Underlag till konsekvensbedömning

avseende personuppgiftsbehandling

ITSL Hubs – Säkra meddelanden, SDK och Videomöten

Version 1.0 – Mars 2026

ITSL Solutions AB

1. Registerutdrag

1.1 Kan användare få registerutdrag?

Ja, ITSL Hubs har fullt stöd för att tillhandahålla registerutdrag i enlighet med artikel 15 i GDPR (den registrerades rätt till tillgång).

1.1.1 Teknisk förmåga

Hubs-plattformen bygger på Nextcloud-teknologi och har inbyggd funktionalitet för hantering av användardata. Följande personuppgifter kan exporteras per användare:

- **Användaruppgifter:** Namn, e-postadress, organisationstillhörighet, telefonnummer och annan kontaktinformation som registrerats i systemet.
- **Autentiseringsdata:** Inloggningsloggar med tidpunkt, IP-adress och inloggningsmetod (ej lösenord, dessa lagras enbart som hashvärden).
- **Aktivitetsloggar:** Händelseloggar kopplade till användarens handlingar, exempelvis filuppladdningar, meddelandehistorik och delningar.
- **Filer och dokument:** Allt material som användaren lagrat, inklusive filer i arbetsytor, skickade och mottagna SDK-meddelanden samt chatthistorik.
- **Metadata:** Eventuell metadata kopplad till användarens aktiviteter, exempelvis tidsstämplar och delade resurser.

1.1.2 Administrativ process

En begäran om registerutdrag hanteras enligt följande:

1. Den registrerade skickar begäran till den personuppgiftsansvariga organisationen (kunden/kommunen).
2. Kundadministratören kan via supporten begäraen export av den registrerades användardata.
3. Vid behov av support kan kunden kontakta ITSL som i egenskap av personuppgiftsbiträde bistår med utdrag av alla personuppgifter kopplade till den berörda användaren.
4. ITSLs supportpersonal har en manuell rutin som sammanställer data från de olika moduler som kunddata förekommer.
5. Utdragen levereras i maskinläsbart format (t.ex. JSON eller CSV) inom de tidsramar som GDPR föreskriver (utan onödigt dröjsmål och senast inom en månad).

Det finns en GDPR-modul som kan installeras som ger användaren möjlighet att via sitt eget konto begära och ladda ner sitt registerutdrag direkt. Den är dock inte implementerad i Hubs i dagsläget. Men kan kan läggas till på begäran

2. Överföring till externa mottagare

2.1 Kommer personuppgifterna att överföras till externa mottagare?

Personuppgifter överförs inte till externa mottagare utanför den avtalade leveranskedjan. All datalagring och behandling sker inom Sverige. Nedan beskrivs de aktörer som har en roll i leveransen och vilken typ av åtkomst de eventuellt har.

2.2 Secuva (driftleverantör)

Roll	Underleverantör för infrastruktur och drift (IaaS)
Förhållande	Personuppgiftsunderbiträde till ITSL Solutions AB
Typ av åtkomst	Secuva har fysisk och administrativ åtkomst till den underliggande infrastrukturen (hypervisor, nätverk, lagring) men INTE till applikationsdata eller personuppgifter i klartext. Hubs är en single-tenant-plattform och all kunddata krypteras med kundunika nycklar.
Datacenter	IP-Onlys datacenter i Hammarby och Sätra, Stockholm, Sverige. Ytterligare en katastrofåterhämtningsplats (DR) i skyddat bergrum i Sverige.
Avtal och krav	Personuppgiftsbiträdesavtal upprättat. Samma SLA-nivåer och säkerhetskrav som gäller för ITSL gentemot kund gäller även för Secuva. Secuvas datacenterpartner IP-Only/GlobalConnect uppfyller Tier-3-standard.
Överföring av PU	Nej. Secuva överför inte personuppgifter till tredje land eller till andra mottagare. All data stannar inom Sverige.

2.3 Ida Infront AB (SDK-partner)

Roll	Partner för säker digital kommunikation (SDK-komponenter)
Förhållande	Samarbetspartner och i tillämpliga fall underbiträde för SDK-relaterade komponenter
Typ av åtkomst	Ida Infront tillhandahåller tekniska komponenter för SDK-kedjan (meddelandetjänst och/eller accesspunkt). SDK-meddelanden som passerar genom deras komponenter är krypterade med O2O-kryptering (organisation-till-organisation), vilket innebär att meddelandeinnehållet är krypterat med mottagarorganisationens publika nyckel och signerat med avsändarens privata nyckel. Ida Infront kan inte läsa meddelandenas innehåll i klartext.
Avtal och krav	ITSL har tagit del av Ida Infronts tredjepartsgranskning av informationssäkerhetsarbetet. Gemensamma genomgångar och tekniska verifieringar genomförs löpande. Underleverantörsavtal och personuppgiftsbiträdesavtal gäller.
Överföring av PU	Nej. SDK-meddelanden är krypterade end-to-end och Ida Infront hanterar inga personuppgifter i klartext. Alla komponenter driftas inom Sverige.

2.4 Övriga

Inga andra externa mottagare tar del av personuppgifterna. Tredjepartsleverantörer som Syndis (penetrationstestning och SOC) arbetar under strikta NDA- och säkerhetsavtal och får aldrig direkt åtkomst till produktionsdata med personuppgifter. Eventuell support sker på extraherade eller anonymiserade data, alternativt i kontrollerade sessioner under uppsikt av ITSL.

Sammanfattningsvis: personuppgifterna lämnar aldrig Sverige och överförs aldrig till tredje land. All behandling sker inom den avtalade leveranskedjan med fullständig kryptering i alla led.

3. Detaljerad behandlingsbeskrivning

3.1 Varifrån hämtas personuppgifterna?

Personuppgifterna i Hubs har flera ursprung beroende på delsystemet:

- **Användarregistrering:** Vid federerad inloggning (SSO/SAML2/OIDC) synkroniseras användaruppgifter automatiskt från kundens Active Directory eller identitetshanteringssystem. Vid lokala konton registreras uppgifterna manuellt av administratör eller användaren själv.
- **SDK-adressbok:** Vid SDK-kommunikation hämtas mottagarorganisationens adressuppgifter från den centrala SDK-adressboken (tillhandahållen av DIGG).
- **Användarnas egen inmatning:** Meddelanden, filer, chattinnehåll och videomötesdata genereras direkt av användarna under deras dagliga arbete i plattformen.
- **e-Legitimation:** Vid inloggning med BankID, Freja eID eller SITHS hämtas identitetsuppgifter från den externa identitetsleverantören. Plattformen lagrar enbart det som krävs för att validera sessionen.
- **Systemgenererade uppgifter:** Loggar, tidsstämplar, IP-adresser och annan metadata skapas automatiskt av systemet under drift.

3.2 Kategorier av personuppgifter

Kategori	Exempel	Lagringsplats
Identitetsuppgifter	Namn, e-post, telefon, organisationstillhörighet	Hubs-databasen (krypterad)
Autentiseringsdata	Hashade lösenord, inloggningsloggar, IP-adresser, MFA-inställningar	Hubs-databasen + loggserver
Kommunikationsinnehåll	SDK-meddelanden, chatthistorik, bilagor	Krypterad fillagring + databas
Mötesdata	Deltagarlista, chattinnehåll under möte, eventuella inspelningar	Krypterad fillagring
Aktivitetsloggar	Filåtkomst, delningar, SDK-sändningar, administrative åtgärder	Central loggserver (separerad)
Metadata	Tidsstämplar, filstorlekar, IP-adresser, sessions-ID	Databas + loggserver

3.3 Flödesschema: Säkra meddelanden (SDK)

Nedan beskrivs det fullständiga flödet för ett SDK-meddelande från avsändare till mottagare. Hela kedjan omfattar kryptering i flera lager.

Steg	Komponent	Åtgärd	Personuppgifter i steget
1	Meddelandeklient (MK) i Hubs	Användaren skapar och skickar ett meddelande via Hubs gränssnitt. Meddelandet paketeras med metadata och bilagor.	Avsändarens identitet, mottagaradress, meddelandeinnehåll (kan innehålla personuppgifter).
2	Intern mailgateway	Tar emot meddelandet via SMTP och omvandlar det till ett API-anrop mot Meddelandetjänsten via SDK API (gränssnitt D) över HTTPS.	Samma personuppgifter som i steg 1. Överföring sker inom systemets interna nät.
3	Meddelandetjänst (MT)	Validerar meddelandet, slår upp mottagare i SDK-adressboken, krypterar innehållet med mottagarens publika nyckel (O2O-kryptering) och signerar med avsändarens privata nyckel.	Personuppgifter krypteras. Enbart metadata för adressering är läsbara för transportlagret.
4	Accesspunkt (AP) avsändare	Tar emot det krypterade meddelandet, kuverterar i AS4-format, signerar och krypterar ytterligare för transport. Skickar till mottagarens AP över TLS.	Personuppgifter dubbelt krypterade (O2O + transportkryptering). AP har ingen tillgång till klartext.
5	SDK-federation (internet)	Meddelandet transporteras mellan accesspunkter. Transportkvittens (ACK) returneras.	Data i transit, fullständigt krypterad.
6	Accesspunkt (AP) mottagare	Tar emot och dekrypterar transportlagret. Levererar det fortfarande O2O-krypterade meddelandet till mottagarens MT.	Personuppgifter fortfarande O2O-krypterade.
7	Meddelandetjänst (MT) mottagare	Dekrypterar meddelandeinnehållet med organisationens privata nyckel. Verifierar avsändarens signatur. Genererar leveranskvittens.	Personuppgifter tillgängliga i klartext inom mottagarens skyddade miljö.
8	Meddelandeklient (MK) mottagare	Användaren notifieras och kan läsa meddelandet i sin Hubs-inkorg.	Personuppgifter visas för behörig användare inom rollbaserad åtkomstkontroll.

Flödesöversikt (textuellt):

```
Användare A (MK) → SMTP → Mailgateway → HTTPS/API → MT (krypterar/signerar) → AP A →
          AS4/TLS → AP B → MT (dekrypterar/verifierar) → MK → Användare B
```

3.4 Flödesschema: Säkra filer (samarbetsyta)

Steg	Komponent	Åtgärd	Personuppgifter i steget
1	Webbläsare/klient	Användaren autentiseras via SSO/AD, BankID, MFA eller lokalt konto. Åtkomst sker via HTTPS/TLS.	Autentiseringsuppgifter (namn, e-post, ev. personnummer vid BankID).
2	Hubs webbapplikation (front-end)	Presenterar gränssnittet. Verifierar session och behörighet via rollbaserad åtkomstkontroll (RBAC).	Sessions-ID, användarroll, behörighetsmatris.
3	Applikationslogik (back-end)	Hanterar filoperationer (uppladdning, nedladdning, delning, redigering). Skannar filer med antivirus (ClamAV). Loggar alla händelser.	Filmetadata (namn, storlek, ägare, tidsstämpling). Filinnehåll kan innehålla personuppgifter.
4	Databas	Lagrar användaruppgifter, behörigheter, delningsinställningar, aktivitetsloggar och metadata. Krypterad med kundunika nycklar.	Användardata, relationer mellan användare och filer, delningshistorik.
5	Fillagring	Filer lagras krypterat på redundanta NetApp-lagringssystem. Server-side-kryptering med AES-256. Backuper tas varje timme.	Filinnehåll (potentiellt personuppgifter), krypterat i vila.
6	Loggserver (separerad)	Central loggning av alla händelser. Åtkomstskyddad och separerad från applikationsservern.	Användar-ID, IP-adress, tidsstämplar, händelsetyp.

Flödesöversikt (textuellt):

```
Användare → HTTPS/TLS → Hubs front-end → Back-end (RBAC + AV-skanning) → Databas (krypterad) + Fillagring (AES-256) + Loggserver
```

3.5 Flödesschema: Videomöten

Steg	Komponent	Åtgärd	Personuppgifter i steget
1	Mötesinitiering	Organisatören skapar ett mötesrum i Hubs. Väljer säkerhetsnivå (öppet, lösenordsskyddat, eller e-legitimation krävs). Genererar möteslänk.	Organisatörens identitet, mötesmetadata (titel, tid).
2	Autentisering av deltagare	Interna deltagare autentiseras via SSO/MFA. Externa deltagare kan krävas legitimera sig via BankID/Freja eID/SITHS (LOA3) eller ansluta med namn via länk.	Namn, e-post, ev. personnummer (vid BankID). Lagras enbart för sessionsvalidering.
3	Lobby/väntrum	Externa deltagare hamnar i väntrum. Moderatorn godkänner inträde. Händelsen loggas.	Deltagarens namn/identitet synlig för moderator.
4	Video/ljud-ström (WebRTC)	Video- och ljudströmmar överförs krypterat (SRTP/DTLS) direkt mellan deltagare (P2P) eller via High Performance Backend vid stora möten. All trafik är krypterad.	Bild och ljud av deltagare (biometriska personuppgifter). Skärmdelningsinnehåll.
5	Chatt under mötet	Textmeddelanden överförs krypterat och lagras i mötesrummets chatthistorik. Finns kvar efter mötet.	Textinnehåll (kan innehålla personuppgifter), avsändaridentitet.
6	Inspelning (valfritt)	Om aktiverat: alla deltagare meddelas. Video sparas som .webm-fil, krypterad, i Hubs fillagring. Åtkomst begränsad till mötesägare.	Video/ljud av alla deltagare (biometrisk data). Lagras krypterat i Sverige.
7	Loggning	Alla möteshändelser loggas: vem som anslöt/lämnade, tidpunkter, eventuell skärmdelning. Loggar sparas på separerad loggserver.	Deltagarlista, IP-adresser, tidsstämplar.

Flödesöversikt (textuellt):

```
Organisatör skapar rum → Deltagare autentiseras (SSO/BankID) → Lobby → WebRTC
(SRTP/DTLS) → Chatt (krypterad) → [Inspelning] → Loggserver
```

4. Sammanfattning av skyddsåtgärder

Skyddsåtgärd	Beskrivning
Kryptering i vila	All data krypteras med kundunika nycklar. Lagringsvolymer krypterade. Möjlighet till AES-256 server-side-kryptering per fil.
Kryptering under transport	TLS 1.2+ för all extern kommunikation. SRTP/DTLS för video. O2O-kryptering för SDK-meddelanden. AS4-transportkryptering.
Åtkomstkontroll	Rollbaserad behörighetsstyrning (RBAC). Principen om minsta behörighet. Stöd för MFA (BankID, TOTP, SMS). SSO via SAML2/OIDC.
Single-tenant	Varje kund har en dedikerad, isolerad instans. Ingen delning av applikation eller data mellan kunder.
Loggning och spårbarhet	Alla händelser loggas centralt. Separerad loggserver. NTP-synkronisering. SOC (Syndis) under anslutning Q1 2026.
Backup och katastrofhantering	Snapshots varje timme, dagliga och veckovisa backuper. RPO ca 1 timme. Krypterade backuper. Redundant DR-plats i skyddat bergrum.
Datalagring i Sverige	All data lagras och behandlas uteslutande i svenska datacenter (Stockholm). Inga överföringar till tredje land.
Penetrationstestning	Årliga penetrationstester via Syndis. Kontinuerlig sårbarhetsskanning. Omvärldsbevakning via CERT-SE och CVE.
Incidenthantering	Dokumenterad incidentprocess. Anmälan till IMY inom 72h vid personuppgiftsincident. Stöd till kundens DPO.

5. Kontaktuppgifter

Leverantör: ITSL Solutions AB

Kontaktperson: Fredrik Jonasson

E-post: fredrik@itsl.se

Telefon: 070-330 11 89