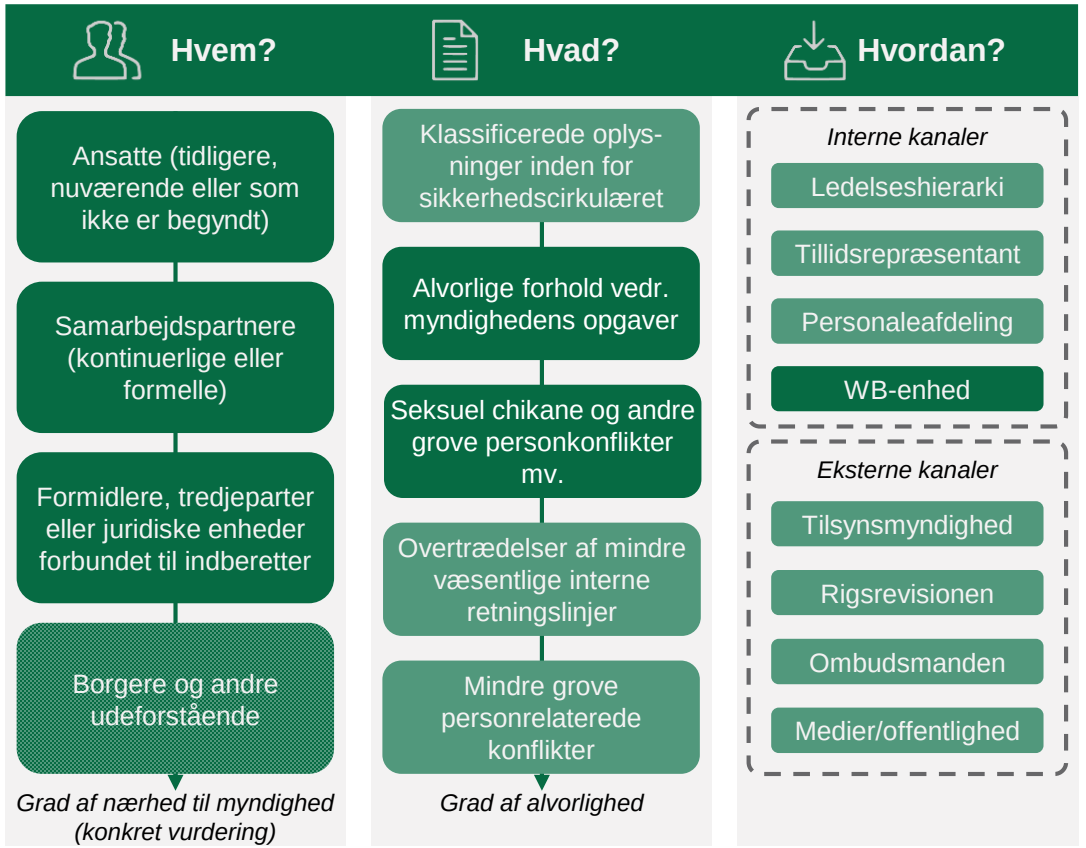
Tre spørgsmål afgrænser, hvornår henvendelser falder inden for de statslige whistleblowerordninger

Den fælles vejledning sætter rammer for ordningerne

Ordningerne er tiltænkt de statslige myndigheders arbejdstagere (både tidligere, nuværende) samt personer, som endnu ikke er begyndt at arbejde hos en omfattet myndighed, men som indberetter oplysninger, der er erhvervet i forbindelse med ansættelsesprocessen eller andre førkontraktuelle forhandlinger. Ordningerne er endvidere tiltænkt samarbejdspartnere, som myndighederne har et mere kontinuerligt og formaliseret samarbejde med, herunder private virksomheder (f.eks. leverandører og underleverandører). Andre, f.eks. borgere, der har en sag hos den pågældende myndighed, vil som udgangspunkt ikke være omfattet.

Ordningerne omfatter kun oplysninger om alvorlige forhold, som er af betydning for myndighedernes opgavevaretagelse. Der forudsættes viden eller begrundet mistanke om, at der er begået sådanne alvorlige forhold. Hvorvidt der er tale om alvorlige forhold beror på en konkret vurdering. Klassificerede oplysninger inden for rammerne af sikkerhedscirkulæret[1], overtrædelser af interne retningslinjer af mindre alvorlig karakter og mindre grove personrelaterede konflikter mv. er således ikke omfattet af ordningerne. Ordningerne skal desuden ses som et supplement til eksisterende muligheder for daglig kommunikation (fx ledelseshierarki, personaleafdeling, tillidsrepræsentanter mv.) og eksterne kanaler (f.eks. tilsynsmyndigheder, Rigsrevisionen eller Folketingets Ombudsmand mv.) Der tilskyndes på den baggrund i vejledningen til, at problemer i første omgang søges løst ved henvendelse til f.eks. nærmeste leder, personale-/HR-afdelingen eller tillidsrepræsentanten.

Afgrænsning af de statslige whistleblowerordninger



ØKONOMISTYRELSEN

[1] Det vil kunne forekomme, at der indberettes klassificeret materiale, hvorfor der skal etableres processer for hvordan disse informationer trækkes ud af systemet og opbevares sikkert.

Analysen danner grundlag for beslutning om systemunderstøttelse af ordningerne

Analysen følger to trin

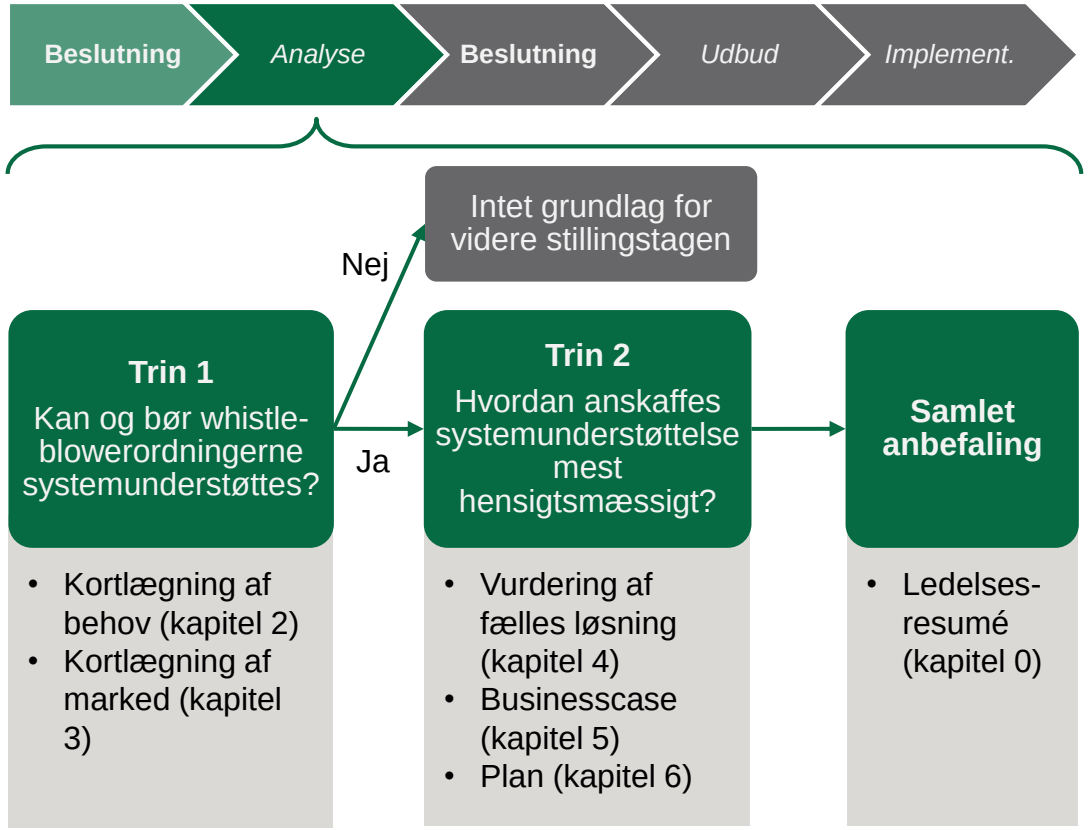
Analysen afdækker to forhold:

1. Om det er hensigtsmæssigt at understøtte de kommende whistleblower-ordninger i staten med et it-system, og
2. Hvordan en it-løsning anskaffes mest hensigtsmæssigt, herunder om det kan gøres som en fælles løsning.

Analysens resultater danner grundlag for beslutning om anskaffelse af evt. fællesstatslig systemunderstøttelse. Analysen har således ikke karakter af en egentlig kravspecifikation af en it-løsning, da en sådan vil blive udarbejdet i forbindelse med udbudsprocessen, såfremt analysens anbefalinger tiltrædes.

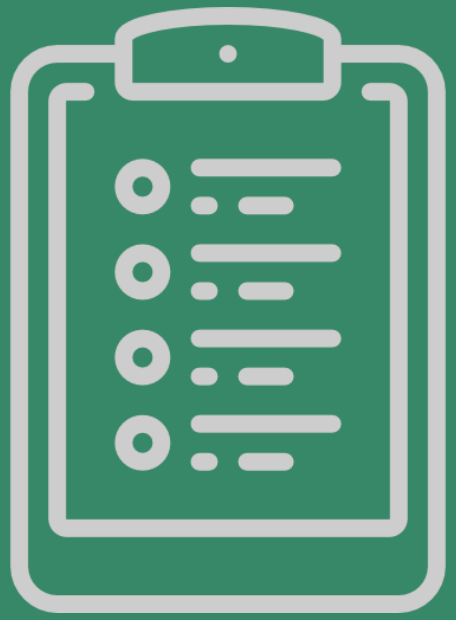
Analysen er gennemført ved to undersøgelsestrin. Første trin er en kort-lægning af regler og rammer for whistleblowerordningernes etablering, eksisterende ordninger i staten, eksisterende løsninger i staten og markedet. Andet trin er en opstilling og vurdering af løsningsscenarier for en fælles løsning ud fra en vurdering af tillid og retssikkerhed, kvalitet i sagsbehandlingen, fleksibilitet ift. lokal tilpasning, samt økonomi. Herefter følger en mere dybdegående vurdering af forventede udgifter ved et fælles whistleblowersystem, samt en plan for, hvordan det kan anskaffes.

Beslutningspunkter ift. eventuel systemanskaffelse



ØKONOMISTYRELSEN

Kapitel 2:
Kortlægning af behov



ØKONOMISTYRELSEN

Behovsafdækningen kortlægger de eksisterende indberetnings-ordninger og behov til systemunderstøttelse på tværs af staten

Behovskortlægningen er baseret på input fra alle ministerier

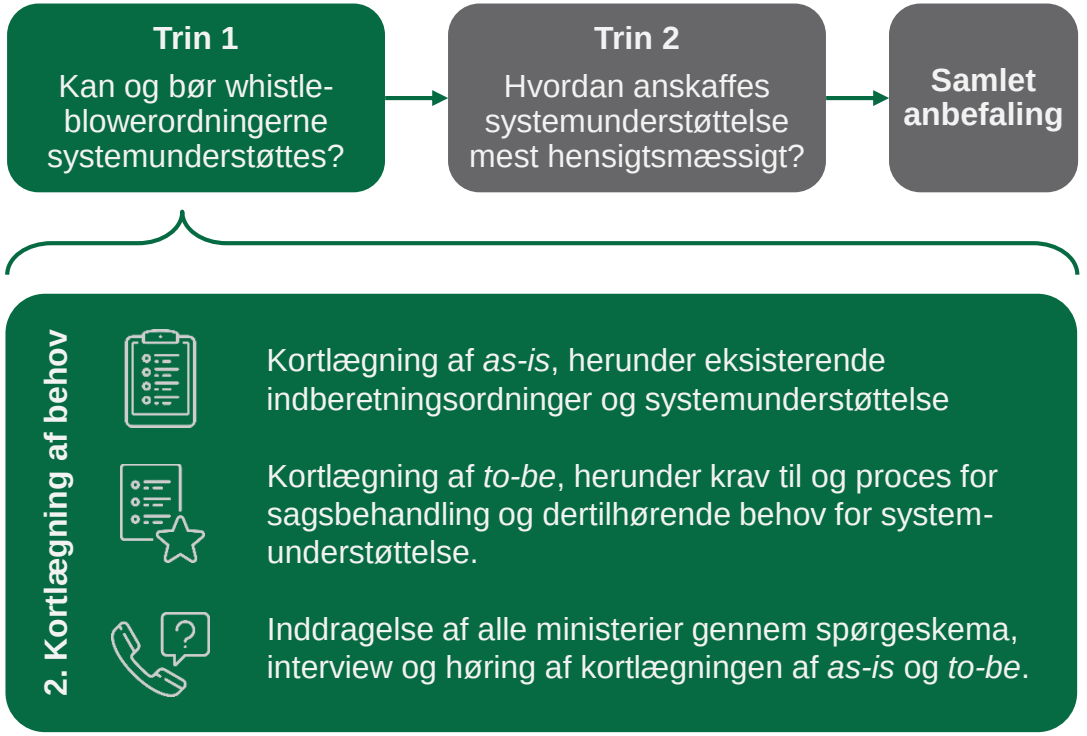
I dette kapitel kortlægges *as-is*, nemlig udbredelsen af eksisterende indberetningsordninger i staten pr. ultimo oktober 2020, herunder anvendelsen af forskellige typer af systemunderstøttelse heraf.

Ordninger og systemunderstøttelse er kortlagt gennem en spørgeskema-undersøgelse af samtlige ministerområder med efterfølgende interview med repræsentanter fra fem ministeriers[1] whistleblowerenheder. Dertil er ordningernes indberetningskanaler, der er offentligt tilgængelige på myndighedernes hjemmesider[2], blevet afprøvet og undersøgt.

Dertil afdækker kapitlet *to-be*, nemlig behov til systemunderstøttelse af de statslige ordninger, der følger af den fællesstatslige vejledning, samt EU's whistleblowerdirektiv.

Retskilderne er blevet operationaliseret i en række procestrin i sagsbehandlingen af indberetninger, der hver medfører en række behov til systemunderstøttelse. Undervejs er behovene sammenlignet på tværs af ministerier. Efterfølgende er de identificerede behov blevet kvalificeret i en høring, hvor alle ministerier har haft mulighed for at afgive bemærkninger til den samlede afdækning.

Metodisk fremgangsmåde i kapitel 2



[1] Interview blev gennemført med ministerier med erfaring med drift af indberetningsordninger, herunder Justitsministeriet, Transport- og Boligministeriet, Skatteministeriet, Udenrigsministeriet og Forsvarsministeriet. Dertil er der talt mere uformelt med øvrige ministerier.
[2] Sagsbehandlersiden af de pågældende løsninger er dermed ikke blevet demonstreret af hensyn til sagernes fortrolighed, men er afdækket ifm. omtalte interviews.

ØKONOMISTYRELSEN

Tre ministerier har etableret indberetningsordninger for hele ministerområdet

Indberetningsordningernes udbredelse i staten er begrænset

Den samlede udbredelse af ordninger i staten er baseret på tre parametre:

1. *Omfattede myndigheder:* Hvilke myndigheder, som departementer har instruktionsbeføjelse over, har etableret ordninger?
2. *Typer af oplysninger:* Hvilke type oplysninger er omfattet? Fx gående fra det smalle, der omfatter oplysninger om strafbare/ulovlige forhold kontra det brede, der også omfatter grove personrelaterede konflikter mv.
3. *Personkreds:* Hvem kan indberette? Fx ansatte (tidligere, nuværende og kommende) til samarbejdspartnere, jf. kapitel 1.

Fx var den samlede udbredelse i KEFM begrænset, da kun én myndighed havde en ordning, selvom de omfattede oplysninger er bredt defineret.

Udbredelse af ordninger i staten (pr. oktober 2020)

	Myndigheder	Oplys.	Personkreds	Udbr.
BUVM	Styrelsen for Uddannelse og Kvalitet	Smalt	Ansatte, forældre	◔
EM[1]	Finanstilsynet, Erhvervs-styrelsen, Konkurrence- og Forbrugerstyrelsen	Mellem	Ansatte, samarbejdsp.	◑
FMN	Alle	Bredt	Alle	●
JM	Departementet, Rigspolitiet, PET, Kriminalforsorgen, Anklagemyndigheden	Bredt	Ansatte, samarbejdsp.	◕
KEFM	Energinet	Bredt	Ansatte, samarbejdsp.	◔
MFVM	Alle	Mellem	Alle	◑
SKM	Skatteforvaltningen, Spillemyndigheden	Smalt	Alle	◔
TRM	Alle	Bredt	Alle	●
UFM[2]	(Innovationsfonden)	Bredt	-	○
UM	Alle	Bredt	Ansatte, samarbejdsp.	●
Resten[3]	-	-	-	○

○ Ingen ordninger ◔ Begrænset udbredelse ◑ Delvis udbredelse ◕ Næsten fuld udbredelse ● Fuld udbredelse

[1] Konkurrence- og Forbrugerstyrelsens ordning skal anses som en kommunikationsordning.
[2] UFM og KERFM har ikke instruktionsbeføjelse overfor hhv. Innovationsfonden og Energinet
[3] BM, FM, KM, KUM, SIM, SUM, STM, UIM har ikke etableret indberetningsordninger (der findes ordninger for socialtilsyn i kommuner, men dette er uden for scope).

Seks ministerier har deres ordninger understøttet af egentlige it-systemer

Der er stor variation i ministeriernes indberetningskanaler

10 ud af de 18 ministerområder har pr. ultimo oktober etableret en eller flere indberetningsordninger. Der ses dog stor variation i ordningernes kompleksitet på tværs af og inden for det enkelte ministerområde, herunder ift. selve kanalerne, *jf. tabellen*. Variationen dækker lige fra Forsvarsministeriet, der havde sin koncernfælles ordning understøttet via e-mail til Erhvervsministeriet, der havde flere parallelle ordninger med forskellige kanaler.

Afhængigt af opgørelsesmetoden for ordningerne, anvendes der i mindst 5 tilfælde designerede e-mailadresser. Hertil kommer 10 ordninger, der anvender en webbaseret spørgeformular. Endelig er 6 af ordningerne understøttet af et egentlig it-system (fx Got Ethics, GlobaLeaks og NemID).

For flere af ordningerne foreligger muligheden for også at indberette pr. telefon og fysisk post (samt e-mail i tilfælde, hvor indberetning sker via formular eller system). Dertil kan indberetter anmode om et fysisk møde. Disse indberetningsmetoder understøtter dog ikke i alle tilfælde anonymitet.

It-understøttelse af ordningerne (pr. oktober 2020)

Myndigheder		Eksempler på ordninger	E-mail	Formular	System
BUVM	STUK	Frie grundskoler, frie gymnasier		1	
EM[1]	FT	Finanstilsynets, markedsmisbrug	1	1	
	ERST	Revisorer, lønkompensation mv.		3	
	KFST	Brud på konkurrenceloven			**1**
FMN	Alle	Forsvarsministeriets WB-ordning	1		
JM[2]	Flere	Fælles ordning			**1**
KEFM	EN	Energinets ordning			**1**
MFVM	MST	Kemikalier, offshoreanlæg mv.	1	2	
	LBST	Ulovligt brug af EU-tilskud	1		
	FST	Skadedyr, sygdom, dyreværn		1	
	NST	Strandbeskyttelse, klitfredning		1	
	FST	Ulovligt fiskeri		1	
SKM[3]	SPM	Brud på hvidvaskloven		1	
	SKST	Skattesnyd, sort arbejde mv.			**1**
TRM	Alle	Hver sin ordning (ét system)			**1**
UFM	IF	Innovationsfondens ordning			**1**
UM	Alle	Controller, Danida Anti-Corruption	1	1	
Sum			**5**	**12**	**6**

[1] Konkurrence- og Forbrugerstyrelsens ordning er ikke en egentlig whistleblowerordning.
[2] Se forrige slide for omfattede myndigheder.
[3] SKM's har i tilkøb til de to ordninger en 'Early Warning'-procedure, der følger almindelige referenceveje fremfor at være en egentlig formaliseret indberetningskanal, samt en Borger- og retsikkerhedschef, der skal anskues som et kontaktpunkt fremfor en egentlig ordning.

De mulige digitale indberetningskanaler fordeler sig på fire løsnings-typer med hver sin funktionalitet

Valg af løsningstype afhænger af ønsket funktionalitet

Digitale indberetningskanaler kan opdeles i fire overordnede typer:

- *Ingen digital løsning*: Henvendelser modtages gennem eksisterende kanaler (fx myndighedens e-mail) uden yderligere vejledning.
- *E-mail:* Henvendelser sendes til en designeret e-mail. Der vejledes om ordningen på separat hjemmeside. Ønskes anonymitet, påhviler det indberetter at udvise understøttende adfærd (bruge en anonym mailkonto[1], ikke angive kontaktinfo eller vedhæfte filer, hvori ens identitet afsløres).
- *Formular*: En spørgeformular på fx myndighedens hjemmeside udfyldes, og indberetning sendes evt. krypteret til dennes postkasse. Tovejskommunikation kan kun ske, hvis indberetter angiver kontaktinfo. Derved sikres anonymitet kun i det omfang, som er tilfældet for e-mails.
- *Specialiseret system:* Indberetter opretter sig med login, kan tilgå sin sag og have tovejskommunikation med myndigheden. Anonymitet, høj grad af datasikkerhed og sagsbehandling understøttes.

Analysen forudsætter, at en løsning skal muliggøre anonym tovejskommunikation, uanset at det evt. senere fravælges. Et system synes at være den eneste løsningstype, der klart understøtter dette, mens e-mail i flere tilfælde ikke vil være tilstrækkeligt[2], og formularer kan være en midlertidig løsning.

[1] E-mailkonti er ikke mere anonyme end, at man kan kontakte udbyderen, der logger aktiviteter.
[2] Datatilsynet stiller dertil krav om, at offentlige myndigheder skal sikre, at e-mails skal krypteres, hvis de indeholder følsomme eller fortrolige personoplysninger. Det kan ikke altid garanteres.
[3] Mundtlighed kun muligt hvis løsningen understøtter lydfiler eller udvekslingen af talebeskeder.
[4] Graden af datasikkerhed og anonymitet afhænger af den konkrete løsning

Funktionalitet i løsningstyperne

Funktionalitet	Ingen	E-mail	Formular	System
Offentlig tilgængelig	✓	✓	✓	✓
Vejledning om ordning		✓	✓	✓
Skriftlig indberetning	✓	✓	✓	✓
Mundtlig indberetning[3]	(✓)	(✓)	(✓)	(✓)
Vedhæftning af filer	✓	✓	✓	✓
Spørgeformular		(✓)	✓	✓
Datasikkerhed[4]		(✓)	(✓)	(✓)
Mulighed for anonymitet[4]		(✓)	(✓)	✓
Tovejskommunikation		(✓)	(✓)	✓
Øvrig sagsunderstøttelse				✓

Kombinationen af anonymitet og tovejskommunikation skal som minimum være muligt i en evt. fælles løsning, men skal kunne fravælges. Dermed er et specialiseret **system**, den mest relevante løsningstype.

ØKONOMISTYRELSEN

Sagstrinene i whistleblowerprocessen kan med fordel understøttes af et system, og ministeriernes behov er meget ensartede

0. Vejledning og design

● *Fuldt ensartede behov*

Myndigheden *skal* kunne vejlede om proces, mulige udfald, rettigheder, adfærd der understøtter anonymitet, anvendelse mv.

Myndigheden *skal* kunne opsætte løsningen, så den afspejler ordningens organisering, og spørgeramme, så info til sagsvurdering sikres.

1. Indberetning

● *Fuldt ensartede behov*

Indberetter *skal* kunne tilgå løsningen, logge ind, og oprette og indsende en indberetning med vedhæftning af relevant dokumentation.

2. Sagsbehandling

● *Fuldt ensartede behov*

Myndigheden *skal* kunne tilgå og behandle indkomne sager i overensstemmelse med gældende retningslinjer.

Myndigheden *skal* kunne tilgå et overblik over sagsmassen.

3. Kommunikation

● *Fuldt ensartede behov*

Myndigheden og **indberetter** *skal* kunne have en afklarende dialog.

Myndigheden *skal* kunne oplyse om sagsstatus, afgørelse og vejlede om videre proces.

Indberetter *skal* kunne oplyse, hvis sag medfører repressalier.

4. Non-funktionelle krav

◔ *Meget ensartede behov*

Løsningen *skal* sikre størst mulig tillid til og fortrolighed ved ordningerne.

Løsningen *skal* leve op til alle relevante lovkrav vedr. data- og informationssikkerhed samt beskyttelse af personhenførbare oplysninger.

Løsning *skal* understøtte sprogversionering.

Behovsafdækninger viser, at der er stor ensartethed i behovene på tværs af staten, da ordningerne skal etableres inden for den samme ramme, jf. Justitsministeriets fælles vejledning og EU's whistleblowerdirektiv. Overordnet set peger de afdækkede behov på et specialiseret it-system.

Figuren viser de typiske procestrin for indberetning og behandling. Ikke alle henvendelser fører til behandlingen af egentlige sager. Dog vil indberetter i alle tilfælde skulle orienteres herom. Implikationerne af de enkelte trin for behov og krav til systemunderstøttelse uddybes på de efterfølgende sider. Behovsafdækningen skal uddybes i en større detaljeringsgrad ifm. udarbejdelsen af en kravspecifikation i et eventuelt udbud.

ØKONOMISTYRELSEN

Overordnet behovsafdækning: Trin 0. Vejledning og design

0. Vejledning og design | 1. Indberetning | 2. Sagsbehandling | 3. Kommunikation | 4. Non-funktionelle krav

De enkelte ministerområder skal som følge af direktivet vejlede om deres ordninger og procedurer[1], herunder bl.a. hvem der kan indberette; hvilke typer oplysninger, der er omfattet; hvordan der indberettes; hvordan indberetningerne behandles; hvilke rettigheder personerne (hhv. indberetter og personerne, som oplysningerne vedrør) har (fx ift. databeskyttelse) mv. Myndigheden skal kunne vejlede herom ved løsningens indgang, herunder hvordan den understøtter ordningen i praksis samt hvordan den understøtter hhv. indberetters adfærd, anonymitet og sikkerhed.

Indberetninger skal indgives til den myndighed, som oplysningerne vedrører, dvs. den udpegede enhed, som skal modtage og behandle indberetningerne. Det kan være en fordel, at indberetter i løsningen kan angive, hvilken myndighed, indberetningen vedrører (se mere jf. trin 2).

Whistleblowerenheder skal behandle indkomne indberetninger og sørge for, at de er tilstrækkeligt oplyst til at vurdere, om der er grundlag for realitetsbehandling, og evt. nærmere undersøgelse. Myndighederne skal derfor kunne definere en spørgeramme for at sikre de fornødne oplysninger til vurdering af sager i relation til eget ressortområde. Løsningen bør derfor understøtte, at spørgerammerne kan justeres efter den enkelte myndigheds informationsbehov, der kan ændres over tid. Indberetter skal møde spørgerammen, når vedkommende opretter en indberetning i løsningen.

	Beskrivelse af overordnede behov
Vejledning	• Det *skal* ved løsningens indgang være muligt at formidle ministerområdets vejledning om ordningens anvendelsesområde, proces for sagsbehandling, hensigtsmæssig adfærd, rettigheder, anonymitet, data- og generel sikkerhed mv. samt løsningens understøttelse heraf. • Vejledningens indhold *skal* kunne tilpasses uden involvering af en ekstern udvikler.
Organisering og opdeling	• Det *skal* være muligt at opdele løsningen i enheder, der afspejler whistleblowerordningerne, sådan at hver enhed har sin afgrænsede del af løsningen, hvorfra det ikke er muligt at tilgå data i eller påvirke øvrige myndigheders dele af løsningen. • Løsningen *skal* kunne tilpasses strukturelle ændringer i ministerområdernes ordninger eller ressortomlægninger (fx ift. brugere, sager mv.). • Det *kan* være en fordel, at dette kan ske uden involveringen af en udvikler.
Spørgeramme	• Myndighederne *skal* (uden indblanding af en udvikler) kunne opsætte og justere i en spørgeramme, som indberetter kan udfylde med information og materiale, der er nødvendig for sagsbehandlingen.

[1] Dette følger af såvel vejledningen samt direktivet, se fx artikel 7, stk. 3, artikel 9, stk. 1. m.fl.
[2] Myndighederne skal opfylde den databeskyttelsesretlige oplysningspligt overfor indberetter på det tidspunkt, hvor personoplysningerne indsamles fra indberetter.

Overordnet behovsafdækning: Trin 1. Indberetning

0. Vejledning og design | **1. Indberetning** | 2. Sagsbehandling | 3. Kommunikation | 4. Non-funktionelle krav

Da ordningen kan anvendes af ansatte, samarbejdspartnere og i visse tilfælde borgere, vil det ikke være hensigtsmæssigt at validere indberetter på forhånd. Således skal løsningen kunne tilgås via en offentligt tilgængelig platform.

Da behandlingen af henvendelser som oftest nødvendiggør gentagende interaktion mellem myndighed og indberetter, skal løsningen understøtte, at indberetter kan tilgå sagen flere gange og efter behov.

Efter at indberetter har oprettet sig som bruger i løsningen, skal denne tilgå og udfylde den myndighedsspecifikke spørgeramme. Således opretter indberetter selv sin sag i løsningen, når denne godkender sin udfyldning af spørgerammen, inden indtastet information tilgår whistleblowerenheden.

Løsningen skal understøtte, at en indberetter kan begrunde sin indberetning skriftligt i fritekst samt evt. dokumentere den, bl.a. ved vedhæftning af relevante dokumenter, film, fotos og lignende filer.

Det ovenforstående skal kunne foregå så indberetter bevarer sin anonymitet, hvis den pågældende myndighed i øvrigt giver mulighed herfor.

	Beskrivelse af overordnede behov
Tilgængelighed	• Indgang til bruger- og sagsoprettelse *skal* være offentligt og nemt tilgængeligt, fx via myndighedernes hjemmesider • Løsningen *skal* leve op til lov om webtilgængelighed
Brugeroprettelse og log-in	• Indberetter *skal* kunne oprette sig med log-in i løsningen • Log-in og kodeord *skal* sikres efter fornødne foranstaltninger, fx sessionstimeout, tvungen periodevis ændring af password, udelukning ved gentaget fejlet log-in mv.
Indberetninger	• Indberetter *skal* kunne foretage en anonym indberetning • Indberetter *skal* kunne angive relevante kontaktinformationer, hvis anonymitet ikke ønskes • Indberetter *skal* kunne uploade/vedhæfte filer i indberetning (filer virusscannes)
Anonymitet	• Indberetters generelle anonymitet *skal* sikres, hvis myndigheden giver mulighed herfor, jf. også trin 3.

ØKONOMISTYRELSEN

Overordnet behovsafdækning: Trin 2. Sagsbehandling

For hvert ministerområdes whistleblowerordninger er der etableret enheder, som skal modtage og behandle indberetningerne. Løsningen skal derfor understøtte, at indberetninger tilgår sagsbehandlere i den relevante enhed. Det bør være muligt, at en indberetning kan overdrages til rette enhed i tilfælde af, at indberetningen indledningsvist er tilgået en forkerte enhed.

Det vil være en fordel, at løsningen gør det muligt for sagsbehandler at markere sagers status, herunder om disse falder inden for ordningens anvendelsesområde, samt sagens udfald på et generelt niveau.

Dertil vil det være en fordel, hvis administratorer i de enkelte myndigheder kan opsætte workflows i løsningen, som understøtter de typiske processer i sagsbehandlingen, fx overholdelse af godkendelser og frist mv.

Ifm. ledelsesrapportering el.lign. vil det være relevant for myndigheder at kunne tilgå et overblik over sagsmassen, herunder fordeling på status samt udvikling over tid. Løsningen bør understøtte et konfigurerbart overblik, der imødegår dette, dog uden indblik i selve sagernes indhold, herunder oplysninger om whistleblowerens identitet mv.

Løsningen bør evt. understøtte, at der kan dannes en rapport (el.lign.) om sagen, som kan overføres til myndighedens eget sagsbehandlingssystem mhp. videre undersøgelse efter myndighedens retningslinjer. Løsningen skal dog ikke integreres til lokale it-systemer.

	Beskrivelse af overordnede behov
For-deling af sager	• Indberetter *skal* kunne angive hvilken myndighed henvendelsen vedrører. • Henvendelser *skal* kunne overdrages fuldstændigt (dvs. slettes fra afgiveres indgang til systemet) til rette enhed[1].
Sags-under-støttelse	• Det *kan* være en fordel, at kunne at markere sagsstatus • Det *kan* være en fordel, at løsningen baggrund af tids-punkt for modtagelse af indberetninger, understøtte sagsbehandler i opfølgning på foreskrevne tidsfrister for kvittering, orientering og lignende til indberetter.
Rappor-tering og ledelses-info	• Det *kan* være en fordel, at kunne tilgå et overblik over sagsmassen, dvs. antal sager fordelt på behandlingstid, typer og status, fx ugyldige, igangværende, afsluttede • Det *kan* være en fordel, at kunne konfigurere og udvikle rapporter efter behov
Aflevе-ring af sager	• Løsningen *skal* kunne danne en rapport eller et lign. format til sikker overdragelse af sager fra systemet til myndighedens eget sagsbehandlingssystem

[1]Det bør ifm. en kravspecifikation afklares nærmere hvordan sletning i øvrigt håndteres i et system, fx om det kan ske automatisk eller om myndigheden selv skal sørge for at implementere politikker herfor i systemet.

Overordnet behovsafdækning: Trin 3. Kommunikation

Løsningen skal understøtte fortrolig og anonym tovejskommunikation mellem enheden og indberetteren.

Løsningen skal understøtte, at enheden kan orientere indberetter om modtagelse af sagen, behandling af denne, evt. resultater og lignende i overensstemmelse med de forudsatte tidsfrister herfor som beskrevet i den fælles vejledning og EU' whistleblowerdirektiv.

Det kan være hensigtsmæssigt, at indberetter kan modtage notifikationer, når der modtages post i løsningen, i det omfang at indberetters fortsatte fulde anonymitet kan sikres. Alternativt skal der kunne vejledes om, at indberetter selv skal logge på løsningen og følge sin sag.

Hvis henvendelserne er utilstrækkeligt oplyst til, at enheden kan vurdere grundlag for realitetsbehandling eller afgørelse af sagen, skal enheden kunne anmode om supplerende information fra indberetter. Hvis henvendelsen falder uden for anvendelsesområdet, skal løsningen understøtte, at sagsbehandler kan vejlede indberetter om sagens videre proces.

Endelig skal indberetter kunne informere myndigheden, hvis denne ifm. med sin indberetning er blevet udsat for repressalier.

	Beskrivelse af overordnede behov
Tovejs-kommu-nikation	• Myndighederne *skal* kunne have en afklarende dialog med indberetter. • Løsningen *skal* udsende mailnotifikationer, når der er nye indlæg på sagerne fra indberetter eller sagsbehandler i løsningen. • Der *skal* kunne sendes mailnotifikationer til en konfigurerbar liste, fx en automatisk kvittering for modtagelse af indberetning til indberetteren hurtigst muligt inden for 7 dage, jf. direktivet.
Ano-nymitet og data-sikker-hed	• Indberetter *skal* sikres anonymitet i kommunikation med myndigheden, hvis indberetteren ønsker det, samt hvis myndigheden i øvrigt stiller muligheden til rådighed. • Al kommunikation over netværk og indberetningernes data *skal* krypteres og sikres efter gældende standarder, så det er sikret imod uvedkommendes adgang under transit.
Repres-salier	• Løsningen *skal* muliggøre, at indberetter kan oplyse, hvis denne oplever repressalier som følge af sin indberetning.

Overordnet behovsafdækning: 4. Non-funktionelle krav

Der skal kunne udpeges én central og et antal lokale systemadministratorer for myndighedernes dele af løsningen. Den centrale administrator skal kunne styre brugeroprettelse og -tildeling til konkrete sagsbehandlere, uden at kunne tilgå indhold i sagerne. Den centrale administrator skal varetage den centrale konfiguration af løsningen, herunder oprette nye, sammenlægge eller opsplitte myndigheder som følge af ressortomlægninger.

Lokale administratorer skal i et vist omfang selv kunne foretage ikke-kritisk konfiguration fx visuel opsætning, justering af workflows mv., medmindre det fx involverer ændringer i rollers adgang i sagsbehandlingen.

Løsningen skal have et omfattende kontrolregime, der muliggør tæt opfølgning på hændelser og handlinger. Således skal løsningen også logge al brugeraktivitet. Løsningen have grundig kontrol med kiggeadgang og sletning af sager (fx indberetninger, der falder uden for anvendelsesområdet), herunder godkendelse, fire-øjne-princip el.lign. Løsningen skal leve op til alle gældende sikkerhedsmæssige regler og love, herunder databeskyttelsesloven og GDPR.

Endelig skal løsningen kunne sprogversioneres efter udvalgte, relevante sprog, så der sikres adgang for ikke-dansktalende whistleblowere.

	Beskrivelse af overordnede behov
Bruger-styring	• Der *skal* være en styring af hvilke sagsbehandlere, der har kigge-, redigerings- og sletteadgang. • Det *skal* være muligt at nedlægge brugere. • Sikker sletning *skal* være muligt, sådan at sagsbehandler kan indstille en anmeldelse til sletning, hvorefter dette godkendes af en anden sagsbehandler. • Administrator *skal* have mulighed for at tilgå overblik over brugere og tildelte rettigheder.
Log-ning	• Der *skal* være logning af administrator- og brugeraktivitet, fx log-in, filoverførsel, tidspunkt for indberetning, hvem der har set en indberetning hvornår, hvem der indstiller til sletning, hvem der foretager det og hvornår, mv. • Loggen *skal* være beskyttet imod ændringer.
Data-sikker-hed	• Løsningen *skal* overholde krav og regler som følger bl.a. af databeskyttelsesretlige regler. • Løsningen *skal* bestå en sikkerhedstest efter større ændringer.
Sprog	• Løsningen *skal* kunne versioneres efter relevante sprog.

[1] Om der bør tillades overførsel til tredjelande skal kortlægges i den risikovurdering (samt i den eventuelle konsekvensanalyse), der evt. skal udarbejdes ifm. et evt. udbud. Her skal det vurderes, om systemet skal omfattes af lokationskravet i databeskyttelseslovens § 3, stk. 9 (den såkaldte krigsregel). Det må dog som minimum forventes at systemet skal opbevares og behandles indenfor EU/EØS grænser.

It-systemunderstøttelse medfører kvalitative gevinster ift. brugervenlighed, retssikkerhed, kvalitet i sagsbehandlingen og kontrol

Et it-system giver fordele for både indberetter og myndighed

Kortlægningen viser, at de identificerede behov *kan* dækkes af løsninger på markedet, og at er der flere fordele ved at understøtte indberetningsordningerne med et it-system fremfor e-mail eller formular.

Der findes nemlig en række gevinster for både indberettere og myndigheder ved et it-system for hvert af de kortlagte trin i sagsprocessen, *jf. tabellen*. Gevinsterne har overvejende en kvalitativ karakter, særligt i form af øget retssikkerhed, fortrolighed og brugervenlighed for indberetter. Dertil kommer administrative fordele for myndigheden (fx understøttelse af fremdrift i sagsbehandlingen), samt et ensartet sundt kontrolmiljø i løsningen fx i form af logning af brugeraktivitet, adgangsbegrænsninger samt overholdelse af krav til data- og informationssikkerhed[1].

Gevinsterne kan kun i et begrænset omfang omsættes økonomisk. Flere af gevinsterne vedrører ikke den direkte behandling af de indkomne sager, men i højere grad, hvordan sager indberettes, og der kan følges op med indberetter. Dertil er den forventede sagsmasse begrænset, mens sagerne varierer meget i indhold og kompleksitet og dermed tidsanvendelse.

Anskaffelse af et it-system kan således anskues som et kvalitetsprojekt, hvor der arbejdes for at opnå høj kvalitet til den mest fordelagtige pris.

Kvalitative gevinster ved understøttelse med et it-system

Sagstrin	Kvalitative gevinster
0. Vejledning og design[2]	**Indberetter:** Gøres bekendt med rettigheder og krav til adfærd mv. ifm. indberetningstidspunktet. **Myndighed**: System kan designes til at afspejle myndighedens ordning, og vejlede om brugen heraf. Spørgerammer forbygger behov for opfølgende dialog med indberetter.
1. Indberetning	**Indberetter:** Kan oprette log-in, indberette og følge op på sager via én brugervenlig platform, der understøtter indberetters anonymitet.
2. Sagsbehandling	**Myndighed:** Får ét samlet overblik over sager, materiale og korrespondence. Kan fordele sager til relevante sagsbehandlere og sikre fremdrift vha. fx mailnotifikationer.
3. Kommunikation	**Indberetter:** Kan svare på spørgsmål, eftersende dokumentation, følge sag, og indberette hvis repressalier. **Myndighed:** Kan stille afklarende spørgsmål til indberetter.
4. Non-funktionelle krav	**Indberetter:** System sikrer tillid til ordningernes sikkerhed og fortrolighed. Sprogversionering sikrer ligebehandling. **Myndighed:** Lovkrav vedr. dokumentation, data- og informationssikkerhed, privacy, personoplysninger mv. kan indbygges. Sundt kontrolmiljø, jf. adgangsbegrænsning, logning, mv. Smidig fordeling sager til korrekte myndigheder.

[1]Overholdelse af disse følger ikke automatisk af valg af et it-system, men beror på en vurdering af den konkrete løsning. Derfor skal der laves en risikovurdering og systemet skal på denne baggrund kravspecificeres, således at det lever op til de nødvendige sikkerhedsstandarder.

[2] Gevinster i dette trin kan dog i et vist omfang også opnås ved e-mail og formularer.

Kapitel 3:
Kortlægning af marked

ØKONOMISTYRELSEN

Markedsafdækningen kortlægger mulighederne i markedet for systemunderstøttelse af de statslige whistleblowerordninger

Mulige systemløsninger er grundigt afdækket

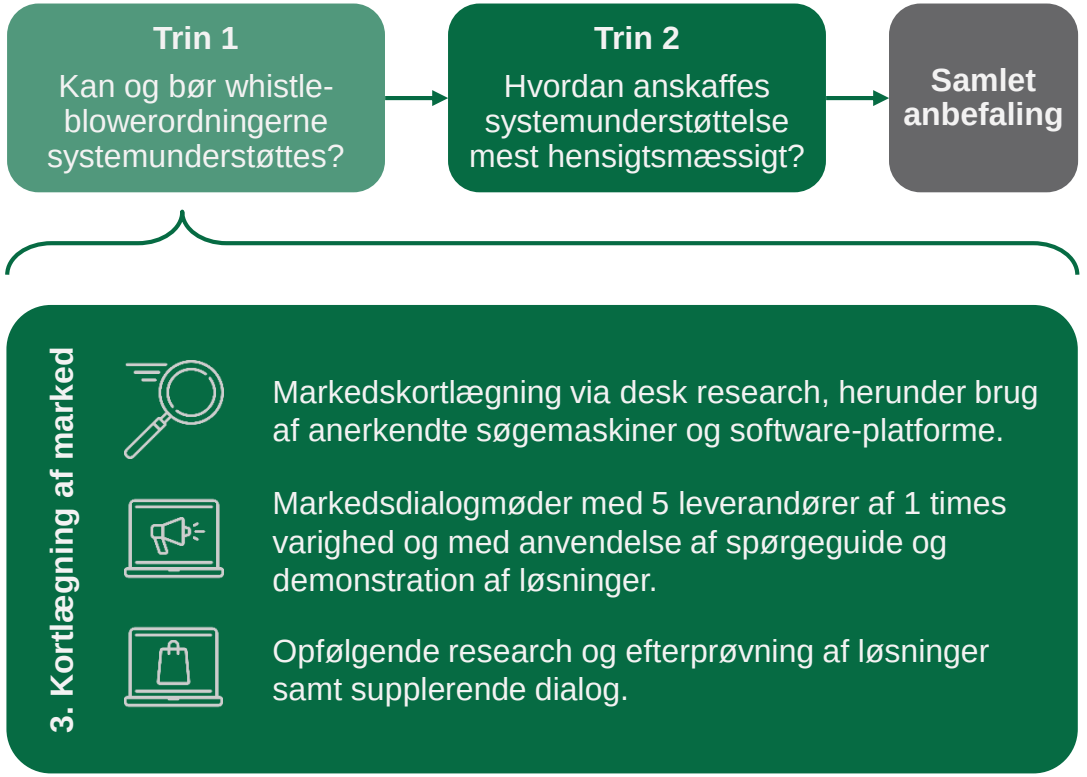
I dette kapitel er mulige løsninger til understøttelse af de identificerede behov i forrige kapitel undersøgt. Det er ske via en grundig desk-research af markedet[1] og dialog med udvalgte leverandører.

Indledningsvist er der foretaget en markedsafdækning baseret på en triangulering af top 10 bedst vurderede løsninger på internationale platforme for peer-to-peer review af software-løsninger[1].

I forlængelse heraf er der udvalgt 5 leverandører til markedsdialogmøder mhp. at opnå mere detaljeret viden om muligheder og begrænsninger ved forskellige løsninger. Under møderne blev der anvendt en interviewguide, der var struktureret efter de behov, der blev identificeret i behovsafdækningen. Dertil blev der spurgt ind til leverandørerne baggrund, herunder brugere og referencer, implementeringsplaner, samt mulige hosting- og driftsmodeller.

Dialogmøderne havde en varighed af 1 time, og blev gennemført via Skype med primært salgschefer og produktejere. På møderne blev løsningernes funktionalitet demonstreret fra både indberetter- og myndighedssiden. Møderne blevet suppleret med opfølgende research og dialog med leverandørerne pr. mail, telefon og Skype. Dertil er der blevet indhentet priseksempler for mulige løsningsscenarier for staten, jf. kapitel 4-5.

Metodisk fremgangsmåde i kapitel 3



[1] Platformene omfatter G2, Capterra, TrustRadius, GetApp, Software Advice og Software Reviews.

ØKONOMISTYRELSEN

Der er gennemført en grundig undersøgelse af markedet, der peger på én relevant type af flere mulige softwareløsninger

Ordningerne kan understøtte af flere softwaretyper

Der er derfor identificeret fire softwaretyper, der kan understøtte de statslige ordninger:

Etik- og compliance: Understøtter træning af ansatte i relevante principper, regler og retningslinjer, fx Kodex VII, GDPR, udbudslove, mv. Typen understøtter således *forebyggelse* af overtrædelser blandt internt ansatte, men egner sig ikke til håndteringen af allerede begåede forhold.

HR-sagsstyring: Omfatter systemer til håndtering af individuelle personalesager for kendte medarbejdere internt i en organisation. Mens typen ikke egner til håndtering af anonyme henvendelser, kan den ses som et supplement til de sager, hvor indberetter ikke ønsker anonymitet.

GRC (Governance, Risk & Compliance): Generelle risikostyringsplatforme til håndtering af og opfølgning på *kendte* risici i organisationen. Mens typen kan have sin relevans til opfølgning på indberettede forhold gennem ordningen, er den mindre relevant ift. opdagelsen af ukendte risici/forhold.

Whistleblowing: Specialiserede systemer til sikker og anonym indberetning i tråd med kortlagte behov og derfor den mest relevante type software. Afdækningen af markedet herfor følger på de næste sider.

Kendetegn og relevans ved de forskellige softwaretyper

Type	Kendetegn	Relevans	Eks.
Whistle-blowing-software	Muliggør at ansatte eller andre anonymt kan indberette overtrædelser til en virksomhed. Understøtter tovejskommunikation via fx hjemmeside, telefon, e-mail, chat, apps, mv.	✓	Se næste side
Etik og compliance-trænings-software	Formidler og understøtter styring af kurser og læringsindhold til ansatte og ledere om regler og interne politikker.	✗	CAMPUS
HR-sags-styrings-software	Understøttelse af behandling af HR-sager og fx spørgsmål, klager, forhandlinger, undersøgelser mv.	✗	Statens HR
GRC-platforme	Kategorisering, vurdering og håndtering af alle typer risici. Støtte til planlægning og gennemførsel af tilsynsopgaver.	✗	Control-Manager

ØKONOMISTYRELSEN

Ud af 16 identificerede løsninger, blev 5 leverandører udvalgt til nærmere undersøgelse og interview

Der synes at være et bred udbud af mulige løsninger

Markedskortlægningen har identificeret 16 løsninger, hvilket indikerer et relativt bredt udbud. Kun en mindre del af de kortlagte løsninger synes dog relevante, idet relevante løsninger indkredses alt efter om løsningen

- er gearet til overholdelse af GDPR (primært europæiske løsninger).
- kan tilgås af andre end registrerede ansatte (kontra offentlig adgang).
- tilbyder relevant funktionalitet (kontra for meget/lidt ift. kortlagte behov).

På baggrund af en screening af løsningerne efter disse hensyn samt et ønske om spredning ift. tilstedeværelse i dansk sammenhæng (både i den offentlige og private sektor), blev der udvalgt 5 leverandører[1] til interview.

Da der er tale om et relativt simpelt system, er det muligt, at it-udviklings-virksomheder også vil kunne tilbyde en løsning i et udbud[2]. Disse kan af gode grunde ikke kortlægges her.

Markedsoversigt for specialiseret whistleblowersoftware

Leverandører	Løsning[3]	Land (etableringsår)	Bruges i DK
DigitalPA	Whistleblowing	Italien (ca. 2000)	
Ethicontrol	Ethicontrol Platform	Estland (2014)	
EQS Group	EQS Integrity Line	Tyskland (2000)	
Freedom of the Press Foundation	SecureDrop	USA (2013)	
Got Ethics	Got Ethics	Danmark (2010)	✓
Hermes Center	GlobaLeaks	Italien (2011)	✓
ICO Solutions	ICO Whistleblowing	Canada (2001)	
Integrity Asia	Canary	Indonesien (2001)	
iTouchVision	WhistleBlower	UK (2009)	
Navex Global	WhistleB	Sverige (2011)	
People Intouch	SpeakUp	Holland (2004)	✓
Riddle Compliance	Whistleblower+Plus	USA (2017)	
Speeki Pte Ltd	Speeki	Singapore (2020)	
Whispli	Whispli	Australien (2016)	
WB Security	IntegrityCounts	Canada (2005)	

Udvalgt til markedsdialog

[1] De fem leverandører, der er udvalgt til markedsdialog, er markeret i tabellen i højre side.
[2] Kortlægningen af eksisterende systemer, viser at dette er sket i mindst et tilfælde før.
[3] Yderligere information om den enkelte løsning kan tilgås via links i tabellen.

ØKONOMISTYRELSEN

Markedskortlægningen viser, at de kortlagte behov kan dækkes af flere leverandører på markedet

Der er flere fordele ved at anvende et whistleblowersystem

Kortlægningen viser, at der findes et bredt udbud af specialiserede systemer, der *kan* understøtte de kortlagte behov ift. etablering af de statslige ordninger. De danske behov synes ikke at adskille sig markant fra lignende kunder, hvilket kan hænge sammen med et europæisk marked i vækst, jf. EU-direktivet. I det omfang der kan sikres en dansk version med høj kvalitet, bør en anskaffelse ikke begrænse sig til løsninger, der allerede findes i det danske marked, da det vil kunne svække konkurrencen. Markedsdialogen viser en udpræget interesse hos leverandørerne, hvilket kan hænge sammen med statens volumen i et potentielt udbud, samt muligheden for at få den danske stat som reference. Dette styrker konkurrencesituationen.

Dertil viser markedskortlægningen, at der bør lægges vægt på løsninger, der opererer og hoster data i EU-lande for at sikre kendskab og efterlevelse af relevante EU-retsakter. Et stort antal af leverandørerne har både private- og offentlige kunder. Det bør overvejes i hvilket omfang, man i et eventuelt udbud bør lægge vægt på leverandører, der har erfaring med særligt offentlige kunder.

Nogle af leverandørerne tilbyder ikke on-premise hosting, men hoster data i Cloud, hvilket stiller særlige krav til datasikkerhed. Det bør derfor overvejes, om man i et udbud bør kravstille on-premise hosting, jf. også kapitel 6.

Konklusioner til trin 1

Trin 1
Kan og bør whistleblowerordningerne systemunderstøttes?

→

Trin 2
Hvordan anskaffes systemunderstøttelse mest hensigtsmæssigt?

→

Samlet anbefaling

Konklusion på Trin 1 (kortlægning af behov og marked)

1) Der er en høj grad af ensartede behov i staten ift. systemunderstøttelse af de statslige whistleblowerordninger
2) Der er flere kvalitative gevinster ved at understøtte ordningerne med et specialiseret it-system fremfor e-mail eller en formular.
3) Der synes være et modent og voksende marked for specialiserede whistleblowersystemer.
4) Løsningerne i markedet er standardløsninger, der i høj grad synes at kunne tilpasses til at understøtte de kortlagte behov

ØKONOMISTYRELSEN

Begrebsoversigt

Definition af oftest anvendte begreber

- **Anskaffelse**: Indkøb og implementering af fx et system, herunder planlægning, udbud og idriftsættelse.
- **Implementering:** Opsætning, idriftsættelse og udrulning af et system.
- **Indberetning:** En henvendelse om et forhold som sendes til en myndighed, der skal vurdere, om det giver anledning til nærmere undersøgelse.
- **Indberetningskanal:** Et medie til kommunikation af indberetninger, fx via telefon, brev, e-mail, system eller lignende.
- **Kontraktform:** Aftale mellem ordre- og tilbudsgiver, der specificerer omfanget og indholdet af varen samt løbetid.
- **Non-funktionelt krav:** Krav til systemets arkitektur, fremfor til funktionalitet og handlemuligheder i systemets design.
- **On-premise:** Software der er installeret og kører på servere inden for en organisations beliggenhed fremfor alsidiges, fx i datacenter eller cloud.
- **Whistleblower:** En person, der oplyser om kritisable forhold fx til statslige myndigheder. Bruges synonymt med indberetter.
- **Whistleblowerløsning:** En løsning, der understøtte indberetning. Bruges synonymt med kanal.
- **Whistleblowerordning:** Organisering, procedurer og reglerne for hvordan en whistleblower kan indberette til fx en myndighed. Bruges synonymt med indberetningsordning.
- **Whistleblowersystem:** Et it-system specifikt udviklet til indberetning og håndtering af whistleblowersager.

ØKONOMISTYRELSEN