

Integritetspolicy för skydd av personuppgifter

Bonnier Fastigheter AB med dotterbolag

Giltig från och med: 2018-05-25

1. Inledning

Bonnier Fastigheter med dotterbolag påverkas liksom våra hyresgäster, kunder, leverantörer och anställda av digitaliseringen. Den ger oss möjligheter men också större ansvar för av att skydda de registrerades uppgifter och integritet.

Inom Bonnier Fastigheter med dotterbolag ska vi behandla personuppgifter enligt principerna i GDPR (General Data Protection Regulation) så att alla vi har kontakt med känner sig trygga med att vi behandlar deras personuppgifter på ett säkert och transparent sätt.

Vår policy fastställer de övergripande principer som gäller för behandling av personuppgifter inom Bonnier Fastigheter med dotterbolag, samt definierar ansvar och fördelar roller och ansvaret i enlighet med dataskyddsförordningen GDPR.

Denna policy gäller all personal som utför uppgifter för Bonnier Fastigheter med dotterbolags räkning i samband med behandling av personuppgifter. Det innefattar även personuppgiftsbiträden som utför databehandling på uppdrag av Bonnier Fastigheter med dotterbolag.

Vår policy är också avsedd att informera de registrerade om vår behandling av personuppgifter.

▬

Definitioner:

De definitioner vi använder i denna policy finner du i bilaga 1.

2. Ansvarsfördelning

Vd

Vd för Bonnier Fastigheter AB med dotterbolag har ansvarar för att verksamheterna är organiserad med tydlig ansvarsfördelning och tillräckliga resurser för att behandla personuppgifter i enlighet med GDPR och denna policy.

Verksamhetsansvariga chefer

Verksamhetsansvariga chefer för företagens respektive avdelningar (liksom personuppgiftsbiträdet) ska säkerställa att enheten organiserats med en tydlig ansvarsfördelning och tillräckliga resurser för behandling av personuppgifter.

Personuppgiftsansvarig

Den personuppgiftsansvarige är alltid ansvarig för behandlingen av personuppgifter. Personuppgiftsansvarig är alltid den juridiska person som styr och beslutar om behandlingen av personuppgifter. Det innebär att Bonnier Fastigheter eller dess dotterbolag är personuppgiftsansvarig för anställdas, konsumenters och leverantörers uppgifter.

Dataskyddsombud (DPO)

Huvuduppgiften för dataskyddsombudet är att se till att GDPR följs inom organisationen. Dataskyddsombudet ska också föra ett register över all behandling av personuppgifter som utförs inom organisationen.

Personuppgiftsbiträde

När externa leverantörer av IT-tjänster, molntjänster och dylikt behandlar personuppgifter för Bonnier Fastigheter eller dess dotterbolag räknas de för personuppgiftsbiträden. Personuppgiftsbiträdet ska behandla personuppgifterna i enlighet med ett avtal om behandling av personuppgifter. Det kan även finnas interna personuppgiftsbiträden, såsom tex konsulter, inom Bonnier Fastigheter med dotterbolag.

Anställda

Alla anställda har personligt ansvar för laglig och korrekt behandling av personuppgifter i sitt dagliga arbete. Genom att följa Bonnier Fastigheter med dotterbolags styrdokument för behandling av personuppgifter bidrar de anställda till att personuppgifter behandlas korrekt inom koncernen.

3. Dataskyddskrav

Förteckning personuppgifter

En förteckning över personuppgifter som omfattar Bonnier Fastigheter med dotterbolag ska ställas samman och underhållas som ett grundläggande krav för lagenlig behandling av personuppgifter. Verksamhetsansvariga chefer ansvarar för att all lokal behandling av personuppgifter dokumenteras.

4. Principer för behandling av personuppgifter

- **Laglig behandling** – när vi behandlar personuppgifter inom företagen ska vi vara säkra på att behandlingen överensstämmer med GDPR och att vi agerar öppet gentemot de registrerade.

Rättslig grund för behandlingen

Personuppgifter får endast behandlas om vissa villkor är uppfyllda, exempelvis:

- om den person som uppgifterna gäller har gett sitt **samtycke**,

- om behandlingen är nödvändig för att **uppfylla ett avtal** där den registrerade personen utgör en part,

- om **behandlingen är nödvändig** för att Bonnier Fastigheter med dotterbolag ska kunna uppfylla en **skyldighet enligt lag** eller

- om Bonnier Fastigheter med dotterbolag har **berättigade intresse** av att behandla personuppgifterna **överbäger individens intresse** av att slippa få sina personuppgifter behandlade.

- **Uppgiftsminimering** – vi som arbetar inom Bonnier Fastigheter med dotterbolag ska aldrig samla in eller behandla fler personuppgifter än vad som krävs för att uppfylla insamlingens ändamål. Det innebär att vi vid varje tillfälle då personuppgifter samlas in ska fråga oss om vår insamling är nödvändig. Om ändamålet med behandlingen av personuppgifterna upphör och inte längre är giltigt så ska vi radera uppgifterna som inte längre behövs.
- **Ändamålsbegränsning** – när vi samlar in personuppgifter ska vi ha tydligt och berättigat ändamål med insamlingen och en vidare behandling. Om ändamålet upphör att gälla så ska vi radera de personuppgifter som behandlats för det ändamålet. Om vi vill behandla personuppgifter för ett nytt ändamål får det inte vara oförenligt med det tidigare ändamålet, till exempel genom att ligga utanför vad den berörda registrerade personen rimligen kan förvänta sig. Vi ska också vara noga med att informera den registrerade om detta samt vilken rättslig grund vi har för att behandla personuppgifterna.
- **Korrekthet** – personuppgifterna ska vara korrekta och uppdaterade. Personuppgifter som är felaktiga eller inaktuella raderas eller rättas.
- **Lagringsminimering** – personuppgifterna ska bara lagras så länge som behövs för ändamålet med behandlingen, eller enligt kraven i tillämplig lagstiftning. När lagringsperioden har löpt ut ska uppgifterna raderas på ett permanent och säkert sätt. Om vi vill behålla personuppgifter längre än vad som krävs för ändamålet med insamlingen av uppgifterna måste vi se till att uppgifterna inte längre kan kopplas till den registrerade, vare sig direkt eller indirekt (anonymisering). När det gäller personuppgifter som samlats in från en person som vi har en kundliknande relation till behåller vi uppgifterna under en period som motsvarar bästa praxis enligt den nationella dataskyddsmyndigheten i respektive land.

5. Personuppgiftsansvarigas och personuppgiftsbiträdens skyldigheter

När personuppgifter behandlas av ett personuppgiftsbiträde på uppdrag av Bonnier Fastigheter med dotterbolag ska vi endast använda personuppgiftsbiträden som ger tillräckliga garantier för att de vidtar lämpliga tekniska och organisatoriska åtgärder för att behandlingen ska uppfylla kraven i dataskyddslagstiftningen och för att skydda den registrerades rättigheter.

Det ska finnas ett juridiskt bindande avtal mellan Bonnier Fastigheter eller dotterbolag och personuppgiftsbiträdet. Avtalet måste uppfylla kraven i dataskyddslagstiftningen och ska specifikt ange ansvarsfördelningen mellan parterna med avseende på behandling av personuppgifter:

- Förteckning över personuppgifter – enligt beskrivning i avsnitt Dataskyddskrav i detta policydokument.
- Inbyggt dataskydd och dataskydd som standard – varje ny tjänst eller affärsprocess som Bonnier Fastigheter med dotterbolag inför och som innebär behandling av personuppgifter ska utformas med tanke på att skydda dessa personuppgifter, till exempel genom att nödvändiga säkerhetsåtgärder byggs in i designen ("inbyggt integritetsskydd"). Varje sådan ny tjänst eller affärsprocess utformas också så att den som standard ser till att det bara är personuppgifter som är nödvändiga för behandlingens specifika ändamål som behandlas ("integritetsskydd som standard").
- Konsekvensbedömning avseende dataskydd – när en typ av behandling, särskilt då ny teknik som nya IT-system eller molntjänster används, sannolikt medför hög risk för en enskild persons integritetsskydd, ska Bonnier Fastigheter med dotterbolag innan behandlingen göra en konsekvensbedömning av hur behandlingsåtgärderna kan komma att påverka skyddet av personuppgifter. Konsekvensbedömningen görs i samråd med dataskyddsombudet.
- Underrättelse om personuppgiftsincident – anställda som misstänker ett brott mot denna policy eller relevant dataskyddslagstiftning ska omedelbart kontakta närmaste chef eller dataskyddsombudet så att företagen uppfyller de lagstadgade kraven på underrättelse.
- Tillgodose de registrerades samtliga rättigheter – enligt beskrivning i avsnitt De registrerades rättigheter nedan i policydokument.
- Säkerhetsåtgärder – en anställd som har tillgång till personuppgifter får endast behandla dem enligt ändamålet med behandlingen och får inte dela, sprida eller på annat sätt vidarebefordra uppgifterna till någon tredje part såvida inte Bonnier Fastigheter med dotterbolag gett uttryckliga instruktioner om detta. Lämpliga tekniska och organisatoriska åtgärder ska vidtas för att skydda personuppgifterna mot oavsiktlig eller olaglig förstöring, oavsiktlig förlust eller förvanskning, otillåten spridning av eller tillgång till uppgifterna samt alla andra former av olaglig behandling. Åtgärderna ska vara lämpliga i förhållande till de risker som behandlingen medför och till den typ av personuppgifter som behandlas.
- Gränsöverskridande dataöverföring – innan överföring av personuppgifter till organisationer utanför EES får inte ske utan godkännande av närmaste chef och samråd med dataskyddsombudet.
- Utbildning och medvetenhet – Bonnier Fastigheter med dotterbolag tillhandahåller adekvat utbildning för alla anställda i linje med de anställdas ansvarsområden.

6. Den registrerades rättigheter

Bonnier Fastigheter med dotterbolag ska bemöta de registrerades önskemål och synpunkter utifrån de krav som lagen ställer på oss eller vad som kan anses vara rimligt, praktiskt och lämpligt. Bedömning av detta görs i samråd med dataskyddsbudet.

- **Öppenhet och information** – personerna vars uppgifter vi behandlar ska informeras om att deras uppgifter behandlas. Informationen ska vara kortfattad, lättillgänglig och klart och tydligt formulerad med de uppgifter som vi är skyldiga att uppge.
- **Rätt att få tillgång** – enskilda personer kan begära att få information om Bonnier Fastigheter med dess dotterbolags behandling av deras personuppgifter.
- **Rätt till rättelse eller radering** – enskilda personer kan begära rättelse eller radering av personuppgifter.
- **Rätt att invända** – enskilda personer kan begära att den automatiska behandling av deras personuppgifter begränsas.
- **Rätt att klaga** - enskilda personer har rätt att komma med klagomål på Bonnier Fastigheter med dess dotterbolags behandling av deras personuppgifter.
- **Rätt till ersättning** - enskilda personer kan ha rätt till ersättning för eventuella skador.

7. Intern granskning

VD för Bonnier Fastigheter AB med dotterbolag är ansvarig för den övergripande tillsynen och tillämpningen av denna policy. Dataskyddsbudet (dataskyddsansvarig på enhetsnivå) är ansvarig för företagets dagliga efterlevnad av denna policy, dataskyddslagstiftningen och interna gallringsrutiner. Dataskyddsbudet kan kontaktas på dpo@bonnierfastigheter.se.

Bilaga 1 Definitioner av begrepp i denna policy

Personuppgiftsansvarig:

personuppgiftsansvarig är den fysiska eller juridiska person, myndighet eller annan organisation som ensam eller tillsammans med andra avgör ändamålet och metoden för behandlingen av personuppgifter. När ändamål och metoder bestäms av EU:s eller medlemsstatens lagstiftning kan även den personuppgiftsansvarige eller specifika kriterier för utnämmandet av denne bestämmas i lag.

Den registrerade:

den fysiska levande person som personuppgifterna gäller. Den registrerade definieras enligt denna policy som en fysisk person som Bonnier Fastigheter med dotterbolag har någon form av relation till, exempelvis en konsument, anställd, konsult eller liknande.

Personuppgiftsbiträde:

en fysisk eller juridisk person, myndighet, institution eller annan organisation som behandlar personuppgifter åt den personuppgiftsansvarige.

Dataskyddslagstiftning:

a) i EU-länder direktivet (95/46/EG) som ersätts av dataskyddsförordningen GDPR (förordning (EU) 2016/679)

b) i länder utanför EU alla liknande eller motsvarande lagar, förordningar eller regler som rör personuppgifter

c) alla bindande riktlinjer eller regler för god praxis som ges ut av en lokal myndighet ansvarig för administrering av dataskyddslagstiftning och/eller

d) alla tillägg till, återantaganden av eller ändringar i de dokument som nämns i punkt (a) till (c) och som kan komma att göras vid behov.

EES:

EU:s medlemsstater samt Island, Liechtenstein, Norge och Schweiz.

EES-personuppgifter:

personuppgifter som rör registrerade inom EES.

Personuppgifter:

varje uppgift som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett personnummer, en lokaliseringssuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Behandling:

en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering,

organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.