Integritetspolicy

För Hökerum Bygg AB och alla bolag i koncernen Familjen Ståhl Invest i Ulricehamn AB

Version 2.0 – September 2021

Denna policy gäller för Hökerum Bygg AB och alla bolag i koncernen Familjen Ståhl Invest i Ulricehamn AB (”koncernen”). Policyn omfattar även bolag som tidigare ingått i koncernen där medlemmar ur Familjen Ståhl är registrerade firmatecknare. Bostadsrättsföreningar där bolag inom ”koncernen” enligt avtal ansvarar för föreningens förvaltning av administration omfattas även av denna policy. I denna policy då ”vi”, ”vår”, ”våra” och ”oss” benämns hänvisar det till något eller alla nämnda bolag och alla dess medarbetare.

Den 25 maj 2018 träder Dataskyddsförordningen i kraft, också benämnd som GDPR (General Data Protection Regulation), vilket ställer fler och högre krav på hur vi som företag hanterar personuppgifter i vårt arbete. Denna policy beskriver hur vi säkerställer att förordningen upprätthålls. Policyn är öppen och tillgänglig för alla medarbetare, samarbetspartners och kunder.

Innehåll

1. SAMMANFATTNING

Följande text används som sammanfattning och informationstext på alla våra hemsidor under sidan ”personuppgifter”. Hela detta dokument är öppet och på samma sida tillgängligt för nedladdning i sin helhet.

Hökerum Bygg vill med denna integritetspolicy visa hur vi säkerställer att alla personuppgifter behandlas i enlighet med dataskyddsförordningen - GDPR.

Vi på Hökerum Bygg uppskattar ditt besök på denna sida. Vi värnar om att på bästa sätt skydda den personliga integriteten och strävar alltid efter att skydda alla personuppgifter på bästa sätt. Nedan följer information om hur vi kan använda personuppgifter och vilka rättigheter individer har.

Denna policy gäller för Hökerum Bygg AB och alla bolag i koncernen Familjen Ståhl Invest i Ulricehamn AB (”koncernen”). Policyn omfattar även bolag som tidigare ingått i koncernen där medlemmar ur Familjen Ståhl är registrerade firmatecknare. Bostadsrättsföreningar där bolag inom ”koncernen” enligt avtal ansvarar för föreningens förvaltning av administration omfattas även av denna policy. I denna policy då ”vi”, ”vår”, ”våra” och ”oss” benämns hänvisar det till något eller alla nämnda bolag och alla dess medarbetare.

Användande av personuppgifter

Via våra hemsidor har personer möjlighet att ställa frågor, beställa information eller ta kontakt med oss. Vi använder endast personuppgifter som behövs för att uppfylla det aktuella syftet. Kontaktuppgifter kan komma att delas med någon av våra samarbetspartners i de fall då en partner behöver engageras för att administrera det aktuella ärendet. I övrigt kommer vi inte att dela information med någon annan part. All eventuell delning med annan part regleras av ett biträdesavtal. När informationen uppfyllt det syfte för vilken den samlades in för kommer alla personuppgifter att gallras eller raderas inom rimlig tidsperiod om inget annat förekommer som rättslig grund som tillhåller oss rätten att spara uppgifterna under en längre period. Exempelvis via lagkrav eller krav från annan myndighet om att utlämna/spara uppgifter för att t ex upptäcka, förebygga eller uppmärksamma bedrägerier och eller andra brott.

Hur skyddas dina personuppgifter?

Vi vidtar alltid tekniska säkerhetsåtgärder för att säkerställa att personuppgifter skyddas mot förstöring genom olyckshändelse, mot obehörig ändring, otillåten spridning av eller otillåten tillgång till uppgifter, liksom mot annat slag av otillåten behandling av personuppgift.

E-post

Bilaga 1 i vår integritetspolicy innehåller en specificerad E-post policy som sammanfattas med följande punkter i enlighet med Integritetsskyddsmyndigheten rekommendationer angående e-posthantering:

- Vi skickar inte känsliga personuppgifter via oskyddade e-postmeddelanden.
- Vi informera på våra hemsidor om denna policy och länkar till den samma i våra e-post signaturer.
- Alla inom organisationen är informerade om denna policy och de regler och rutiner som gäller för hur vi behandlar personuppgifter som kan förekomma i e-postmeddelanden.

Dina rättigheter

En person som är registrerad i något av våra system har rätt att begära ett utdrag. Registerutdraget är kostnadsfritt för den registrerade en gång per kalenderår. Om personen begär flera registerutdrag i snabb följd har vi rätt att ta ut en administrativ ersättning för att lämna ut materialet eller i vissa fall neka att lämna ut uppgifterna.

En begäran om personuppgiftsutdrag administreras endast om den inkommer till någon av följande e-postadresser:

- personuppgift@hokerumbygg.se
- personuppgift@villastromsfors.se

En begäran kommer att hanteras inom 30 arbetsdagar från att personen i fråga har fått en bekräftelse på att ärendet har registrerats av oss.

Personer har också rätt att begära rättelse av felaktiga uppgifter, ändra uppgifter som tidigare lämnats, eller återkalla ett tidigare lämnat samtycke och meddela att fortsatt behandling av personuppgifter motsättes eller att personen inte önskar ta emot fortsatt information från oss.

Personuppgifter kommer i sådant fall att raderas så snart det är möjligt med hänsyn till andra eventuella åtaganden vi kan ha mot personen. För rättning eller ändring av personuppgifter kontakta er kontaktperson direkt eller skicka ett e-postmeddelande till någon av våra personuppgifts adresser. För att kunna tillgodose personens önskemål om rättning, ändring eller radering ange fullständiga uppgifter samt ange i vilket sammanhang uppgifter har lämnats till oss. Utan denna information, tillsammans med en säker identifiering, saknar vi möjlighet att kontrollera, rätta eller radera personuppgifter.

Vi värnar om att på bästa sätt skydda den personliga integriteten och strävar alltid efter att skydda alla personuppgifter på bästa sätt.

Vårt ansvar

Vi är personuppgiftsansvariga och ansvaret för att behandlingen av personuppgifter sker korrekt ligger på hela vår verksamhet med VD och styrelsen som ytterst ansvariga.

2. INFORMATION

2.1 PERSONUPPGIFTER

En personuppgift är en uppgift som ensamt eller tillsammans med andra uppgifter kan användas av någon för att identifiera en nu fysiskt levande person. Företagsuppgifter omfattas inte av förordningen.

Exempel på personuppgifter är: Personnummer, adress, e-post, telefonnummer, kundnummer och IP-adress. Alla uppgifter som ensamma eller tillsammans med andra uppgifter kan användas för att identifiera en fysisk person är en personuppgift.

2.2 KÄNSLIGA PERSONUPPGIFTER

Vissa typer av personuppgifter bedöms som känsliga och får endast behandlas om det finns direkt stöd i lag eller om den registrerade har gett sitt uttryckliga samtycke. I dessa fall sätts dessutom extra stor hänsyn till säkerheten och den registrerades integritet.

Exempel på känsliga personuppgifter är: Etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, genetiska eller biometriska uppgifter, hälsa eller sexuell läggning.

Det betyder att det är mycket viktigt vid nya registreringar och behandlingar att vi kontrollera att de inte innehåller några känsliga personuppgifter som vi inte har någon rättslig grund till att behandla. Endast om det verkligen är motiverat får en sådan uppgift behandlas i våra system. Om en kund skriver eller skickar in material som exempelvis innehåller hälsouppgifter och det inte är absolut nödvändigt för utförandet av vårt uppdrag ska inte sådana uppgifter sparas utan raderas efter att eventuella övriga uppgifter noterats i våra system.

2.3 BEHANDLING

När vi gör något med en personuppgift kallas det för att behandla uppgiften. När en uppgift behandlas måste det ske säkert och med skydd för integriteten för personuppgiften. Exempel på en behandling är, insamling, registrering, lagring, spridning, samkörning och radering.

2.4 LAGRING

Vi lagrar all information i olika moln tjänster. Alla dessa tjänster använder sig av fysisk datalagring inom EU/EES och är alla reglerade av biträdesavtal mellan oss och tredjepart.

2.5 GALLRING

Vi får inte spara personuppgifter i våra system som vi inte har behov av. Gallring sker inom rimlig tid efter att det gällande syftet och korresponderade rättslig grund har utgått. Vid t ex en eventuell juridisk process kan det finnas ett berättigat intresse av att bevara personuppgifter längre. Normala intervallen för gallring är dock olika beroende på vilken typ av personuppgift som sparas, för vilket syften den har sparats, samt med vilken rättslig grund som den har sparats.

2.6 RÄTTELSE

En person som är registrerad i något av våra system har rätt att få sina uppgifter rättade om de är felaktiga. Om det visar sig att informationen vi har registrerat är felaktig rättas den så snart som möjligt.

2.7 RADERING

En person som är registrerad i något av våra system har rätt att få sina uppgifter raderade om det inte längre finns syfte för oss att bevara uppgifterna. Den registrerade måste då kontakta oss och meddela att den vill att vi tar bort information om personen i våra system.

När ett registrerat begär att bli raderad måste vi så snart som möjligt utreda om uppgifterna verkligen kan och ska raderas samt säkert identifiera personen. Kommer vi fram till att vi inte längre har ett syfte och en rättslig grund för behandlingen av personuppgiften kommer uppgifterna att raderas. Om utredningen visar att vi fortfarande har ett syfte för bevaring av uppgifterna, eller att det t ex finns en rättslig förpliktelse för att fortsatt behandla personuppgifterna raderas de inte. Exempelvis om det finns ett lagkrav eller krav från annan myndighet om att utlämna/spara uppgifter för att t ex upptäcka, förebygga eller uppmärksamma bedrägerier och eller andra brott.

2.8 RÄTT ATT BEHANDLA UPPGIFTERNA

För att få behandla uppgifterna måste vi ha en rättslig grund som tillåter oss att behandla uppgifterna. De rättsliga grunderna är uppräknade i dataskyddsförordningen och inga andra än de som uttryckligen skrivits där är tillåtna.

De grunder som kan bli aktuella för oss är:

- Samtycke
    - Samtycke från den registrerade
    - Kan vara muntligt eller skriftligt
- Avtal
    - Behandlingen är nödvändig för att fullgöra ett avtal som exempel:
        - Anställningsavtal
        - Förhandsavtal
        - Hyreskontrakt
- Rättslig förpliktelse
    - Det finns lagkrav eller myndighetsbeslut som kräver att uppgifterna behandlas, till exempel, Bokföringslagen
- Skydd för grundläggande intressen
    - Det finns ett allmänt intresse för att behandla personuppgiften
- Intresseavvägning
    - Vi har ett berättigat intresse för att behandla personuppgifterna

2.8 PERSONUPPGIFTSBITRÄDEN

Vi använder oss av underleverantörer och samarbetspartners till olika saker i vår verksamhet. Dessa underleverantörer kan behandla personuppgifter som vi samlat in och därmed också ansvarar för. Vi har tecknat personuppgiftsbiträdesavtal med våra personuppgiftsbiträden. Avtalet klargör att våra biträden ej får behandla personuppgifter för egen räkning och att de ska behandlas utifrån våra regler och policys som återfinns i detta dokument.

2.9 SÄKERHET

Dataskyddsförordningen kräver att system där personuppgifter behandlas sätter säkerhet främst, inte bara rent tekniskt utan även fysisk säkerhet i lokaler där data sparas samt rutiner för hur vi arbetar med personuppgifter i systemet.

Det innebär bland annat att vi har behörighetsstyrning i hur användare har rätt att använda våra system. Systemen får därmed flera nivåer av säkerhet, medarbetare ska endast kunna se de uppgifter de behöver för att kunna utföra sina arbetsuppgifter.

Vi vidtar alltid tekniska säkerhetsåtgärder för att säkerställa att personuppgifter skyddas mot förstöring genom olyckshändelse, mot obehörig ändring, otillåten spridning av eller otillåten tillgång till uppgifter, liksom mot annat slag av otillåten behandling av personuppgift.

2.10 PERSONUPPGIFTSINCIDENT

En personuppgiftsincident är när personuppgifter oavsiktligt eller olagligt förstörs, förloras, ändras, sprids eller på annat sätt behandlas på ett sätt som kan skada eller kränka den registrerade.

Exempel på personuppgiftsincidenter är:

- Någon stjäl en dator/telefon där personuppgifter är sparade
- En hacker tar sig in i en databas
- En medarbetare raderar felaktigt en person ur ett register
- En eller flera datorer får sina hårddiskar krypterade av ett virus

Observera att listan inte är uttömmande och att fler situationer kan kvalificera som personuppgiftsincidenter.

Vissa incidenter måste rapporteras till myndigheterna

Vid allvarliga incidenter ska också de registrerade som drabbats informeras.

En allvarlig personuppgiftsincident måste inom 72 timmar från det att vi blir medvetna om incidenten rapporteras till Integritetsskyddsmyndigheten.

Om personuppgifter skickas fel, försvinner, ändras utan lov eller liknande ska medarbetaren omgående kontakta IT-ansvarig eller annan ansvarig. Det är mycket viktigt att ansvarig medarbetare får informationen så tidigt som möjligt. Vi samlar så mycket information som möjligt om vad som hänt men ändrar eller raderar ingenting innan ansvariga kan påbörja en utredning.

Rutin vid personuppgiftsincident

När en medarbetare upptäcker en händelse som kan vara en personuppgiftsincident är det viktigt att denne samlar all möjlig information och kontaktar närmaste chef och IT-ansvarig eller annan systemadministratör.

Ansvarig utreder incidenten och vidtar de nödvändiga åtgärder efter bedömning av ärendets omständigheter och allvarlighet.

BILAGA 1: E-POST POLICY

Denna bilaga med specificerad e-post policy är till för alla våra medarbetare, kunder och samarbetspartners. Den beskriver för alla berörda parter hur vi ska hanterar e-postmeddelande som innehåller personuppgifter.

Denna policy är till för att hjälpa oss att hantera personuppgifter som kan förekomma i e-post på ett rättsligt sätt samt för att hjälpa oss att förekomma och förebygga att e-post innehållande personuppgifter hanteras på ett felaktigt sätt.

Inkommande E-post

Då e-post är ett av våra främsta verktyg för att kommunicera med alla nämnda parter hänvisar vi till en intresseavvägning för att kunna bedriva våra verksamheter som rättslig grund för att ta emot inkommande e-postmeddelanden. Det är av intresse för oss att öppna och i ett första läge läsa och behandla innehållet. Vi förutsätter att samma intresse finns hos avsändarparten.

Personuppgifter i E-post

De flesta e-postadresser kan i sig definieras som en personuppgift, då de innehåller ett personnamn i kombination med ett företagsnamn. Många meddelanden innehåller också en signatur från avsändaren som innehåller fler kontakt/personuppgifter. Personuppgifter av denna karaktär förutsätter vi att avsändarpersonen i och med sitt meddelande samtycker till att vi behandlar som kontaktinformation och kan sparas för vidare framtida kontakt.

Innehåller meddelandet fler personuppgifter så som lägenhetsnummer, kundnummer, ytterligare kontaktuppgifter eller andra personuppgifter av enklare natura ska vi alltid granska innehållet innan eventuell vidare behandling av uppgifterna som finns i meddelandet. I de fall då det är möjligt och systemstöd finns tillgängligt, så förs informationen över till ett strukturerat system, alternativt flyttas informationen över till annat dokument som i sin tur är säkerhetsanpassat utefter det aktuella syftet samt informationens natur.

Känsliga personuppgifter i E-post

Om ett e-postmeddelande skulle innehålla personuppgifter av känslig karaktär ålägger vi oss att efter en förtydligad kontakt insamla ett specifikt samtycke om att behandla personuppgiften. Återfinns inget syfte eller annat stöd för att behandla uppgiften raderas meddelandet. Om det efter granskning och införskaffat samtycke finns grund till behandling av uppgiften skall vi alltid föra ut den känsliga uppgiften från våra e-postprogram till annat system eller dokument med anpassade säkerhetsåtgärder. Vi skall heller aldrig vidarebefordra eller på annat sätt skicka vidare e-postmeddelanden som innehåller känsliga personuppgifter. De uppgifter som kan behöva delas internt eller med annan part i enlighet med det insamlade samtycket kommer att göras så på ett säkert sätt med andra systemstöd eller kommunikationsverktyg än normal e-post.

Övrigt

Vi använder ej e-post som ett verktyg för att lagra information utan endast för kommunikation. Personuppgifter som behöver lagras förs ut till andra säkerhetsanpassade system eller dokument.

Vi ska alltid vara ansvarsfulla i till vem vi skickar information och ska ha tillgång till uppdaterad kontaktinformation för att säkerställa att information inte skickas till fel eller ej behörig part.

Alla våra användare med tillgång till e-post har ett säkert lösenord och den primära enheten som används för e-posthantering är i sin tur lösenordskyddad. Alla extra eller mobila enheter där e-post kontot också kan vara installerade på ska alla vara lösenordskyddade.

Policyn gäller också alla övriga e-post mappar som kan finnas så som skickat, borttaget och utkast. I visa fall kan en konversation som innehåller personuppgifter i sin helhet arkiveras från kontot och sparas som en separat fil om det finns anledning och stöd för den typen av behandling.

Vi uppmanar alla användare att bibehålla en konstant gallring av sin e-post samt att den är väl sorterad och strukturerad för att förenkla en framtida gallrings process.

Vi särskiljer ej på e-post från kunder, samarbetspartners eller interna e-postmeddelanden, granskning och säkerhetsbedömning gäller alltid. Denna policy gäller för alla meddelanden som skickas eller tas emot av någon av våra e-postadresser.

Vi informerar alla mottagare om hela vår integritetspolicy inklusive denna bilaga angående e-post, genom att i alla våra signaturer hänvisa till våra hemsidor där denna information finns publicerad i sin helhet.

I och med denna policy anser vi att vi har uppfyllt de krav som gäller e-posthantering i samband med dataskyddsförordningen samt tagit tillvara på Integritetsskyddsmyndigheten rekommendationer angående e-posthantering som kan innehålla personuppgifter och som sammanfattas med följande punkter:

- Vi skickar inte känsliga personuppgifter via oskyddade e-postmeddelanden.
- Vi informera på våra hemsidor om denna policy och länkar till den samma i våra e-post signaturer.
- Alla inom organisationen är informerade om denna policy och de regler och rutiner som gäller för hur vi behandlar personuppgifter som kan förekomma i e-postmeddelanden.