pureservice

PURESERVICE TJENESTEAVTALE

Innhold

pureservice

1 Generelt

1.1 Definisjoner

«Tjenesteavtalen» og «Hovedavtalen» refererer til denne avtalen.

«Pureservice» refererer til Pureservice AS, org.nr 929 782 216.

«Kunde eller kunden» refererer til organisasjonen som har signert avtalen.

«Pureservice Support» refererer til teamet i Pureservice som jobber med å løse kundens problemer og/eller spørsmål knyttet til tjenesten.

«Hendelse» betyr omstendigheter som resulterer i brudd på avtalt tjenestenivå.

«Tjeneste» refererer til Pureservice tjenesten og/eller programvaren i henhold til avtale.

«Tjenestenivå» beskriver standardene som Pureservice jobber for og som måler nivået på tjenesten som tilbys som beskrevet under.

«Oppdrag» refererer til et arbeide som Pureservice skal utføre for Kunde.

«Oppdragsavtale» beskriver et spesifikt oppdrag, inkludert ønsket resultat, plan for gjennomføring og estimert omfang.

«Kreditering» er for en prosentvis andel av månedlig avgift som betales for tjenesten for et tjenestenivå som ikke oppfyller kravene i denne avtalen.

«Abonnement» er en avtale mellom Kunde og Pureservice, hvor Kunde forplikter seg til å betale for Tjenesten i en definert tidsperiode.

«Kundedata» omfatter alt som lastes opp eller lagres i forbindelse med bruk av tjenesten.

1.2 Avtalens gyldighet

Avtalen omfatter bruk av tjenesten og tilhørende tjenester. Ved å ta i bruk tjenesten godkjenner kunden denne avtalen. Hvis kunden ikke godkjenner vilkårene, kan tjenesten ikke tas i bruk.

Avtalen er gyldig så lenge kunden har et aktivt abonnement. Øvrige betingelser finnes i Pureservice Standardbetingelser.

1.3 Endring av avtalen

Denne avtale erstatter alle tidligere tjeneste- og lisensavtaler. Tillegg til eller avvik fra denne avtale er kun gyldig om skriftlig avtale med henvisning til denne avtale foreligger. Pureservice kan endre avtalevilkårene med virkning fra første avtalefornyelse.

1.4 Betalingsbetingelser

Som del av avtalen godtar Kunde å betale godtgjørelse for tjenesten i henhold til gjeldende priser og Pureservice Standardbetingelser. Pureservice kan begrense tilgang til eller avslutte tjenesten hvis betaling uteblir.

1.5 Uthenting av data fra tjenesten

Kunden kan i løpet av avtaleperioden hente ut egne data (kundedata) fra systemet. Dersom Pureservice skal bistå med å hente ut data vil kostnaden belastes kunden etter gjeldende priser. Etter avtalens utløp vil Pureservice deaktivere tilgang og slette kundedata. Data som er slettet vil kunne være umulig å hente tilbake.

1.6 Mislighold og sanksjoner

Dersom kunden vesentlig misligholder hele eller deler av forpliktelser overfor Pureservice, kan Pureservice ta nødvendige skritt ved å påpeke mangler, fjerne innhold i tjenesten eller stenge tilgang til tjenesten med umiddelbar virkning. Som vesentlig mislighold regnes blant annet ethvert brudd på begrensningene i kundens bruksrett til tjenesten. Ved heving eller annet opphør av avtalen kan Pureservice kreve at kunden returnerer alt mottatt materiell (eksempelvis programvare og brukerdokumentasjon) til Pureservice, samt at alle programvareeksemplarer slettes og avinstalleres.

Pureservice forbeholder seg retten til å forfølge ethvert mislighold gjennom sivilrettslige og/eller strafferettslige reaksjoner.

1.7 Register for varsling

Pureservice fører register over kontaktpersoner hos kunden. Kontaktpersoner i registeret varsles per epost eller på andre egnede måter om endring av avtalevilkår, varsel om mislighold av avtale og andre relevante meldinger. Standard oppføring i registeret er kontaktperson hos kunden som har signert på avtaledokumentene med Pureservice. Kunden er ansvarlig for å å oppdatere kontaktinformasjon i Tjenesten eller melde fra til Pureservice Support dersom kontaktpersoner eller kontaktinformasjon i registeret skal endres eller legges til. Pureservice er ikke ansvarlig for at varsler og meldinger ikke kommer kunden i hende dersom kunden ikke har meldt fra.

1.8 Taushetsplikt

All informasjon som utveksles mellom partene i forbindelse med leveranse og konsum av Tjenesten er konfidensiell informasjon. Kunde og Pureservice forplikter seg til ikke å utlevere til tredjepart noen form for informasjon som er mottatt fra den annen part i forbindelse med aktiviteter eller arbeid relatert til Tjenesten. Denne forpliktelsen vedvarer også etter opphør av Abonnementet.

Taushetsplikten gjelder ikke for informasjon som er:

– Offentlig kjent når informasjonen blir gitt.

– I mottakende parts kjennskap før informasjonen ble overlevert.

1.9 Lovvalg

Denne Avtalen og tvister som er oppstått som følge av denne, skal reguleres og fortolkes i overensstemmelse med norsk rett.

1.10 Konflikter

Uenighet om virkning, innhold eller gjennomføring av Avtalen skal forsøkes løst ved forhandlinger. Fører ikke forhandlingene frem, kan hver av partene kreve saken avgjort ved de alminnelige domstoler. Dersom partene avtaler det, skal saken avgjøres ved voldgift etter Lov av 14.05.2004 nr. 25: Lov om voldgift. Dersom partene ønsker konfidensiell behandling av voldgiftssaken, herunder voldgiftsrettens avgjørelse med motiver, skal dette avtales skriftlig mellom partene samtidig som voldgift avtales. Saken skal føres der hvor Pureservice har sin forretningsadresse når saken påbegynnes for domstolen eller voldgiftsretten.

2 Bruk av tjenesten

2.1 Bruksrett

Kunden har en ikke-eksklusiv og begrenset bruksrett til tjenesten.

Bruksretten gir Kunde tilgang til – og rett til å bruke – de brukerlisenser, moduler, applikasjoner, integrasjoner, API og eventuelle andre tillegg som Kunde abonnerer på.

Brukerlisenser gjelder for samtidig bruk hvor samtidig bruk defineres som aktivitet i løsningen i løpet av én klokketime. I de tilfeller hvor kunden har flere instanser av tjenesten beregnes samtidig bruk pr. instans isolert, som så legges sammen til et totalbehov. Pureservice forbeholder seg retten til å informere ved underlisensiering.

Å aktivt benytte én lisens på to eller flere sesjoner anses som brudd på lisensavtalen.

Kunden har ikke rett til å overdra, leie ut, lease, låne ut eller på annen måte tilby andre rett til på noen måte å disponere over tjenesten, lisenskoder og/eller tilhørende dokumentasjon, uten skriftlig og uttrykkelig forhåndssamtykke fra Pureservice.

Bruksretten opphører fra den dag Kunde ikke lenger har et aktivt abonnement.

2.2 Installasjon, eksemplarfremstilling, dekompilering mv.

Dersom tjenesten installeres lokalt (hos kunde eller kundens driftsleverandør) gir lisensen en rett til å installere og bruke tjenesten på én enkelt server (fysisk eller virtuell). Nødvendige tilleggs-komponenter (integrasjon mot email, Active Directory, datalyttere, serviceportal, o.l.) installeres etter behov. Ut over det som er nødvendig for lovlig bruk av tjenesten med tilhørende dokumentasjon, har kunden ikke rett til å fremstille eksemplarer av verken programvare, brukerdokumentasjon eller annet materiell som følger denne, uansett om det er elektronisk eller papirbasert. Kunden har rett til å fremstille sikkerhetseksemplarer av programvare i den utstrekning det er nødvendig for utnyttelsen, og i samsvar med ufravikelig lov. Kunden har ikke rett til å dekompilere (ta fra hverandre) programkoden i den hensikt å tilegne seg de teknikker som er benyttet av Pureservice. Kunden har ikke rett til å endre, redigere og/eller lage avledede arbeider av programvare (for eksempel fjerne faste designmaler som Pureservice eller Pureservice logo).

2.3 Endringer i tjenesten

Kunden har ikke anledning eller rett til å gjøre endringer i tjenesten med mindre dette er skriftlig avtalt mellom Pureservice og kunden. Dette inkluderer innhold i skreddersydd arbeidsflyt.

2.4 3. parts programvare

Kunden må selv bekoste eventuelle øvrige programvarelisenser som f.eks. server operativsystem, databaser, etc.

2.5 Kundedata

Kundedata forblir kundens eiendel og kundens ansvar. Kundedata som er lagret i tjenesten vil bli behandlet i form av lagring, flytting, sikkerhetskopiering og analyse for på beste mulige måte å kunne beskytte kundedata og for å kunne forbedre tjenesten.

Pureservice vil i alt arbeide med å håndtere kundedata ta nødvendige skritt for å sikre konsistens, integritet og tilgjengelighet. Med mindre det foreligger misligholdelse av denne avtalen, vil ikke data kunne fjernes fra tjenesten uten skriftlig samtykke fra kunden.

2.6 Personvern

Kunden godtar som del av denne avtalen at Pureservice kan få tilgang til, frembringe og lagre informasjon knyttet til bruk av tjenesten, inkludert informasjon og data som Pureservice samler rundt bruken av tjenesten når dette anses nødvendig for å operere i samsvar med til enhver tid gjeldende lover og regler.

Pureservice kan trekke ut statistikker og bruksmønstre av anonymiserte data. Slik statistikk og bruksmønstre kan lagres enten på Pureservices servere, servere som Pureservice disponerer i en skytjeneste eller i relevante nettjenester. Det er Pureservices ansvar å sørge for tilfredsstillende sikkerhet rundt disse dataene.

Som med alle tilbydere av skytjenester, vil Pureservice måtte følge pålegg fra rettslige instanser for lagring av data i datasentre. Pureservice vil være forpliktet til å følge pålegg for tilgjengeliggjøring av informasjon eller kundedata knyttet til formelle undersøkelser eller søksmål.

For Pureservice skytjeneste se kapittel 8 Databehandleravtale med Pureservice.

For Pureservice personvernserklæring se:
https://pureservice.com/trust/datahandtering-og-personvern-i-pureservice-i-skyen

2.7 Ansvarsbegrensninger

Den totale erstatning Kunden kan kreve under hele avtaleperioden er begrenset til et beløp som tilsvarer det vederlaget Kunden har betalt de siste 12 månedene før den skadevoldende handling/misligholdet oppsto.

Kunden kan ikke kreve erstatning for indirekte tap. Indirekte tap omfatter, men er ikke begrenset til, tapt fortjeneste av enhver art, tapte besparelser eller krav fra tredjeparter, herunder krav fra tredjepartsleverandør som følge av Kundens brudd på tredjepartsvilkår, samt i tillegg annet som regnes som indirekte tap etter norsk rett.

Erstatningsbegrensningen gjelder imidlertid ikke dersom Pureservice eller noen denne svarer for, har utvist grov uaktsomhet eller forsett.

Andre sanksjoner skal komme til fradrag i eventuell erstatning for samme forhold.

2.8 Immaterielle rettigheter

Pureservice har fullstendig eiendoms-, opphavs-, patent- og mønsterrett og alle øvrige eksisterende og fremtidige rettigheter tilknyttet alle former for dataprogrammer, integrasjoner, applikasjoner, databaser, dokumentasjon og liknende. Pureservice har eiendoms- og alle immaterielle rettigheter til eventuelle forslag fra kunden til endring av eksisterende Pureservice produkter og tjenester og/eller forslag til nye produkter eller tjenester, uansett forslagets form og/eller innhold. Slike rettigheter tilfaller Pureservice vederlagsfritt, med mindre annet skriftlig og uttrykkelig avtales i det enkelte tilfelle.

2.9 Overdragelse

Pureservice har rett til å overdra eller på annen måte overføre sine rettigheter og/eller plikter under denne avtale til tredjepart.

Behandlingsansvarlig skal varsles senest 90 dager før overdragelse slik at avtalen kan sies opp iht. gjeldende vilkår.

3 Tjenestebeskrivelse

3.1 Introduksjon

Pureservice tilbyr Service Management tjeneste. Tjenesten gjøres tilgjengelig for brukerne gjennom nettleser eller en mobil app. Pureservice følger etablerte beste praksis for prosesstøtte, forretningsfunksjonalitet, sikkerhet og kvalitet i leveransen.

3.2 Service design

Tjenesten leveres på to måter;

– som en skytjeneste (SaaS – Software-as-a-Service). Skytjenesten leveres gjennom datasentre i Norge. Løsningen leveres på dedikerte servere eller på en felles plattform med full dataisolasjon

– installert på kundens egne servere

Tjenesten leveres med mulighet for autentisering mot kundens katalogtjeneste (Active Directory, CRM-system eller tilsvarende) for å forenkle tilgangen til løsningen og administrasjon av sluttbrukere/kunder.

Pureservice bruker en underleverandør som vert for å tilby tjenesten som en skytjeneste. Pureservice er ansvarlig for tjenesten levert av underleverandør på samme måte som om Pureservice selv sto for leveransen. Tjenesteleveransen leveres i henhold til inngått SLA-avtale som sikrer optimal ytelse og tilgjengelighet for kunden.

3.3 Oppdateringer

Pureservice vil automatisk verifisere kundens versjon av tjenesten, samt vedlikeholde og oppdatere systemet. For større oppdateringer vil Pureservice varsle kunden i rimelig tid før oppdatering gjøres. Mindre oppdateringer kan gjøres uten nærmere varsel. Pureservice kan ikke garantere at oppdateringer i tjenesten støtter de til enhver tid gjeldende systemene som løsningen opprinnelig ble implementert på og integrert med.

3.4 Pureservice Continuous Delivery

Pureservice Continuous Delivery sørger for at tjenesten alltid kjører på siste versjon. URL mot https://*.pureservice.com må være tilgjengelig fra applikasjonsserver.

3.5 Pureservice OnPremise infrastruktur

Når tjenesten installeres på kundens egne servere, består infrastrukturen av følgende hovedkomponenter;

– Applikasjonsserver

– Databaseserver - for lagring av alle data og konfigurasjoner i tjenesten

– Emailserver - som muliggjør mottak og utsendelse av email knyttet til registrering og oppfølging av saker

3.6 Installasjon driftet av 3. part

Dedikerte instanser av applikasjonsserver og databaseserver kan implementeres i driftssenter hos 3. part og driftes og vedlikeholdes i henhold til inngåtte avtaler mellom kunden og 3. part.

Kostnaden for driftstjenester fra 3. part bæres fullt ut av kunden. Eventuelle tilleggskostnader i forbindelse med oppsett, konfigurering, forvaltning og lignende bæres også av kunden.

3.7 Kundens ansvar for Pureservice skytjeneste

– Administrere konfigurerbare data i tjenesten (brukere, brukergrupper, rettigheter, kategoriseringer, arbeidsflyt, soner, osv.)
– Sikre at brukere har nødvendige nettverkstilganger og tilgang til tjenesten på internett
– Sikre at nødvendige lokale tjenester (Active Directory sync, emailtjeneste, etc.) kjører og er tilgjengelig for tjenesten
– Installere og vedlikeholde støttet klientprogramvare for tilgang til tjenesten

3.8 Kundens ansvar for Pureservice lokalt installert

– Administrere konfigurerbare data i tjenesten (brukere, brukergrupper, rettigheter, kategoriseringer, arbeidsflyt, soner, osv.)
– Sikre at nødvendige lokale tjenester (Active Directory sync, emailtjeneste, etc.) kjører og er tilgjengelig for tjenesten
– Tilgjengeliggjøring av relevante tjenester på internett (gjennom DMZ eller liknende) dersom brukere skal ha tilgang til selvbetjeningsportal og/eller via mobil app
– Installere og vedlikeholde støttet klientprogramvare for tilgang til tjenesten
– Installere oppgraderinger når disse gjøres tilgjengelig fra Pureservice
– Sikkerhetskopiere data

3.9 Pureservice ansvarsområder for skytjenesten

– Sikkerhetskopiere data
– Oppgradere til nye versjoner

3.10 Sikkerhet

Pureservice utvikler, tester og verifiserer tjenesten basert på retningslinjene i «OWASP top 10». SaaS-tjenesten kjører i Microsoft Azure som er SOC 2 Type 2 Compliant og ISO 27001:2013 sertifisert i henhold til ISO 27002 best practices. Se Microsoft Trust Center for ytterligere informasjon.

3.11 Krypterte kundedata

SaaS-tjenesten benytter seg av kryptering for å sikre kundedata. Dette gjelder også for brukerhemmeligheter som en administrator i løsningen vil benytte for å koble opp mot aktuell eposttjener. Brukerhemmeligheten benyttes kun i sin dekrypterte tilstand for å opprette kobling mot eposttjeneren.

3.12 Selvbetjent administrasjon og konfigurasjon

Pureservice gir kunden mulighet til selv å administrere og konfigurere en rekke nøkkelaspekter ved tjenesten. Selvbetjening gjøres gjennom standard web-grensesnitt.

3.13 Tilgang for brukere og applikasjoner

Tjenesten kan aksesseres gjennom standard nettleser, Pureservice mobilapp eller programmatisk gjennom tjenestens APIer for tilpasninger og integrasjoner. Hvilke nettlesere som til enhver tid er støttet finnes på www.pureservice.com. Pureservice anbefaler at siste støttede versjon av de ulike nettlesere benyttes for å få fullt utbytte av tjenesten.

3.14 Katastrofeberedskap Pureservice skytjeneste

Tjenesten kjøres i datasentre som er bygget for å tilby høy tilgjengelighet og driftes ut fra prinsipper som skal minimere nedetid i tjenesten knyttet til drift og vedlikehold.

Omstendigheter knyttet til hardware og software-feil, katastrofer og menneskelige feil kan påvirke tjenestens tilgjengelighet. Pureservice har derfor implementert rutiner for katastrofeberedskap som skal håndtere risiko for å sikre tjenestens tilgjengelighet.

3.15 Flytte fra skytjeneste til egne servere, og vice versa

Pureservice åpner for å endre bruken av tjenesten som en skytjeneste til installasjon på egne servere, og vice versa. Det vil være en servicekost forbundet med en slik flytting, for detaljer vennligst kontakt Pureservice.

4 Tjenestenivå (SLA) Pureservice skytjeneste

4.1 Akseptabel bruk

Kunden må overholde krav til konfigurasjon, bruke støttet plattform og følge betingelsene beskrevet i tjenestebeskrivelsen for at denne avtale om tjenestenivå (SLA) skal gjelde.

For å sikre stabil og god ytelse for alle kunder, er det en grense på 100 API-kall per minutt per kunde. Dersom denne grensen overskrides, kan ytterligere API-forespørsler bli midlertidig blokkert.

4.2 SLA ekskluderinger

Denne SLA gjelder ikke for ytelse eller tilgjengelighet;

- Tjenesten installert på Kundens egne servere eller hos 3. part
- Grunnet faktorer utenfor Pureservice sin kontroll
- Som følge av hendelser eller mangel på hendelse fra kunden eller 3. part
- Forårsaket av bruk av tjenesten uten å ta hensyn til råd fra Pureservice om endret konfigurasjon eller bruk av tjenesten
- I forbindelse med planlagt vedlikehold
- I forbindelse med beta-testing eller prøvetid
- For testinstans

4.3 Kreditering av tjenesteavgift

- Måten og metoden for beregning av krediteringsbeløp er beskrevet nedenfor
- Kreditering av tjenesteavgift er eneste finansielle erstatning ved overtredelse av SLA
- Tjenesteavgift kreditert i en kalendermåned skal ikke under noen omstendigheter overstige kundens månedlige tjenesteavgift
- Kreditering gjelder ikke for engangsavgifter knyttet til leveranse av tjenesten
- Kreditering forutsetter at kunden melder fra til Pureservice Support når nedetid inntreffer
- Retten til kreditering bortfaller dersom kunden ikke påberoper dette skriftlig innen 4 uker etter nedetid

4.4 Oppetidsmåling pr måned

”Nedetid” defineres som tiden når ingen av kundens brukere kan logge inn og benytte tjenesten i henhold til tjenestebeskrivelsen. Nedetid omfatter ikke tidsperioder når tjenesten ikke er tilgjengelig som resultat av planlagt nedetid knyttet til vedlikehold eller oppgradering av tjenesten, eller endringer avtalt med kunden.

”Planlagt nedetid” defineres som nedetid innenfor forhåndsavtalte tidsvinduer eller nedetid i forbindelse med større systemoppgraderinger. Planlagt nedetid anses ikke som nedetid.

”Total tid” er total tid tilgjengelig i en kalendermåned. ”Månedlig oppetid-%” reflekteres i formelen;

$$Månedlig\ oppetid\% = \frac{Total\ tid\ -\ Nedetid}{Total\ tid}$$

4.5 Garantert oppetid

Månedlig oppetid-%	Kreditering av tjeneste
< 99.5%	25%
< 99%	50%
< 95%	100%

5 Customer Success

Avtalen inkluderer støtte til etablering og onboarding, samt løpende oppfølging når tjenesten er i drift/produksjon.

5.1 Støtte til etablering og onboarding

Etablering og onboarding har et todelt formål; gjøre Tjenesten klar til bruk, og hjelpe og forberede Kunde til å ta i bruk tjenesten.

Under listes typiske aktiviteter. Kunde og Pureservice vil samarbeide om – og delta i – disse aktivitetene. Pureservice vil informere Kunde om fordeling av ansvar og deltakelse ved oppstart av etablering og onboarding.

– Forberedelse
– Teknisk etablering
– Opplæring
– Kick-off
– Konfigurering
– Helsesjekk
– Go-live
– Evaluering

5.2 Løpende oppfølging

Når tjenesten er i drift / produksjon tilbyr Customer Success rådgivning til Kunde. Denne rådgivningen inkluderer;

– Navngitt Customer Success Manager (CSM)
– Oppfølgingsplan som avtales med kunde
– Adgang til å booke tid i CSM sin kalender
– Diskusjon, anbefalinger og tips om bruk av tjenesten, relevante bruksscenario, beste praksis og erfaringer fra bruk hos andre kunder
– Artikler og beskrivelser relatert til tjenesten

Følgende er ikke inkludert;

– Bistand til å gjøre konfigurasjonsendringer, tilpasninger eller utarbeidelse av arbeidsflyt
– Kundetilpassede integrasjoner

6 Pureservice Support

Avtalen gir mulighet for å ta kontakt med Pureservice Support ved spørsmål eller feilsituasjoner.

Avtalen gjelder henvendelser relatert til løsningen som er implementert. Herunder ligger kombinasjonene mellom produkt, database, infrastruktur og eventuelle integrasjoner.

Support gis på gjeldende og forrige delversjon av tjenesten.

Feilretting grunnet Kundes forhold dekkes ikke av Pureservice Support og kan bli belastet Kunde etter gjeldende timesatser.

Pureservice Support er betjent via telefon, web-portalen og e-post i normal kontortid, 0800-1600. Unntaket er helger, helligdager og offentlige høytidsdager.

Pureservice Support Tlf 22 12 00 26

support@pureservice.com

https://support.pureservice.com/

Inkludert i Pureservice Support

Telefon - og mailsupport på produktspørsmål	■
Websupport – melde saker og se status via servicedesk.pureservice.com	■
Support på norsk	■
Responstid, tid fra saken er meldt til saken er påbegynt	2 timer
Antall personer som kan henvende seg til Pureservice Support	3
Kontaktpersoner skal ha deltatt på gratis brukeropplæring, i regi av Pureservice: https://www.pureservice.com/kurs/	■

7 Konsulentoppdrag

Ved leveranse av oppdrag gjelder følgende;

7.1 Forpliktelser

Kunden plikter å gi Pureservice tilgang til all den informasjon som ansees være nødvendig for at Pureservice skal være i stand til å utføre oppdraget i henhold til oppdragsavtalen.

Kunden stiller med personell som kan gi nødvendig tilgang til systemer og applikasjoner slik at Pureservice får utført sitt oppdrag.

Pureservice er på sin side pliktig til å innhente alle opplysninger som anses som nødvendig for å levere oppdraget som avtalt.

Oppstår det forsinkelser, eller mulighet for forsinkelser, i forhold til avtalt fremdriftsplan, skal Pureservice, uten ugrunnet opphold, informere kunden.

Før sluttføring av oppdrag skal Pureservice ha utført en funksjonell test i henhold til oppdragsbeskrivelsen.

7.2 Endringer

Kunden har til enhver tid rett til, ved skriftlig endringsordre, å foreta endringer i oppdrag ved å forandre Pureservices oppgaver eller fremdriftsplan. Dette forutsetter at endringen ligger innenfor hva partene med rimelighet kunne forvente da oppdraget ble avtalt.

Pureservice skal snarest mulig etter mottagelse av en endringsordre skriftlig meddele Kunden hvilke virkninger endringene får for pris, fremdriftsplan eller andre forhold.

Tidsforbruk utover estimert tid som skyldes uforutsette problemer i Kundens driftsmiljø eller forhold hos Kunden som hindrer Pureservice fra å gjennomføre oppdraget i henhold til plan belastes med samme rater som for utførelse av oppdraget.

Ved kansellering/forskyving 7 dager før planlagt konsulentdag faktureres 50% av beløpet. Ved kansellering/forskyving 3 dager før, faktureres hele beløpet.

Dersom oppdraget innebærer å utvikle eller endre en integrasjon omfatter oppdraget kun gjeldende versjon av integrerte tjenester. Eventuelt arbeid knyttet til nye versjoner av integrerte tjenester skal godtgjøres i henhold til avtalte timepriser.

Utbedringer som følge av mangler ved utførelsen av oppdraget skal utføres av Pureservice for egen regning, forutsatt at Kunden har reklamert innen rimelig tid og senest 3 måneder etter mangelen fant sted.

7.3 Akseptanse

Kundens akseptanse av oppdraget skjer etter at oppdrag er meldt sluttført av Pureservice. Etter dette har Kunde en 2 -to- ukers frist til å melde akseptanse. Om ikke Pureservice har mottatt melding om at oppdraget ikke er akseptert innen denne fristen regnes oppdraget likevel som akseptert.

8 Databehandleravtale

Standardavtalevilkår
I henhold til artikkel 28 nummer 3, i Europaparlamentets og Rådets forordning 2016/679 (personvernforordningen) med henblikk på databehandlerens behandling av personopplysninger

mellom

Kunden, som følger av Hovedavtalen, se nedenfor,

heretter «den behandlingsansvarlige»

og

Pureservice

heretter «databehandleren»

som hver for seg er en «part» og sammen utgjør «partene»

HAR AVTALT følgende standardavtalevilkår (Vilkårene) med henblikk på å overholde personvernforordningen og sikre beskyttelse av fysiske personers grunnleggende rettigheter og friheter.

8.1 Innledning

8.1.1 Disse Vilkårene fastsetter den behandlingsansvarlige og databehandlerens rettigheter og plikter når databehandleren utfører behandling av personopplysninger på vegne av den behandlingsansvarlige.

8.1.2 Disse Vilkårene er utformet med for å sikre partenes etterlevelse av artikkel 28 nummer 3 i Europaparlamentets og Rådets forordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (personvernforordningen).

8.1.3 I forbindelse med avtale mellom behandlingsansvarlig og databehandler om leveranse (Hovedavtalen) som disse Vilkårene er knyttet til behandler databehandleren personopplysninger på vegne av den behandlingsansvarlige i overensstemmelse med disse Vilkårene.

8.1.4 Vilkårene har forrang i forhold til eventuelle tilsvarende bestemmelser i andre avtaler mellom partene.

8.1.5 Det er fire vedlegg til disse Vilkårene, og vedleggene utgjør en integrert del av Vilkårene.

8.1.6 Vedlegg A inneholder nærmere opplysninger om behandlingen av personopplysninger, herunder om behandlingens formål og art, typen av personopplysninger, kategoriene av registrerte og behandlingens varighet.

8.1.7 Vedlegg B inneholder den behandlingsansvarliges betingelser for databehandlerens bruk av underdatabehandlere og en liste over underdatabehandlere som den behandlingsansvarlige har godkjent.

8.1.8 Vedlegg C inneholder den behandlingsansvarliges instruks når det gjelder databehandlerens behandling av personopplysninger, en beskrivelse av de sikkerhetstiltakene som databehandleren som minimum skal gjennomføre, og hvordan revisjoner av databehandleren og eventuelle underdatabehandlere skal utføres.

8.1.9 Vedlegg D inneholder bestemmelser om andre aktiviteter som ikke er omfattet av Vilkårene.

8.1.10 Vilkårene med tilhørende vedlegg skal oppbevares skriftlig, herunder elektronisk, av begge parter.

8.1.11 Disse Vilkårene fritar ikke databehandleren fra plikter som databehandleren er pålagt etter personvernforordningen eller annen lovgivning.

8.2 Den behandlingsansvarliges rettigheter og plikter

8.2.1 Den behandlingsansvarlige er ansvarlig for å sikre at behandlingen av personopplysninger skjer i overensstemmelse med personvernforordningen (se personvernforordningen artikkel 24), gjeldende personopplysningsvernbestemmelser i unionsretten eller medlemsstatenes[1] nasjonale rett og disse Vilkårene.

8.2.2 Den behandlingsansvarlige har rett og plikt til å bestemme formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes.

8.2.3 Den behandlingsansvarlige er ansvarlig for, blant annet, å sikre at det foreligger et behandlingsgrunnlag for behandlingen av personopplysninger som databehandleren instrueres om å gjøre.

8.3 Databehandleren handler etter instrukser

8.3.1 Databehandleren skal bare behandle personopplysninger etter dokumenterte instrukser fra den behandlingsansvarlige, med mindre noe annet kreves av unionsretten eller medlemsstatenes nasjonale rett som databehandleren er underlagt. Disse instruksene skal være spesifisert i vedlegg A og C. Etterfølgende instrukser kan også gis av den behandlingsansvarlige mens det skjer behandling av personopplysninger, men instruksene skal alltid være dokumenterte og oppbevares skriftlig, herunder elektronisk, sammen med disse Vilkårene.

8.3.2 Databehandleren skal omgående underrette den behandlingsansvarlige dersom en instruks fra den behandlingsansvarlige, etter databehandlerens mening, er i strid med personvernforordningen eller gjeldende personopplysningsvernbestemmelser i unionsretten eller medlemsstatenes nasjonale rett.

8.4 Konfidensialitet

8.4.1 Databehandleren kan bare gi tilgang til personopplysninger som behandles på den behandlingsansvarliges vegne til personer underlagt databehandlerens instruksjonsmyndighet som har forpliktet seg til konfidensialitet eller er underlagt en passende lovbestemt taushetsplikt, og bare i det nødvendige omfang. Listen av personer som har fått tilgang skal gjennomgås fortløpende. På bakgrunn av en slik gjennomgang kan tilgangen til personopplysninger stenges, dersom den ikke lenger er nødvendig, og personopplysningene skal deretter ikke lenger være tilgjengelig for disse personene.

[1] Henvisninger til «medlemsstater» i disse Vilkårene skal forstås som en henvisning til stater som er del av det europeiske økonomiske samarbeidsområdet (EØS-stater).

8.4.2 Databehandleren skal etter anmodning fra den behandlingsansvarlige kunne påvise at de aktuelle personene underlagt databehandlerens instruksjonsmyndighet er underlagt ovennevnte taushetsplikt.

8.5 Sikkerhet ved behandlingen

8.5.1 Personvernforordningen artikkel 32 fastslår at, idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen.

Den behandlingsansvarlige skal vurdere risikoene for fysiske personers rettigheter og friheter som behandlingen utgjør og gjennomføre tiltak for å imøtegå disse risikoene. Avhengig av relevans kan tiltakene omfatte:

a. pseudonymisering og kryptering av personopplysninger
b. evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene
c. evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse
d. en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.

8.5.2 Ifølge personvernforordningen artikkel 32 skal databehandleren – uavhengig av den behandlingsansvarlige – også vurdere risikoene for fysiske personers rettigheter og friheter som behandlingen utgjør, og gjennomføre tiltak for å imøtegå risikoene. Med henblikk på denne vurderingen skal den behandlingsansvarlige stille den nødvendige informasjonen til rådighet for databehandleren som gjør vedkommende i stand til å identifisere og vurdere slike risikoer.

8.5.3 Databehandleren skal også bistå den behandlingsansvarlige med å overholde den behandlingsansvarliges plikter etter personvernforordningen artikkel 32, ved blant annet å stille til den behandlingsansvarliges rådighet nødvendig informasjon om de tekniske og organisatoriske sikkerhetstiltakene som databehandleren allerede har gjennomført i henhold til personvernforordningen artikkel 32, samt all annen informasjon som er nødvendig for at den behandlingsansvarlige skal kunne overholde sine plikter etter personvernforordningen artikkel 32.

Hvis imøtegåelse av de identifiserte risikoene – etter den behandlingsansvarliges vurdering – krever at det gjennomføres ytterligere tiltak enn det databehandleren allerede har gjennomført, skal den behandlingsansvarlige angi disse tiltakene i vedlegg C.

8.6 Bruk av underdatabehandlere

8.6.1 Databehandleren skal oppfylle betingelsene som er fastsatt i personvernforordningen artikkel 28 nummer 2 og nummer 4 for å gjøre bruk av en annen databehandler (en underdatabehandler).

8.6.2 Databehandleren må således ikke bruke en underdatabehandler for å oppfylle Vilkårene uten på forhånd å ha innhentet en generell skriftlig godkjennelse fra den behandlingsansvarlige.

8.6.3 Databehandleren har den behandlingsansvarliges generelle godkjennelse til å benytte underdatabehandlere. Databehandleren skal skriftlig underrette den behandlingsansvarlige om eventuelle planlagte endringer som gjelder tilføyelse eller utskiftning av underdatabehandlere med minst fire ukers varsel og dermed gi den behandlingsansvarlige mulighet til å motsette seg slike endringer før den eller de beskrevne underdatabehandler(e) engasjeres. Lengre varslingsfrister for spesifikke underdatabehandlertjenester kan angis i vedlegg B. Listen over underdatabehandlere som den behandlingsansvarlige allerede har godkjent fremgår av vedlegg B.

8.6.4 Når databehandleren engasjerer en underdatabehandler for å utføre spesifikke behandlingsaktiviteter på vegne av den behandlingsansvarlige, skal underleverandøren pålegges de samme forpliktelsene med hensyn til vern av personopplysninger som er fastsatt i disse Vilkårene, ved hjelp av en avtale eller et annet rettslig dokument i henhold til unionsretten eller medlemsstatenes nasjonale rett, der det særlig gis tilstrekkelige garantier for at det vil bli gjennomført tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i denne forordning.

Databehandleren er derfor ansvarlig for å kreve at underdatabehandleren som minimum overholder databehandlerens forpliktelser etter disse Vilkårene og personvernforordningen.

8.6.5 En kopi av slik underdatabehandleravtale og eventuelle etterfølgende endringer skal – ved den behandlingsansvarliges anmodning – sendes til den behandlingsansvarlige, som på denne måten har mulighet for å sørge for at underdatabehandleren er pålagt de samme forpliktelsene med hensyn til vern av personopplysninger som er fastsatt i disse Vilkårene. Kommersielle bestemmelser som ikke påvirker det personopplysningsvernrettslige innholdet av underdatabehandleravtalen, er ikke underlagt kravet om kopi til den behandlingsansvarlige.

8.6.6 Databehandleren skal i underdatabehandleravtalen inkludere den behandlingsansvarlige som begunstiget tredjepart i tilfelle databehandleren går konkurs, slik at den behandlingsansvarlige kan tre inn i databehandlerens rettigheter og gjøre dem gjeldende overfor underdatabehandler, hvilket for eksempel setter den behandlingsansvarlige i stand til å instruere underdatabehandleren om å slette eller tilbakeføre personopplysningene.

8.6.7 Hvis underdatabehandleren ikke oppfyller sine personopplysningsvernforpliktelser blir databehandleren fullt ut ansvarlig overfor den behandlingsansvarlige når det gjelder oppfyllelse av underdatabehandlerens forpliktelser. Dette påvirker ikke de registrertes rettigheter etter personvernforordningen – særlig de nedfestet i personvernforordningen artikkel 79 og 82 – overfor den behandlingsansvarlige og databehandleren, herunder underdatabehandleren.

8.7 Overføring til tredjeland eller internasjonale organisasjoner

8.7.1 Databehandleren kan kun overføre personopplysninger til tredjeland eller internasjonale organisasjoner etter dokumentert instruks fra den behandlingsansvarlige, og slik overføring skal alltid skje i overensstemmelse med personvernforordningen kapittel V.

8.7.2 Hvis overføring av personopplysninger til tredjeland eller internasjonale organisasjoner, som databehandleren ikke er blitt instruert av den behandlingsansvarlige om å gjennomføre, kreves i henhold til unionsretten eller medlemsstatenes nasjonale rett som databehandleren er underlagt, skal databehandleren underrette den behandlingsansvarlige om nevnte rettslige krav før behandlingen, med mindre denne rett av hensyn til viktige allmenne interesser forbyr en slik underretning.

8.7.3 Uten dokumentert instruks fra den behandlingsansvarlige kan databehandleren innenfor rammene av disse Vilkårene således ikke:

a. overføre personopplysninger til en behandlingsansvarlig eller databehandler i et tredjeland eller en internasjonal organisasjon
b. overlate behandling av personopplysninger til en underdatabehandler i et tredjeland
c. behandle personopplysningene i et tredjeland

8.7.4 Den behandlingsansvarliges instruks når det gjelder overføring av personopplysninger til et tredjeland, herunder det eventuelle overføringsgrunnlaget i personvernforordningen kapittel V som overføringen er basert på, skal angis i vedlegg C.6.

8.7.5 Disse Vilkårene skal ikke forveksles med standard personvernbestemmelser som omhandlet i personvernforordningen artikkel 46 nummer 2 bokstav c og d, og disse Vilkårene kan ikke utgjøre et grunnlag for overføring av personopplysninger under personvernforordningen kapittel V.

8.8 Bistand til den behandlingsansvarlige

8.8.1 Databehandleren bistår, idet det tas hensyn til behandlingens art og i den grad det er mulig, ved hjelp av egnede tekniske og organisatoriske tiltak, den behandlingsansvarlige med å oppfylle vedkommendes plikt til å svare på anmodninger som den registrerte inngir med henblikk på å utøve sine rettigheter fastsatt i personvernforordningen kapittel III.

Dette innebærer at databehandleren så langt det er mulig skal bistå den behandlingsansvarlige i den behandlingsansvarlige oppfyllelse av:

d. opplysningsplikten ved innsamling av personopplysninger fra den registrerte
e. opplysningsplikten dersom personopplysninger ikke er blitt samlet inn fra den registrerte
f. den registrertes rett til innsyn
g. retten til retting
h. retten til sletting («retten til å bli glemt»)
i. retten til begrensning av behandling
j. underretningsplikten i forbindelse med retting eller sletting av personopplysninger eller begrensning av behandling
k. retten til dataportabilitet
l. retten til å protestere
m. retten til ikke å være gjenstand for en avgjørelse som utelukkende er basert på automatisk behandling, herunder profilering

8.8.2 I tillegg til databehandlerens forpliktelse til å bistå den behandlingsansvarlige i henhold til Vilkårene 8.5.3, bistår databehandleren også, idet det tas hensyn til behandlingens art og den informasjonen som er tilgjengelig for databehandleren, den behandlingsansvarlige med:

a. den behandlingsansvarliges forpliktelse ved brudd på personopplysningssikkerheten til uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde bruddet på personopplysningssikkerheten til den kompetente tilsynsmyndigheten, i Norge (Datatilsynet), med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter

b. den behandlingsansvarliges forpliktelse til uten ugrunnet opphold å underrette den registrerte om bruddet på personopplysningssikkerheten når det er sannsynlig at bruddet vil medføre en høy risiko for fysiske personers rettigheter og friheter

c. den behandlingsansvarliges forpliktelse til før behandlingen å foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet (vurdering av personvernkonsekvenser)

d. den behandlingsansvarliges forpliktelse til å rådføre seg med den kompetente tilsynsmyndigheten, i Norge (Datatilsynet), før behandlingen dersom en vurdering av personvernkonsekvenser tilsier at behandlingen vil medføre en høy risiko dersom den behandlingsansvarlige ikke treffer tiltak for å redusere risikoen.

8.8.3 Partene skal i vedlegg C oppgi de egnede tekniske og organisatoriske tiltakene gjennom hvilke databehandleren skal bistå den behandlingsansvarlige, samt omfanget og utstrekningen av den påkrevde bistanden. Dette gjelder for forpliktelsene som følger av Vilkårene 8.8.1. og 8.8.2.

8.9 Underretning om brudd på personopplysningssikkerheten

8.9.1 Ved brudd på personopplysningssikkerheten skal databehandleren underrette den behandlingsansvarlige om bruddet uten ugrunnet opphold etter å ha fått kjennskap til det.

8.9.2 Databehandlerens underretning til den behandlingsansvarlige skal om mulig skje innen 24 timer etter at databehandleren har fått kjennskap til bruddet på personopplysningssikkerheten, slik at den behandlingsansvarlige kan overholde sin forpliktelse til å melde bruddet til den kompetente tilsynsmyndigheten, jf. personvernforordningen artikkel 33.

8.9.3 I overensstemmelse med 8.8.2 bokstav a skal databehandleren bistå den behandlingsansvarlige med å melde bruddet til den kompetente tilsynsmyndigheten. Det innebærer at databehandleren skal bistå med å fremskaffe informasjon listet opp nedenfor, som ifølge personvernforordningen artikkel 33 nummer 3 skal fremgå av den behandlingsansvarliges melding av bruddet til den kompetente tilsynsmyndigheten:

a. arten av bruddet på personopplysningssikkerheten, herunder, når det er mulig, kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt

b. de sannsynlige konsekvenser av bruddet på personopplysningssikkerheten

c. de tiltak som den behandlingsansvarlige har truffet eller foreslår å treffe for å håndtere bruddet på personopplysningssikkerheten, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følge av bruddet.

8.9.4 Partene skal i vedlegg C oppgi all informasjon som databehandleren skal fremskaffe når vedkommende bistår den behandlingsansvarlige med å melde brudd på personopplysningssikkerheten til den kompetente tilsynsmyndigheten.

8.10 Sletting og returnering av opplysninger

8.10.1 Ved opphør av databehandlertjenestene skal databehandleren slette alle personopplysninger som er blitt behandlet på vegne av den behandlingsansvarlige og bekrefte overfor den behandlingsansvarlige at opplysningene er slettet eller levere tilbake alle personopplysningene og slette eksisterende kopier, etter behandlingsansvarliges valg, med mindre unionsretten eller medlemsstatenes nasjonale rett krever oppbevaring av personopplysningene.

8.11 Revisjon, herunder inspeksjon

8.11.1 Databehandleren skal stille til den behandlingsansvarliges disposisjon all informasjon som er nødvendig for å påvise etterlevelse av forpliktelsene etter personvernforordningen artikkel 28 og disse Vilkårene. Videre skal databehandleren muliggjøre og bidra til revisjoner, herunder inspeksjoner, som utføres av den behandlingsansvarlige eller en annen revisor som er bemyndiget av den behandlingsansvarlige.

8.11.2 Prosedyrene for den behandlingsansvarliges revisjoner, herunder inspeksjoner, av databehandleren og underdatabehandlere er spesifisert i vedlegg C.7 og C.8.

8.11.3 Databehandleren forplikter seg til å gi tilsynsmyndighetene, som etter gjeldende lovgivning har tilgang til den behandlingsansvarliges eller databehandlerens lokaler, eller representanter som opptrer på slike tilsynsmyndigheters vegne, adgang til databehandlerens fysiske lokaler ved presentasjon av behørig legitimasjon.

8.12 Partenes avtale om andre forhold

8.12.1 Partene kan avtale andre bestemmelser som gjelder databehandlertjenestene, f.eks. erstatningsansvar, så lenge disse andre bestemmelsene ikke direkte eller indirekte strider mot disse Vilkårene eller er til skade for den registrertes grunnleggende rettigheter og friheter og beskyttelsen som følger av personvernforordningen.

8.13 Ikrafttredelse og opphør

8.13.1 Vilkårene trer i kraft på datoen for begge partenes underskrift.

8.13.2 Begge partene kan kreve Vilkårene reforhandlet dersom lovendringer eller uhensiktsmessigheter i Vilkårene gir grunn til dette.

8.13.3 Vilkårene gjelder så lenge databehandlertjenestene varer. I denne perioden kan Vilkårene ikke sies opp, med mindre partene avtaler andre vilkår som regulerer levering av databehandlertjenestene.

8.13.4 Hvis leveringen av databehandlertjenestene opphører, og personopplysningene er slettet eller returnert til den behandlingsansvarlige i overensstemmelse med Vilkårene 8.10.1 og vedlegg C.4, kan Vilkårene sies opp med skriftlig varsel av begge partene.

8.13.5 Inngåelse av avtalen

Disse vilkårene er inngått som del av Hovedavtalen mellom behandlingsansvarlig og databehandler.

8.14 Kontaktpersoner hos den behandlingsansvarlige og databehandleren

8.14.1 Partene kan kontakte hverandre via nedenstående kontaktpersoner.

8.14.2 Partene forplikter seg til å orientere hverandre løpende om endringer som gjelder kontaktpersoner.

8.14.3 De samme kontaktpersoner som eventuelt følger av Hovedavtalen mellom behandlingsansvarlig og databehandler skal gjelde.

8.15 Vedlegg A: Opplysninger om behandlingen

A.1. Formålet med databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige er:

Formålet med behandlingen er å oppfylle avtalen som er inngått mellom behandlingsansvarlig (kunde) og databehandler (leverandør), se nærmere Hovedavtalen.

A.2. Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige skal primært dreier seg om (behandlingens art):

Lagring og nødvendig prosessering som del av tjenestene etter Hovedavtalen. Hovedavtalen går ut på at behandlingsansvarlig skal benytte databehandlers programvare for digital registrering, lagring og oppfølging av henvendelser fra behandlingsansvarliges ansatte (”saker”). Databehandler skal stille en dedikert instans av tjenesten som leveres etter Hovedavtalen til rådighet for behandlingsansvarlig, samt å utføre nødvendig vedlikehold av systemet. Systemet skal brukes til oppbevaring av den behandlingsansvarliges opplysninger knyttet til registrering og oppfølging av saker knyttet til egne ansatte, kunder og deres ansatte/kontaktpersoner samt andre relevante kontakter.

A.3. Behandlingen omfatter følgende typer av personopplysninger om de registrerte:

Navn, e-postadresse og telefonnummer på brukere samt annen informasjon og opplysninger som behandlingsansvarlig legger inn i systemet som leveres etter Hovedavtalen som en følge av bruken av systemet.

A.4. Behandlingen omfatter følgende kategorier av registrerte:

Ansatte hos behandlingsansvarlig, kunder av behandlingsansvarlig, kontaktpersoner hos kunder og leverandører hos behandlingsansvarlig samt for andre som kunden gir tilgang til systemet samt andre personer som omfattes av opplysninger som kunden legger inn i systemet.

A.5. Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige kan begynne etter at Vilkårene har trådt i kraft. Behandlingen har følgende varighet:

Ved opphør av Hovedavtalen, og denne databehandleravtale, skal databehandler tilbakelevere alle personopplysninger som er mottatt på vegne av den behandlingsansvarlige og som omfattes av denne avtalen. Slik tilbakelevering kan gjøres i form av utskrift og/eller kopi av kundedata i databaser som er omfattet. Kostnader ved dette bæres av den behandlingsansvarlige.

Med mindre behandlingsansvarlig ønsker det vil databehandler slette alle data som inneholder opplysninger som omfattes av databehandleravtalen. Dette gjelder også for eventuelle sikkerhetskopier. Databehandler skal skriftlig dokumentere at sletting er foretatt innen rimelig tid etter avtalens opphør. Ovennevnte gjelder såfremt det ikke foreligger lovmessig plikt til oppbevaring. Sletting vil da skje så snart denne plikten ikke lenger foreligger.

8.16 Vedlegg B: Underdatabehandlere

B.1. Godkjente underdatabehandlere

Ved Vilkårenes ikrafttredelse godkjenner den behandlingsansvarlige bruken av følgende underdatabehandlere:

Underdatabehandler	Land hvor behandlingen skal skje	Beskrivelse av behandlingen
Microsoft Norge AS (Azure), se: https://www.microsoft.com/en-us/trustcenter/	Norge	Vert for å tilby programvaren i nettskyen (ved Pureservice SaaS)
Mailgun, eid av Sinch AB i Sverige	EØS	Mottak og leveranse av epost. Kun for kunder som ikke har egen epostserver

Ved Vilkårenes ikrafttredelse har den behandlingsansvarlige godkjent bruken av ovennevnte underdatabehandlere for den behandlingsaktiviteten som er beskrevet for vedkommende. For endringer av underdatabehandlere, se punkt 8.6 i Vilkårene.

8.17 Vedlegg C: Instruks for behandling av personopplysninger

C.1. Behandlingens gjenstand/instruks for behandlingen

Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige skjer ved at databehandleren utfører følgende:

Se punkt A.2 ovenfor.

Databehandler skal for øvrig følge de plikter som er pålagt databehandler som sådan etter personvernregelverket, herunder personvernforordningen og personopplysningsloven, samt annen relevant lovgivning.

Databehandlers personell vil ikke ha tilgang til kundedata under normal drift, og har heller ikke behov for det. Ved feilsøking på tjenesten eller i forbindelse med feilsøking for behandlingsansvarlig har dev-ops teamet tilgang til kundedata lagret i tjenesten. Alle medlemmer av dev-ops teamet har fått utvidet opplæring i sikkerhet og personvern.

Databehandler kan ta ut statistikk og metadata om sakene, eksempelvis antall saker og aktiverte moduler, bruksmønstre mv.. Slik statistikk skal være anonymisert i forkant av overføring til databehandlerens sine servere og skal ikke inneholde personopplysninger. Slik statistikk og bruksmønstre kan lagres enten på databehandlers servere, servere som databehandler disponerer i en skytjeneste eller i relevante nettjenester. Det er databehandlers ansvar å sørge for tilfredsstillende sikkerhet rundt disse dataene.

Som med alle tilbydere av skytjenester, vil databehandler måtte følge pålegg fra offentlige myndigheter, påtalemyndigheter mv. for lagring av data i datasentre. Databehandler vil være forpliktet til å følge pålegg for tilgjengeliggjøring av informasjon eller kundedata knyttet til formelle undersøkelser eller søksmål.

Databehandler kan benytte tjenestedata for å optimalisere løsningen og utvikle nye tjenester. Tjenestedata kan f.eks. være om en avgrenset funksjon i løsningen (Change og/eller SLA) er aktivert eller ikke og inkluderer ikke personopplysninger eller sensitiv informasjon.

C.2. Informasjonssikkerhet

Sikkerhetsnivået skal gjenspeile:

Databehandleren skal sikre personopplysningene at det gjennomføres egnede tekniske og organisatoriske tiltak for å sikre personopplysning som behandles etter avtalen hensyntatt hva som er teknisk mulig, kostnader ved sikringen, og behandlingen av personopplysning som skal gjøres og risikoen ved slik behandling knyttet til personvernet til de som personopplysningene er knyttet til. Herunder, avhengig av hva som er nødvendig og egnet for sikringen:

Organisatoriske tiltak

- Det er etablert internkontroll/styringssystem for informasjonssikkerhet som er godkjent av ledelsen og som er kjent og implementert i organisasjonen, med opplæring, regelmessige kontroller for å avdekke om rutinene følges, og regelmessig revisjon (GDPR art. 32).
- Pureservice kjører i et datasenter som er SOC 2 Type 2 Compliant og ISO 27001:2013 sertifisert iht. ISO 27002 best practices.
- Ansatte i Pureservice er pålagt å følge et sett med sikkerhetsinstrukser og kun ansatte med tjenstlige behov har tilgang til produksjonsplattformen.

- Utviklingsteamet jobber etter SCRUM-metoden og benytter GIT versjonskontrollsystem. Endringer testes i separate miljøer før de godkjennes for slipp til produksjonsmiljøet. Dette muliggjøres ved bruk av separate oppdateringskanaler (dev, main, preview og release) i våre releaserutiner og en oppdatering publiseres ikke før integriteten på pakken er verifisert og testet. I disse stegene ligger det også manuelle godkjenningsrutiner. Det er automatiserte tester i forkant av alle kanaler. Før en oppdatering godkjennes går den gjennom en kvalitetskontroll i en egen QA-prosess.
- Pureservice DevOps teamet oppdaterer jevnlig infrastrukturen etter behov. Endringer som påvirker kunder i særlig grad annonseres i nyhetsfunksjonen i applikasjonen. Vedlikehold og oppdatering på lavere infrastrukturnivå, f.eks. OS-oppdateringer, retting av feil på infrastrukturkomponenter utføres automatisk og regelmessig av Microsoft.
- Endringer planlegges og utføres av DevOps-teamet. Teamet tester endringer i egnet miljø før endringer eventuelt overføres til produksjon. Alle endringer som planlegges gjennomgår en risikovurdering i forkant.
- Pureservice har etablert et CSIRT (Computer Security Incident Response Team) som følger opp alle sikkerhetshendelser. Teamet undersøker type hendelse og utfører nødvendige tiltak for å rette disse. Dette omfatter også varsling til kundens hovedkontakt dersom kundedata kan ha blitt påvirket, eller opprettelse av en sak til datatilsynet dersom det er oppdaget mulige brudd på personvernforordningen.
- Pureservice har flere kilder som kan føre til registrering av avvik. Eksempler på dette er overvåking/alarmer, manuell analyse av hendelseslogger eller kundemeldte avvik via vår servicedesk. Alle avvik registreres og behandles videre av DevOps eller CSIRT.
- Beredskap dekkes av en 24/7-vaktplan og CSIRT.
- Varsler som omhandler sårbarheter som er av interesse for alle kunder publiseres i applikasjonen. Dersom en sårbarhet er kundemeldt varsles det først gjennom versjonshistorikk når sårbarheten er rettet.
- Pureservice gjennomfører årlig penetrasjons- og sikkerhetstest med en ekstern leverandør. Testene tar utgangspunkt i OWASP topp 10.
- Behandlingsansvarlig eller representant for denne kan gjennomføre penetrasjonstester på sin egen Pureservice skyinstans inntil én gang per år og må godkjennes på forhånd ved å kontakte Pureservice support.

Tekniske tiltak

- Alle data blir lagret i minimum to fysisk adskilte databaseinstanser for å sikre tilgjengelighet. Multitenant arkitektur med adskilte databaser per kundeinstans.
- Alle databaser er kryptert ved lagring. Data er kryptert under transport mellom brukerenhet og Pureservice i skyen.
- Det gjøres kontinuerlig overvåking av ytelse og tilgjengelighet.
- Pureservice driftes og utvikles av personell med kunnskap og erfaring i sikkerhetsarbeid.
- Pureservice utvikler, tester og verifiserer Pureservice basert på retningslinjene i OWASP topp 10. Det gjøres eksterne sikkerhetsrevisjoner med penetrasjonstesting på nettverks- og applikasjonsnivå.
- Brukerautentisering og tilgangskontroll per instans.

- Kontinuerlig oppdatering av koden sikrer at alle kunder til enhver tid er oppdatert med funksjonalitet og sikkerhetsfunksjonalitet.
- Sikkerhetskopi av alle data kontinuerlig innenfor siste 30 dager.
- Løsningen leveres på Microsoft Azure plattformen, som er robust designet for å opprettholde tilgjengeligheten til enhver tid. Tjenestene overvåkes kontinuerlig med nødvendige varslingsrutiner for å opprettholde et akseptabelt tjenestenivå som beskrevet i tjenesteavtalen. Sikkerhet på skyplattform (Azure) håndteres av Microsoft, se mer her om tiltakene: https://www.microsoft.com/en-us/trustcenter/.
- Pureservice støtter Single Sign-On for integrasjon med virksomhetens eksisterende Identity Provider gjennom OpenID Connect, SAML. OAuth 2.0, WS-Federation med flere. Om kunden f.eks. benytter Azure AD som identitetstilbyder «IdP» så vil MFA, hvitelisting, regelsett for tilganger og avansert tilgangskontroll styres fra Azure AD.
- Pureservice støtter multifaktor-autentisering gjennom integrasjon med virksomhetens eksisterende Identity Provider.
- Pureservice oppdateres jevnlig med kode som tilfører ny funksjonalitet eller som adresserer kjente feil. Oppgradering av Pureservice i skyen annonseres i nyhetsfunksjonen i Pureservice og skjer automatisk på varslet tidspunkt. Utviklingsteamet gjennomgår opplæring i sikker utvikling i forbindelse med penetrasjon- og sikkerhetstesting hvert år og er ellers kontinuerlig oppdatert på trusler definert i for eksempel OWASP topp 10-listen.
- Pureservice benytter funksjonalitet i Microsoft Azure Security Center for kontinuerlig sikkerhetsovervåking av Pureservice i skyen.

Ytterligere informasjon om organisering av sikkerhetsarbeidet og tiltak er beskrevet i vår CAIQ – se https://pureservice.com/trust

I tillegg til ovennevnte så gjennomfører databehandler jevnlig sikkerhetsrevisjoner for systemer og lignende som omfattes av denne avtalen. Revisjonen kan omfatte gjennomgang av rutiner, stikkprøvekontroller, mer omfattende stedlige kontroller og andre egnede kontrolltiltak.

Behandlingsansvarlige kan kreve å få gjennomført en gjennomgang og revisjon av tjenesten, systemer og dokumentasjon for å sikre at den er lovmessig, og databehandler skal muliggjøre og bidra til slike revisjoner. Hver av partene dekker sine kostnader ved revisjoner. Bruker behandlingsansvarlig ekstern revisor, skal behandlingsansvarlig dekke kostnadene til denne.

Databehandleren har allikevel rett og plikt til å treffe beslutninger om hvilke tekniske og organisatoriske sikkerhetstiltak som skal gjennomføres for å etablere det nødvendige (og avtalte) sikkerhetsnivået.

C.3 Bistand til den behandlingsansvarlige

Databehandleren skal i den grad det er mulig – i det nedenfor beskrevne omfang og utstrekning – bistå den behandlingsansvarlige i samsvar med Vilkårene 8.8.1 og 8.8.2 ved å gjennomføre følgende tekniske og organisatoriske tiltak:

Bistand til behandlingsansvarlig av databehandler skal følge den bistandsplikt som er pålagt etter personvernregelverket, herunder personvernforordningen og personopplysningsloven.

Dersom databehandler får kjennskap til ulovlig tilgang til behandlingsansvarliges data lagret hos databehandler eller databehandlers underleverandører, skal databehandler uten ugrunnet opphold 1) informere om typen databrudd og berørte registrerte, 2) undersøke sikkerhetsbruddet og gi

behandlingsansvarlige detaljert informasjon om sikkerhetsbruddet, 3) iverksette og informere om ansvarlige og rimelige tiltak for å avhjelpe virkningen av sikkerhetsbruddet og begrense skadene.

Melding om mistenkte sikkerhetsbrudd kan sendes til: personvern@pureservice.com, som da vil håndtere saken for databehandler. Slik melding endrer ikke behandlingsansvarliges plikt til å melde avvik/personvernbrudd til Datatilsynet og eventuelt til de registrerte.

Bistand fra databehandleren til behandlingsansvarlig ut over det som følger av denne avtalen og som er plikter som tilligger databehandleren etter personvernregelverket, vil måtte utføres etter databehandlerens til enhver tid gjeldende timesatser som bistand. Dette gjelder oppgaver som å slette personopplysninger utenfor det som gjøres automatisk eller behandlingsansvarlig kan gjøre gjennom løsningen, gi innsyn i personopplysning ut over det som kan gjøres gjennom løsningen, bistå behandlingsansvarlig med risikovurderinger og dokumentasjon, mv.

C.4 Oppbevaringsperiode/sletteprosedyrer

Se punkt A.5 ovenfor.

C.5 Lokasjon for behandling

Behandling av personopplysninger som omfattes av Vilkårene kan ikke, uten den behandlingsansvarliges skriftlige godkjennelse etter Vilkårenes punkt 8, finne sted på andre lokasjoner enn følgende:

Behandlingen skal kun skje innenfor EØS.

Lokasjon for underdatabehandleres behandling av personopplysningene følger av tabellen under punkt B1.

C.6 Instruks for overføring av personopplysninger til tredjeland

Databehandleren kan kun overføre personopplysninger til tredjeland dersom behandlingsansvarlig har skriftlig samtykket til slik overføring, og det foreligger et lovlig grunnlag for overføring.

Hvis ikke den behandlingsansvarlige i Vilkårene eller etterfølgende gir en dokumentert instruks som gjelder overføring av personopplysninger til et tredjeland eller internasjonal organisasjon, kan ikke databehandleren, innen rammene av Vilkårene, gjennomføre slike overføringer.

C.7 Prosedyrer for den behandlingsansvarliges revisjoner, herunder inspeksjoner, av behandlingen av personopplysninger som er overlatt til databehandleren

Ingen utover det som er regulert i personvernforordningen (GDPR) artikkel 28.

8.18 Vedlegg D: Partenes regulering av andre forhold

Følgende endringer skal gjøres i Vilkårene:

Punkt 8.6.6 skal utgå.

I punkt 8.8.2a slettes «og når det er mulig, senest 72 timer».

I punkt 8.9.2 skal «om mulig skje innen 24 timer» erstattes med «uten ugrunnet opphold».

Krav knyttet til databehandling er omfattet av de samme ansvarsreguleringer og ansvarsbegrensninger som følger av Hovedavtalen.

Pureservice gjør oppmerksom på at dersom Kunden gir egne kunder eller samarbeidspartnere tilgang til løsningen, skjer dette under Kundens fulle ansvar som behandlingsansvarlig. Egen regulering må etableres dersom slike tredjeparter utøver selvstendig behandlingsansvar.

Endringslogg

Dato	Versjon	Endret / oppdatert / nytt	Gyldig fra
26.6.2025	2.8	Endret: 1.7 Presisert at kunde er ansvarlig for å oppdatere kontaktinformasjon 4.1 Presisert grense for API-kall 8.15 Utvidet dekning i A.4 8.18 Presisert kundes ansvar som behandlingsansvarlig	26.6.2025
15.10.2024	2.7	Endret: 1.3 Forenklet tekst, presisert at eventuelle endringer gjelder fra neste fornyelse 8 Rettet opp referanser	
24.09.2024	2.6	Rettet skrivefeil Sinch AB	24.09.2024
01.08.2024	2.5	Endret: 8.4 Presisert punkt om endring og varsling av endring av underleverandør Endret 8 Databehandleravtalen er byttet ut med standard avtale anbefalt av Datatilsynet	01.08.2024
05.02.2024	2.4	Endret: Ryddet i definisjon og omtale av kundes data: «kundedata» 5.2 Fjernet krav til antall brukere for tilgang til Customer Success 8.11 Korrigert skrivemåte firmanavnet til Microsoft Generelle språkendringer som ikke endrer innhold Byttet ut «Pureservice» med «tjenesten» der det er relevant	05.02.2024
18.10.2023	2.3	Endret: 3.2 Presisert at tjenesten leveres gjennom datasentre i Norge Generelle språkendringer og kapittelreferanse som ikke endrer innhold	18.10.2023
02.10.2023	2.2	Endret: 2.6 Presisert uttrekk av statistikker og bruksdata 6 Rettet telefonnummeret til Pureservice Support 6 Endret responstid fra 4 til 2 timer Nytt 1.8 Lagt til punkt om taushetsplikt 7 Nytt kapittel Konsulentoppdrag	02.10.2023
21.2.2023	2.1	Endret: 1.1 Lagt inn definisjon av «Abonnement» 1.2 Byttet ut «Tjenesten er gyldig ...» med «Avtalen er gyldig ...» 2.1 Skrevet om og presisert teksten som beskriver bruksrett 2.1/2.2 Endret fra ordet «disposisjon» til «bruk» 5 Lagt inn tjenestebeskrivelse for Customer Success 5 Pureservice Support er nå kapittel 6 6 Oppdatert lenke til Pureservice kurs 6 Presisert tekst om feilretting og hva som dekkes av avtalen	22.2.2023
05.01.2023	2.0	Endret: 1.1 Org.nr for virksomheten 3.2 Spesifisert lokasjon datasentre 3.5 Oppdatert beskrivelse av Pureservice infrastruktur 3.13 Spesifisert at Pureservice kan aksesseres også gjennom mobilapp 4.2 SLA gjelder ikke Pureservice testinstans Mindre tekstlige endringer/presiseringer	05.01.2023

For tidligere endringer vennligst ta kontakt med Pureservice.