# Bolagets policy för behandling av personuppgifter

## 1 Bakgrund och syfte

1.1 Svea Boende värnar om sina kunders, leverantörer, partners och anställdas integritet och är alltid mån om att följa gällande dataskyddsregelverk. Var och en har rätt till skydd av de personuppgifter som rör honom eller henne.

1.2 Svea Boende har därför antagit denna Policy för behandling av personuppgifter för att säkerställa att alla inom organisationen följer dataskyddsreglerna. Det här dokumentet avser att ge dig som medarbetare närmare vägledning om hur du ska behandla personuppgifter.

1.3 Den 25 maj 2018 börjar dataskyddsförordningen tillämpas. Den medför ett förstärkt skydd för de personer vars personuppgifter behandlas och den ställer fler och hårdare krav på organisationer som behandlar personuppgifter.

1.4 Om en behandling av personuppgifter skulle strida mot bestämmelserna i dataskyddsförordningen finns risken för intrång i den personliga integriteten för de registrerade, men även risken för skadat anseende för [Bolaget]. Vidare kan Bolaget dessutom bli skyldig att utge skadestånd eller påföras en administrativ sanktionsavgift på upp till tjugo miljoner euro eller 4 % av den totala globala årsomsättningen, beroende på vilket värde som är högst. För att undvika sådana konsekvenser är alla medarbetare skyldiga att följa dessa riktlinjer.

## 2 Tillämpningsområde och omfattning

2.1 Policyn gäller för Svea Boende alla anställda och konsulter, på alla marknader och vid var tid.

2.2 Svea Boende styrelse ska se till att denna Policy efterlevs, vilket bland annat innefattar utbildning för alla anställda. Informationen till de anställda ska även innefatta information om att överträdelse av policyn kan komma att medföra t ex arbetsrättsliga konsekvenser.

## 3 Grundläggande principer

3.1 De grundläggande principer som beskrivs nedan ska alltid iakttas när personuppgifter behandlas. Svea Boende ansvarar för och ska kunna visa att principerna efterlevs. 3.1.1 *Laglighet, skälighet, transparens* – Personuppgifter ska behandlas lagligt, korrekt och transparent i förhållande till den registrerade. Det innebär att varje typ av behandling ska baseras på en giltig s k laglig grund, såsom exempelvis fullgörande av avtal, fullgöra en rättslig förpliktelse, utföra en uppgift av allmänt intresse, berättigat intresse eller samtycke (se avsnitt 5 nedan). Kan man inte identifiera någon laglig grund som är tillämplig för behandlingen får behandlingen således inte utföras. Utgångspunkten för denna princip är tydlig kommunikation med den registrerade om bl a för vilka ändamål personuppgifterna behandlas, vilken typ av behandling som utförs, om och hur personuppgifterna delas med andra, hur länge personuppgifterna lagras och hur man kommer i kontakt med Svea Boende. De registrerade ska alltså ges tydlig och transparent information om behandlingen av deras personuppgifter.

3.1.2 *Ändamålsbegränsning* – Personuppgifter får endast samlas in och på annat sätt behandlas för särskilda, uttryckligt angivna och berättigade ändamål och de får inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.

3.1.3 *Uppgiftsminimering* – Personuppgifter som behandlas ska vara adekvata, relevanta och inte alltför omfattande i förhållande till ändamålen. Säkerställ att uppgifterna som samlas in verkligen behövs och fråga inte efter information bara för att den kanske kan vara bra att ha.

3.1.4 *Riktighet* – personuppgifter som behandlas ska vara korrekta och om nödvändigt uppdaterade. Vidta lämpliga åtgärder för att se till att felaktiga eller ofullständiga uppgifter rättas, exempelvis rutiner för ändring av adress vid flytt med en sammanställning av system och register där adressen lagras. Undvik dock att lagra kopior av uppgifterna i många system i syfte att undvika felkällor och att ouppdaterad information sparas.

3.1.5 *Lagringsbegränsning* – Personuppgifter får inte lagras under längre tid än nödvändigt med hänsyn till ändamålen med behandlingen. När uppgifterna inte längre behövs måste dessa gallras, vilket innebär att de antingen måste raderas eller avidentifieras.

3.1.6 Principen om ansvarsskyldighet innebär att Svea Boende måste kunna visa att dataskyddsförordningen efterlevs. Bolaget måste därför exempelvis dokumentera implementerade och planerade processer och åtgärder som avser dataskyddsfrågor.

Vidare ska det finnas ett register över alla typer av behandlingar av personuppgifter som utförs och Svea Boende ska kunna redovisa ett sådant register för tillsynsmyndigheten när så krävs.

## 4 Personuppgifter

4.1 *Personuppgifter* är alla uppgifter som avser en identifierad eller identifierbar fysisk person och som direkt eller indirekt kan identifiera en person. Exempel på personuppgifter är namn, kontaktuppgifter, lokaliseringsuppgifter eller faktorer som är specifika för en persons fysiska, ekonomiska, kulturella eller sociala identitet. Uppgifter som enskilt inte når upp till kraven kan tillsammans ändå utgöra personuppgifter.

4.2 All behandling av personuppgifter omfattas av dataskyddsförordningen och dess regler. Med *behandling* menas en åtgärd eller kombination av åtgärder avseende personuppgifter, som utförs helt eller delvis automatiserat. Även personuppgifter i e-post och i dokument på servrar, i en enkel lista, på webbplatser och i annat ostrukturerat material omfattas.

4.3 Behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter, uppgifter om hälsa eller uppgifter om en persons sexualliv eller sexuella läggning (s k *särskilda kategorier av personuppgifter*) är som huvudregel förbjuden. För att sådan behandling ska vara tillåten krävs ett giltigt undantag från förbudet. De vanligaste undantagen är att den registrerade lämnat samtycke eller själv offentliggjort uppgifterna, för att utöva rättigheter eller fullgöra skyldigheter inom arbetsrätten, för att kunna fastställa, göra gällande eller försvara rättsliga anspråk eller för hälso- och sjukvårdsändamål.

4.4 Behandling av *personnummer* får bara utföras om det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

4.5 Behandling av uppgifter om *lagöverträdelser* (fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder men sannolikt inte uppgift om misstanke om brott) får endast behandlas i vissa särskilda fall. Vi får behandla personuppgifter om behandlingen är nödvändig för att rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras i ett enskilt fall eller för penningtvättskontroll.

## 5 Laglig grund för behandlingen av personuppgifter

5.1 En behandling av personuppgifter är endast laglig om och i den mån någon av följande grunder är tillämplig.

5.1.1 Den registrerade har lämnat sitt *samtycke* till att personuppgifterna behandlas för ett eller flera specifika ändamål. Särskilda krav finns som måste vara uppfyllda för att samtycket ska vara giltigt.

5.1.2 Behandlingen är nödvändig för att *fullgöra ett avtal* i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.

5.1.3 Behandlingen är nödvändig för att *fullgöra en rättslig förpliktelse* som åvilar [Bolaget]. Som exempel kan här nämnas kontrolluppgifter som lämnas till Skatteverket.

5.1.4 Behandlingen är nödvändig för att skydda intressen som är av *grundläggande betydelse* för den registrerade eller för en annan fysisk person (t ex när det är fara för livet).

5.1.5 Behandlingen är nödvändig för ändamål som rör [Bolagets] eller tredje parts intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, (*intresseavvägning*). Vid intresseavvägning tillkommer särskilda krav på dokumentation avseende den bedömning som gjorts.

## 6 Säkerhetsåtgärder, behörighetsstyrning och åtkomst, radering

6.1 Personuppgifterna ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna med användning av tekniska och organisatoriska åtgärder. Organisatoriska säkerhetsåtgärder kan innebära att behörighetskontroll används för de system som innehåller personuppgifter, loggning av åtkomst till personuppgifter eller att datorer och dylikt som innehåller personuppgifter ska förvaras så att obehörig åtkomst försvåras och inte lämnas framme. Exempel på tekniska åtgärder som måste kontrolleras är om Bolaget har tillräckliga back-up rutiner, tillräckliga brandväggar, lösenordskyddade trådlösa nätverk, uppdaterat virusskydd, lösenordsskydd för mobila enheter såsom mobiltelefoner och surfplattor, skydd mot obehörig intern åtkomst, lösenordskrav, kryptering vid behov, loggning av, åtkomst till och användning av IT-system m m.

6.2 Personuppgifter får inte bevaras längre än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Genom att upprätta och följa en gallringsrutin för respektive databas/behandling säkerställer man det strukturerade gallringsarbetet. Även personuppgifter i så kallat ostrukturerat material såsom i dokument på servrar, i en enkel lista, på webbplatser etc behöver raderas när ändamålet med behandlingen är uppfyllt.

## 7 Överföring till tredje land

7.1 För överföring av personuppgifter till länder utanför EU och EES (så kallad tredjelandsöverföring) gäller särskilda regler. Dataskyddsförordningen innebär att alla EU:s medlemsstater samt EES-länderna har ett likvärdigt skydd för personuppgifter och personlig integritet och därför kan personuppgifter föras över fritt inom det området utan begränsningar. För länder utanför det området finns däremot inte några generella regler som ger motsvarande garantier och därför får tredjelandsöverföring endast ske under särskilda förutsättningar. Det här berör varje form av överföring av information över gränserna, t ex många online IT-tjänster, molnbaserade tjänster, tjänster för extern åtkomst eller globala databaser m m och behöver analyseras särskilt.

## 8 Konsekvensbedömning

8.1 Svea Boende har en särskild rutin på plats för att kunna identifiera och hantera särskilda integritetsrisker inom verksamheten och för strukturerad uppföljning. Särskilda risker för fysiska personers rättigheter och friheter kan exempelvis förekomma i samband med en viss typ av behandling av uppgifter, särskilt känsliga uppgifter, behandling i särskilt stor omfattning, användning av ny teknik eller dylikt.

8.2 Om en ny eller ändrad personuppgiftsbehandling i visst avseende sannolikt kan komma att medföra hög risk för fysiska personers rättigheter och friheter ska rutinen följas och en bedömning göras av effekterna av de påtänkta behandlingarna för skyddet av personuppgifter innan behandlingen påbörjas.

8.3 Innan sådan personuppgiftsbehandling påbörjas ska ansvarig på bolaget kontaktas för utredning om en konsekvensbedömning krävs och vid behov utförs konsekvensbedömning tillsammans med den ansvarige genom [besvarande av vissa särskilda frågor, arbetsmöten samt riskbedömning].

## 9 Registerutdrag och utlämnande

9.1 Dataskyddsförordningen ger de registrerade ett flertal rättigheter vad gäller behandling av personuppgifter. Det är [Bolagets] uppgift att uppfylla dessa rättigheter och tillse att tillräckliga processer härför finns för att tillmötesgå de registrerade. 9.1.1 Den registrerade har rätt till *information* när personuppgifterna samlas in. Denna information ska tillhandahållas i en lättillgänglig skriftlig form med ett klart och tydligt språk. I dataskyddsförordningen föreskrivs ett antal tydliga krav som måste vara uppfyllda och kraven varierar beroende på om informationen har samlats in från den registrerade själv eller från tredje man.

9.1.2 Den registrerade har rätt att få bekräftelse på huruvida personuppgifter som tillhör denne behandlas, och i sådana fall få en kopia av personuppgifterna (*registerutdrag*). Denna rättighet gäller oberoende av den plats där personuppgifterna behandlas.

9.1.3 Om personuppgifter som behandlas är felaktiga eller ofullständiga kan den registrerade kräva *korrigering*. Om den registrerade visar att ändamålet för vilket personuppgifterna behandlas inte längre är tillåtet, nödvändigt eller rimligt under omständigheterna, ska de aktuella personuppgifterna *raderas*, om det inte finns några lagbestämmelser som anger annat.

9.1.4 Den registrerade har rätt att överföra personuppgifter som denne lämnat till [Bolaget] till annan personuppgiftsansvarig (rätt till *dataportabilitet*) om behandlingen stöds på de lagliga grunderna avtal eller samtycke. Personuppgifterna ska tillhandahållas den registrerade i ett strukturerat, allmänt använt och maskinläsbart format. Om det är tekniskt möjligt kan den registrerade begära att uppgifterna överförs direkt till annan personuppgiftsansvarig. Rätten gäller endast för de personuppgifter som den registrerade själv har lämnat till [Bolaget].

9.1.5 Den registrerade har i vissa fall rätt att kräva att [Bolaget] *begränsar behandlingen* av dennes personuppgifter, d v s begränsar behandlingen till vissa avgränsade syften. Rätten till begränsning gäller bland annat när den registrerade anser att uppgifterna är felaktiga och har begärt att personuppgifterna rättas. Den registrerade kan då begära att behandlingen av personuppgifterna begränsas under tiden uppgifternas korrekthet utreds. När begränsningen upphör ska den enskilde informeras om detta.

9.1.6 Den registrerade har rätt att *invända mot behandling* av personuppgifter som stöds på legitimt intresse som rättslig grund. Vid en invändning ska Bolaget upphöra med behandlingen om man inte kan visa tvingande legitima grunder för behandlingen som överväger den registrerades intressen, rättigheter och friheter eller om behandlingen av personuppgifter utförs för etablering, utövande eller försvar av rättsliga anspråk.

9.1.7 I vissa fall har den registrerade rätt att begära radering av sina personuppgifter (”*rätten att bli bortglömd*”). Ett exempel är när samtycke är den lagliga grunden för behandlingen och den registrerade återkallar sitt samtycke.

9.1.8 När personuppgifter behandlas för *direktmarknadsföring* har den registrerade rätt att när som helst invända mot behandling av personuppgifter om denne. Om en registrerad motsätter sig behandling av personuppgifter för direktmarknadsändamål ska behandling för sådana ändamål upphöra.

**10 Personuppgiftsincidenter**

10.1 En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstörelse, förlust, ändring eller obehörig åtkomst till personuppgifter. Exempel på personuppgiftsincidenter kan vara stöld av kundregister, oavsiktligt avslöjande av löneinformation via e-post till fel mottagare, en anställd tar hem en okrypterad arbetsdator som senare stjäls i ett inbrott och som leder till att information om anställda eller kunder avslöjas, personuppgifter publiceras på webben av misstag, en bärbar dator innehållande personuppgifter tappas bort eller stjäls, m m.

10.2 Personuppgiftsincidenter kan behöva anmälas till tillsynsmyndigheten inom 72 timmar från upptäckten av incidenten om det är sannolikt att det föreligger en risk för fysiska personers rättigheter och friheter. Inträffade incidenter ska dokumenteras och man kan behöva underrätta berörda registrerade.

10.3 Vid en misstänkt personuppgiftsincident kontakta omedelbart ansvarig på [Bolaget] Det är sedan ansvarig som avgör om tillsynsmyndigheten eller de registrerade behöver underrättas.

**11 Övrigt**

11.1 För definitioner avseende termer som används i den här policyn hänvisas till dataskyddsförordningen.

11.2 Denna policy ska uppdateras årligen eller vid behov baserat på instruktioner från Svea Boende styrelse.

**12 Frågor**

Vid frågor som anknyter till behandling av personuppgifter, vänligen kontakta ansvarig på Svea Boende.

_____

Policy antagen av Svea Boende styrelse.