PURESERVICE TJÄNSTEAVTAL

Innhold

pureservice

1 Allmänt

1.1 Definitioner

”Tjänsteavtalet” och ”Huvudavtalet” syftar på detta avtal.

”Pureservice” syftar på Pureservice AS, org.nr 929 782 216.

”Kund eller kunden” syftar på den organisation som har undertecknat avtalet.

”Pureservice Support” syftar på teamet inom Pureservice som arbetar med att lösa kundens problem och/eller frågor relaterade till tjänsten.

”Händelse” betyder omständigheter som resulterar i brott mot avtalad tjänstenivå.

”Tjänst” syftar på Pureservice-tjänsten och/eller programvaran i enlighet med avtal.

”Tjänstenivå” beskriver de standarder som Pureservice arbetar mot och som mäter nivån på den tjänst som erbjuds enligt beskrivningen nedan.

”Uppdrag” syftar på ett arbete som Pureservice ska utföra för Kunden.

”Uppdragsavtal” beskriver ett specifikt uppdrag, inklusive önskat resultat, plan för genomförande och uppskattad omfattning.

”Kreditering” är en procentuell andel av månadsavgiften som betalas för tjänsten för en tjänstenivå som inte uppfyller kraven i detta avtal.

”Abonnemang” är ett avtal mellan Kund och Pureservice, där Kund förbinder sig att betala för Tjänsten under en definierad tidsperiod.

”Kunddata” omfattar allt som laddas upp eller lagras i samband med användning av tjänsten.

1.2 Avtalets giltighet

Avtalet omfattar användning av tjänsten och tillhörande tjänster. Genom att ta tjänsten i bruk godkänner kunden detta avtal.

Om kunden inte godkänner villkoren kan tjänsten inte tas i bruk.

Avtalet är giltigt så länge kunden har ett aktivt abonnemang. Övriga villkor finns i Pureservice Standardvillkor.

1.3 Ändring av avtalet

Detta avtal ersätter alla tidigare tjänste- och licensavtal. Tillägg till eller avvikelser från detta avtal är endast giltiga om skriftligt avtal med hänvisning till detta avtal föreligger.

Pureservice kan ändra avtalsvillkoren med verkan från första avtalsförnyelse.

1.4 Betalningsvillkor

Som del av avtalet godkänner Kunden att betala ersättning för tjänsten i enlighet med gällande priser och Pureservice Standardvillkor.

Pureservice kan begränsa tillgången till eller avsluta tjänsten om betalning uteblir.

1.5 Uthämtning av data från tjänsten

Kunden kan under avtalsperioden kostnadsfritt hämta ut egna data (kunddata) från systemet. Pureservice erbjuder databaskopiering ("databasdump") kostnadsfritt. Om Pureservice ska bistå

med ytterligare datautdrag kommer kostnaden att debiteras kunden enligt gällande timpriser. Efter avtalets upphörande kommer Pureservice att avaktivera tillgång och radera kunddata. Data som har raderats kan vara omöjliga att återställa.

1.6 Misskötsel och sanktioner

Vid väsentlig misskötsel av Kundens förpliktelser, inklusive betalningsdröjsmål som överstiger 30 dagar, ska Pureservice skriftligen meddela Kunden med en rimlig frist för att rätta till förhållandet – normalt inte kortare än 10 arbetsdagar.

Om misskötseln inte är åtgärdad inom fristen kan Pureservice efter eget val:

– debitera dröjsmålsränta enligt lagen om dröjsmålsränta, och/eller

– med 5 arbetsdagars skriftligt varsel tillfälligt stänga tillgången till tjänsten tills betalning sker, och/eller

– häva avtalet med 30 dagars skriftligt varsel.

Stängning med omedelbar verkan utan föregående varsel kan endast ske vid dokumenterat missbruk av tjänsten som utgör ett säkerhetshot, eller vid grovt brott mot användningsrättsbestämmelserna i punkterna 2.1, 2.2 och 2.3.

Om Pureservice väsentligt missköter sina förpliktelser enligt avtalet ska Kunden skriftligen meddela Pureservice med rimlig frist för att rätta till förhållandet. Om rättelse inte sker inom fristen kan Kunden:

– kräva proportionellt prisavdrag, och/eller

– häva avtalet med omedelbar verkan.

Vid hävning till följd av Pureservices misskötsel ska Kunden krediteras en proportionell andel av förutbetalda abonnemangsbelopp för återstående avtalsperiod.

1.7 Register för avisering

Pureservice för register över kontaktpersoner hos kunden. Kontaktpersoner i registret aviseras per e-post eller på andra lämpliga sätt om ändring av avtalsvillkor, avisering om misskötsel av avtal och andra relevanta meddelanden.

Standarduppföring i registret är kontaktperson hos kunden som har undertecknat avtalsdokumenten med Pureservice.

Kunden är ansvarig för att uppdatera kontaktinformation i Tjänsten eller meddela Pureservice Support om kontaktpersoner eller kontaktinformation i registret ska ändras eller läggas till.

Pureservice är inte ansvarig för att aviseringar och meddelanden inte når kunden om kunden inte har meddelat detta.

1.8 Tystnadsplikt

All information som utbyts mellan parterna i samband med leverans och konsumtion av Tjänsten är konfidentiell information.

Kund och Pureservice förbinder sig att inte lämna ut till tredje part någon form av information som mottagits från den andra parten i samband med aktiviteter eller arbete relaterat till Tjänsten.

Denna förpliktelse kvarstår även efter att Abonnemanget har upphört.

Tystnadsplikten gäller inte för information som är:

– Offentligt känd när informationen lämnas,

– I den mottagande partens kännedom innan informationen överlämnades.

Bestämmelsen hindrar inte användningen av Kundens namn och/eller logotyp som anges i punkt 1.11.

1.9 Lagval

Detta Avtal och tvister som har uppstått till följd av detta, ska regleras och tolkas i överensstämmelse med norsk rätt.

1.10 Konflikter

Oenighet om verkan, innehåll eller genomförande av Avtalet ska försökas lösas genom förhandlingar. Leder inte förhandlingarna fram, kan vardera parten kräva att saken avgörs vid de allmänna domstolarna.

Om parterna avtalar det, ska saken avgöras genom skiljedom enligt Lag av 14.05.2004 nr. 25: Lag om skiljedom (norsk: *Dersom partene avtaler det, skal saken avgjøres ved voldgift etter Lov av 14.05.2004 nr. 25: Lov om voldgift*).

Om parterna önskar konfidentiell behandling av skiljedomsärendet, inklusive skiljedomstolens avgörande med motiv, ska detta avtalas skriftligen mellan parterna samtidigt som skiljedom avtalas.

Ärendet ska föras där Pureservice har sin affärsadress när ärendet påbörjas vid domstolen eller skiljedomstolen.

1.11 Marknadsföring och referenser

Kunden ger Pureservice rätt att använda Kundens namn och logotyp i Pureservices marknadsföring enbart för att identifiera Kunden som användare av tjänsten. Användningen kan ske i referenslistor, kundcase, presentationer, anbud/erbjudanden, webbplatser och sociala medier. Pressmeddelanden och citat från Kundens anställda kräver skriftligt förhandsgodkännande från Kunden. Kunden kan när som helst skriftligen reservera sig mot fortsatt användning; sådan reservation gäller framåt i tiden.

Denna rätt gäller under avtalsperioden och i upp till 12 månader efter upphörande.

2 Användning av tjänsten

2.1 Användningsrätt

Kunden har en icke-exklusiv och begränsad användningsrätt till tjänsten.

Användningsrätten ger Kund tillgång till – och rätt att använda – de användarlicenser, moduler, applikationer, integrationer, API och eventuella andra tillägg som Kund abonnerar på.

Användarlicenser gäller för samtidig användning där samtidig användning definieras som aktivitet i lösningen under en klocktimme.

I de fall kunden har flera instanser av tjänsten beräknas samtidig användning per instans isolerat, som sedan läggs samman till ett totalbehov. Pureservice förbehåller sig rätten att informera vid underlicensiering.

Att aktivt utnyttja en licens på två eller flera sessioner anses som brott mot licensavtalet.

Kunden har inte rätt att överlåta, hyra ut, leasa, låna ut eller på annat sätt erbjuda andra rätt att på något sätt disponera över tjänsten, licenskoder och/eller tillhörande dokumentation, utan skriftligt och uttryckligt förhandsmedgivande från Pureservice.

Användningsrätten upphör från den dag Kund inte längre har ett aktivt abonnemang.

2.2 Installation, framställning av exemplar, dekompilering m.m.

Om tjänsten installeras lokalt (hos kund eller kundens driftsleverantör) ger licensen en rätt att installera och använda tjänsten på en enda server (fysisk eller virtuell).

Nödvändiga tilläggskomponenter (integration mot e-post, Active Directory, datalyssnare, serviceportal, o.l.) installeras vid behov.

Utöver vad som är nödvändigt för laglig användning av tjänsten med tillhörande dokumentation, har kunden inte rätt att framställa exemplar av varken programvara, användardokumentation eller annat material som följer denna, oavsett om det är elektroniskt eller pappersbaserat.

Kunden har rätt att framställa säkerhetskopior av programvara i den utsträckning det är nödvändigt för utnyttjandet, och i enlighet med tvingande lag.

Kunden har inte rätt att dekompilera (plocka isär) programkoden i syfte att tillägna sig de tekniker som har använts av Pureservice.

Kunden har inte rätt att ändra, redigera och/eller skapa härledda arbeten av programvara (till exempel ta bort fasta designmallar som Pureservice eller Pureservice logotyp).

2.3 Ändringar i tjänsten

Kunden har inte möjlighet eller rätt att göra ändringar i tjänsten om detta inte är skriftligen avtalat mellan Pureservice och kunden.

Detta inkluderar innehåll i skräddarsydda arbetsflöden.

2.4 Tredje parts programvara

Kunden måste själv bekosta eventuella övriga programvarulicenser som t.ex. serveroperativsystem, databaser, etc.

2.5 Kunddata

Kunddata förblir kundens egendom och kundens ansvar. Kunddata som är lagrade i tjänsten kommer att behandlas i form av lagring, flyttning, säkerhetskopiering och analys för att på bästa möjliga sätt kunna skydda kunddata och för att kunna förbättra tjänsten.

Pureservice kommer i allt arbete med att hantera kunddata att vidta nödvändiga steg för att säkerställa konsistens, integritet och tillgänglighet.

Om inte det föreligger misskötsel av detta avtal, kommer data inte att kunna tas bort från tjänsten utan skriftligt samtycke från kunden.

2.6 Personuppgifter

Kunden godtar som del av detta avtal att Pureservice kan få tillgång till, frambringa och lagra information kopplad till användning av tjänsten, inklusive information och data som Pureservice samlar in kring användningen av tjänsten när detta anses nödvändigt för att operera i enlighet med vid var tid gällande lagar och regler.

Pureservice kan dra ut statistik och användningsmönster av anonymiserade data.

Sådan statistik och användningsmönster kan lagras antingen på Pureservices servrar, servrar som Pureservice disponerar i en molntjänst eller i relevanta nättjänster.

Det är Pureservices ansvar att säkerställa tillfredsställande säkerhet kring dessa data.

Som med alla leverantörer av molntjänster, kommer Pureservice att behöva följa påbud från rättsliga instanser för lagring av data i datacenter.

Pureservice kommer att vara förpliktigad att följa påbud för tillgängliggörande av information eller kunddata kopplat till formella undersökningar eller stämningar.

För Pureservice molntjänst se kapitel 8 Biträdesavtal för personuppgiftsbehandling med Pureservice.

För Pureservices personuppgiftspolicy se: https://Pureservice.com/trust/datahandtering-og-personvern-i-Pureservice-i-skyen

2.7 Ansvarsbegränsningar

Den totala ersättning Kunden kan kräva under hela avtalsperioden är begränsad till ett belopp som motsvarar den ersättning Kunden har betalat de senaste 12 månaderna innan den skadevållande handlingen/misskötseln uppstod.

Kunden kan inte kräva ersättning för indirekta förluster. Indirekta förluster omfattar, men är inte begränsade till, förlorad vinst av varje slag, förlorade besparingar eller krav från tredje parter, inklusive krav från tredjepartsleverantör till följd av Kundens brott mot tredjepartsvillkor, samt dessutom annat som räknas som indirekt förlust enligt norsk rätt.

Ersättningsbegränsningen gäller dock inte om Pureservice eller någon som Pureservice svarar för, har visat grov oaktsamhet eller uppsåt.

Andra sanktioner ska avräknas från eventuell ersättning för samma förhållande.

2.8 Immateriella rättigheter

Pureservice har fullständig äganderätt, upphovsrätt, patent- och mönsterrätt och alla övriga befintliga och framtida rättigheter kopplade till alla former av dataprogram, integrationer, applikationer, databaser, dokumentation och liknande.

Pureservice har äganderätt och alla immateriella rättigheter till eventuella förslag från kunden till ändring av befintliga Pureservice produkter och tjänster och/eller förslag till nya produkter eller tjänster, oavsett förslagets form och/eller innehåll. Sådana rättigheter tillfaller Pureservice vederlagsfritt, om inte annat skriftligen och uttryckligen avtalas i det enskilda fallet.

2.9 Överlåtelse

Pureservice har rätt att överlåta eller på annat sätt överföra sina rättigheter och/eller skyldigheter enligt detta avtal till tredje part.

Personuppgiftsansvarig ska aviseras senast 90 dagar före överlåtelsen så att avtalet kan sägas upp i enlighet med gällande villkor.

3 Tjänstebeskrivning

3.1 Introduktion

Pureservice erbjuder Service Management-tjänst. Tjänsten görs tillgänglig för användarna via webbläsare eller en mobilapp.

Pureservice följer etablerade bästa praxis för processtöd, affärsfunktionalitet, säkerhet och kvalitet i leveransen.

3.2 Service design

Tjänsten levereras på två sätt;

– Som en molntjänst (SaaS – Software-as-a-Service). Molntjänsten levereras via datacenter i Sverige. Lösningen levereras på dedikerade servrar eller på en gemensam plattform med full dataseparation

– Installerad på kundens egna servrar

Tjänsten levereras med möjlighet till autentisering mot kundens katalogtjänst (Entra ID, CRM-system eller motsvarande) för att förenkla åtkomsten till lösningen och administrationen av slutanvändare/kunder.

Pureservice använder en underleverantör som värd för att erbjuda tjänsten som en molntjänst. Pureservice är ansvarig för tjänsten som levereras av underleverantör på samma sätt som om Pureservice själv stod för leveransen. Tjänsteleveransen levereras i enlighet med ingått SLA-avtal som säkerställer optimal prestanda och tillgänglighet för kunden.

3.3 Uppdateringar

Pureservice kommer automatiskt att verifiera kundens version av tjänsten, samt underhålla och uppdatera systemet. För större uppdateringar kommer Pureservice att avisera kunden i rimlig tid innan uppdateringen görs. Mindre uppdateringar kan göras utan närmare avisering. Pureservice kan inte garantera att uppdateringar i tjänsten stöder de vid var tid gällande systemen som lösningen ursprungligen implementerades på och integrerades med.

3.4 Pureservice Continuous Delivery

Pureservice Continuous Delivery säkerställer att tjänsten alltid körs på senaste versionen.

URL mot https://*.pureservice.com måste vara tillgänglig från applikationsserver.

3.5 Pureservice OnPremise infrastruktur

När tjänsten installeras på kundens egna servrar, består infrastrukturen av följande huvudkomponenter;

– Applikationsserver

– Databasserver - för lagring av alla data och konfigurationer i tjänsten

– E-postserver - som möjliggör mottagning och utsändning av e-post kopplat till registrering och uppföljning av ärenden.

3.6 Installation driftad av tredje part

Dedikerade instanser av applikationsserver och databasserver kan implementeras i driftscenter hos tredje part och driftas och underhålls i enlighet med ingångna avtal mellan kunden och tredje part.

Kostnaden för driftstjänster från tredje part bärs fullt ut av kunden. Eventuella tilläggskostnader i samband med uppsättning, konfigurering, förvaltning och liknande bärs också av kunden.

3.7 Kundens ansvar för Pureservice molntjänst

- Administrera konfigurerbara data i tjänsten (användare, användargrupper, rättigheter, kategoriseringar, arbetsflöden, zoner, osv)
- Säkerställa att användare har nödvändiga nätverksåtkomster och tillgång till tjänsten på internet
- Säkerställa att nödvändiga lokala tjänster (Active Directory sync, e-posttjänst, etc.) körs och är tillgängliga för tjänsten
- Installera och underhålla stödd klientprogramvara för åtkomst till tjänsten.

3.8 Kundens ansvar för Pureservice lokalt installerat

- Administrera konfigurerbara data i tjänsten (användare, användargrupper, rättigheter, kategoriseringar, arbetsflöden, zoner, osv)
- Säkerställa att nödvändiga lokala tjänster (Active Directory sync, e-posttjänst, etc.) körs och är tillgängliga för tjänsten
- Tillgängliggöra relevanta tjänster på internet (genom DMZ eller liknande) om användare ska ha tillgång till självbetjäningsportal och/eller via mobilapp
- Installera och underhålla stödd klientprogramvara för åtkomst till tjänsten
- Installera uppgraderingar när dessa görs tillgängliga från Pureservice
- Säkerhetskopiera data

3.9 Pureservices ansvarsområden för molntjänsten

- Säkerhetskopiera data
- Uppgradera till nya versioner

3.10 Säkerhet

Pureservice utvecklar, testar och verifierar tjänsten baserat på riktlinjerna i ”OWASP top 10”.

SaaS-tjänsten körs i Microsoft Azure som är SOC 2 Type 2 Compliant och ISO 27001:2013 certifierad i enlighet med ISO 27002 best practices. Se Microsoft Trust Center för ytterligare information.

3.11 Krypterade kunddata

SaaS-tjänsten använder sig av kryptering för att säkra kunddata. Detta gäller även för användarhemligheter som en administratör i lösningen kommer att använda för att koppla upp mot aktuell e-postserver. Användarhemligheten används endast i sitt dekrypterade tillstånd för att upprätta koppling mot e-postservern.

3.12 Självbetjänad administration och konfiguration

Pureservice ger kunden möjlighet att själv administrera och konfigurera en rad nyckelaspekter av tjänsten. Självbetjäning sker via standard webbgränssnitt.

3.13 Åtkomst för användare och applikationer

Tjänsten kan nås via standardwebbläsare, Pureservice mobilapp eller programmatiskt via tjänstens API:er för anpassningar och integrationer. Vilka webbläsare som vid var tid stöds finns på www.pureservice.com. Pureservice rekommenderar att senaste stödda versionen av de olika webbläsarna används för att få fullt utbyte av tjänsten.

3.14 Katastrofberedskap Pureservice molntjänst

Tjänsten körs i datacenter som är byggda för att erbjuda hög tillgänglighet och driftas utifrån principer som ska minimera nedtid i tjänsten kopplat till drift och underhåll.

Omständigheter kopplade till hårdvaru- och mjukvarufel, katastrofer och mänskliga fel kan påverka tjänstens tillgänglighet.

Pureservice har därför implementerat rutiner för katastrofberedskap som ska hantera risk för att säkerställa tjänstens tillgänglighet.

3.15 Flytta från molntjänst till egna servrar, och vice versa

Pureservice möjliggör byte av användning av tjänsten från molntjänst till installation på egna servrar, och vice versa. En servicekostnad kan tillkomma i samband med en sådan flytt. För detaljer vänligen kontakta Pureservice.

4 Tjänstenivå (SLA) Pureservice molntjänst

4.1 Acceptabel användning

Kunden måste följa krav på konfiguration, använda stödd plattform och följa villkoren beskrivna i tjänstebeskrivningen för att detta avtal om tjänstenivå (SLA) ska gälla.

För att säkerställa stabil och god prestanda för alla kunder, är det en gräns på 100 API-anrop per minut per kund. Om denna gräns överskrids, kan ytterligare API-förfrågningar bli tillfälligt blockerade.

4.2 SLA exkluderingar

Denna SLA gäller inte för prestanda eller tillgänglighet;

– Tjänsten installerad på Kundens egna servrar eller hos tredje part
– På grund av faktorer utanför Pureservices kontroll
– Till följd av händelser eller brist på händelse från kunden eller tredje part
– Orsakad av användning av tjänsten utan att ta hänsyn till råd från Pureservice om ändrad konfiguration eller användning av tjänsten
– I samband med planerat underhåll
– I samband med beta-testning eller provtid
– För testinstans.

4.3 Kreditering av tjänsteavgift

– Sättet och metoden för beräkning av krediteringsbelopp är beskrivet nedan.
– Kreditering av tjänsteavgift är enda finansiella ersättning vid överträdelse av SLA.
– Tjänsteavgift krediterad i en kalendermånad ska under inga omständigheter överstiga kundens månatliga tjänsteavgift.
– Kreditering gäller inte för engångsavgifter kopplade till leverans av tjänsten.
– Kreditering förutsätter att kunden meddelar Pureservice Support när nedtid inträffar.
– Rätten till kreditering förfaller om kunden inte åberopar detta skriftligen inom 4 veckor efter nedtid.

4.4 Upptidsmätning per månad

”Nedtid” definieras som tiden när ingen av kundens användare kan logga in och använda tjänsten i enlighet med tjänstebeskrivningen. Nedtid omfattar inte tidsperioder när tjänsten inte är tillgänglig som resultat av planerad nedtid kopplad till underhåll eller uppgradering av tjänsten, eller ändringar avtalade med kunden.

”Planerad nedtid” definieras som nedtid inom förhandsavtalade tidsfönster eller nedtid i samband med större systemuppgraderingar. Planerad nedtid anses inte som nedtid.

”Total tid” är total tid tillgänglig i en kalendermånad. ”Månatlig upptid%” reflekteras i formeln;

$$Månatlig\ upptid\% = \frac{Total\ tid\ -\ Nedtid}{Total\ tid}$$

4.5 Garanterad upptid

Månatlig upptid-%	Kreditering av tjänst
< 99.5%	25%
< 99%	50%
< 95%	100%

5 Customer Success

Avtalet inkluderar stöd för etablering och onboarding, samt löpande uppföljning när tjänsten är i drift/produktion.

5.1 Stöd för etablering och onboarding

Etablering och onboarding har ett tudelat syfte: att göra tjänsten klar att användas, och att stödja och förbereda Kunden att ta tjänsten i bruk.

Ansvarsfördelning, förberedelser och uppgifter beskrivs i dokumentet Etablering och onboarding av Pureservice. Detta dokument levereras till Kunden i god tid före uppstart av etablering och onboarding.

5.2 Löpande uppföljning

När tjänsten är i drift / produktion erbjuder Customer Success rådgivning till Kund. Denna rådgivning inkluderar:

– Namngiven Customer Success Manager (CSM)

– Uppföljningsplan som avtalas med kund

– Möjlighet att boka tid i CSM:s kalender

– Rekommendationer och tips om användning av tjänsten

– Artiklar, videor och beskrivningar relaterade till tjänsten

Följande är inte inkluderat:

– Bistånd med att göra konfigurationsändringar, anpassningar eller utarbetande av arbetsflöde

– Kundanpassade integrationer

6 Pureservice Support

Avtalet ger möjlighet att kontakta Pureservice Support vid frågor eller felsituationer.

Avtalet gäller förfrågningar relaterade till den implementerade lösningen. Härunder ligger kombinationerna mellan produkt, databas, infrastruktur och eventuella integrationer.

Support ges på gällande och föregående delversion av tjänsten.

Felrättning på grund av Kundens förhållanden täcks inte av Pureservice Support och kan komma att debiteras Kund efter gällande timpriser.

Pureservice Support är bemannad via telefon, webbportalen och e-post under normal kontorstid, 08:00-16:00. Undantag är helger, helgdagar och allmänna högtidsdagar.

Pureservice Support Tlf +47 22 12 00 26

support@pureservice.com

https://support.pureservice.com/

Inkluderat i Pureservice Support	
Telefon- och e-postsupport på produktfrågor	■
Webbssupport – anmäla ärenden och se status via servicedesk.pureservice.com	■
Support på skandinaviskt språk	■
Responstid, tid från ärendet är anmält till ärendet är påbörjat	2 timmar
Antal personer som kan kontakta Pureservice Support	3
Kontaktpersoner ska ha deltagit i gratis användarutbildning, arrangerad av Pureservice: https://www.pureservice.com/kurs/	

7 Konsultuppdrag

Vid leverans av uppdrag gäller följande;

7.1 Förpliktelser

Kunden förpliktar sig att ge Pureservice tillgång till all information som anses nödvändig för att Pureservice ska kunna utföra uppdraget i enlighet med uppdragsavtalet.

Kunden tillhandahåller personal som kan ge nödvändig tillgång till system och applikationer så att Pureservice kan utföra sitt uppdrag.

Pureservice är å sin sida skyldig att inhämta alla upplysningar som anses nödvändiga för att leverera uppdraget som avtalat.

Uppstår förseningar, eller möjlighet till förseningar, i förhållande till avtalad framdriftsplan, ska Pureservice, utan oskäligt uppehåll, informera kunden.

Före slutförande av uppdrag ska Pureservice ha utfört en funktionell test i enlighet med uppdragsbeskrivningen.

7.2 Ändringar

Kunden har när som helst rätt att, genom skriftlig ändringsorder, göra ändringar i uppdrag genom att förändra Pureservices uppgifter eller framdriftsplan.

Detta förutsätter att ändringen ligger inom vad parterna med rimlighet kunde förvänta sig när uppdraget avtalades.

Pureservice ska snarast möjligt efter mottagande av en ändringsorder skriftligen meddela Kunden vilka verkningar ändringarna får för pris, framdriftsplan eller andra förhållanden.

Tidsåtgång utöver estimerad tid som beror på oförutsedda problem i Kundens driftsmiljö eller förhållanden hos Kunden som hindrar Pureservice från att genomföra uppdraget i enlighet med plan debiteras med samma priser som för utförande av uppdraget.

Vid avbokning av konsultdagar 3 dagar före planerat konsultdatum faktureras 50 % av beloppet. Vid avbokning 1 dag före faktureras hela beloppet.

Om uppdraget innebär att utveckla eller ändra en integration omfattar uppdraget endast gällande version av integrerade tjänster.

Eventuellt arbete kopplat till nya versioner av integrerade tjänster ska ersättas i enlighet med avtalade timpriser.

Förbättringar till följd av brister i utförandet av uppdraget ska utföras av Pureservice på egen bekostnad, förutsatt att Kunden har reklamerat inom rimlig tid och senast 3 månader efter bristen uppstod.

7.3 Acceptans

Kundens acceptans av uppdraget sker efter att uppdraget har meddelats slutfört av Pureservice.

Efter detta har Kund en 2 -två- veckors frist att meddela acceptans.

Om Pureservice inte har mottagit meddelande om att uppdraget inte är accepterat inom denna frist räknas uppdraget ändå som accepterat.

8 Personuppgiftsbiträdesavtal

Standardavtalsklausuler
Standardavtalsklausuler enligt artikel 28.3 i förordning (EU) 2016/679 (den allmänna dataskyddsförordningen) med avseende på personuppgiftsbiträdets behandling av personuppgifter

mellan

Kunden, enligt Huvudavtalet, se nedan

(personuppgiftsansvarig)

och

Pureservice

(personuppgiftsbiträde)

var och en ”part”, tillsammans ”parterna”

HAR ENATS OM följande avtalsklausuler (”klausulerna”) för att uppfylla kraven i den allmänna dataskyddsförordningen och säkerställa skyddet av den registrerades rättigheter.

8.1 Ingress

8.1.1 I följande avtalsklausuler (”klausulerna”) anges rättigheter och skyldigheter för den personuppgiftsansvarige och personuppgiftsbiträdet vid behandling av personuppgifter på uppdrag av den personuppgiftsansvarige.

8.1.2 Klausulerna har utformats för att säkerställa parternas uppfyllande av artikel 28.3 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

8.1.3 I samband med avtalet mellan den personuppgiftsansvarige och personuppgiftsbiträdet om leverans (Huvudavtalet), som dessa Villkor är knutna till, behandlar personuppgiftsbiträdet personuppgifter för den personuppgiftsansvariges räkning i enlighet med dessa Villkor.

8.1.4 Klausulerna ska ha företräde framför liknande bestämmelser i andra avtal mellan parterna.

8.1.5 Det finns fyra tillägg till klausulerna, vilka utgör en integrerad del av klausulerna.

8.1.6 Tillägg A innehåller information om behandlingen av personuppgifter, inklusive behandlingens syfte och art, typ av personuppgifter, kategorier av registrerade och behandlingens varaktighet.

8.1.7 Tillägg B innehåller den personuppgiftsansvariges villkor för personuppgiftsbiträdets användning av underleverantörer, samt en lista med underleverantörer som är godkända av den personuppgiftsansvarige.

8.1.8 Tillägg C innehåller den personuppgiftsansvariges anvisningar avseende behandlingen av personuppgifter, minimiuppsättningen säkerhetsåtgärder som krävs av personuppgiftsbiträdet, samt hur granskningar av personuppgiftsbiträdet och eventuella underleverantörer ska utföras.

8.1.9 Tillägg D innehåller bestämmelser för andra aktiviteter som inte omfattas av klausulerna.

8.1.10 Klausulerna och tilläggen ska lagras både skriftligt och elektroniskt av båda parterna.

8.1.11 Klausulerna undantar inte personuppgiftsbiträdet från skyldigheter som personuppgiftsbiträdet omfattas av enligt den allmänna dataskyddsförordningen eller annan lagstiftning.

8.2 Den personuppgiftsansvariges rättigheter och skyldigheter

8.2.1 Den personuppgiftsansvarige är ansvarig för att säkerställa att behandlingen av personuppgifter utförs i enlighet med den allmänna dataskyddsförordningen (se artikel 24 i den allmänna dataskyddsförordningen), tillämpliga dataskyddsbestämmelser i EU eller medlemsstaten1 och klausulerna.

8.2.2 Den personuppgiftsansvarige har rätt och skyldighet att besluta om syften och medel för behandlingen av personuppgifter.

8.2.3 Den personuppgiftsansvarige är bland annat ansvarig för att den behandling av personuppgifter som personuppgiftsbiträden ombeds utföra har rättslig grund.

8.3 Personuppgiftsbiträden ska följa anvisningarna

8.3.1 Personuppgiftsbiträden får enbart behandla personuppgifter enligt dokumenterade anvisningar från den personuppgiftsansvarige, såvida de inte är skyldiga att göra detta enligt unionens eller medlemsstatens lagstiftning som de omfattas av. Sådana anvisningar anges i tilläggen A och C. Efterföljande anvisningar kan också ges av den personuppgiftsansvarige under behandlingen av personuppgifterna, men sådana anvisningar ska alltid dokumenteras och lagras skriftligt samt elektroniskt i anslutning till klausulerna.

8.3.2 Personuppgiftsbiträdet ska omedelbart informera den personuppgiftsansvarige om dessa anvisningar enligt personuppgiftsbiträdets uppfattning inte följer den allmänna dataskyddsförordningen eller tillämpliga dataskyddsbestämmelser i EU eller medlemsstaten.

8.4 Sekretess

8.4.1 Personuppgiftsbiträdet ska endast bevilja tillgång till de personuppgifter som behandlas på uppdrag av den personuppgiftsansvarige för personer som är underställda personuppgiftsbiträdet och har åtagit sig att bevara sekretessen, eller som omfattas av en lämplig lagstadgad och behovsenlig tystnadsplikt. Förteckningen över de personer som har beviljats tillgång ska granskas regelbundet. Med granskningen som grund kan sådan tillgång till personuppgifter återkallas om tillgången inte längre är nödvändig. Personuppgifterna är därefter inte längre tillgängliga för dessa personer.

8.4.2 Personuppgiftsbiträdet ska på begäran av den personuppgiftsansvarige kunna visa att berörda personer som är underställda personuppgiftsbiträdet iakttar ovannämnda sekretess.

[1] Hänvisningar till ”medlemsstater” i klausulerna ska tolkas som hänvisningar till ”EES-medlemsstater”.

8.5 Säkerhet vid behandling

8.5.1 I artikel 32 i den allmänna dataskyddsförordningen anges att med beaktande av tidigare känd teknik, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt risken, av varierande sannolikhets- och allvarlighetsgrad, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.

Den personuppgiftsansvarige ska utvärdera riskerna avseende fysiska personers rättigheter och friheter vid behandlingen och vidta åtgärder för att minska dessa risker. Beroende på relevans kan dessa åtgärder inkludera följande:

a) Pseudonymisering och kryptering av personuppgifter.

b) Möjligheten att säkerställa fortlöpande sekretess, integritet, tillgänglighet och motståndskraft i systemen och tjänsterna för behandlingen.

c) Möjligheten att återställa tillgängligheten och tillgången till personuppgifter inom rimlig tid vid en fysisk eller teknisk incident.

d) Ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten i de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

8.5.2 Enligt artikel 32 i den allmänna dataskyddsförordningen ska personuppgiftsbiträdet även – fristående från den personuppgiftsansvarige – utvärdera riskerna för fysiska personers rättigheter och friheter vid behandlingen och vidta åtgärder för att minska dessa risker. Det innebär att den personuppgiftsansvarige ska förse personuppgiftsbiträdet med all information som krävs för identifiering och utvärdering av sådana risker.

8.5.3 Dessutom ska personuppgiftsbiträdet bistå den personuppgiftsansvarige i att säkerställa efterlevnad av den personuppgiftsansvariges skyldigheter enligt artikel 32 i den allmänna dataskyddsförordningen, genom att bland annat förse den personuppgiftsansvarige med information avseende tekniska och organisatoriska åtgärder som redan har genomförts av personuppgiftsbiträdet enligt artikel 32 i den allmänna dataskyddsförordningen, samt all övrig information som krävs för att den personuppgiftsansvarige ska kunna fullgöra sin skyldighet enligt artikel 32.

Om därefter – enligt den personuppgiftsansvariges bedömning – en minskning av identifierade risker kräver att ytterligare åtgärder vidtas av personuppgiftsbiträdet än de som redan har vidtagits enligt artikel 32 i den allmänna dataskyddsförordningen, ska den personuppgiftsansvarige ange att dessa ytterligare åtgärder ska vidtas i tillägg C.

8.6 Användning av underleverantörer

8.6.1 Personuppgiftsbiträdet ska uppfylla de krav som anges i artikel 28.2 och 28.4 i den allmänna dataskyddsförordningen om ett annat personuppgiftsbiträde anlitas (en underleverantör).

8.6.2 Personuppgiftsbiträdet får därför inte anlita ett annat personuppgiftsbiträde (underleverantör) enligt klausulerna utan ett föregående allmänt skriftligt tillstånd från den personuppgiftsansvarige.

8.6.3 Personuppgiftsbiträdet har den personuppgiftsansvariges allmänna tillstånd att anlita underleverantörer. Personuppgiftsbiträdet ska skriftligen informera den personuppgiftsansvarige om alla avsiktliga förändringar avseende tillägg eller utbyte av underleverantörer minst fyra veckor i förväg och därmed ge den personuppgiftsansvarige möjlighet att invända mot sådana förändringar innan berörd underleverantör anlitas. Längre tidsperioder för förhandsinformation om specifika underleverantörstjänster kan anges i tillägg B. Den förteckning över underleverantörer som redan har godkänts av den personuppgiftsansvarige återfinns i tillägg B.

8.6.4 Om personuppgiftsbiträdet använder en underleverantör för att utföra specifik behandling på uppdrag av den personuppgiftsansvarige, gäller samma dataskyddskyldigheter som anges i klausulerna för underleverantören via avtal eller annan rättsakt enligt EU:s eller medlemsstatens rätt, i synnerhet avseende tillräckliga garantier att vidta lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i klausulerna och den allmänna dataskyddsförordningen.

8.6.5 Personuppgiftsbiträdet ska därför kräva att underleverantören som ett minimum fullgör de skyldigheter som gäller för personuppgiftsbiträdet enligt klausulerna och den allmänna dataskyddsförordningen.

8.6.6 En kopia av ett sådant underleverantörsavtal och efterföljande ändringar ska – på begäran av den personuppgiftsansvarige – skickas till den personuppgiftsansvarige och därmed ge den personuppgiftsansvarige möjlighet att säkerställa att samma dataskyddsskyldigheter som anges i klausulerna gäller för underleverantören. Klausuler för verksamhetsrelaterade frågor som inte påverkar det rättsliga dataskyddsinnehållet i underleverantörsavtalet, behöver inte lämnas till den personuppgiftsansvarige.

8.6.7 Personuppgiftsbiträdet ska godkänna en klausul om berättigad tredje part med underleverantören där – i händelse av att personuppgiftsbiträdet går i konkurs – den personuppgiftsansvarige ska vara berättigad tredje part i underleverantörsavtalet och ha rätt att se till att den underleverantör som anlitats av personuppgiftsbiträdet följer avtalet, t.ex. genom att låta den personuppgiftsansvarige ge underleverantören i uppgift att ta bort eller återlämna personuppgifter.

8.6.8 Om underleverantören inte fullgör sina dataskyddsskyldigheter är personuppgiftsbiträdet helt ansvarigt inför den personuppgiftsansvarige när det gäller fullgörandet av underleverantörens skyldigheter. Detta påverkar inte de registrerades rättigheter enligt den allmänna dataskyddsförordningen – särskilt de som föreskrivs i artiklarna 79 och 82 i den allmänna dataskyddsförordningen – gentemot den personuppgiftsansvarige och personuppgiftsbiträdet, inklusive underleverantören.

8.7 Överföring av uppgifter till tredjeland eller internationella organisationer

8.7.1 All överföring av personuppgifter till tredjeland eller internationella organisationer av personuppgiftsbiträdet får endast utföras enligt dokumenterade anvisningar från den personuppgiftsansvarige och ska alltid utföras i enlighet med kapitel V i den allmänna dataskyddsförordningen.

8.7.2 Om överföringar till tredjeland eller internationella organisationer, vilka personuppgiftsbiträdet inte har anvisats att utföra av den personuppgiftsansvarige, krävs enligt EU:s eller medlemsstatens lagstiftning som omfattar personuppgiftsbiträdet, ska personuppgiftsbiträdet informera den personuppgiftsansvarige om det rättsliga kravet innan behandlingen utförs, såvida inte sådan information är förbjuden i lagstiftningen av hänsyn till allmänintresset.

8.7.3 Utan dokumenterade anvisningar från den personuppgiftsansvarige har personuppgiftsbiträdet därför inte rätt att inom ramen för klausulerna

a) överföra personuppgifter till en personuppgiftsansvarig eller ett personuppgiftsbiträde i ett tredjeland eller i en internationell organisation,

b) överföra behandlingen av personuppgifter till en underleverantör i ett tredjeland,

c) låta personuppgifterna behandlas av ett personuppgiftsbiträde i ett tredjeland.

8.7.4 Anvisningarna från den personuppgiftsansvarige avseende överföring av personuppgifter till ett tredjeland, däribland, om tillämpligt, det överföringsverktyg enligt kapitel V i den allmänna dataskyddsförordningen som de bygger på, ska anges i tillägg C.6.

8.7.5 Klausulerna får inte förväxlas med standarddataskyddsklausulerna enligt artikel 46.2 c och d i den allmänna dataskyddsförordningen, och klausulerna kan inte åberopas av parterna som ett överföringsverktyg enligt kapitel V i den allmänna dataskyddsförordningen.

8.8 Stöd till den personuppgiftsansvarige

8.8.1 Med beaktande av behandlingens art ska personuppgiftsbiträdet bistå den personuppgiftsansvarige med lämpliga tekniska och organisatoriska åtgärder när det är möjligt, i syfte att fullgöra den personuppgiftsansvariges skyldigheter att besvara förfrågningar om utövande av den registrerades rättigheter enligt kapitel III i den allmänna dataskyddsförordningen.

Detta innebär att datauppgiftsbiträdet så långt det är möjligt ska bistå den personuppgiftsansvarige vid den personuppgiftsansvariges efterlevnad av

a) rätten till information när personuppgifter samlas in från den registrerade,

b) rätten till information när personuppgifter inte har erhållits från den registrerade,

c) den registrerades rätt till tillgång,

d) rätten till rättelse,

e) rätten till radering (”rätten att bli bortglömd”).

f) rätten till begränsning av behandling,

g) anmälningsskyldighet avseende rättelse eller radering av personuppgifter och begränsning av behandling,

h) rätten till dataportabilitet,

i) rätten att göra invändningar,

j) rätten att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripet profilering.

8.8.2 Förutom personuppgiftsbiträdets skyldighet att bistå den personuppgiftsansvarige enligt klausul 6.4, ska personuppgiftsbiträdet dessutom, med beaktande av behandlingens art och den information som finns tillgänglig för personuppgiftsbiträdet, bistå den personuppgiftsansvarige för att säkerställa efterlevnad av

a) den personuppgiftsansvariges skyldighet att utan dröjsmål och vid behov, inte senare än 72 timmar efter upptäckten, meddela personuppgiftsincidenten till behörig tillsynsmyndighet i Sverige, Integirtetsskyddsmyndigheten (IMY), såvida inte personuppgiftsincidenten troligen inte innebär någon risk för fysiska personers rättigheter och friheter,

b) den personuppgiftsansvariges skyldighet att utan dröjsmål underrätta den registrerade om personuppgiftsincidenten, när personuppgiftsincidenten troligen resulterar i en hög risk för fysiska personers rättigheter och friheter,

c) den personuppgiftsansvariges skyldighet att utföra en bedömning av den påverkan som de planerade behandlingsåtgärderna får på skyddet av personuppgifter (en konsekvensanalys av dataskyddet),

d) den personuppgiftsansvariges skyldighet att samråda med den behöriga tillsynsmyndigheten i Sverige, Integirtetsskyddsmyn-digheten (IMY), före behandlingen där en konsekvensbedömning av dataskyddet visar att behandlingen skulle innebära en hög risk om inga åtgärder vidtas av den personuppgiftsansvarige för att minska risken.

8.8.3 Parterna ska i tillägg C ange de lämpliga tekniska och organisatoriska åtgärder som personuppgiftsbiträdet ska bistå den personuppgiftsansvarige med, samt omfattningen för det stöd som krävs. Detta avser de skyldigheter som anges i klausul 9.1 och 9.2.

8.9 Underrättelse om personuppgiftsincident

8.9.1 Vid en personuppgiftsincident ska personuppgiftsbiträdet, utan onödigt dröjsmål efter upptäckten, anmäla incidenten till den personuppgiftsansvarige.

8.9.2 Personuppgiftsbiträdets underrättelse till den personuppgiftsansvarige ska om möjligt äga rum inom 24 timmar efter det att personuppgiftsbiträdet har fått vetskap om personuppgiftsincidenten, för att göra det möjligt för den personuppgiftsansvarige att fullgöra skyldigheten att underrätta behörig tillsynsmyndighet om personuppgiftsincidenten, jfr artikel 33 i den allmänna dataskyddsförordningen.

8.9.3 I enlighet med klausul 9.2 a ska personuppgiftsbiträdet bistå den personuppgiftsansvarige med att underrätta behörig tillsynsmyndighet om personuppgiftsincidenten och bistå vid insamlingen av den information som anges nedan, vilket enligt artikel 33.3 i den allmänna dataskyddsförordningen ska anges i den personuppgiftsansvariges underrättelse till behörig tillsynsmyndighet:

a) Personuppgiftens art, inbegripet om så är möjligt de kategorier och ungefärliga antal registrerade som berörs, samt de kategorier och ungefärliga antal personuppgiftsposter som berörs.

b) De troliga konsekvenserna av personuppgiftsincidenten.

c) De åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att hantera personuppgiftsincidenten, inbegripet när så är lämpligt åtgärder för att mildra dess potentiella skadliga effekter.

8.9.4 Parterna ska i tillägg D fastställa allt som ska anges av personuppgiftsbiträdet som stöd när den personuppgiftsansvarige underrättar den behöriga tillsynsmyndigheten om personuppgiftsincidenten.

8.10 Radera och återlämna uppgifter

8.10.1 När personuppgiftsbehandlingen avslutas ska personuppgiftsbiträdet radera alla personuppgifter som har behandlats på uppdrag av den personuppgiftsansvarige samt intyga för den personuppgiftsansvarige att detta har gjorts eller återlämna alla personuppgifter till den personuppgiftsansvarige och radera befintliga kopior, såvida inte det enligt unionens eller medlemsstatens lagstiftning krävs att personuppgifterna lagras.

8.11 Granskning och inspektion

8.11.1 Personuppgiftsbiträdet ska för den personuppgiftsansvarige tillgängliggöra all information som krävs för att visa att de skyldigheter som anges i artikel 28 och i klausulerna efterlevs, samt underlätta och bidra till granskningar och inspektioner som utförs av den personuppgiftsansvarige eller annan granskare på uppdrag av den personuppgiftsansvarige.

8.11.2 Förfaranden som är tillämpliga vid den personuppgiftsansvariges granskningar och inspektioner som utförs av personuppgiftsbiträdet och underleverantörer, anges i tilläggen C.7 och C.8.

8.11.3 Personuppgiftsbiträdet ska ge de tillsynsmyndigheter som enligt tillämplig lagstiftning har tillgång till den personuppgiftsansvariges och personuppgiftsbiträdets lokaler, eller ombud som agerar på uppdrag av sådana tillsynsmyndigheter, tillgång till personuppgiftsbiträdets fysiska lokaler vid uppvisande av lämplig id-handling.

8.12 Parternas överenskommelse om andra villkor

8.12.1 Parterna får komma överens om andra klausuler avseende behandlingen av personuppgifter genom att exempelvis ange ansvarsskyldighet, så länge de inte strider direkt eller indirekt mot klausulerna eller den registrerades grundläggande rättigheter eller friheter och det skydd som anges i den allmänna dataskyddsförordningen.

8.13 Inledande och avslutande

8.13.1 Klausulerna börjar gälla det datum då båda parter har undertecknat dem.

8.13.2 Båda parterna ska ha rätt att kräva att klausulerna omförhandlas om ändringar i lagen eller klausulerna ger anledning till en sådan omförhandling.

8.13.3 Klausulerna ska gälla under den tid då tjänsterna för personuppgiftsbehandling erbjuds. Under den tid då personuppgiftsbehandlingen utförs kan klausulerna inte upphävas, såvida inte parterna har enats om andra klausuler som styr personuppgiftsbehandlingen.

8.13.4 Om personuppgiftsbehandlingen avslutas och personuppgifterna raderas eller återlämnas till den personuppgiftsansvarige i enlighet med klausul 11.1 och tillägg C.4, kan klausulerna upphävas skriftligen av någon av parterna.

8.13.5 Ingåendet av avtalet
Dessa villkor har ingåtts som en del av Huvudavtalet mellan den personuppgiftsansvarige och personuppgiftsbiträdet.

8.14 Kontakter/kontaktpunkter för den personuppgiftsansvarige och personuppgiftsbiträdet

8.14.1 Parterna kan kontakta varandra via följande kontakter/kontaktpunkter.

8.14.2 Parterna är skyldiga att omedelbart informera varandra om ändringar i kontakter/kontaktpunkter.

8.14.3 Samma kontaktpersoner som eventuellt anges i Huvudavtalet mellan den personuppgiftsansvarige och personuppgiftsbiträdet ska gälla.

8.15 Tillägg A: Information om behandlingen

A.1 Syftet med personuppgiftsbiträdets behandling av personuppgifter på uppdrag av den personuppgiftsansvarige:

Syftet med behandlingen är att fullgöra avtalet som har ingåtts mellan den personuppgiftsansvarige (kunden) och personuppgiftsbiträdet (leverantören), se vidare Huvudavtalet

A.2 Personuppgiftsbiträdets behandling av personuppgifter på uppdrag av den personuppgiftsansvarige ska huvudsakligen avse (behandlingens art):

Lagring och nödvändig behandling som en del av tjänsterna enligt Huvudavtalet. Huvudavtalet innebär att den personuppgiftsansvarige ska använda personuppgiftsbiträdets programvara för digital registrering, lagring och uppföljning av ärenden från den personuppgiftsansvariges anställda ("ärenden"). Personuppgiftsbiträdet ska tillhandahålla en dedikerad instans av tjänsten som levereras enligt Huvudavtalet till den personuppgiftsansvarige, samt utföra nödvändigt underhåll av systemet. Systemet ska användas för lagring av den personuppgiftsansvariges uppgifter relaterade till registrering och uppföljning av ärenden kopplade till egna anställda, kunder och deras anställda/kontaktpersoner samt andra relevanta kontakter.

A.3 Behandlingen inkluderar följande typer av personuppgifter om registrerade:

Namn, e-postadress och telefonnummer till användare samt annan information och uppgifter som den personuppgiftsansvarige lägger in i systemet som tillhandahålls enligt Huvudavtalet, till följd av användningen av systemet.

A.4 Behandlingen inkluderar följande kategorier av registrerade:

Anställda hos den personuppgiftsansvarige, den personuppgiftsansvariges kunder, kontaktpersoner hos kunder och leverantörer till den personuppgiftsansvarige samt andra som kunden ger tillgång till systemet, samt andra personer som omfattas av uppgifter som kunden lägger in i systemet.

A.5 Personuppgiftsbiträdets behandling av personuppgifter på uppdrag av den personuppgiftsansvarige får utföras när klausulerna börjar gälla. Behandlingen har följande varaktighet:

Vid upphörande av Huvudavtalet och detta personuppgiftsbiträdesavtal ska personuppgiftsbiträdet återlämna alla personuppgifter som mottagits för den personuppgiftsansvariges räkning och som omfattas av detta avtal. Sådan återlämning kan ske i form av utskrift och/eller kopia av kunddata i berörda databaser. Kostnaderna för detta bärs av den personuppgiftsansvarige.

Om inte den personuppgiftsansvarige önskar annat ska personuppgiftsbiträdet radera all data som innehåller uppgifter som omfattas av personuppgiftsbiträdesavtalet. Detta gäller även eventuella säkerhetskopior. Personuppgiftsbiträdet ska skriftligen dokumentera att raderingen har genomförts inom rimlig tid efter avtalets upphörande. Ovanstående gäller förutsatt att det inte föreligger någon lagstadgad skyldighet att behålla uppgifterna. Radering ska då ske så snart denna skyldighet inte längre gäller.

8.16 Tillägg B: Godkända underleverantörer

B.1 Godkända underleverantörer

När klausulerna börjar gälla godkänner den personuppgiftsansvarige att följande underleverantörer anlitas:

Namn	Land där behandlingen ska ske	Beskrivning av behandlingen
Microsoft Sverige AS (Azure), se mer: https://www.microsoft.com/en-us/trustcenter/	EES	Värd för att erbjuda programvaran i molnet (vid Pureservice SaaS)
Mailgun, ägt av Sich AB i Sverige	EES	Mottagning och leverans av e-post. Endast för kunder som inte har egen e-postserver

Den personuppgiftsansvarige ska när klausulerna börjar gälla godkänna användningen av ovannämnda underleverantörer för den behandling som beskrivs för parten. För ändringar av underbiträden, se punkt 8.6 i Villkoren.

8.17 Tillägg C: Instruktion avseende användningen av personuppgifter

C.1 Föremål/instruktion för behandlingen

Personuppgiftsbiträdets behandling av personuppgifter på uppdrag av den personuppgiftsansvarige ska utföras av personuppgiftsbiträdet som utför följande:

Se punkt A.2 ovan.

Personuppgiftsbiträdet ska i övrigt följa de skyldigheter som åläggs personuppgiftsbiträdet som sådan enligt dataskyddsförordningen, personuppgiftslagen samt annan relevant lagstiftning.

Personuppgiftsbiträdets personal kommer inte att ha tillgång till kunddata under normal drift, och har heller inget behov av det. Vid felsökning av tjänsten eller i samband med felsökning för den personuppgiftsansvarige har dev-ops-teamet tillgång till kunddata som lagras i tjänsten. Alla medlemmar i dev-ops-teamet har fått utökad utbildning i säkerhet och dataskydd.

Personuppgiftsbiträdet kan ta ut statistik och metadata om ärenden, exempelvis antal ärenden och aktiverade moduler, användarmönster med mera. Sådan statistik ska vara anonymiserad innan överföring till personuppgiftsbiträdets servrar och får inte innehålla personuppgifter. Sådan statistik och användarmönster kan lagras antingen på personuppgiftsbiträdets servrar, servrar som personuppgiftsbiträdet disponerar i en molntjänst eller i relevanta webbtjänster. Det är personuppgiftsbiträdets ansvar att säkerställa tillfredsställande säkerhet kring dessa data.

Som med alla leverantörer av molntjänster måste personuppgiftsbiträdet följa föreläggganden från offentliga myndigheter, åklagarmyndigheter med flera, avseende lagring av data i datacenter. Personuppgiftsbiträdet är förpliktigat att följa föreläggganden om tillgängliggörande av information eller kunddata kopplade till formella utredningar eller rättsprocesser.

Personuppgiftsbiträdet kan använda tjänstedata för att optimera lösningen och utveckla nya tjänster. Tjänstedata kan exempelvis vara om en avgränsad funktion i lösningen (Change och/eller SLA) är aktiverad eller inte och inkluderar inte personuppgifter eller känslig information.

C.2 Säkerhet vid behandling

Säkerhetsnivån ska vara anpassad till följande:

Personuppgiftsbiträdet ska säkerställa att lämpliga tekniska och organisatoriska åtgärder vidtas för att skydda personuppgifterna som behandlas enligt avtalet, med hänsyn till vad som är tekniskt möjligt, kostnaderna för skyddet, den behandling av personuppgifter som ska utföras samt risken för den personliga integriteten för de registrerade. Detta innefattar, beroende på vad som är nödvändigt och lämpligt för skyddet:

Organisatoriska åtgärder

- Det finns ett etablerat internkontroll-/styrningssystem för informationssäkerhet som är godkänt av ledningen och som är känt och implementerat i organisationen, med utbildning, regelbundna kontroller för att säkerställa att rutiner följs samt regelbunden revision (GDPR art. 32).
- Pureservice körs i ett datacenter som är SOC 2 Type 2 Compliant och ISO 27001:2013-certifierat enligt ISO 27002:s bästa praxis.
- Anställda på Pureservice är skyldiga att följa ett säkerhetsinstruktsionspaket och endast anställda med arbetsrelaterat behov har tillgång till produktionsplattformen.
- Utvecklingsteamet arbetar enligt SCRUM-metoden och använder GIT versionskontrollsystem. Ändringar testas i separata miljöer innan de godkänns för release till produktionsmiljön. Detta möjliggörs genom användning av separata uppdateringskanaler (dev, main, preview och release) i våra release-rutiner, och en uppdatering publiceras inte innan paketets integritet har

verifierats och testats. Dessa steg inkluderar också manuella godkännanderutiner. Automatiserade tester genomförs innan alla kanaler. Innan en uppdatering godkänns genomgår den en kvalitetskontroll i en separat QA-process.

– Pureservice DevOps-team uppdaterar regelbundet infrastrukturen vid behov. Ändringar som i särskilt hög grad påverkar kunder annonseras i nyhetsfunktionen i applikationen. Underhåll och uppdateringar på lägre infrastrukturnivå, t.ex. OS-uppdateringar och korrigeringar av fel i infrastrukturelement utförs automatiskt och regelbundet av Microsoft.
– Ändringar planeras och genomförs av DevOps-teamet. Teamet testar ändringar i lämplig miljö innan eventuella ändringar överförs till produktion. Alla planerade ändringar genomgår en riskbedömning i förväg.
– Pureservice har etablerat ett CSIRT (Computer Security Incident Response Team) som hanterar alla säkerhetsincidenter. Teamet undersöker typen av incident och vidtar nödvändiga åtgärder för att åtgärda dessa. Detta inkluderar även avisering till kundens huvudkontakt om kunddata kan ha påverkats, eller att en anmälan görs till dataskyddsmyndigheten om potentiella brott mot dataskyddsförordningen upptäcks.
– Pureservice har flera källor som kan leda till registrering av avvikelser. Exempel på detta är övervakning/larm, manuell analys av loggar eller kundanmälningar via vår servicedesk. Alla avvikelser registreras och behandlas vidare av DevOps eller CSIRT.
– Beredskap täcks av en 24/7-vaktplan och CSIRT.
– Aviseringar som rör sårbarheter som är av intresse för alla kunder publiceras i applikationen. Om en sårbarhet är kundrapporterad, meddelas detta först genom versionshistorik när sårbarheten är åtgärdad.
– Pureservice genomför årligen penetrationstest och säkerhetstest med extern leverantör. Tester baseras på OWASP topp 10.
– Den personuppgiftsansvarige eller dess representant kan genomföra penetrationstester på sin egen Pureservice-molninstans upp till en gång per år och måste godkännas i förväg genom att kontakta Pureservice support.

Tekniska åtgärder

– All data lagras i minst två fysiskt separerade databasinstanser för att säkerställa tillgänglighet. Multitenant-arkitektur med separata databaser per kundinstans.
– Alla databaser är krypterade vid lagring. Data krypteras under transport mellan användarenheten och Pureservice i molnet.
– Kontinuerlig övervakning av prestanda och tillgänglighet sker.
– Pureservice drivs och utvecklas av personal med kunskap och erfarenhet inom säkerhetsarbete.
– Pureservice utvecklar, testar och verifierar systemet baserat på riktlinjerna i OWASP topp 10. Externa säkerhetsrevisioner med penetrationstestning görs på nätverks- och applikationsnivå.
– Användarautentisering och åtkomstkontroll per instans.
– Kontinuerlig uppdatering av koden säkerställer att alla kunder alltid har uppdaterad funktionalitet och säkerhetsfunktioner.
– Säkerhetskopiering av all data sker kontinuerligt med en återställningsperiod på 30 dagar.
– Lösningen levereras på Microsoft Azure-plattformen, som är robust designad för att upprätthålla tillgänglighet hela tiden. Tjänsterna övervakas kontinuerligt med nödvändiga

varningsrutiner för att upprätthålla en acceptabel servicenivå enligt tjänsteavtalet. Säkerheten på molnplattformen (Azure) hanteras av Microsoft, mer information om åtgärderna finns här: https://www.microsoft.com/en-us/trustcenter/.

– Pureservice stödjer Single Sign-On för integration med företagets befintliga Identity Provider via OpenID Connect, SAML, OAuth 2.0, WS-Federation med flera. Om kunden exempelvis använder Entra ID som identitetsleverantör (IdP) styrs MFA, vitlistning, regelverk för åtkomster och avancerad åtkomstkontroll från Entra ID.
– Pureservice stödjer multifaktorautentisering genom integration med företagets befintliga Identity Provider.
– Pureservice uppdateras regelbundet med kod som tillför ny funktionalitet eller som åtgärdar kända fel. Uppgraderingar av Pureservice i molnet annonseras i nyhetsfunktionen i Pureservice och sker automatiskt vid angiven tidpunkt. Utvecklingsteamet genomgår utbildning i säker utveckling i samband med penetrationstest och säkerhetstest varje år och är kontinuerligt uppdaterat om hot definierade i till exempel OWASP topp 10-listan.
– Pureservice använder funktioner i Microsoft Azure Security Center för kontinuerlig säkerhetsövervakning av Pureservice i molnet.

Ytterligare information om organiseringen av säkerhetsarbetet och åtgärder finns beskrivet i vår CAIQ – se https://pureservice.com/trust

Utöver ovanstående genomför personuppgiftsbiträdet regelbundet säkerhetsrevisioner för system och liknande som omfattas av detta avtal. Revisionen kan innefatta granskning av rutiner, stickprovskontroller, mer omfattande platsbesök och andra lämpliga kontrollåtgärder.

Den personuppgiftsansvarige kan kräva att en genomgång och revision av tjänsten, system och dokumentation genomförs för att säkerställa att det är lagligt, och personuppgiftsbiträdet ska möjliggöra och bidra till sådana revisioner. Varje part står för sina egna kostnader vid revisioner. Om den personuppgiftsansvarige anlitar en extern revisor ska denne också bekosta denne.

Personuppgiftsbiträdet har dock rätt och skyldighet att fatta beslut om vilka tekniska och organisatoriska säkerhetsåtgärder som ska genomföras för att etablera den nödvändiga (och avtalade) säkerhetsnivån.

C.3 Stöd till den personuppgiftsansvarige

Personuppgiftsbiträdet ska så långt det är möjligt – inom ramen för det stöd som anges nedan – bistå den personuppgiftsansvarige i enlighet med klausul 9.1 och 9.2 genom att vidta följande tekniska och organisatoriska åtgärder:

Assistans från personuppgiftsbiträdet till den personuppgiftsansvarige ska följa den assistansplikt som åligger enligt dataskyddsförordningen och personuppgiftslagen.

Om personuppgiftsbiträdet får kännedom om otillåten åtkomst till den personuppgiftsansvariges data som lagras hos personuppgiftsbiträdet eller personuppgiftsbiträdets underleverantörer, ska personuppgiftsbiträdet utan onödigt dröjsmål:

1. informera om typen av dataintrång och berörda registrerade,
2. undersöka säkerhetsintrånget och ge den personuppgiftsansvarige detaljerad information om säkerhetsintrånget,
3. vidta och informera om ansvariga och rimliga åtgärder för att mildra effekterna av säkerhetsintrånget och begränsa skadorna.

Meddelanden om misstänkta säkerhetsintrång kan skickas till: personvern@pureservice.com, som då hanterar ärendet för personuppgiftsbiträdet. Sådan anmälan påverkar inte den personuppgiftsansvariges skyldighet att anmäla avvikelser/personuppgiftsincidenter till Datainspektionen och eventuellt till de registrerade.

Assistans från personuppgiftsbiträdet till den personuppgiftsansvarige utöver vad som följer av detta avtal och de skyldigheter som åligger personuppgiftsbiträdet enligt dataskyddslagstiftningen, ska utföras enligt personuppgiftsbiträdets gällande timpriser för assistans. Detta gäller uppgifter som att radera personuppgifter utöver vad som sker automatiskt eller vad den personuppgiftsansvarige kan göra via lösningen, ge insyn i personuppgifter utöver vad som kan göras via lösningen, bistå den personuppgiftsansvarige med riskbedömningar och dokumentation med mera.

C.4 Lagringsperiod/raderingsåtgärder

Se punkt A.5 ovan

C.5 Behandlingsplats

Behandlingen av personuppgifter enligt klausulerna får inte utföras på andra platser än följande, om inte ett skriftligt förhandstillstånd har getts av den personuppgiftsansvarige enligt villkorens punkt 8:

Behandlingen ska endast ske inom EES.

Platsen för underbiträdens behandling av personuppgifterna framgår av tabellen under punkt B1.

C.6 Instruktion om överföring av personuppgifter till tredjeland

Personuppgiftsbiträdet får endast överföra personuppgifter till tredjeland om den personuppgiftsansvarige har lämnat skriftligt samtycke till sådan överföring och det finns en laglig grund för överföringen.

Om inte den personuppgiftsansvarige i Villkoren eller därefter lämnar en dokumenterad instruktion som avser överföring av personuppgifter till ett tredjeland eller en internationell organisation, får personuppgiftsbiträdet inte, inom ramen för Villkoren, genomföra sådana överföringar.

C.7 Förfarandet vid den personuppgiftsansvariges granskningar och inspektioner av personuppgiftsbiträdets behandling av personuppgifter

Inga andra än vad som anges i Bestämmelserna.

8.18 Tillägg D: Parternas övriga avtalsvillkor

Följande ändringar ska göras i Villkoren:

Punkt 8.6.6 ska tas bort.

I punkt 8.8.2a tas frasen «och när det är möjligt, senast 72 timmar» bort.

I punkt 8.9.2 ska «om möjligt ske inom 24 timmar» ersättas med «utan onödigt dröjsmål».

Krav kopplade till personuppgiftsbehandling omfattas av samma ansvarsfördelning och ansvarsbegränsningar som följer av Huvudavtalet.

Pureservice uppmärksammar att om Kunden ger sina egna kunder eller samarbetspartner tillgång till lösningen, sker detta under Kundens fulla ansvar som personuppgiftsansvarig. En särskild reglering måste upprättas om sådana tredje parter utövar självständigt personuppgiftsansvar.

Ändringslogg

Datum	Version	Ändrat / uppdaterat / nytt	Giltigt från
22.4.2026	3.0	Ändrat 1.5 Förtydligat att Pureservice erbjuder databaskopiering kostnadsfritt 1.6 Reviderat punkten så att den är balanserad mellan Kund och Pureservice 3.15 Förtydligat att en servicekostnad kan tillkomma i samband med migrering 5 Uppdaterad beskrivning av Customer Success 7.2 Reviderat så att texten om avbokning av konsultdagar överensstämmer med Pureservice Standardvillkor	22.4.2026
22.10.2025	2.9	Nytt punkt: 1.11 Lagt till rätt att använda kundens namn och logotyp i marknadsföring Ändrat: 1.8 Förtydligat med hänsyn till punkt 1.11	22.10.2025
1.8.2025	2.8	Svensk version	1.8.2025

För tidigare ändringar vänligen kontakta Pureservice.