

PERSONUPPGIFTSBITRÄDESAVTAL – BESKRIVNING AV BEHANDLINGEN

Kategorier av registrerade vars personuppgifter behandlas

Personuppgiftsbiträdet (Trygg.chat) kommer att behandla personuppgifter om följande kategorier av registrerade för den personuppgiftsansvariges (Invidzonen) räkning:

- a) Anställda hos den personuppgiftsansvarige (kansliet mfl) som via Trygg.chat utför arbetsuppgifter för den personuppgiftsansvariges räkning.
- b) Uppdragstagare, såsom volontärer, som via Trygg.chat utför uppdrag för den personuppgiftsansvariges räkning.
- c) BESÖKARE som kontaktar den personuppgiftsansvarige via Trygg.chat
- d) ANDRA personer som besökare eller företrädare för den personuppgiftsansvarige lämnar uppgifter om i samtal som förs via Trygg.chat.

Kategorier av personuppgifter

- a) Användaruppgifter (gäller VOLONTÄRER) avser namn, telefonnummer, profilbild, kontaktuppgifter, inloggningsuppgifter.
- b) Personuppgifter (gäller BESÖKARE) avser uppgifter som BESÖKARE lämnar om sig själva och ANDRA personer i samband med sin kontakt med IZ genom chatten. Personuppgifter om ANDRA personer kan exempelvis vara namn på person som BESÖKAREN nämner i ett samtal.
- c) Personuppgifter (gäller VOLONTÄRER) som VOLONTÄRER eventuellt lämnar om sig själva och ANDRA i samband med sin kontakt med BESÖKAREN genom chatten. Personuppgifter om ANDRA personer kan exempelvis vara namn på person som VOLONTÄREN nämner i ett samtal.
- d) Personuppgifter (gäller VOLONTÄRER) i form av anteckningar, kategoriseringar och andra uppgifter som VOLONTÄRER eventuellt lämnar om BESÖKAREN och ANDRA personer som en del av organisationens dokumentation och hantering av samtal.
- e) Personuppgifter (gäller VOLONTÄRER) i form av anteckningar, kategoriseringar och andra uppgifter som VOLONTÄRER eventuellt lämnar om sig själva och andra VOLONTÄRER som en del av organisationens dokumentation och hantering av samtal.
- f) Personuppgifter som IZ väljer att registrera om sina VOLONTÄRER eller ber VOLONTÄRERNA registrera, såsom språkkunskaper, ålder och vissa levda erfarenheter.

Känsliga uppgifter som behandlas (i tillämpliga fall) och tillämpade begränsningar eller skyddsåtgärder som fullt ut tar hänsyn till uppgifternas art och de risker som är förknippade med dem, t.ex. strikt ändamålsbegränsning, åtkomstbegränsningar (inbegripet åtkomst endast för personal som har gått en specialiserad utbildning), registrering av åtkomst till uppgifterna, begränsningar för vidareöverföring eller ytterligare säkerhetsåtgärder.

Särskilda kategorier av personuppgifter (känsliga uppgifter) som kan komma att behandlas av leverantören:

- a) Etniskt ursprung
- b) Politiska åsikter
- c) Religioös eller filosofisk övertygelse
- d) Medlemskap i en fackförening
- e) Hälsa
- f) En persons sexualliv eller sexuella läggning

Personuppgifterna kan röra både VOLONTÄRER (anställda och uppdragstagare) och BESÖKARE samt andra personer. Eftersom VOLONTÄRER och BESÖKARE för fria samtal med varandra i Trygg.chat kan alla ovan listade känsliga personuppgifter potentiellt förekomma i samtalen och därmed behandlas.

Den personuppgiftsansvarige ansvarar för att göra inställningar i Trygg.chat för efter hur många dagar innehållet i chattmeddelanden ska gallras. Den personuppgiftsansvarige kan även låta VOLONTÄRER avgöra för vilka chattar som innehållet i chattmeddelanden över huvud taget ska sparas. VOLONTÄRER tillgång till chattmeddelandena styrs genom behörigheter som den personuppgiftsansvarige tilldelar. Innehållet i chattmeddelanden visas för leverantörens medarbetare i krypterat format.

Känsliga uppgifter kan även registreras via enkäter som fylls i av den personuppgiftsansvariges BESÖKARE och VOLONTÄRER. Den personuppgiftsansvarige utformar enkäterna och styr därmed över vilka uppgifter som ska samlas in. Enkät svar och även kategoriseringar som VOLONTÄRER gör för individuella samtal redovisas i Tjänsten för de VOLONTÄRER som den personuppgiftsansvarige har gett viss behörighet.

Utgångspunkten i gällande lagstiftning är att det är förbjudet att behandla känsliga personuppgifter, men det finns en rad undantag. Den personuppgiftsansvarige ansvarar i förekommande fall för att den har rätt att behandla sådana. Det går att läsa mer på till exempel IMY:s Integritetsmyndighetens, hemsida www.imy.se.

Behandlingens art

Följande behandlingar utförs eller kan komma att utföras av leverantören:

- a) Lagra och säkerhetskopiera data om samtal och samtalens innehåll, BESÖKARE och VOLONTÄRER i Trygg.chat
- b) Radera data om samtal och samtalens innehåll, BESÖKARE och VOLONTÄRER i Trygg.chat
- c) Bearbeta och presentera/visa data om samtal och samtalens innehåll, BESÖKARE och VOLONTÄRER i Trygg.chat
- d) Administrera användaruppgifter i Trygg.chat.
- e) Överföra kundens data om samtal, BESÖKARE och VOLONTÄRER ifrån Trygg.chat till kunden.
- f) Samköra data inom och mellan kunder (statistik) i Trygg.chat. Statistiken får inte i sig utgöra personuppgift.
- g) Migrera data, inklusive personuppgifter, som kommer från den personuppgiftsansvariges tidigare chattverktyg in i Trygg.chat.

Personuppgifter kan komma att lagras och /eller behandlas i länder inom EU/EES.

Ändamål för vilka personuppgifterna behandlas för den personuppgiftsansvariges räkning

Ändamålet med personuppgiftsbiträdes behandling av personuppgifter åt den personuppgiftsansvarige är

- att möjliggöra samtal mellan den personuppgiftsansvariges BESÖKARE och den personuppgiftsansvariges VOLONTÄRER i den digitala samtalstjänsten Trygg.Chat,
- att möjliggöra för den personuppgiftsansvarige att organisera och kommunicera med anställda och uppdragstagare som använder Trygg.chat.

Personuppgiftsbiträdet har inte rätt att behandla personuppgifter i syfte att utveckla och förbättra Trygg.chat.

Behandlingens varaktighet

Personuppgiftsbiträdet behandlar personuppgifter för den personuppgiftsansvariges räkning så länge som personuppgiftsbiträdet använder Trygg.chat och en tid därefter, närmare bestämt till och med den dag som personuppgifterna raderas enligt villkor i avtal mellan parterna.

För behandling som utförs av personuppgiftsbiträden (eller underleverantörer), ange även föremålet för behandlingen, behandlingens art och dess varaktighet

Webbhotell som tjänsten Trygg.chat ligger på. Lagring av samtal som genomförs i Trygg.chat samt lagring och visning av övrig data som matas in i och hanteras i Trygg.chat. Skapar säkerhetskopior och överför dessa till lagringstjänst.

Lagring av säkerhetskopior av Trygg.chat-data och raderar säkerhetskopior efter viss tid. Tar emot och lagrar ljud och videofiler som skapas genom Trygg.Chat och raderar ljud och videofiler efter viss tid. Överför ljud- och videofiler till kundens dator när kunden lyssnar/tittar.

För telefoni-, ljud- och videotjänster som integreras i Trygg.chat: inspelning av ljud och videofiler som lagras och när samtalet är slut förs en kopia över till lagringstjänst. Inspelningen raderas.

Behandlingens varaktighet är densamma som för personuppgiftsbitrådets övriga behandling.

TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER, INBEGRIPET TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER FÖR ATT SÄKERSTÄLLA DATASÄKERHETEN

En beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som den eller de berörda personuppgiftsbiträdena vidtagit (inbegripet eventuella relevanta certifieringar) för att säkerställa en lämplig säkerhetsnivå, med beaktande av behandlingens art, omfattning, sammanhang och syfte samt riskerna för fysiska personers rättigheter och friheter.

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

Behandlingen av personuppgifter sker på servrar som levereras av ett externt företag. Den fysiska åtkomstkontrollen görs av HUAB:s underleverantör av servrar.

Åtkomstkontroll avseende system – Åtgärder som förhindrar obehöriga att använda IT-system:

Personuppgiftsbitrådets personal använder tvåfaktoraутentisering för alla IT-system där det är möjligt.

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:

Personuppgiftsbiträdet anpassar anställdas behörigheter i IT-system per individ eller roll, baserat på de arbetsuppgifter och ansvarsområden som anställda har. Innehållet i chattmeddelanden (där känsliga personuppgifter kan förekomma) visas för leverantörens medarbetare i krypterat format.

Personer hos den personuppgiftsansvariga som är behöriga att använda Trygg.chat delas in i organisationer och team och tilldelas roller som begränsar tillgången till personuppgifter, både vad gäller att visa och ändra dem. Användarnamn och lösenord är personliga. Kunden är ansvarig för att bjuda in nya VOLONTÄRER via personlig mailadress och tilldela VOLONTÄRER rätt roll. I Trygg.chat-manualen finns information om hur VOLONTÄRER tilldelas roller och vad olika roller har behörighet att göra.

Personuppgiftsbiträdet ger inte VOLONTÄRER tillgång till den personuppgiftsansvariges Trygg.chat- miljö om inte behörig representant för den personuppgiftsansvariga uttryckligen bett om det.

Personuppgiftsbitrådets anställda har som regel inte reguljära VOLONTÄRER i personuppgiftsansvarigas miljö i Trygg.chat. Det kan dock förekomma att anställd hos personuppgiftsbitrådet efter överenskommelse med personuppgiftsansvarig skapar eller genom den personuppgiftsansvariges försorg tillfälligt får en VOLONTÄRER skapad åt sig för att till exempel hjälpa till med utbildning för VOLONTÄRER eller hjälpa till med felsökning.

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

När personuppgifter i Trygg.chat förs över från produktionsservrar är datan alltid krypterad. Se även ovan om begränsningar av vem som kan visa/se personuppgifter i Trygg.chat.

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:

Där det är möjligt lagras information i databasen om vem som har matat in personuppgifter i Trygg.chat. Bland annat lagras information om vem som skapat inbjudningar till nya VOLONTÄRER och vem som skrivit individuella chattmeddelanden. BESÖKARE som uppger sina eller andras personuppgifter i Trygg.chat är vanligen anonyma och då går det följaktligen inte att veta vem – vilken person - som matat in uppgifterna.

Alla försök att logga in på Trygg.chat-servrar loggas. I övrigt loggas de åtgärder som ingår i standarduppsättningen för Linuxservrar.

Tillgänglighetskontroll – Åtgärder för att säkerställa att personuppgifter skyddas mot oavsiktlig förstörelse eller förlust och att de kan återställas

Personer hos den personuppgiftsansvariga som är behöriga att använda Trygg.chat delas in i organisationer och team och tilldelas roller som begränsar tillgången till personuppgifter – både att se och ändra dem.

Personuppgiftsbitrådet gör regelbundna automatiska säkerhetskopior av Trygg.chat-databasen, inklusive personuppgifter. Säkerhetskopiering görs minst en gång per dygn. Säkerhetskopior sparas minst 30 dagar och högst 120 dagar.

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

Alla personuppgifter lagras på ett strukturerat sätt i databasen och kan därför särskiljas.

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

Kunden/personuppgiftsansvarig ställer själv in efter hur lång tid lagrade samtal ska gallras automatiskt och kopplingen mellan BESÖKAREN och statistik ska brytas. Efter att säkerhetskopiering är förbrukad är personuppgifterna slutgiltigt gallrade. Trygg.chat är byggt efter principen att spara så få uppgifter så kort tid som möjligt när det handlar om personuppgifter.

Personuppgiftsansvarigs inställning för gallring inte är samma sak som radering av säkerhetskopior. I Trygg.chat kan personuppgiftsansvarig välja att låta chattmeddelanden ligga kvar ett visst antal dagar innan de raderas och inte längre kan visas i gränssnittet. Men eftersom personuppgiftsbitrådet har säkerhetskopior finns personuppgifterna i praktiken ändå kvar i säkerhetskopiering innan kopian i sin tur raderas.

Kunden/personuppgiftsansvarig kan själv radera uppgifter om VOLONTÄRER under avtalstiden.

Vid avtalets upphörande har leverantören rutiner för att alla personuppgifter rensas efter tid som anges i avtalet mellan kund och leverantör.

Säkerhetskopior sparas endast en kortare tid (se ovan).

I fråga om överföringar till personuppgiftsbiträden (eller underleverantörer), beskriv även de specifika tekniska och organisatoriska åtgärder som personuppgiftsbiträdet (eller underleverantören) ska vidta för att kunna bistå den personuppgiftsansvarige.

Inga åtgärder krävs utöver det som ovan beskrivits.

Beskrivning av de specifika tekniska och organisatoriska åtgärder som personuppgiftsbiträdet ska vidta för att kunna bistå den personuppgiftsansvarige (se Klausul 8.d i detta avtal)

Personuppgiftsbiträdet har utfört en konsekvensbedömning avseende dataskydd och kommit fram till att behandlingen inte medför en hög risk för fysiska personers rättigheter och friheter, givet de förebyggande åtgärder som beskrivs ovan.

Angående skyldigheterna i artikel 32 i förordning (EU) 2016/679 (se klausul 8.c.4 i detta avtal): Regleringen avser hur medgivande till behandling av personuppgifter ska utformas, i det fall databehandling utgår från den grunden. Trygg.chat har en teknisk lösning (enkätfråga) som gör det möjligt för den personuppgiftsansvarige kan låta sina BESÖKARE lämna sitt medgivande till behandlingen direkt i widgeten.

FÖRTECKNING ÖVER UNDERLEVERANTÖRER

Denna bilaga måste fyllas i vid särskilt godkännande av underleverantörer (klausul 7.7 a).

Den personuppgiftsansvarige har godkänt användningen av följande underleverantörer:

1. Namn: Yelles AB (556931-6788)

Adress: Ovabacksgattu 10, 79370 Tällberg

Beskrivning av behandlingen (inklusive en tydlig ansvarsfördelning om flera underleverantörer har godkänts):

Yelles AB ansvarar för webbhotellet som tjänsten Trygg.chat ligger på. Lagring av samtal som genomförs i Trygg.chat samt lagring och visning av övrig data som matas in i och hanteras i Trygg.chat. Skapar säkerhetskopior och överför dessa till lagringstjänst.

2. Namn: Amazon Web Services

Adress: Avenue John F. Kennedy 38, LUXEMBOURG, 1855, LUXEMBOURG

Beskrivning av behandlingen (inklusive en tydlig ansvarsfördelning om flera underleverantörer har godkänts):

Amazon Web Services lagrar säkerhetskopior av Trygg.chat-data och raderar säkerhetskopior efter viss tid.

3. Namn: Stream.io, Inc

Adress: 1215 Spruce Street Suite 300, Boulder, CO 80302

Beskrivning av behandlingen (inklusive en tydlig ansvarsfördelning om flera underleverantörer har godkänts):

Stream.io, Inc levererar ljudsamtals- och videosamtalstjänster som integreras i Trygg.chat. Ljud- och videosamtal kan spelas in, lagras och spelas upp om kunden väljer det. Överför ljud- och videofiler till kundens dator när kunden lyssnar/tittar. Ljud kan transkriberas till textfiler som visas och lagras om kunden väljer det. Ljud- och videofiler samt textfiler raderas efter viss tid.