

Aroseken Fastighet AB  
Badhusgatan 5  
722 15 Västerås

## **Tillsyn enligt personuppgiftslagen (1998:204) – användning av s.k. elektroniska nycklar hos ett bostadsbolag**

### **Datainspektionens beslut**

Datainspektionen konstaterar att Aroseken Fastighet AB inte får spara passage-loggar under längre tid än två veckor för ändamålen teknisk felsökning och underhåll.

Datainspektionen finner att Aroseken Fastighet AB:s behandling av personuppgifter på denna punkt inte är förenlig med 9 § personuppgiftslagen. Datainspektionen förutsätter dock att Aroseken Fastighet AB vidtar åtgärder för att komma tillrätta med den påpekade bristen.

Ärendet avslutas.

### **Redogörelse för tillsynsärendet**

Datainspektion har under året arbetat med ett tillsynsprojekt för att granska bostadsbolags och bostadsrättsföreningars behandling av personuppgifter i samband med att s.k. elektroniska nycklar används.

Som ett led i projektet genomförde Datainspektionen en inspektion hos Aroseken Fastighet AB (Aroseken) den 10 april 2007. Vid inspektionen framkom att Aroseken använder elektroniska nycklar till följande gemensamma utrymmen; källarförråd, cykelrum, soprum, tvättstugor och portentréer. Bokning av tvättstugor sker via elektroniska bokningstavlor i fastigheten. Bolaget använder också en typ av porttelefon som kallas "FreeCall" i sina studentlägenheter. Hyresgästen låter registrera sitt telefonnummer i systemet. Den som vill besöka hyresgästen ringer upp denne. Hyresgästen ringer därefter upp systemet från den telefon vars nummer är registrerat. Portentrén öppnas om den uppringande telefonen är densamma som har registrerats i systemet. Användningen av "FreeCall" loggas i systemet. De hyresgäster som har valt att inte använda "FreeCall" får gå ner till porten och öppna för sina besökare.

Efter att Aroseken fått tillfälle att yttra sig över inspektionsprotokollet begärde Datainspektionen att bolaget skulle komma in med en skriftlig åtgärdsplan. Åtgärdsplanen skulle innehålla en beskrivning av vilka åtgärder som bolaget hade

vidtagit eller skulle komma att vidta med anledning av de brister i bolagets behandling av personuppgifter i förhållande till personuppgiftslagen som vi har påpekat.

Aroseken har kommit in med en åtgärdsplan med i huvudsak följande innehåll.

Vad gäller de elektroniska nycklarna kopplas varje nyckelnummer till ett lägenhetsnummer. Det har ansetts nödvändigt att veta vem eller vilka som har viss nyckel för snabb och effektiv spärrning då en sådan nyckel har förkommit. Vad gäller systemet för inpassering, "Free-Call", lagras systemet respektive hyresgästs telefonnummer för att säkerställa att endast den som är behörig att öppna en ytterdörr. Ovanstående uppgifter anser bolaget vara absolut nödvändigt för att systemen ska fungera och för att upprätthålla en acceptabel nivå på säkerhet för hyresgästerna. Sammantaget anser bolaget att de aktuella systemen är till stor nytta för hyresgästerna genom en smidigare inpassering, tvättstugebokning samt mottagande av besökare.

För inpassering och tvättstugebokning används lägenhetsnummer. Bolaget anser dock inte att ett lägenhetsnummer i sig är en ren personuppgift. Lägenhetsnumret är bolagets interna benämning på ett uthyrningsobjekt. Den som får tillgång till bolagets uthyrningssystem kan förstås göra en koppling till ett "hushåll", men det är inte något integrerat system och dessutom behörighetsbegränsat.

Uppgifterna som kopplar ett visst nyckelnummer till ett visst lägenhetsnummer kommer att sparas så länge hyresförhållandet består. Detsamma gäller hyresgästens telefonnummer i "FreeCall". Anledningen till detta är att systemen annars inte skulle gå att hantera, såsom beskrivits ovan.

När det gäller gallring av de uppgifter som registreras i loggarna för inpassering, tvättstugebokning och besöksinpassering kommer nya rutiner att införas omgående. Vad gäller loggar för inpassering anser bolaget det angeläget att spara dessa under en kortare tid för att kunna felsöka och åtgärda fel i systemets funktionalitet då det fallerar av olika anledningar. Bolaget har valt en månad som frekvens för rensning för att säkerställa att rensning verkligen sker då den kan sammanläggas med andra administrativa rutiner med samma frekvens. Vad gäller loggar för tvättstugebokning behöver de sparas i en månad, då en bokning av tvättstugan kan göras upp till 30 dagar i förväg.

Bolaget anser att 10 § punkten f personuppgiftslagen i viss mån bör vara tillämplig. Bolaget anser att den eventuella negativa inverkan som loggningen innebär för hyresgästen är mindre än nyttan av att kunna erbjuda ett system som är driftsäkert och väl fungerande. Dessutom ska samtliga hyresgäster informeras om vilka uppgifter som lagras och skälet därtill.

Nya hyresgäster kommer att muntligen och skriftligen informeras i samband med kontraktsskrivning. Redan befintliga hyresgäster kommer att informeras skriftligen inom två månader i samband med utskick av hyresavi.

Bolaget har tecknat ett personuppgiftsbiträdesavtal med sitt personuppgiftsbiträde.

Bolaget avser inte att vidta några ytterligare säkerhetsåtgärder än de som redovisats vid Datainspektionens besök. Bolaget anser att de åtgärder som är rimliga att vidta har beaktats vad gäller antalet användarkonton, inpassering, lokal installation av systemövervakande program samt säkerhetskopiering.

### **Skäl för beslutet**

#### *Allmänt*

I ett elektroniskt nyckelsystem kan man, till skillnad från ett system med ”vanliga” nycklar, enkelt spärra en borttappad nyckel och andra nycklar och lås behöver inte bytas ut. Huvudskälet för ett bostadsbolag eller en bostadsrättsförening att införa ett system med elektroniska nycklar är att underlätta sin hantering av nycklar.

Den behandling av personuppgifter som utförs i elektroniska nyckelsystem hos bostadsbolag och bostadsrättsföreningar sker i mycket nära anslutning till den privata sfären, dvs. bostaden. Med tanke på detta finns anledning att i särskilt hög grad beakta integritetsintresset.

Bostadsbolag eller bostadsrättsföreningar som använder elektroniska nyckelsystem registrerar ”nycklar”, lägenhetsnummer och vilken behörighet respektive ”nyckel” ska ha i systemet. Detta behövs för att systemet över huvud taget ska fungera och är närmast att betrakta som administrativa åtgärder.

Datainspektionen har en restriktiv syn på att använda uppgifterna i de elektroniska nyckelsystemen för andra ändamål än att öppna dörrar, boka tvättider och liknande. Vi anser att det inte är godtagbart att man i de elektroniska nyckelsystemen lagrar stora uppgiftsmängder för andra ändamål.

Den elektroniska nyckeln består i många fall av en liten bricka. För att t.ex. låsa upp en dörr hålls brickan framför en läsare. I samband med detta kan brickans identitetsnummer, lägenhetsnumret samt tidpunkten och platsen (vilken läsare) registreras i en databas. På detta sätt skapas en s.k. passagelogg.

Registrering av passageloggar innebär ett intrång i den personliga integriteten. Den möjliggör övervakning av när enskilda personer går till och från utrymme- na i anslutning till sin bostad. Från integritetssynpunkt är möjligheten att övervaka enskilda känslig och uppgifterna kan missbrukas. För att få behandla personuppgifter i passageloggar måste höga krav ställas på behandlingen och ändamålen med den. Behandlingen måste också vara proportionerlig i förhållande till det intrång i den personliga integriteten som registreringen innebär.

*Vilka regler är tillämpliga?*

Personuppgiftslagen gäller i första hand sådan behandling av personuppgifter som är automatiserad (5 § personuppgiftslagen). Med personuppgift menas all slags information som direkt eller indirekt kan hänföras till en person som är i livet (3 § personuppgiftslagen).

Datainspektionen har i tidigare ärenden gjort bedömningen att elektroniska nyckelsystem i bostadsrätts- och hyreshus, där lägenhetsnummer kan kopplas till en eller flera personer, innebär en behandling av personuppgifter i personuppgiftslagens mening (se bl.a. dnr 330-2002 och 970-2004).

Den behandling av personuppgifter som Aroseken utför i sitt elektroniska nyckelsystem omfattas således av personuppgiftslagen. Även bolagets behandling av personuppgifter i "FreeCall" omfattas av personuppgiftslagen.

Datainspektionen anser vidare att materialet är strukturerat på ett sådant sätt att de s.k. hanteringsreglerna i personuppgiftslagen är tillämpliga på den aktuella behandlingen (5 a § personuppgiftslagen).

*Är behandlingen av personuppgifter förenlig med personuppgiftslagen?*

I 9 § personuppgiftslagen ställs ett antal grundläggande krav när det gäller behandling av personuppgifter upp. Den personuppgiftsansvarige ska se till att personuppgifter samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål. Personuppgifterna får sedan inte behandlas för något ändamål som är oförenligt med dem för vilka uppgifterna samlades in. De personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen och fler uppgifter än nödvändigt med hänsyn till ändamålen får inte behandlas. Personuppgifter får inte heller sparas under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Som huvudregel får personuppgifter bara behandlas om den registrerade har lämnat sitt samtycke till behandlingen. Behandlingen kan dock vara tillåten om den är nödvändig av vissa andra skäl. Till exempel kan behandlingen vara tillåten om den är nödvändig för att fullgöra en rättslig skyldighet eller för att ett berättigat intresse hos bolaget ska kunna tillgodoses och detta intresse väger tyngre än intresset av skydd av den personliga integriteten (10 § personuppgiftslagen).

Faktorer som spelar in vid en sådan s.k. intresseavvägning avseende ett bostadsbolags behandling av personuppgifter i ett elektroniskt nyckelsystem är exempelvis för vilket ändamål personuppgifterna behandlas, om samma ändamål kan uppfyllas på ett mindre integritetskänsligt sätt, om de boende motsätter sig behandlingen, vilka gallringsrutiner som finns, vilken information de boende får samt säkerheten kring uppgifterna. Dessa faktorer har betydelse även vid en intresseavvägning avseende "FreeCall".

Aroseken har i sin åtgärdsplan preciserat för vilka ändamål bolaget behandlar personuppgifter i det elektroniska nyckelsystemet och i "FreeCall", vilka upp-

gifter som behandlas samt hur länge bolaget avser att spara uppgifterna. Bolaget har uppgett att det behandlar personuppgifter i de båda systemen med stöd av en s.k. intresseavvägning i 10 § personuppgiftslagen.

Aroseken har uppgett att bolaget behandlar uppgifter om ”nycklar”, lägenhetsnummer och hyresgästers telefonnummer så länge hyresförhållandet består för att systemen ska fungera och en acceptabel säkerhetsnivå för hyresgästerna ska kunna upprätthållas.

Datainspektionen konstaterar att dessa ändamål inte kräver att passageloggar registreras, utan att det som avses är de administrativa åtgärder som tidigare har beskrivits. Det har inte framkommit något som tyder på att Arosekens behandling av personuppgifter i denna del inte uppfyller de grundläggande kraven eller annars skulle vara otillåten enligt personuppgiftslagen.

Bolaget behandlar vidare personuppgifter i passageloggar för teknisk felsökning och underhåll. För detta ändamål sparas passageloggarna sparas under en månad.

Datainspektionen har i tidigare ärenden uttalat att en passagelogg, med stöd av en intresseavvägning, får sparas om det är nödvändigt för att få systemet att fungera tillfredställande. I de ärendena avsågs en lagringstid om en vecka respektive 15 dagar.

Mot denna bakgrund anser Datainspektionen att Arosekens behandling av personuppgifter i passageloggar för teknisk felsökning och underhåll är tillåten med stöd av en intresseavvägning. För att behandlingen ska kunna anses vara proportionerlig med det intrång i de registrerades personliga integritet som den kan innebära får Aroseken dock inte spara passageloggarna under längre tid än två veckor. Under denna tid bör bolaget ha hunnit genomföra en felsökning och hittat de tekniska problem som kan hittas genom en sökning i passageloggarna. De administrativa fördelar som en lagringstid på en månad skulle innebära för bolaget förändrar inte Datainspektionens bedömning. Inte heller säkerhetskopior över passageloggar får sparas under längre tid än två veckor.

Aroseken behandlar vidare personuppgifter i loggar för tvättstugebokning under 30 dagar. En behandling av personuppgifter i s.k. bokningsloggar får anses mindre integritetskänslig än motsvarande behandling i passageloggar. En sådan behandling är att jämföra med den behandling av personuppgifter som utförs då bokning sker på papper. Datainspektionen anser därför att Arosekens behandling av personuppgifter i bokningsloggar inte strider mot de grundläggande kraven och är tillåten enligt personuppgiftslagen med stöd av en intresseavvägning.

*Uppfylls kraven på information till de registrerade?*

Det är viktigt att alla boende informeras om den behandlingen av personuppgifter som sker bl.a. för att de boende ska känna till vilka uppgifter som registreras och kunna ta tillvara sina rättigheter.

Enligt 23-25 §§ personuppgiftslagen ska den personuppgiftsansvarige, i detta fall Aroseken, självant lämna information om behandlingen av personuppgifter till de registrerade.

Informationen bör innehålla

- a) den personuppgiftsansvariges identitet (namn, adress, telefonnummer, organisationsnummer och i förekommande fall e-postadress),
- b) ändamålen med behandlingen av personuppgifter,
- c) all övrig information som behövs för att den registrerade ska kunna ta tillvara sina rättigheter i samband med behandlingen, såsom
  - vilka kategorier av uppgifter som behandlas,
  - hur länge uppgifterna sparas,
  - mottagare eller kategorier av mottagare av uppgifterna (dvs. till vilka uppgifterna kommer att lämnas ut),
  - rätten att gratis en gång årligen efter ansökan få information samt
  - rätten till rättelse.

Under förutsättning att den information som Aroseken kommer att lämna till sina hyresgäster har det innehåll som har beskrivits ovan bedömer Datainspektionen att bolaget kommer att uppfylla personuppgiftslagens krav på information. Informationen ska i förekommande fall även omfatta den behandling av personuppgifter som sker i "FreeCall".

*Uppfylls kravet på avtal med personuppgiftsbiträden?*

Den personuppgiftsansvarige är ansvarig för den behandling av personuppgifter som utförs. Genom att ge andra, utanför den personuppgiftsansvariges egen organisation, som behandlar personuppgifter för den personuppgiftsansvariges räkning tydliga instruktioner om hur uppgifterna ska behandlas får den personuppgiftsansvarige bättre kontroll över den behandling som sker.

Det ska finnas ett skriftligt avtal mellan den personuppgiftsansvarige och ett personuppgiftsbiträde, ett s.k. personuppgiftsbiträdesavtal. Avtalet ska reglera hur biträdet ska behandla uppgifterna och vilka säkerhetsåtgärder som ska vidtas (30 § personuppgiftslagen).

Aroseken har tecknat avtal med sitt personuppgiftsbiträde. Aroseken uppfyller därmed personuppgiftslagens krav på personuppgiftsbiträdesavtal.

*Vidtas lämpliga säkerhetsåtgärder?*

För att förhindra missbruk av de personuppgifter som behandlas är det viktigt att säkerheten kring uppgifterna är god.

Enligt 31 § personuppgiftslagen ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att åstadkomma ett lämpligt skydd för de personuppgifter som behandlas. Vilken säkerhetsnivå som är lämplig avgörs av de tekniska möjligheter som finns, vad det skulle kosta att genomföra åtgärderna, de särskilda risker som finns med behandlingen och hur pass känsliga de behandlade uppgifterna är.

Datainspektionen bedömer att de tekniska och organisatoriska åtgärder som Aroseken har vidtagit ger ett lämpligt skydd för de personuppgifter som bolaget behandlar i det elektroniska nyckelsystemet.

#### *Slutsatser*

Hanteringsreglerna i personuppgiftslagen är tillämpliga på den behandling av personuppgifter som Arosekens användning av elektroniska nycklar i bolagets gemensamma utrymmen och "FreeCall" innebär.

Datainspektionen konstaterar att Arosekens behandling av personuppgifter i passageloggar för teknisk felsökning och underhåll är tillåten med stöd av en intresseavvägning. Passageloggarna får dock inte sparas under längre tid än två veckor.

Datainspektionen finner att Arosekens behandling av personuppgifter på denna punkt inte är förenlig med 9 § personuppgiftslagen. Datainspektionen förutsätter dock att Aroseken vidtar åtgärder för att komma tillrätta med den påpekade bristen i sin behandling av personuppgifter i det elektroniska nyckelsystemet och "FreeCall".

Med dessa påpekanden ska ärendet avslutas. Ärendet kan dock komma att följas upp.

#### **Hur man överklagar**

Om ni vill överklaga beslutet skall ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut som överklagas och den ändring som ni begär. Inspektionen måste ha fått ert överklagande inom tre veckor från den dag ni fick ta del av beslutet, annars kan överklagandet inte prövas. Datainspektionen sänder överklagandet vidare till Länsrätten i Stockholms län för prövning om inspektionen inte själv ändrar beslutet på det sätt ni har begärt.

---

Detta beslut har - efter hörande av Datainspektionens styrelse - fattats av generaldirektören Göran Gräslund i närvaro av chefsjuristen Leif Lindgren, teamledaren Catharina Fernquist, IT-säkerhetsspecialisten Adolf Slama samt juristerna Jonas Agnvall och Malin Fredholm, föredragande.

Göran Gräslund

Malin Fredholm