Bilag 1 – Kundens kravspesifikasjon

Versjonshåndtering

Versjon	Dato	Initiert av	Endringsårsak
1.0	25.09.2017	Kunden	Til utlysing

Innhold

1. Innledning

1.1 Bakgrunn for anskaffelsen

I 2010 anskaffet Difi Microsoft Dynamics CRM. Tilpasningene ble utlyst eksternt og et konsulentselskap vant anbudet. Anskaffelsen av CRM omfattet installasjon og tilpassing av programvaren, og dekket ikke vedlikehold av systemet.

I 2013 anskaffet vi et synkroniseringsverktøy, Scribe som blir benyttet som bindeledd mellom CRM-systemet og Samarbeidsportalen (se Bilag 1 vedlegg 1) for at datane skal kunne flyte imellom komponentene. Samarbeidsportalen er informasjons- og varslingskanalen ut mot Difis kunder.

Bakgrunnen for anskaffelsen er nå at vi ønsker å gå over til skybasert løsning, og å profesjonalisere forvaltningen rundt fellesløsningene til Difi ved å tilby våre kunder og leverandører større grad av selvbetjening og bedre innsikt i bruken av fellesløsningene.

1.2 Omfanget av anskaffelsen

Anskaffelsen skal dekke Difis behov for et CRM- og sakssystem for å forvalte Difis fellesløsninger. Se Bilag 1 vedlegg 2 for utfyllende beskrivelse om hvordan Leverandørens løsning skal henge sammen med den eksterne informasjons- og varslingsportalen Samarbeidsportalen, samt administrasjonsgrensesnittene til ID-porten og KRR (og andre Difis fellesløsninger).

2. Veiledning til kravtabellen

I de følgende kapitler fremgår hvilke krav som Kunden setter til Leverandøren og den tjenesten som skal leveres. Leverandøren skal besvare kravene i sitt løsningsforslag i bilag 2.

Kravene er strukturert etter tre typer tjenester; plattformtjenester, enkelttjenester og støttetjenester. For hvert krav er det angitt til hvilken kategori kravet tilhører, samt om kravet skal utdypes.

Kravene er delt inn i følgende kategorier:

A: Dette er minstekrav som Leverandøren i utgangspunktet skal oppfylle. Dersom Leverandøren svarer nei på ett eller flere A krav vil Kunden vurdere hvilken betydning ikke-oppfyllelsen har for driftsløsningen. A kravene evalueres ikke i forhold til tildelingskriteriene. Ikke-oppfyllelse av ett eller flere A-krav som sammen anses som vesentlig vil medføre avvisning. Ikke-oppfyllelse av A-krav som ikke anses som vesentlig vil medføre et skjønnsmessig trekk i forbindelse med evalueringen av tilbudene vurdert opp mot tildelingskriteriene.

B: Dette er krav med medium viktighet for oppdragsgiver, beskrevet i kravsmatrisene. Leverandørens grad av oppfyllelse av disse kravene vil inngå i evaluering av tilbudene.

For hvert krav er det angitt om Leverandøren skal utdype sitt svar på kravet (se kolonne merket «U»):

J (JA): Leverandørens løsningsforslag må beskrives i bilag 2.

N (Nei): Leverandøren skal ikke beskrive sitt løsningsforslag

Instruksjoner om Leverandørens besvarelse av kravene er beskrevet i bilag 2 vedlegg 1.

3. Tekniske krav

3.1 Skyteneste

Nr.	Krav	A B	U (J/N)
3.1.1	Løsningen skal leveres som en skyteneste av type «Programvare som tjeneste» (software as a service – SaaS). Det vil si at Kunden skal benytte Leverandørens applikasjon(er) på en nettsky-infrastruktur.	A	N
3.1.2	Alle forbindelser mellom server og bruker/klient skal ha sikre forbindelser. Eksempelvis https. Forbindelsene skal tilfredsstille spesifikasjoner i henhold til følgende anbefalinger: https://www.nsm.stat.no/blogg/veiledning-i-https/ https://www.nsm.stat.no/blogg/veiledning-i-tls/ https://www.nsm.stat.no/blogg/oppdaterte-kryptokrav/	A	N
3.1.3	Løsningen må støtte integrering med ADFS for Single sign-on.	A	N
3.1.4	Løsningen må støtte integrering med e-post i Office 365.	A	N
3.1 5	Løsningen skal ha et produksjonslikt testmiljø.	A	N
3.1.6	Kundens data som lagres i Leverandørens løsning skal kunne eksporteres på strukturert måte for å muliggjøre dataportabilitet.	A	N
3.1.7	Utvalgte data fra gammel løsning skal migreres over til ny løsning.	A	N

3.2 Mobile enheter

Nr.	Krav	A B	U (J/ N)
	Løsningen må støtte siste versjon av alle moderne nettlesere for PC som Internet Explorer, Microsoft Edge, Firefox, Safari og Chrome. Det skal ikke være behov for nettleserutvidelser (plug-ins).	B	N
3.2.2	All funksjonalitet beskrevet i kapittel 6, 7 og 8 skal være tilgjengelig på mobile enheter (mobiltelefon og nettbrett) og på klienter utenfor virksomhetens eget datanettverk.	B	J

3.3 Tilgjengelighet

Nr.	Krav	A B	U (J/ N)
	Responstiden skal være i henhold til Billag 4 – Tjenestenivå.	A	N
3.3.2	Løsningen skal ha en garantert oppetid i henhold til Billag 4 – Tjenestenivå.	A	N
3.3.3	Jobben som synkroniserer data mellom Leverandørens løsning og komponentene Samarbeidsportalen og Difis fellesløsninger skal ha en garantert oppetid på 99, 5 % pr. måned i henhold til Billag 4 – Tjenestenivå.	A	N
3.3.4	Synkronisering av data inn og ut av løsningen skal skje på en stabil måte som motvirker datainkonsistens.	B	J

4. Lisenser

Nr.	Krav	A B	U (J/N)
	Det skal tilbys opptil 50 brukerlisenser til løsningen, deriblant tre systemadministratorer.	A	N
4.2	Det skal være mulig for Kunden å kjøpe flere lisenser utover de første 50, både brukerlisenser og systemadministratorer.	A	N
4.3	Det skal gjennomføres brukeropplæring for 50 brukere på Kundens lokasjon	A	N

	(Leikanger) fordelt på to ulike tidspunkt med tilhørende opplæringsmateriell.		
4.4	Det skal gjennomføres utvidet opplæring (eget opplæringsprogram) for tre systemadministratorer. Dette kan gjennomføres på lokasjonen til Leverandøren i Norge med tilhørende opplæringsmateriell.	A	N
4.5	Alle brukerlisenser skal ha full tilgang til å bruke funksjonalitet beskrevet i kapittel 6, 7, 8 og 9.	A	N

5. Informasjonssikkerhet

5.1 Overordnede krav til informasjonssikkerhet

Nr.	Krav	A B	U (J/ N)
	Leverandøren skal ha funksjoner som ivaretar konfidensialitet, integritet, og tilgjengelighet i systemene. Dokumentasjonen skal være tilgjengelig for Kunden på forespørsel.	A	N
	Leverandøren skal ha styringssystem for informasjonssikkerhet som skal dekke alle organisasjonsenheter som inngår i leveransen. Sertifisering etter ISO/IEC 27001 eller tilsvarende som knytter seg til at tjenesteleveransen er tilstrekkelig for å dekke kravet.	A	J
	Løsningen skal være motstandsdyktig mot angrep på konfidensialitet, integritet og tilgjengelighet.	A	J
5.1.4	Leverandøren skal beskrive eventuelle avvik mellom standard for styring av informasjonssikkerhet og eget styringssystem.	A	J
5.1.5	Oppdatert beskrivelse av kvalitetssikrings- og styringssystemet skal til enhver tid være tilgjengelig for Kunden.	A	N
5.1.6	Det skal fremgå av styringssystemet for informasjonssikkerhet hvordan sikkerhets- og prosesskrav i lov og forskrift om behandling av personopplysninger tilfredsstilles.	A	N
5.1.7	Leverandøren skal ha egnede tekniske og organisatoriske sikkerhetstiltak for å kunne håndtere de opplysninger Kunden har beskrevet at løsningen skal behandle. Tiltakene skal garantere et sikkerhetsnivå som står i forhold til risikoen og som følger etablert beste praksis på området.	A	J
5.1.8	Tjenesten skal ha fysiske og logiske tilgangsbegrensninger for å hindre at utro tjenere får innsyn i kundens data.	A	N
	Roller og ansvarsfordeling for informasjonssikkerhet skal være klart definert i Leverandørens organisasjon og skal involvere alle som utfører arbeid i forbindelse med leveranse av løsningen.	A	N
5.1.10	All kommunikasjon over Internett skal gå i kryptert kanal.	A	N

5.2 Behandling av personopplysninger

Nr.	Krav	A B	U (J/N)
	Leverandøren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.	A	N
5.2.2	Løsningen må driftes iht. personopplysningsloven.	A	N
5.2.3	Ved avvik skal avviksmelding etter personopplysningsforskriftens § 2-6 gjøres tilgjengelig for Kunden.	A	N
5.2.4	Leverandøren skal ikke overlate personopplysninger til andre for lagring eller bearbeidelse uten etter avtale med Kunden.	A	N
5.2.5	Leverandøren skal sørge for at eventuelle underleverandører som	A	N

	Leverandøren benytter, og som behandler personopplysninger, påtar seg tilsvarende forpliktelser som Leverandøren har som databehandler etter denne avtalen.		
5.2.6	Alle data skal lagres innenfor EØS-området.	A	N
5.2.7	Hvis Leverandøren eller underleverandør er etablert i et annet EØS-land skal personopplysninger behandles iht Personverndirektivet (Direktiv 95/46/EF) og lokal lovgivning som implementerer dette.	A	N
5.2.8	Leverandøren skal sørge for at det ikke blandes sammen personopplysninger mellom ulike behandlingsansvarlige kunder.	A	J

5.3 Sikkerhetspolicy

Nr.	Krav	A B	U (J/N)
	Leverandøren skal ha en sikkerhetspolicy som skal legges fram for Kunden på forespørsel.	A	N
5.3.2	Leverandøren skal ha en beskrevet rutine for å informere Kunden om vedtatte relevante endringer i sikkerhetspolicyen.	B	N
5.3.3	Leverandørens sikkerhetspolicy skal omfatte hele verdikjeden for løsningen.	A	N
5.3.4	Det skal finnes etablerte prosesser for revisjon og oppdatering av sikkerhetspolicyen.	A	N

5.4 Styring av risiko

Nr.	Krav	A B	U (J/N)
	Det skal minst en gang årlig, og ved endringer som har betydning for informasjonssikkerheten, gjennomføres risiko- og sårbarhetsanalyse knyttet til alt som omfatter leveransen av løsningen. Dersom Leverandør inkluderer bruk av underleverandør(er) skal deres leveranser også inkluderes, eller egen risikoanalyse skal være gjennomført.	A	N
	Utestående tiltak som adresserer uakseptabel risiko skal dokumenteres og gjøres tilgjengelig for Kunden.	A	N
	Leverandøren skal på forespørsel gi Kunden innsyn i risikoanalysene for løsningen.	B	N
	Leverandøren skal gjennomføre sikkerhetstester i egen infrastruktur. Sikkerhetstestene skal utføres av uavhengig tredjepart. Dette kan eksempelvis være penetrasjonstester.	A	N
	Leverandøren skal før produksjonssetting av vesentlige endringer gjennomføre risikovurderinger.	A	N

5.5 Administrasjon av aktiva

Nr.	Krav	A B	U (J/N)
	Når lagret informasjon og lagringsmedier skal slettes, skal dette skje i samsvar med gjeldende føringer for sikker sletting fra Datatilsynet.	A	N
5.5.2	Ved avhending, kassering eller gjenbruk av enheter og utstyr som har vært benyttet i forbindelse med løsningen, skal Leverandøren iverksette en sikker og forsvarlig prosess.	A	N
5.5.3	Leverandøren skal på forespørsel kunne dokumentere rutiner for å ivareta sikker sletting, og evt. destruksjon, av dokumenter, informasjon og lagringsmedier.	B	N
5.5.4	Leverandøren kan ikke bruke Kundens data til egne formål.	A	N

5.6 Personellsikkerhet

Nr.	Krav	A B	U (J/N)
	Leverandøren skal innhente taushetserklæring fra ansatte, underleverandører og tredjeparter som handler på vegne av Leverandøren i forbindelse med levering av løsningen.	A	N
5.6.2	Leverandøren skal gjennom ISMS ha et dokumentert regime for personellsikkerhet.	A	N
5.6.3	Leverandøren skal gjennomføre opplæring i informasjonssikkerhet for alt personell - både for eget, samarbeidende og innleid personell med relevans for denne avtalen.	A	N

5.7 Kommunikasjons- og driftsadministrasjon

Nr.	Krav	A B	U (J/N)
	Leverandøren skal dokumentere ansvar og prosedyrer for administrasjon og drift av IT-infrastruktur i sikkerhetsdokumentasjonen sin.	A	N
5.7.2	Der det er hensiktsmessig bør Leverandøren ha en arbeidsdeling mellom administrasjon og utførelse av oppgaver for å redusere faren for utilsiktede/uautoriserte hendelser eller overlagt misbruk av systemer eller tjenester.	B	N
5.7.3	Loggprosedyrene for Tjenesten skal gi mulighet for en pålitelig kobling mellom en handling og personen som er ansvarlig for handlingen. Leverandøren skal beskrive hvordan dette oppnås.	A	J
5.7.4	Leverandøren skal ha integrerte mekanismer for å overvåke forsøk på ikke-autorisert adgang.	A	N
5.7.5	Tilgangssystemet internt skal ha en logg/oversikt som viser hvilke rettigheter hver enkelt bruker har hatt til enhver tid.	A	N
5.7.6	Alle logger skal være beskyttet og kun være tilgjengelig for autorisert personell. Tilgang til logger skal logges.	A	N

5.8 Aksesskontroll

Nr.	Krav	A B	U (J/N)
	Leverandøren skal sikre at informasjon, data og programmer kun er tilgjengelig for autoriserte personer.	A	N
5.8.2	Leverandøren skal sikre at tilgang til interne nettverkskomponenter skal skje på en kontrollert måte. Dette for å sikre at brukere som har tilgang til nettverk og nettverkskomponenter, ikke kompromitterer sikkerheten.	A	N
5.8.3	Leverandøren skal ha rutine for ajourhold av autorisasjon og tilganger, herunder tilbaketrekking av autorisasjon og tilganger når en person fratrer driftsoppgaver knyttet til løsningen.	A	N
5.8.4	Leverandør er ansvarlig for at kun autorisert personale skal kunne utføre driftsoperasjoner.	A	N

5.9 Utvikling og vedlikehold av informasjonssystemer

Nr.	Krav	A B	U (J/N)
	Leverandøren skal tilby forpliktede maksimumstider for påbegynt retting av feil av ulik alvorlighetsgrad i henhold til Bilag 4 - Tjenestenivå.	A	N
	Leverandøren skal ha et regime for håndtering av sikkerhetsoppdateringer i driftsløsningen.	A	N
5.9.3	Leverandøren skal ha system som forhindrer eller sikrer at man oppdager uautoriserte eller ikke-planlagte endringer av komponenter i løsningen, applikasjonsfiler eller andre kritiske filer på server. Dersom det ikke er mulig å forhindre endringene skal det umiddelbart foretas tilbakerulling til godkjent versjon.	A	N
5.9.4	Leverandøren skal tilrettelegge sine systemer, slik at effektiv og relevant rapportering og varsling kan gjennomføres ved informasjonssikkerhetsbrudd.	A	N
5.9.5	Endringer i Leverandørens løsning med tilhørende grensesnitt skal testes og godkjennes i eget testmiljø før utrulling til produksjon.	A	N

5.10 Kontinuitetsplanlegging

Nr.	Krav	A B	U (J/N)
	Leverandøren skal ha etablert, dokumentert og vedlikeholdt kontinuitets- og beredskapsplan som dekker krisesituasjoner, håndtering av sikkerhetsbrudd, sikkerhetskopi- og reservedriftsløsninger for løsningen.	A	N
5.10.2	Leverandøren skal holde kontinuitets- og beredskapsplan løpende oppdatert gjennom regelmessig test og øvelse.	A	N

5.11 Gjenoppretting av data

Nr.	Krav	A B	U (J/N)
	Leverandøren skal ha mekanismer som ivaretar at det ikke tåles tap av data i tjenesten utover 1 time.	A	J
5.11.2	Leverandøren skal jevnlig verifisere innhold i sikkerhetskopier og teste gjenoppretting av data for å verifisere kvaliteten på sikkerhetskopiene.	A	N
5.11.3	Data skal være gjenopprettet innen den frist som framgår av Bilag 4 - Tjenestenivå.	A	N
5.11.4	Sikkerhetskopiert informasjon skal oppbevares i minimum 3 måneder.	A	N

6. Funksjonelle krav

6.1 Overordnede funksjonelle krav

Nr.	Krav	A B	U (J/N)
	Løsningen skal ha god brukervennlighet.	B	J
6.1.2	Leverandøren bør følge de til enhver tid gjeldende *forvaltningsstandarder* (www.standard.difi.no) som er relevante for tjenesteleveransen, som f.eks. *nettbaserte tjenester*. Nye relevante standarder skal implementeres innen rimelig tid.	B	N

6.2 Virksomhet

Nr.	Krav	A B	U (J/ N)
	Det skal tilbys oppslag mot oppdaterte data fra Enhetsregisteret basert på minimum virksomhetsnavn.	A	N
6.2.2	Det skal være mulig å kategorisere virksomheter som A, B og C-kunder.	B	N
6.2.3	Det skal kunne opprettes kundeansvarlige (oppslag mot Difi-bruker) for en virksomhet.	B	N
6.2.4	Organisasjonsnummer skal være unik ID, og det skal ikke være mulig å opprette duplikater.	A	N

6.3 Kontakt

Nr.	Krav	A B	U (J/N)
6.3.1	E-postadresse er unik ID, og det skal ikke være mulig å registrere duplikater.	B	N
6.3.2	Det skal være mulig å opprette relasjoner til flere virksomheter per kontakt, men et kontaktpunkt skal tilhøre en virksomhet.	B	N
6.3.3	Kontakt skal kunne knyttes som varslingspunkt til en *integrasjon* (kundens- og leverandørens tjeneste – se Bilag 1 vedlegg 2).	A	N

6.4 Kalenderaktivitet

Nr.	Krav	A B	U (J/N)
	Det skal være mulig å opprette kalender aktivitet på kundens- og leverandørens tjeneste (*integrasjon*).	B	N
6.4.2	Det skal være mulig å opprette regelmessige kalenderaktiviteter.	B	N
6.4.3	Difi-bruker skal kunne få oversikt over kalenderaktivitetene for alle kunder og leverandører i et slags årshjul.	B	J

6.5 Sak

Nr.	Krav	A B	U (J/N)
	Det skal være automatisk konvertering til sak ved innkommende aktiviteter (e-post, skjema), og eventuelle strukturerte data skal automatisk registreres i sak.	B	J
	Sak skal ha knytning til virksomhet og kontakt.	A	N
	Sak skal inneholde dato for oppretting.	A	N
	Sak skal inneholde forhåndsvisning av tilhørende aktiviteter i saksvisningen.	B	J
	Det skal være mulig å kategorisere ulike sakstyper.	A	N
	Sak skal inneholde saksstatus.	A	N
	Det skal være mulighet for å sette ulik SLA på ulike sakstyper.	B	N
	Saker skal ha unike og søkbare saksnummer.	A	N
	Automatisk ruting av innkommende e-post basert på regler (makro) til definerte køer/grupper	B	J
	Det skal være mulig å automatisere eskalering av sak basert på SLA.	A	N

7. Maler

Nr.	Krav	A B	U (J/N)
	Det skal være enkelt og intuitivt å opprette maler.	B	J
7.2	Det skal væra god funksjonalitet for å opprette og vedlikeholde svarmaler i Word.	B	J
7.3	Det skal være nyhetsbrev-funksjonalitet (mulighet for innlasting av bilde, lenker, tabeller etc.).	B	J
7.4	Svarmalene skal være søkbare og bygges i en struktur.	B	N
7.5	Det skal være mulig å få statistikk over bruken av malene.	B	N

8. Statistikk, søk og rapporter

Nr.	Krav	A B	U (J/N)
	Det skal være mulig å opprette og dele forhandsdefinerte og dynamiske rapporter og spørringer på alle entiteter og tidsperioder.	B	J
8.2	Det skal være mulig å opprette Adhoc-rapporter og spørringer på alle entiteter og tidsperioder.	B	J
8.3	Det skal være mulig å opprette dynamiske Dashboards.	B	J
8.4	Det skal være mulig å filtrere statistikk og rapporter på alle entiteter og tidsperioder.	B	J
8.5	Det skal være mulig å eksportere rapporter i CSV.	A	N
8.6	Det skal være mulig å importere data i CSV.	B	N
8.7	Det skal være et globalt tilgjengelig søkefelt som søker på alle entiteter og felt i løsningen.	A	N
8.8	Det skal være et avansert søk med mulighet til filtrering på felt, entitet og tidsperiode.	B	J
8.9	Det skal være et lokalt søkefelt for hver visning (entitet).	B	N

9. Varsling

Nr.	Krav	A B	U (J/N)
	Det skal være enkelt å sende ut varsel basert på forhåndsdefinerte varslingslister.	B	J
9.2	Det skal være enkelt å opprette Adhoc-varslingslister (ikke forhandsdefinerte).	B	J
9.3	Det skal være nyhetsbrev-funksjonalitet (bilder, lenker, tabeller etc.).	B	J
9.4	Varslingslister skal være dynamiske og holdes vedlike ett sted.	A	N
9.5	Det skal være logging og historikk over utsendte varsel.	B	J
9.6	Det skal være mulig å bruke forhåndsdefinerte maler ved utsending av varsel.	B	J

10. Logging

Nr.	Krav	A B	U (J/N)
	Alle endringer av data skal logges og tidsstempels slik at den konkrete endringen er sporbar.	A	N
10.2	For alle endringer av data i løsningen (opprettelse, endring og sletting) skal det logges hvilken bruker som endrer data.	A	N
10.3	Tidspunkt for opprettelse av et dataobjekt forblir uendret gjennom hele levetiden til dataobjektet.	B	J
10.4	Det skal være mulig å sortere logger på tidspunkt for opprettelse, endring og sletting av data.	B	J

11. Systemadministrators rettigheter

Nr.	Krav	A B	U (J/N)
	Systemadministrator skal kunne gjøre endringer og tilpassinger på alle skjema og entiteter i løsningen.	B	J
11.2	Systemadministrator skal kunne legge til og fjerne skjema og entiteter i løsningen.	B	J
11.3	Systemadministrator skal kunne legge til og fjerne brukere (lisenser) og roller i løsningen.	A	N
11.4	Systemadministrator skal kunne opprette nye team og grupper i løsningen.	A	N
11.5	Systemadministrator skal kunne legge til, endre eller fjerne køer i løsningen.	A	N
11.6	Systemadministrator skal kunne opprette, endre eller slette saksrutingsregler og arbeidsflyter. Endre eksisterende regelinformasjon, for eksempel betingelser, rekkefølge og handling.	B	J
11.7	Systemansvarlig skal kunne opprette og definere ulike servicenivå/SLA for ulike køer/grupper i løsningen.	B	J

12. Synkronisering av data

Nr.	Krav	A B	U (J/N)
12.1	Leverandøren skal etablere en datadrevet integrasjon mellom tjenesten ID-porten admin og Leverandørens løsning.	A	N
12.2	Tjenestedata iht. datamodellen i Bilag 1 vedlegg 2 skal synkroniseres fra ID-porten admin til Leverandørens løsning på en måte som er sikker og stabil.	B	J
12.3	Tjenestedata skal hentes over *REST-API for uthenting av tjenestedata* (beskrevet i Bilag 1 vedlegg 1) og lagres som en del av entiteten «Integrasjon», beskrevet i datamodellen (beskrevet i Bilag 1 vedlegg 2).	A	N
12.4	Leverandøren skal etablere datadreven integrasjon mellom løsningen og Samarbeidsportalen (se Bilag 1 vedlegg 1) eller tilby et portalgrensesnitt som gir innsyn og redigeringsmuligheter i tjenestedata. Leverandøren skal beskrive hvilken av disse løsningene som tilbys og beskrive selve løsningen. Hvis leverandøren tilbyr portalportalgrensesnitt som løsning, skal kravene 12.4.1 og 12.4.2 også besvares.	B	J
12.4.1	Dersom Leverandøren tilbyr portalgrensesnitt som løsning for krav 12.4, skal	B	J

	grensesnittet tilby lese- og skrivetilgang til kontakt- og kundedata for brukere som er autentisert med autentiseringsløsningen MiDifi (se bilag 1 vedlegg 1).		
12.4.2	Dersom Leverandør tilbyr portalgrensesnitt som løsning for krav 1.4 skal løsningen tilby Single Sign-On med MiDifi (se Bilag 1 vedlegg 1).	B	J
12.5	Leverandøren skal gjøre data som inngår i entitetene *integrasjon*, *virksomhet*, *kontakt* og *saker* (se Bilag 1 vedlegg 2) tilgjengelig i Samarbeidsportalen på en måte som er sikker og stabil.	B	J

13. Opsjoner

13.1 Opsjon på synkronisering av nye tjenestedata

Nr.	Krav	A B	U (J/N)
13.1.1	Leverandøren tilbyr opsjon på synkronisering av nye tjenestedata	A	N
13.1.2	Leverandøren etablerer nye datadrevne integrasjoner mellom Difis fellestjenester (åpne eller OAUTH-sikrede REST-APIer) og Leverandørens løsning etter modellen beskrevet i Bilag 1 vedlegg 2.	A	N

13.2 Opsjon på oppslagstjeneste for bruksvilkår

Nr.	Krav	A B	U (J/N)
13.2.1	Leverandøren tilbyr opsjon på oppslagstjeneste for bruksvilkår.	A	N
13.2.2	Oppslagstjenesten skal tilby webserviceoppslag mot Leverandørens løsning basert på org.nr. (f.eks. request av typen <HarGodkjentBruksvilkår-foresporsel> <tjeneste> <org.nr>). Responsen skal gi status for hvorvidt den aktuelle organisasjonen har akseptert bruksvilkår (response av typen <tjeneste> <org.nr> <JA/NEI>).	B	J
13.2.3	Oppslagstjenesten skal svare innen 1 sekund ifm integrasjon av nye klienter mot Difis fellestjenester.	B	N

13.3 Opsjon på konsulentbistand/konsulentoppdrag

Nr.	Krav	A B	U (J/N)
13.3.1	Leverandøren tilbyr opsjon på konsulentbistand/konsulentoppdrag utover det Leverandøren er pålagt ifm etablering av løsningen eller annen konsulentbistand knyttet til Leverandørens tjeneste etter denne avtalen.	A	N
13.3.2	Konsulentene som tilbys til konsulentbistand/konsulentoppdrag skal ha minimum 3 år relevant erfaring og ha kjennskap til Kundens løsning.	A	N