

Bostadsaktiebolaget Poseidon  
Box 1  
424 21 Angered

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

### **Datainspektionens beslut**

Datainspektionen konstaterar

- att Bostadsaktiebolaget Poseidons behandling av personuppgifter i andra loggar än bokningsloggar inte är nödvändig för att uppfylla ändamålet att vid tekniska fel återskapa tvättstuge- och bastubokningar och att behandlingen innebär att fler personuppgifter än nödvändigt med hänsyn till ändamålet behandlas samt
- att Bostadsaktiebolaget Poseidon inte ställer krav på regelbundna byten av lösenord till de administrativa användarkontona i bolagets elektroniska nyckelsystem.

Datainspektionen finner att Bostadsaktiebolaget Poseidons behandling av personuppgifter på dessa punkter inte är förenlig med 9, 10 och 31 §§ personuppgiftslagen. Datainspektionen förutsätter dock att Bostadsaktiebolaget Poseidon vidtar åtgärder för att komma tillrätta med de påpekade bristerna.

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 Bostadsaktiebolaget Poseidon (Poseidon) och deras s.k. IT-hus den 25 maj 2007. Vid inspektionen framkom att Poseidon i den aktuella fastigheten använder elektroniska nycklar till källare, tvättstugor, portentréer, parkeringshus och bastu. Det elektroniska nyckelsystemet omfattar även lägenhetsdörrar och postlådor. Bokning av tvättstuga och bastu sker via systemet.

Efter att Poseidon 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 påpekade.

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

Ändamålet med behandling av personuppgifter är att administrera behörigheter för PC-styrda system för elektroniska nycklar, såsom tvättstuge- och bastubokning, kortlås samt kodlås för öppning av dörrar. I en av bolagets fastigheter (det s.k. IT-huset innehållande 37 lägenheter) är lägenhetsdörrarna, förutom niotillhållarlås, försedda med elektroniska nycklar. Systemet används även för den elektroniska namntavlan i trappuppgången.

För att administrera behörigheter i systemet registreras kontraktsnumret. För att även kunna hantera elektroniska namntavlor i trappuppgången registreras hyresgästens namn kopplat till kontraktsnumret.

Under den tid en person har ett giltigt kontrakt ligger behörighetsuppgifterna registrerade i systemet. När personen avflyttar raderas uppgifterna från systemet.

Samtliga loggar från systemet sparas i sju dagar. I loggen kan följande utläsas.

- Identitetsnummer på kortet
- Lägenhetsnummer
- Datum och klockslag
- Händelsetyp t.ex. ”dörr upplåst”
- Plats, t.ex. vilken dörr som låsts upp

Anledningen till att loggarna sparas är att det finns behov att vid tekniska fel gå tillbaka, läsa och återskapa tvättstuge- och bastubokningar. Bolaget sparas dock alla typer av loggar på grund av att de olika typerna av loggar inte går att särskilja vid en återläsning och att alla typer av loggarna därför återskapas samtidigt i den nuvarande versionen av nyckelsystemet. Bolaget har kontakt med systemleverantören i denna fråga och problemet ser ut att kunna lösas i nästa version av systemet.

När det gäller elektroniska nycklar som används på lägenhetsdörrar åberopar bolaget samtycke från de registrerade som rättslig grund för behandlingen av personuppgifter. I övrigt åberopar bolaget en s.k. intresseavvägning (10 § punkten f personuppgiftslagen) till stöd för behandlingen av personuppgifter i sitt elektroniska nyckelsystem.

Ett allmänt samtycke, dvs. inte kopplat till en specifik elektronisk nyckel, kommer att inhämtas från samtliga personer i hushållet genom

deras underskrifter i samband med nyckelkvittens. Samtidigt kommer information att ges. Informationen kommer att lämnas om den personuppgiftsansvariges identitet, ändamålet med behandlingen, vilka uppgifter som lagras, gallring, rätten till att gratis en gång per år få information om registrerade personuppgifter samt rätten till rättelse vid fel. Denna rutin kommer att införas under hösten 2007.

Ett allmänt samtycke från befintliga hyresgäster kommer att inhämtas senast den 31 oktober 2007. Kontraktsinnehavaren kommer att kontaktas via brev innehållande information om den aktuella behandlingen av personuppgifter samt en svarstalong angående samtycke/ej samtycke som ska returneras underskriven.

Om samtycke inte ges finns alternativet att använda vanliga nycklar då samtliga lägenheter, entrédörr samt gemensamma utrymmen i "IT-huset" även är försedda med traditionella lås. I "IT-huset" krävs ett elektronisk kort för åtkomst till postbox samt för bokning av bastu och tvättstuga. Om samtycke inte ges till elektronisk lägenhetsnyckel får ett separat kort som endast går till tvättstugan, bastun och postboxen läggas upp.

Personuppgiftsbiträdesavtal kommer att upprättas med systemleverantörer och det bolag som ansvarar för driften av databaserna under hösten 2007.

Det är systemadministratören som lägger upp respektive avslutar administrativa användare, s.k. operatörer, i enlighet med beslut från behörig chef. Det finns en operatör för "IT-husets" system; områdets husvärd. Varje användare har ett eget ID och lösenord till systemet. Lösenordet måste vara minst sex tecken och slumpas fram av en slumpgenerator. I systemet finns idag inget krav på lösenordsbyte. Bolaget kommer att påtala denna brist för systemleverantören. Citrix används för att publicera MultiAccess. Man kan endast komma åt programmet om man har behörighet till det via Active Directory i Windows. Windows kräver lösenordsbyte var tredje månad.

Administrativa händelser loggas automatiskt i systemet. Här loggas när administrativa användare har loggat in, vad de har utfört för ändringar, när data sänds och liknande. Det är endast systemadministratören som har åtkomst till systemets loggar.

En full backup av SQL-databasen görs en gång per dygn och transaktionsloggen backas var 6:e timme. Dessa backuper sparas enligt bolagets backup-regler, innebärande att dagsbackup sparas i fem dagar, veckobackup sparas i 90 dagar och månadsbackup sparas i 10 år. Kopior förvaras skyddat i reservdatorhallen på IT-supporten.

## 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, speciellt då systemet som i Poseidons fall omfattar även själva lägenhetsdörrarna.

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 sin bostad eller utrymmena i anslutning till den. 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 Poseidon utför i sitt elektroniska nyckelsystem omfattas således 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 (10 § personuppgiftslagen). Ett samtycke ska vara frivilligt. Det innebär att den enskilde ska ha en verklig valmöjlighet. Den enskilde ska också ha fått information om hur personuppgifterna kommer att behandlas innan samtycke lämnas.

Behandlingen av personuppgifter kan också vara tillåten om den är nödvändig av vissa andra skäl. Till exempel kan behandlingen vara tillåten om den är nödvändig för att ett berättigat intresse hos bolaget ska kunna tillgodoses och detta intresse väger tyngre än intresset av skydd av den personliga integriteten.

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.

Poseidon har i sin åtgärdsplan preciserat för vilka ändamål bolaget behandlar personuppgifter i det elektroniska nyckelsystemet, vilka uppgifter som behandlas samt hur länge bolaget avser att spara uppgifterna. Bolaget har åberopat samtycke från de registrerade som rättslig grund för behandlingen av personuppgifter när det gäller elektroniska nycklar som används på lägenhetsdörrar. I övrigt har bolaget åberopat en s.k. intresseavvägning till stöd för behandlingen av personuppgifter.

Ett av de ändamål med sin behandling av personuppgifter i det elektroniska nyckelsystemet som Poseidon har angett är att administrera behörigheter i sitt elektroniska nyckelsystem.

Datainspektionen konstaterar att detta ändamål inte kräver att passageloggar registreras, utan att det är tillräckligt med de administrativa åtgärder som tidiga-

re har beskrivits. Det har inte framkommit något som tyder på att Poseidons behandling av personuppgifter i denna del inte uppfyller de grundläggande kraven eller annars skulle vara otillåten enligt personuppgiftslagen.

Poseidon har också uppgett att bolaget sparar loggar – även passageloggar hänförliga till lägenhetsdörrar – i sju dagar för att möjliggöra att vid tekniska fel gå tillbaka för att läsa och återskapa tvättstuge- och bastubokningar.

En behandling av personuppgifter i bokningsloggar är att jämföras med den behandling av personuppgifter som utförs då bokning av en lokal sker på papper. En sådan behandling får anses mindre integritetskänslig än motsvarande behandling i passageloggar. Poseidons behandling av personuppgifter i bokningsloggar under sju dagar för det aktuella ändamålet är därför tillåten med stöd av en intresseavvägning och strider inte heller mot de grundläggande kraven i personuppgiftslagen. Även säkerhetskopior över dessa loggar får sparas under samma tid.

Datainspektionen anser dock att behandlingen av personuppgifter i andra loggar än bokningsloggar inte är nödvändig för att uppfylla ändamålet och innebär att fler personuppgifter än nödvändigt med hänsyn till ändamålet behandlas.

*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 Poseidon, självständigt 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 Poseidon i sin information klargör vilken behandling av personuppgifter som utförs om den registrerade samtycker till den och vilken behandling som sker även utan samtycke uppfyller de informationsinsatser som Poseidon har beskrivit i sin åtgärdsplan, enligt Datainspektionens bedömning, personuppgiftslagens krav på information till de registrerade.

*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).

Poseidon har uppgett att bolaget kommer att skriva avtal med de personuppgiftsbiträden som bolaget anlitar. Således kommer Poseidon att uppfylla 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.

Det ska bl.a. finnas regler för längd och sammansättning samt byte av lösenord till de administrativa användarkontona som ger ett lämpligt skydd för de personuppgifter som behandlas. I Poseidons elektroniska nyckelsystem finns idag inget krav på byte av lösenord. Bolaget har uppgett att det kommer att påtala denna brist för systemleverantören.

Datainspektionen bedömer att de tekniska och organisatoriska åtgärder som Poseidon i övrigt har beskrivit i sin åtgärdsplan 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 Poseidons användning av elektroniska nycklar innebär.

Datainspektionen konstaterar att Poseidons behandling av personuppgifter i andra loggar än bokningsloggar inte är nödvändig för att uppfylla ändamålet att vid tekniska fel återskapa tvättstuge- och bastubokningar. Behandling innebär också att fler personuppgifter än nödvändigt med hänsyn till ändamålet behandlas.

Datainspektionen konstaterar vidare att Poseidon har en brist i säkerheten kring de behandlade personuppgifterna genom att inte ställa krav på regelbundna by-

ten av lösenord till de administrativa användarkontona i bolagets elektroniska nyckelsystem.

Sammantaget finner Datainspektionen att Poseidons behandling av personuppgifter enligt vad som framgår ovan inte är förenlig med 9, 10 och 31 §§ personuppgiftslagen. Datainspektionen förutsätter dock att Poseidon vidtar åtgärder för att komma tillrätta med de påpekade bristerna i sin behandling av personuppgifter i det elektroniska nyckelsystemet.

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