

DATASKYDDSPOLICY FÖR HANTERING AV PERSONUPPGIFTER

Denna koncernövergripande policy är framtagen av Ekonomichef i samverkan med Bolagsjurist och Dataskyddskonsult. Den koncernövergripande policyn är vägledande för Balders samtliga dotterbolag men lokala avvikelser kan förekomma. Policyn ses över årligen och är antagen av bolagets styrelse.

1. BAKGRUND

Denna policy baseras på kraven enligt EU:s allmänna dataskyddsförordning (GDPR – Europaparlamentets och rådets förordning [EU] 2016/679) ("GDPR") och ska beskriva hur Fastighets AB Balder-koncernen ("Balder") behandlar information som direkt eller indirekt kan hänföras till fysiska individer ("personuppgifter"). Alla individer vars personuppgifter behandlas inom ramen för Balders verksamhet ska vara trygga med hur vi detta sker. Balders målsättning är att på ett tydligt och transparent sätt alltid redogöra vilka och på vilket sätt som personuppgifter behandlas i vår verksamhet och att möta gällande dataskyddslagstiftning på ett korrekt sätt.

Det ska noteras att det förekommer andra centrala dokument inom ramen för Balders dataskydd som benämns "policy", vilket dock inte ska förväxlas med Balders styrdokumentation, där denna Dataskyddspolicy ingår, o e. Dessa dokument markeras med * under Punkt 9 nedan.

2. SYFTE

Syftet med denna policy är att på ett övergripande plan ge riktlinjer för hur personuppgifter kan behandlas, för vilka syften och på vilket sätt.

Denna policy ska säkerställa att Balder:

- följer gällande dataskyddslagstiftning
- lagrar och hanterar personuppgifter på ett korrekt och enhetligt sätt
- kommunicerar tydligt och öppet gällande hur personuppgifter hanteras i verksamheten
- kan tillmötesgå anställdas, kunders och andra intressenters rättigheter
- skyddar den egna verksamheten mot hot och därmed minimerar integritetsrisker

3. OMFATTNING

Policyn har tagits fram av dataskyddsansvarig inom Balder och omfattar all behandling av personuppgifter som utförs inom koncernen. Dataskyddsansvarig är ekonomichef, som kan delegera roll, uppgift och/eller ansvar till bolagsjurist eller dataskyddskonsult. Policyn ska kompletteras med riktlinjer och rutiner för informationssäkerhet samt andra specifika verksamhetsområden.

Riktlinjerna ska efterlevas av ledning, anställda och likaså av andra personer som arbetar på uppdrag av eller under översyn av Balder, exempelvis konsulter eller partners.

4. GÄLLANDE DATASKYDDSLAGSTIFTNING

Hantering av och skyddet för personuppgifter regleras övergripande av EU:s allmänna dataskyddsförordning (GDPR - Europaparlamentets och rådets förordning [EU] 2016/679) samt kompletterande svensk lagstiftning i form av den kompletterande dataskyddslagen och tillhörande förordning (SFS 2018:218 och SFS 2018:219). Ytterligare relevant lagstiftning kan tillkomma.

Inom ramen för Balders verksamhet är huvudsakligen följande lagar och bestämmelser tillämpliga:

- EU:s allmänna dataskyddsförordning (GDPR)
- Den kompletterande svenska dataskyddslagen
- Diskrimineringslagen
- Arbetsmiljölagsstiftning och Arbetsmiljöverkets föreskrifter
- Semesterlagen
- Föräldraledighetslagen
- Lagen om sjuklön
- Lagen om anställningsskydd
- Lagen om medbestämmande i arbetslivet
- Arbetslöshetsförsäkringslagen
- Utsökningsbalken
- Bokföringslagen
- Marknadsföringslagen
- Marknadsmissbruksförordningen (samt kompletterande lagstiftning)
- Aktiebolagslagen
- Lag om skydd för personer som rapporterar om missförhållanden ("Visselblåsarlagen")

5. VIKTIGA BEGREPP OCH DEFINITIONER

Denna policy rör hantering av personuppgifter. Personuppgifter är all information som kan användas för att identifiera en enskild person, direkt eller indirekt. Begreppet personuppgifter inkluderar (men är inte begränsat till):

- Personuppgifter av generell karaktär, såsom namn, personnummer, e-postadress, telefonnummer, adress, postnummer, fotografi och videoinspelning, svar i marknadsundersökningar,
- Rekryteringsrelaterade personuppgifter, såsom profil på sociala medier, CV, personligt brev,
- Anställningsrelaterade personuppgifter, såsom anställningsform, anställningstid, kön, löne- och pensionsuppgifter, sjukfrånvaro, personuppgifter kopplat till en uppsägning eller ett avskedande, bankuppgifter, arbetad tid, anställningstid, medlemskap i fackförening,
- Personuppgifter relaterade till hyresgäst, intressent till BRF eller projekt etc, såsom objekts-, avtals-, lägenhetsnummer, lånelöfte, löneuppgifter, inkomst och ev bidrag,

- Referensutlåtanden och intyg avseende kandidater och hyresgäster,
- Personuppgifter relaterad till utföranden av arbetsuppdrag, såsom GPS-uppgifter för registrering i körjournal, medarbetarsamtal och personliga mål,
- Teknisk information såsom IP-adress, surfhistorik, cookies, inloggningsuppgifter, taggar och loggar avseende passersystem, energimätarinformation,
- Aktieägarrelaterade uppgifter, såsom närstående samt hemmavarande barn, innehav av aktier, samt röstetal.

I uttrycket **behandling av personuppgifter** inkluderas allting som görs där personuppgifter förekommer, exempelvis administration av, kommunikation med och lagring av sådana uppgifter för olika ändamål och i olika sammanhang.

I den mån **känsliga personuppgifter** förekommer i Balders verksamhet gäller särskilda regler för dessa. Känsliga personuppgifter är:

- Uppgifter som avslöjar ras eller etniskt ursprung,
- Uppgifter som avslöjar politiska åsikter,
- Uppgifter som avslöjar religiös eller filosofisk övertygelse,
- Uppgifter om medlemskap i fackförening,
- Uppgifter om hälsa,
- Uppgifter om sexualliv eller sexuell läggning,
- Genetiska uppgifter, och
- Biometriska uppgifter för att entydigt identifiera en fysisk person.

Observera att även uppgifter som indirekt avslöjar känslig information av detta slag inkluderas. Balder, och primärt Fastighets AB Balder, är **personuppgiftsansvarig** för de flesta av de personuppgiftsbehandlingar som förekommer i verksamheten. Med detta menas att organisationen är den juridiska person som är ytterst ansvarig för personuppgifterna, och som bestämmer över ändamål och medel. I specifika fall kan det vara så att någon annan än Balder är personuppgiftsansvarig. Roller och ansvarsfördelning mellan organisationen och eventuella **personuppgiftsbiträden** ska framgå för varje behandling i registerförteckningen.

6. ÄNDAMÅL MED BEHANDLING AV PERSONUPPGIFTER

Balder behandlar personuppgifter om anställda eller kandidater i den mån det är nödvändigt för att hantera och administrera rekryteringar samt för att Balder och anställda ska kunna utföra sina skyldigheter och tillvarata sina rättigheter enligt anställningsavtal, samt utföra sina arbetsuppgifter och övriga åtaganden i samband med anställningen.

Balder behandlar personuppgifter med ändamål att administrera, kommunicera och avtala med hyresgäster eller intressenter som visat intresse för våra objekt eller projekt och/eller önskar köpa eller hyra en bostad eller lokal, alternativt redan hyr en bostad, lokal, parkering, garage eller förråd från Balder, antingen i egenskap av privatperson eller som representant för en verksamhet.

För att ha ett fungerande IT-system och för att kunna bedriva Balders verksamhet på ett effektivt sätt behandlar Balder personuppgifter, vilket inkluderar att dessa delas med IT-leverantörer som behandlar personuppgifter på Balders uppdrag och instruktioner.

Balder behandlar personuppgifter för att administrera och följa upp deltagande i tävlingar, event samt marknadsundersökningar och utvärderingar, samt för att hantera, lagra och nyttja bild- eller filmmaterial.

Balder behandlar personuppgifter för att administrera och utföra brottsförebyggande och trygghetsskapande arbete samt för att hantera rättsliga anspråk där Balder är involverade, eller i övriga rättsliga ärenden.

Balder behandlar personuppgifter för att ingå och administrera kontakter och avtal med leverantörer eller partners.

Balder behandlar personuppgifter i syfte att tillhandahålla och administrera kontakter och besök med oss via vår hemsida eller sociala medier, eller när Balder skickar marknadsföring.

Balder hanterar rapporterade visseblåsningsärenden och uppfyller de skyldigheter som följer därav.

7. GENERELLA RIKTLINJER

7.1 Utbildning

Alla anställda ska få grundläggande dataskyddsutbildning, för att säkerställa förståelse för vikten av att hantera personuppgifter korrekt. Ansvarig för att utbildningen genomförs är dataskyddsansvarig.

Varje avdelning ansvarar för att berörda medarbetare får ta del av sådana instruktioner och rutiner som är relevanta för dem, och sådan information som behövs för att var och en ska kunna utföra sitt arbete i linje med dataskyddslagstiftningen. Detta inkluderar, men är inte begränsat till, utbildning av nyanställda.

7.2 Registerförteckning

Detaljerad information om varje slags behandling av personuppgifter som förekommer i processer, IT-system och på olika avdelningar inom ramen för Balders verksamhet ska finnas dokumenterad i organisationens registerförteckning. Förteckningen ska löpande hållas uppdaterad och fungera som ett heltäckande register över alla personuppgifts-behandlingar, i enlighet med kraven i artikel 30 GDPR.

Registerförteckningen administreras av dataskyddsansvarig. System- och informationsägare samt avdelningsansvariga kan komma att tilldelas ansvar för specifika delar av registerförteckningen i samarbete med dataskyddsansvarig. Förteckningen kan visas upp för tillsynsmyndigheten på begäran.

7.3 Rättslig grund

Varje behandling av personuppgifter ska ha en specificerad så kallad **rättslig grund** för att det ska vara lagligt att hantera personuppgifterna. Inga personuppgifter får behandlas hos Balder utan att det finns en identifierad och lämplig rättslig grund. En godtagbar rättslig grund kan exempelvis vara ett avtal som ska uppfyllas, ett berättigat intresse, en laglig skyldighet (till

exempel enligt bokföringslagen eller diskrimineringslagen) eller ett faktiskt samtycke från de registrerade. Alla de olika möjliga rättsliga grunderna finns listade i artikel 6 GDPR.

Det är inte tillåtet att behandla känsliga personuppgifter förutom i specifika undantagsfall, som i så fall ska finnas beskrivna i registerförteckningen samt i kompletterande policydokument/rutinbeskrivningar.

7.4 Ändamålsbegränsning och uppgiftsminimering

Personuppgifter får endast behandlas för specifika ändamål, i den utsträckning de behövs och i enlighet med dataskyddslagstiftningen.

Endast sådana personuppgifter som faktiskt behövs får samlas in och sparas. Inga uppgifter får sparas med lösa motiveringar såsom att de "kanske kan vara bra att ha".

Behandling av personuppgifter i nya sammanhang (för nya ändamål) måste alltid på förhand utvärderas och kontrolleras med dataskyddsansvarig, för att säkerställa att den nya hanteringen inte riskerar att kränka de registrerade personernas integritet eller på annat sätt bryta mot dataskyddslagstiftningen.

7.5 Behörighetsbegränsning

De personuppgifter som förekommer i verksamheten ska endast vara tillgängliga för personer som specifikt behöver dem i sitt arbete. För känsliga personuppgifter ska en snävare behörighetstilldelning generellt sett gälla än för mer harmlösa uppgifter.

7.6 Lagringsminimering

Personuppgifter som inte längre behövs (och som man inte heller är skyldig att spara) ska gallras löpande. Observera att det kan finnas lagkrav på att arkivera och spara uppgifter, men det ska finnas gallringsrutiner för varje process och varje system där personuppgifter förekommer. Var och en som arbetar där är skyldig att följa dessa rutiner.

Personuppgifter får inte användas på annat sätt eller överföras till och/eller behandlas på annan plats (system/lagringsställe/enhet) än vad som följer av gällande rutiner och instruktioner.

7.7 Information till registrerade

Alla vars personuppgifter hanteras av Balder har rätt till information om hur deras personuppgifter hanteras. Detta gäller såväl anställda som hyresgäster och andra grupper. Informationen ska vara lättillgänglig samt tillräckligt utförlig för att motsvara kraven i dataskyddslagstiftningen. Informationen ska lämnas på ett klart och tydligt sätt.

Informationen lämnas i huvudsak via intranätet (för anställda) och på den offentliga webbplatsen i form av en informationssida riktad till hyresgäster, bostadsrättsintressenter/köpare och användare.

7.8 De registrerades rättigheter

Balder ska ha rutiner och instruktioner på plats för hur organisationen ska fullgöra sina skyldigheter gentemot de registrerade. De registrerades rättigheter framgår av 3 kapitlet GDPR (artiklarna 12–23), och dessa rättigheter ska Balder vara beredda att tillmötesgå i alla situationer där det krävs. Detta omfattar ovan nämnda informationsskyldighet, men också rätten till tillgång (begäran om registerutdrag), rättelse, radering, begränsning, dataportabilitet samt rätten att invända.

7.9 Lagring och informationssäkerhet

Alla personuppgifter som finns hos Balder ska skyddas genom säkra servrar och andra lämpliga tekniska och organisatoriska säkerhetsåtgärder i enlighet med artikel 32 GDPR. Känsliga personuppgifter kräver generellt högre säkerhet än mer harmlösa uppgifter. Vidare specifikationer gällande informationssäkerhet inom Balder finns i separat IT-policy/Informationssäkerhetspolicy.

7.10 Utlämnande av personuppgifter till tredje part

Balder delar personuppgifter med bolag inom koncernen och med samarbetspartners och leverantörer på det sätt som beskrivs nedan.

- Balder delar personuppgifter med det bolag inom Balder-koncernen som hyr ut den aktuella bostaden, garaget, parkeringsplatsen eller förrådet,
- Balder delar personuppgifter om representanter för en organisation som är potentiella, nuvarande eller tidigare leverantörer eller partners med det bolag i koncernen som den aktuella kontakten eller avtalet rör,
- Balder delar personuppgifter med företag som Balder anlitar för utförande av olika servicetjänster och som behandlar personuppgifter på Balders uppdrag och enligt Balders instruktioner, t.ex. olika IT-leverantörer, partners för administration av marknadsföring och bolag som hanterar lön, annan ersättning och personalförmåner.
- Balder kan komma att lämna ut personuppgifter till myndigheter, t.ex. till Skatteverket, Försäkringskassan och Kronofogden, till Socialtjänsten i samband med en orosanmälan och till Polisen i samband med en polisanmälan,
- Vid uteblivna betalningar lämnas personuppgifter till inkassobolag som är självständigt personuppgiftsansvarig och bedriver inkassoverksamhet,
- Balder delar personuppgifter med myndigheter och domstolar i de fall Balder har en rättslig skyldighet att göra det eller i de fall som vi har ett rättsligt anspråk,
- Balder delar personuppgifter i sociala medier, såsom vid deltagande i en tävling eller ifall Balder publicerar en bild som personer medverkar i,
- Balder kan komma att dela personuppgifter till IT- och analysverktyg, såsom Google och Meta, vid analys av användningen av Balders hemsida i syfte att förbättra funktionaliteten på hemsidan samt tillhandahålla relevant och anpassad marknadsföring,
- Personuppgifter kommer att delas med företag som Balder samarbetar med och som i vissa fall har ett självständigt ansvar som personuppgiftsansvariga för de personuppgifter som de mottar, såsom försäkringsbolag, banker och revisionsbyråer.

Att lämna ut uppgifter på det sättet är i sig en behandling av personuppgifter. Det ska alltid finnas en laglig grund för ett sådant utlämnande och de registrerade ska ha fått information om att deras uppgifter lämnas ut utanför Balder.

7.11 Behandling av dina personuppgifter utanför EU/EES

De IT-leverantörer som vi använder oss av kan komma att överföra personuppgifter utanför EU/EES. Detta görs om det finns stöd för överföringen enligt GDPR. Det innebär att överföringen kan grundas på exempelvis EU-kommissionens beslut eller standardavtalsklausuler med kompletterande säkerhetsåtgärder.

7.12 Biträdesavtal

Balder anlitar endast personuppgiftsbiträden som garanterar lämpliga tekniska och organisatoriska åtgärder och på andra sätt kan ge garantier för att kraven i GDPR uppfylls också när en annan aktör behandlar personuppgifter för vår räkning. Det ska finnas skriftliga biträdesavtal med samtliga leverantörer och andra personuppgiftsbiträden. Dataskyddsansvarig ansvarar tillsammans med respektive informationsägare för att kontrollera att biträdesavtal finns och speglar kraven i artikel 28 GDPR.

7.13 Incidentrapportering

Var och en som upptäcker eller misstänker en incident som skulle kunna innebära en integritetsrisk, ska rapportera detta vidare till dataskyddsansvarig. En personuppgiftsincident kan vara allt ifrån att någon har tappat en mobiltelefon till en hackerattack där kundinformation och kontokortsinformation blivit stulna. Dataskyddsansvarig ansvarar för rutiner kring hantering av incidenter hos Balder. Mer information finns i separat Rutin för Hantering av personuppgiftsincidenter.

8. ROLLER OCH ANSVAR

Följande personer har särskilt ansvar för delar av dataskyddsarbetet:

- IT-chef
Ansvarar för upprättande av erforderlig säkerhet och uppfyllande av gällande IT- och säkerhetspolicy. IT-chef ingår i Incidenthanteringsgruppen.
- Ekonomichef
Utgör Dataskyddsansvarig och ansvarar för Balders regelefterlevnad av gällande dataskyddslagstiftning. Ekonomichef ingår i Incidenthanteringsgruppen.
- Dataskyddskonsult
Ansvarar för att på Dataskyddsansvarigs uppdrag säkerställa verksamhetens arbete med dataskydd och uppfyllande av GDPR. Dataskyddskonsulten ingår i Incidenthanteringsgruppen.
- GDPR-nätverket

GDPR-nätverkets medlemmar ska på instruktion och vägledning från Dataskyddsansvarig tillse och möjliggöra att Balders medarbetare har tillräcklig kännedom om GDPR och Balders interna styrande dokument och externa policydokument.

Medlemmen ansvarar för sitt verksamhetsområde, alternativt det system som en systemägare ansvarar för, samt vidare-förmedlar kunskap till organisationen och är Dataskyddskonsultens primära kontakt och länk gentemot sina respektive verksamheter och/eller system.

Varje avdelning som hanterar personuppgifter i sin verksamhet måste säkerställa att uppgifterna behandlas i enlighet med denna policy samt följer kompletterande uppsatta instruktioner.

Var och en som arbetar inom ramen för Balders verksamhet är skyldig att följa denna policy samt att samarbeta med ansvariga personer när det är relevant.

9. TILLSYNSMYNDIGHET

Balder har gjort bedömningen att ansvarig tillsynsmyndighet för verksamheten är Integritets- skyddsmyndigheten (IMY).

Enskilda personer som har klagomål gällande Balders hantering av personuppgifter har rätt att kontakta IMY.

10. KOMPLETTERANDE POLICYER OCH INSTRUKTIONER

Vidare riktlinjer och instruktioner som rör Balders personuppgiftsbehandling finns i följande dokument.

- Rutin för Hantering av personuppgiftsincidenter
- Rutin - Rättighetsutövning GDPR
- IT-policy
- Informationspolicy
- Visselblåsarpolicy
- Generell integritetspolicy*
- Integritetspolicy för uthyrning till privatpersoner*
- Integritetspolicy för kommersiell uthyrning*
- Integritetspolicy för nyproduktion*
- Integritetspolicy för rekrytering*
- Integritetspolicy för anställda*
- Integritetspolicy för anhöriga*
- Integritetspolicy för aktieägare, styrelseledamöter och personer med insiderinformation*
- Integritetspolicy visselblåsningsfunktion*

Göteborg 9 februari 2024

Styrelsen för Fastighets AB Balder