Bilaga specifikation över behandlingen av personuppgifter i samband med MoIntjänster och IT-Infrastrukturtjänster

Utgivet av IT&Telekomföretagen 2017

1. KONTAKTUPPGIFTER

	Leverantören	Kunden
Namn och organisationsnummer	Se huvudavtal	Se huvudavtal
Företrädare	Se huvudavtal	Se huvudavtal
Dataskyddsombud, om något		

2. INSTRUKTIONER

2.1 Kortfattad beskrivning av Tjänsten och ändamålen med behandlingen

Ange alla ändamål för vilka personuppgifter ska behandlas av leverantören:

Leverantören tillhandahåller moln och / eller driftstjänsterna Litium On Demand, Litium Growth Cloud och Litium Drift till kunden som specificerats i Avtalet. Vid leverans av Tjänsten kommer leverantören att behandla personuppgifter för kundens räkning. Syftet med behandlingen är bistå kunden i sitt åtagandet gentemot den registrerade.

2.2 Kategorier av personuppgifter

Ange vilka personuppgifter som ska behandlas av leverantören:

Namn, kontaktuppgifter, Ip-adresser, e-mail-addresser, köpinformation/orderinformation, telefonnummer

Ange vilka särskilda kategorier av personuppgifter som ska behandlas av leverantören (om några):

N/A

2.3 Kategorier av registrerade

Ange vilka kategorier av registrerade som leverantören kommer att behandla personuppgifter om och dess omfattning:

Kundens användare av Tjänsten, Administratörs-användare av Tjänsten.
Kundens webb-besökare(slutkunder).

2.4 Behandlingsaktiviteter (lagring, administrering, samkörning av register osv.)

Ange vilka behandlingar som kommer att utföras av leverantören:

Lagring, administrering, överföring, backup, felsökning, Insamling av data i samband med felsökning, uppsättning och konfigurering av produktion, test och utvecklingsmiljöer

2.5 Plats för behandling av personuppgifter

Ange alla länder där personuppgifter kan komma att lagras och/eller behandlas av leverantören:

Alla personuppgifter inom Tjänsten lagras och behandlas inom Sverige. Undantag för detta är stödprocesserna Kund och partner-Support, felsökning och test, där data kan komma att behandlas på andra platser enligt listning av underbiträden i punkt 4.

Artikelnummer: Alm_178

2.6 Användning i syfte att förbättra Tjänsten

Om leverantören ska ha rätt att behandla personuppgifter ”i syfte att utveckla och förbättra Tjänsten” ska detta uttryckligen framgå av nedanstående ifyllda tabell.

Specifikation över de kategorier av personuppgifter som får användas i syfte att förbättra tjänster som kunden har beställt (t.ex: namn, adress):
Namn, kontaktuppgifter, Ip-adresser, e-mailaddresser, köpinformation/orderinformation, telefonnummer
Dessa personuppgifter ska hämtas från följande behandlingar som leverantören utför för kundens räkning (t.ex: backup, lagring, felsökning):
Lagring, administrering, överföring, backup, felsökning, Insamling av data i samband med felsökning, uppsättning av produktion, test och utvecklingsmiljöer
Och får endast användas av leverantören i syfte att förbättra och/eller utveckla följande typer av tjänster eller kategorier av tjänster som kunden beställt (t.ex: leverantörens felhanteringsprocess):
Upprätthållande av Tjänsten, förbättring av Tjänsten och felhanteringprocessen

3. SÄKERHETSÅTGÄRDER

Ange alla organisatoriska och tekniska säkerhetsåtgärder som ska implementeras av leverantören (leverantörens interna säkerhetsföreskrifter ska finnas på den webbplats eller annan åtkomlig plats som är angiven i Specifikationen):

Inga speciella säkerhetsåtgärder utöver det som specificerats under punkt 3 nedan behöver implementeras för att leverantörens skall kunna utföra sin roll som personuppgiftsbiträde till kunden gällande behandling av personuppgifter i samband med Tjänsten.

3.1.1 Fysisk åtkomstkontroll

Åtgärder som förhindrar obehörigas fysiska tillgång till IT-system där behandling av personuppgifter sker:

Datahallar som används är inbrott-skyddade, kameraövervakade och bevakas av bevakningsbolag, endast behörig teknisk personal har tillträde. Passersystemet loggar alla passeringar.

3.1.2 Åtkomstkontroll avseende system

Åtgärder som förhindrar obehöriga att använda IT-system:

Administrationsgränssnitt och åtkomst till IT-System skyddas med rättighetssystem. Enbart leverantören och dess underleverantörer med rättighet till behandling av personuppgifter har access. Åtkomst för andra personuppgiftsbiträden så som kundens implementeringspartner ges enbart efter godkännande av kunden.

3.1.3 Åtkomstkontroll avseende personuppgifter

Åtgärder för att säkerställa att personer som är behöriga att använda IT- systemet endast bereds tillgång till personuppgifter som omfattas av personernas fastställda behörigheter:

Rättighetsstyrning i produkten gör att kundens utsedda administratörer kan styra detta.
Tilldelning av rättigheter för servrar där Tjänsten driftas ges av leverantören endast på skriftlig begäran från behörig person hos kunden.

3.1.4 Åtkomstkontroll vid överföringar

Åtgärder för att säkerställa att personuppgifter inte obehörigen kan läsas, kopieras, ändras eller raderas vid elektronisk överföring eller vid överföring eller lagring på lagringsenheter samt att mottagare kan identifieras och kontrolleras då överföring av personuppgifter sker via elektronisk överföring:

Tillgång till personuppgifter ges enbart genom Kundens godkännande. Kunden kan ge denna tillgång själv eller beställa tillgång av leverantören.
Vid administrering av IT-system används certifikat (TLS) för att säkra kommunikationen.
Administrering genom administrationsgränssnittet tillhandahåller kunden certifikat (TLS) för att säkra kommunikationen.

3.1.5 Kontroll över inmatning av personuppgifter

Åtgärder för att säkerställa att det i efterhand går att granska och avgöra om personuppgifter har matats in, ändrats eller raderats i IT-systemet och vem som har vidtagit åtgärden:

Loggning sker i plattformen vid inloggning om användaren har åtkomst av delar som innefattar personuppgifter.
Loggning på servernivå sker vid all administrering av IT-systemet.

3.1.6 Tillgänglighetskontroll

Åtgärder för att säkerställa att personuppgifter skyddas mot oavsiktlig förstörelse eller förlust:

Backup ingår enligt Avtalet för Tjänsten.

3.1.7 Särskiljningskontroll

Åtgärder för att säkerställa att personuppgifter som samlats in för olika ändamål kan behandlas separat:

Hanteras av kunden genom stöd i produkten där de olika ändamålen ligger i olika moduler som kan rättighetsstyras individuellt.

3.1.8 Lagringsregler

Åtgärder för att tillse att personuppgifter gallras under och efter avtalstiden när användningen inte längre är nödvändig för det ursprungliga ändamålet:

Hanteras av kunden genom stöd i produkten där de olika ändamålen ligger i olika moduler som kan rättighetsstyras individuellt.

Under avtalstiden: Så snart som möjligt och senast inom __ från det att kunden begärde att personuppgifterna skulle raderas.

Produkten innehåller funktionalitet som gör att gallring kan utföras av kunden, ingen gallring sker av leverantören.

Efter att avtalet har upphört att gälla: se punkten 8.2 i Biträdesavtalet.

Leverantören behåller inga personuppgiftsdata från Tjänsten efter avtalets upphörande.

3.1.9 Säkerhetsföreskrifter

Ange leverantörens interna säkerhetsföreskrifter som ska gälla för personuppgiftsbehandlingen, alternativt hänvisa till webbplats eller annan åtkomlig plats där dessa säkerhetsföreskrifter finns tillgängliga:

Litium delar inte sina säkerhetsföreskrifter publikt.
Mer info finns på https://www.litium.se/legal

3.1.10 Certifieringar m.m.

Ange eventuella certifieringsmekanismer eller uppförandekoder för dataskydd som leverantören innehar eller har åtagit sig att följa:

Inte aktuellt

(Vänligen notera att det idag inte finns en av Datainspektionen godkänd uppförandekod eller certifieringsmekanism som personuppgiftsbiträden kan välja att ansluta sig till)

4. PÅ FÖRHAND GODKÄNDA UNDERBITRÄDEN

Leverantören har rätt att använda följande underbiträden för att behandla personuppgifter inom ramen för Biträdesavtalet:

Namn	Plats för behandling (land)
DGC Access AB	Sweden
Microsoft Inc.	EU/EES Enligt val av kunden
Niteco Vietnam Company Limited	Vietnam (endast för Stödprocesserna Support, felsökning och test)