

Integritetspolicy för STICAB Scandinavian Technical Insulation Company AB. (Org. nr. 556907-6325 Nedan kallad "STICAB")

Syftet med denna Integritetspolicy är att säkerställa att STICAB's behandling av personuppgifter görs på lagliga skäl och i enlighet med GDPR:s principer. Samt att vi hanterar våra kunders, anställdas och leverantörers personuppgifter på ett säkert och öppet sätt.

1. Introduktion

På samma sätt som samhället i helhet har STICAB, våra kunder, anställda och leverantörer påverkats av digitalisering och globalisering vilket har lett till betydande ökning av användning och spridning av personuppgifter. Digitalisering betyder ökade möjligheter, men också ett större behov av skydd för de registrerade personuppgifter och integritet. Denna policy beskriver de övergripande principerna som gäller för personuppgiftsbehandling inom Taktik.

1.1. Syfte

Syftet med denna policy är att definiera STICABs ansvar samt utse roller och ansvar för att följa dataskyddsförordningen (GDPR).

1.2. Mål

Målsättningen är att STICABs behandling av personuppgifter sker på laglig grund och i enlighet med GDPR:s principer för att säkerställa för våra kunder, anställda och leverantörer att vi hanterar deras personuppgifter på ett säkert och öppet sätt.

1.3. Definitioner

I denna policy används följande definitioner:

Personuppgiftsansvarig

Den fysiska eller juridiska personen, den offentliga myndigheten, byrå eller annat organ som, ensam eller gemensamt med andra, bestämmer syftet och sättet att behandla personliga data.

Personuppgiftslämnare

Den levande person till vilken personuppgifterna gäller. En personuppgiftslämnare definieras i denna policy som en person som STICAB har någon form av relation med, t.ex. kund, anställd, konsult eller annat.

Personuppgiftsbiträde

En fysisk eller juridisk person, offentlig myndighet, institution eller annan som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Personuppgift

All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet räknas enligt personuppgiftslagen som personuppgifter. Även bilder (foton) och ljudupptagningar på individer som behandlas i dator kan vara personuppgifter även om inga namn nämns. Krypterade uppgifter och olika slags elektroniska identiteter, som exempelvis IP-nummer, räknas som personuppgifter om de kan kopplas till fysiska personer.

Personuppgiftsbehandling

Alla former av åtgärder med personuppgifter är personuppgiftsbehandling, till exempel insamling, registrering, organisering, strukturering, lagring, bearbetning, ändring, framtagning, läsning, användning, utlämning, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

1.4. Omfattning

Omfattningen av denna policy är begränsad till personuppgiftsbehandling som krävs enligt de allmänna uppgifterna Skyddsförordning (GDPR). Detta omfattar STICAB, externa konsulter som utför uppgifter på uppdrag av STICAB och personuppgiftsbiträden som utför databehandling på uppdrag av STICAB.

Utöver de allmänna riktlinjerna i denna policy måste detaljerade krav i lokala dataskyddslagar, i tillämpliga fall, följas av anställda vid behandling av personuppgifter.

I det fallet STICABs är personuppgiftsbiträde för en extern organisation ska databehandlingen vara gjord i enlighet med denna policy, om inget annat anges i ett personuppgiftsbiträdesavtal mellan STICAB och den personuppgiftsansvarige.

1.5. Målgrupper

Integritetspolicyn gäller all personal som utför uppgifter på uppdrag av STICAB avseende behandling av personuppgifter. Det är också avsett att ligga till grund för information till personuppgiftslämnare rörande personuppgiftsbehandling. Det gäller även för personuppgiftsbiträden som utför personuppgifter på uppdrag av STICAB.

2. Roller och ansvar

Nedan beskriver vi roller.

2.1. VD

VD ska säkerställa att STICAB är ordentligt organiserade med delegerat ansvar och tillräckliga resurser för behandling av personuppgifter inom bolaget och är ytterst ansvarig. VD nås via mikael.nilsson@sticab.se

2.2. HR

Human resource ansvarig har ansvaret att identifiera informationssäkerhetsrisker för personal, kunder och leverantörer samt föreslå lämplig informationskontroll och uppföljning av informationssäkerhetskontrollerna. HR nås via mikael.nilsson@sticab.se

2.3. Personuppgiftsansvarig

Personuppgiftsansvarig är alltid ansvarig för behandling av personuppgifter. Personuppgiftsansvarig är alltid den juridiska personen som kontrollerar och beslutar om hantering av personuppgifter.

2.4. Ansvarig för Personuppgiftsfrågor / Privacy Officer (PO)

Rollens uppgift är att säkerställa tillhandahållande av GDPR i sin organisation. Denna är också skyldig att hålla ett register över alla processer som inbegriper personuppgifter som utförs av organisation. PO nås via mikael.nilsson@sticab.se

2.5. Personuppgiftsbiträde

Externa leverantörer av IT-verksamhet, molntjänster och liknande där personuppgifter behandlas för STICABs räkning kallas personuppgiftsbiträden. Ett personuppgiftsbiträde ska utföra uppgifterna som finns specificerade i ett personuppgiftsbiträdesavtal.

2.6. Anställda

Alla anställda är personligen ansvariga för en laglig och korrekt behandling av personuppgifter i deras dagliga arbete. Genom att följa STICABs styrande dokument rörande personuppgiftsbehandling bidrar medarbetarna till efterlevnad av korrekt personuppgiftsbehandling.

3. Dataskyddskrav

Nedan beskriver vi hur personuppgifter och dataskydd hanteras.

3.1. Rättslig grund för bearbetning

Personuppgifter får endast behandlas om vissa villkor är uppfyllda, till exempel (A) om den person till vilken personuppgifterna hänförs har givit sitt medgivande till behandlingen. (B) Behandlingen är nödvändig för utförandet av ett kontrakt som personen är part i. (C) Behandlingen är nödvändig för att STICAB ska uppfylla en laglig skyldighet. eller (D) STICABs legitima intresse att behandla personuppgifter uppväger individens intresse att inte få sina personuppgifter behandlade.

3.2. Principer för behandling av personuppgifter

Laglighet, korrekthet och öppenhet - Vid behandling av personuppgifter inom STICAB ska vi säkerställa att behandlingen är laglig, och att vi är transparenta mot personuppgiftslämnare.

Uppgiftsminimering - Inom STICAB samlar vi aldrig in och hanterar mer personuppgifter än vad som krävs för att uppfylla uppgifternas ändamål. Det betyder att vi måste fråga oss själva i varje samling av personliga data om det är nödvändigt. Om syftet med databehandling har löpt ut måste vi ta bort personuppgifter som inte längre behövs.

Ändamålsbegränsning - Vid insamling av personuppgifter måste vi ha ett tydligt och legitimt syfte med insamlingen och behandlingen. Om ändamålet inte längre är giltigt, måste vi ta bort de personuppgifter som behandlas enligt det ändamålet. Om vi vill behandla personuppgifter för ett nytt syfte får det inte vara oförenligt med det ursprungliga syftet, exempelvis utanför vad den berörda personuppgiftslämnaren rimligen skulle förvänta sig. Vi måste också se till att informera personuppgiftslämnaren om detta, och med vilken juridisk grund vi behandlar personuppgifterna.

Noggrannhet - Personuppgifter måste vara korrekta och aktuella. Personuppgifter som är felaktig eller ofullständig bör raderas eller korrigeras.

Lagringsminimering - Personuppgifter ska endast lagras så länge som nödvändigt för de ändamål för vilka uppgifterna behandlas, eller enligt vad som krävs enligt gällande lag. När den tiden har löpt ut ska personuppgifterna raderas permanent på ett säkert sätt. Om vi vill behålla personuppgifter under en längre period än vad som krävs för ändamålet måste vi se till att uppgifterna inte längre kan kopplas ihop till en person, direkt eller indirekt (anonymisering). För personuppgifter som vi mottagit från en person vi har en kundrelation med, behåller vi dessa under den tidsperiod som utgör praxis bestämd av den nationella dataskyddsmyndigheten.

Integritet och konfidentialitet - Personuppgifterna ska skyddas bland annat mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse. STICAB ska därför vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna.

Ansvarsskyldighet – STICAB ansvarar för att principerna om personuppgiftsbehandling följs när personuppgifter behandlas och ska kunna visa på vilket sätt man följer dem.

3.3. Personuppgiftslämnarens rättigheter

STICAB ska svara på personuppgiftslämnarens önskemål på det sätt som krävs enligt gällande lag eller på annat sätt anses vara rimligt praktiskt och lämpligt i samråd med vår PO.

Öppenhet och information - Personer vars personuppgifter behandlas bör informeras på ett tydligt sätt. Ett sådant meddelande bör vara koncist, enkelt tillgänglig, skrivas i tydligt och enkelt språk och måste innehålla viss specifik Information.

Rätt till information - En individ kan begära att få information om STICABs behandling av personuppgifter.

Rätt till rättelse och radering - En individ kan begära att ens personuppgifter ska korrigeras eller raderas.

Rätt att göra invändningar - En individ har i vissa fall rätt att invända mot den personuppgiftsansvariges behandling av hans eller hennes personuppgifter.

Rätten att invända - Gäller när personuppgifter behandlas för att utföra en uppgift av allmänt intresse, som ett led i myndighetsutövning eller efter en intresseavvägning.

En individ har rätt att klaga mot STICABs behandling av sina Personuppgifter.

En individ har rätt till ersättning för skada.

3.4. Personuppgiftsansvarige och personuppgiftsbiträdets skyldigheter

När bearbetningen ska utföras av ett personuppgiftsbiträde på uppdrag av den personuppgiftsansvarige, ska personuppgiftsansvarige endast använda sig av personuppgiftsbiträden som kan lämna tillräckliga garantier för att ha implementerat tillräckligt tekniskt och organisatoriskt skydd, för att kunna möta kraven från GDPR och därmed skydda personuppgiftslämnaren

Det ska finnas ett rättsligt bindande avtal mellan personuppgiftsansvarige och personuppgiftsbiträdet som uppfyller kraven i dataskyddslagarna och vilken fördelning av ansvar som gjorts mellan parterna avseende personuppgiftsbehandlingen:

Dataskydd genom "privacy by design" - Varje ny tjänst eller affärsprocess som introduceras av STICAB och som innebär behandling av personuppgifter bör vara utformad för att ta hänsyn till skyddet av sådana data, till exempel genom att se till att nödvändiga säkerhetsåtgärder är inbyggda i dess design ("privacy by design"). Varje sådan ny tjänst eller affärsprocess ska också utformas för att se till att som standard endast personuppgifter som är nödvändiga för det specifika syftet med behandlingen behandlas ("privacy by default").

Konsekvensbedömning av dataskydd - Där det finns höga risker vid behandling av personuppgifter, i synnerhet när det rör nya teknologier, molntjänster och andra IT-system, bör STICAB före en sådan bearbetning genomföra en konsekvensbedömning. STICAB ska då följa datainspektionens riktlinjer om konsekvensbedömning.

Rapportering av personuppgiftsincidenter - anställda som misstänker att denna policy eller relevanta dataskyddslagar har brutits ska kontakta STICAB PO omedelbart för att STICAB ska kunna följa lagstadgade anmälningskrav.

Tillhandahållande av personuppgiftslämnarens rättigheter - som anges i kapitel 3.2 i denna policy.

Säkerhetsåtgärder - En anställd som har tillgång till personuppgifter får endast bearbeta uppgifterna i enlighet med syftet för behandlingen, och får inte dela, distribuera eller på annat sätt avslöja personuppgifterna till en tredje part om inte instrueras att göra det av STICAB. Lämpliga tekniska och organisatoriska åtgärder bör genomföras skydda personuppgifter mot oavsiktlig eller olaglig förstörelse, oavsiktlig dataförlust eller ändring, obehörigt utlämnande eller åtkomst och andra olagliga former av bearbetning. Lämpliga skyddsåtgärder i förhållande till risken skall vidtas.

Överföring av personuppgifter utanför EU och EEA är endast tillåten när den importerande enheten har lämnat tillräckliga garantier för att personuppgifter kommer att skyddas tillräckligt. Detta kan åstadkommas genom att använda en av EU:s standardiserade dataöverföringsavtal. Kontakta PO för ytterligare information.

Utbildning och medvetenhet – STICAB ger tillräcklig utbildning för alla anställda, baserad på anställdas roll och ansvar.

4. Personuppgiftshantering på STICAB

Nedan beskriver vi vår personuppgiftshantering.

4.1. Personuppgifter där STICAB är personuppgiftsansvarig

4.1.1 Uppgifter på våra företagskunder

För att kunna uppfylla avtalet med kund registreras kontaktuppgifter som exempelvis, faktura- och leveransadress. Dessa uppgifter registreras i vårt affärssystem och behandlas i fakturerings- och bokföringssyfte.

4.1.2. Leverantörer & underleverantörer

Eftersom vi köper en del tjänster som vi kan vara i behov av så behandlas personuppgifter även på dig som leverantör eller underleverantör. Detta för att vi ska kunna göra utbetalningar eller kontakta dig på ett eller annat sätt så att du effektivt ska kunna utföra ditt uppdrag eller erbjuda din produkt eller tjänst.

Detta gäller följande kategorier av registrerade:

- Medarbetare på ett leverantörsföretag
- Inhyrd bemanningspersonal
- Konsulter
- praktikanter

4.1.3. Potentiella medarbetare

Vi behandlar även uppgifter i och med att det inkommer jobbansökningar till oss.

4.2. Vad vi använder dina personuppgifter till

När vi bearbetar dina personuppgifter gör vi det med ditt samtycke och/eller på behovsbasis, i syfte att kunna driva vår verksamhet, uppfylla våra avtalsenliga och juridiska skyldigheter, skydda våra system eller uppfylla andra berättigade intressen, främst relaterade till sälj- och marknadsföringsaktiviteter.

4.2.1. Fullgöra förpliktelser som uppdragsgivare

För att STICAB ska kunna fullgöra sina förpliktelser som uppdragsgivare och för att säkerställa en säker och effektiv administration är det nödvändigt för STICAB att samla in, behandla och lagra personuppgifter på frilansare, konsulter och andra underleverantörer. Endast personuppgifter som har ett samband med uppdraget behandlas.

4.2.2. Kundsupport

Vi använder uppgifter för att ge support- och stödtjänster till dig så att du kan utnyttja våra Tjänster.

4.3. Typer av personuppgifter som vi behandlar och för vilka ändamål

Vi använder inte uppgifter till annat ändamål än vad som står beskrivet i denna policy. De data vi behandlar kan innefatta följande:

4.3.1. Namn och kontaktuppgifter

Vi samlar in för- och efternamn, e-postadress, postadress, telefonnummer, leveransuppgifter och andra liknande kontaktuppgifter. Dessa uppgifter behandlas för att vi ska kunna fullgöra avtal och åtaganden med våra kunder, samarbetspartners och personal.

4.3.2. Personnummer och betalningsinformation

För att kunna uppfylla våra avtal med leverantörer, underleverantörer, kunder och samarbetspartners behöver vi inhämta betalningsinformation. Notera att personnummer endast registreras på personal för att vi ska kunna registrera och utbetala avtalade ersättningar och rapportera dessa till Skatteverket.

4.3.3. Enhets- och användningsdata

Det kan innefatta även information om operativsystem, också IP-adress, enhets-id, nationella inställningar och språkinställningar.

4.3.4. Film och Foto

Medverkan i samband med företagspresentationer, kunduppdrag och liknande görs endast med inblandade och identifierade medverkandes medgivande så som på sociala medier och företagets hemsida.

4.3.5. Support och feedbackuppgifter

Vi samlar också in information som du tillhandahåller oss och innehållet i meddelanden som du skickar till oss, såsom feedback eller frågor och information du lämnar för kundsupport.

4.3.6. Känsliga personuppgifter

Vi behandlar i regel ingen känslig information, undantaget ett fåtal intervjusituationer där innehållet i sig kan vara av känslig natur.

4.4. Vilka dina personuppgifter kan komma att delas till och varför vi delar dem

I de fall där vi delar information om dig med andra har vi sett till att dessa företag följer våra krav för dataskydd och de är inte tillåtna att använda personuppgifter de tar emot för något annat syfte än vad som avtalats.

4.5. System och molnleverantörer

Det kan ibland vara nödvändigt för oss att dela din information med externa bolag för att underlätta vår verksamhet, leverera våra tjänster samt fullgöra våra skyldigheter. Det kan exempelvis handla om system- och molnleverantörer vi använder oss av för att föra vårt arbete framåt. Dessa får dock inte gå och titta i vår data utan explicit tillåtelse.

4.6. E-post och annan ostrukturerad data

STICAB har en särskild intern policy för behandling av personuppgifter i e-post och annan ostrukturerad data. För det första måste vi ha en rättslig grund för att hantera e-post. STICAB kan likt andra företag och privata organisationer därför som regel behandla personuppgifter i inkommande e-post med stöd av en intresseavvägning. Policyn säger också att STICAB inte ska använda e-post för att systematisk hantering av personuppgifter, samt att gallring skall ske.

4.7. Övrigt

Slutligen kan vi komma att behöva lämna ut eller spara dina uppgifter när vi anser att det är nödvändigt för att:

- Följa lagen eller rättslig process och ge ut information till polis och andra behöriga myndigheter.
- Skydda våra kunder, exempelvis för att förhindra skräppost eller bedrägeriförsök, eller för att underlätta förhindrande av dödsfall eller allvarlig skada.
- Hantera och upprätthålla säkerheten för våra tjänster, däribland att förhindra eller stoppa en attack på våra system eller nätverk.

- Skydda rättigheter eller egendom som tillhör STICAB, inklusive verkställa de villkor som styr användning av tjänsterna, men om vi får information om att någon använder våra tjänster för att handla med stulen immateriell eller fysisk egendom som tillhör STICAB kommer vi inte att själva undersöka en kunds privata innehåll, utan vi kan då överlåta ärendet till en polismyndighet.

5. Kontakta oss

Om du har en fråga om vad som gäller för dina personuppgifter, begäran om registerutdrag, ett klagomål eller en fråga till vår PO, kontaktar du oss genom att maila oss på mikael.nilsson@sticab.se. Vi svarar på frågor inom 20 dagar.

6. Internrevision

STICAB kommer att göra objektiva interna revisioner av denna policy, inklusive dataskydd på periodisk bas. VD på STICAB ansvarar för övergripande övervakning och genomförande av denna policy. VD ansvarar för STICABs dagliga överensstämmelse med denna policy och dataskyddslagar.

Stockholm 2018-05-15