

HSB Brf Tullen nr 623 i Nacka  
Diligensvägen 19  
131 48 Nacka

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

### **Datainspektionens beslut**

Datainspektionen konstaterar

- att den behandlingen av passageloggar som HSB Brf Tullen nr 623 i Nacka utför för att debitera medlemmarna för användning av gemensamma lokaler kan utföras på ett mindre integritetskänsligt sätt,
- att det inte är nödvändigt för HSB Brf Tullen nr 623 i Nacka att behandla personuppgifter under längre tid än en vecka för statistiska ändamål och
- att HSB Brf Tullen nr 623 i Nacka i sitt elektroniska nyckelsystem exponerar lösenord för webbaccess mer än nödvändigt.

Datainspektionen finner att HSB Brf Tullen nr 623 i Nackas behandling av personuppgifter på dessa punkter inte är förenlig med 9, 10 och 31 §§ personuppgiftslagen. Datainspektionen förutsätter dock att HSB Brf Tullen nr 623 i Nacka 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 HSB Brf Tullen nr 623 i Nacka (Brf Tullen) den 3 april 2007. Vid inspektionen framkom att Brf Tullen använder elektroniska nycklar till följande gemensamma utrymmen; tvättstugor, bastu, hobbyrum, solarium, festlokal, gåstrum, förrådsutrymmen, vägbommar, styrelserummet och portentréerna. Vissa av utrymmena kan även bokas och debiteras genom det elektroniska nyckelsystemet. Bokning sker via elektroniska bokningstavlor i fastigheten eller föreningens hemsida. Styrelsen för Brf Tullen fattade beslut om att införa det elektroniska nyckelsystemet.

Efter att Brf Tullen fått tillfälle att yttra sig över inspektionsprotokollet begärde Datainspektionen att föreningen skulle komma in med en skriftlig åtgärdsplan. Åtgärdsplanen skulle innehålla en beskrivning av vilka åtgärder som föreningen hade vidtagit eller skulle komma att vidta med anledning av de brister i föreningens behandling av personuppgifter i förhållande till personuppgiftslagen som vi påpekade.

Brf Tullen har kommit in med en åtgärdsplan med i huvudsak följande innehåll.

Brf Tullen behandlar personuppgifter vid användningen av elektroniska nycklar för följande ändamål.

- Öppning av dörrar till de lokaler lägenhetsinnehavarna har tillträde
- Bokning av lokaler och debitering av deras användning
- Statistik över lokalutnyttjande

I samband med att nyckeln används registreras dess identitet, tidpunkten, vilken nyckelläsare som användes och vad som hände (dörr öppnades, lokal bokades eller avbokades).

För debitering av lokaler används logguppgifter om att lokalen har öppnats. Föreningen skickar varje månad en sammanställning över vad varje medlem ska debiteras till HSB, som sköter föreningens fakturering. HSB fakturerar medlemmarna var tredje månad, med en månads eftersläpning. Uppgiften om inpassagen sparas i 150 dagar för att föreningen ska kunna gå tillbaka och se att inpassagen skett för det fall att en medlem skulle ha invändningar mot fakturan. I övrigt behandlas inga personuppgifter för att hålla reda på öppningen av dörrar.

För att få ut statistik om lokalutnyttjande sammanställs hur mycket de olika lokalerna har utnyttjats och av vilka lägenheter. Uppgifterna sparas i 150 dagar.

Uppgifter gällande övriga dörrar sparas i tio dagar för att möjliggöra tekniskt underhåll.

Som rättslig grund åberopar föreningen 10 § punkten f i personuppgiftslagen. Föreningen har börjat använda elektroniska nycklar för att öka medlemmarnas trygghet och säkerhet beträffande vem som kan komma in i föreningens lokaler och utrymmen. Det blir följden av att det nu är mycket enklare att ha kontroll över de nycklar som finns. Om en nyckel kommer på avvägar, räcker det med att ta bort nyckelns behörighet. Tidigare var föreningen tvungen att byta lås och dela ut nya nycklar. Det påverkade föreningens driftskostnader och därmed medlemmarnas månadsavgift. Eventuell kränkning av den personliga integriteten anser föreningen vara minimal, eftersom det inte direkt går att härleda vilken person som använt en elektronisk nyckel. Det registreras bara uppgifter om till vilken lägenhet nyckeln hör.

Föreningen kommer att informera alla lägenhetsinnehavare. Vid ägarbyte informeras de nya lägenhetsinnehavarna fortlöpande. Information kommer också att finnas på föreningens hemsida [www.brftullen.se](http://www.brftullen.se). Informationen kommer att beskriva varför föreningen använder elektroniska nycklar, vilka uppgifter som används samt hur de behandlas och hur länge de sparas. Föreningen ska även informera om rätten att gratis få tillgång till vilka uppgifter som är lagrade om respektive lägenhet och att felaktiga uppgifter rättas.

Föreningen kommer vidare att skriva avtal med sin systemleverantör. Leverantören kommer också att ta emot föreningens säkerhetskopior.

Föreningen har två typer av administrativa användarkonton till systemet. Typ 1 har behörighet att ändra alla poster i databasen. Typ 2 kan endast läsa poster tillhörande bokningsobjekt. Kontona tillhör någon i föreningens styrelse eller av styrelsen betrodd medlem. Vem som har konton ses över när innehavarnas arbetsuppgifter ändras och årligen vid styrelseval. Föreningen kommer att göra alla konton personliga. Lösenorden ska bestå av minst sex tecken med både bokstäver och siffror samt ska ändras minst årligen. Föreningen uppmanar också leverantören av systemet att lägga in funktioner för automatisk lösenordshanteringen.

Föreningen kommer att se till att administrativa händelser i systemet loggas. I den mån systemet inte loggar automatiskt kommer föreningen att föra manuell loggbok.

Föreningen uppmanar vidare leverantören att se till att datakommunikationen är krypterad vid överföring av säkerhetskopior och webbaccess för administration av systemet.

Säkerhetskopiering av systemet kommer att ske regelbundet, antagligen dagligen. Föreningen kommer att avtala med leverantören om att förvara och testa kopiorna samt att inte spara dem längre än gällande gallringstid för originalinformationen.

Samtliga åtgärder har föreningen för avsikt att utföra under 2007.

### **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 Brf Tullen 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. 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 föreningen 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 en bostadsrättsförenings 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 beslutet att införa nyckelsystemet – inklusive ändamålen för behandlingen – har fattats på en föreningsstämma, vilka gallringsrutiner som finns, vilken information de boende får samt säkerheten kring uppgifterna.

Brf Tullen har i sin åtgärdsplan preciserat för vilka ändamål föreningen behandlar personuppgifter i det elektroniska nyckelsystemet, vilka uppgifter som behandlas och hur länge uppgifterna sparas. Föreningen har vidare uppgett att den behandlar personuppgifter i systemet med stöd av en s.k. intresseavvägning i 10 § personuppgiftslagen.

Ett av de ändamål med sin behandling av personuppgifter i det elektroniska nyckelsystemet som Brf Tullen har angett är att öppna dörrar till lokaler dit lägenhetsinnehavarna har tillträde.

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

Ett ändamål med behandlingen av passageloggar som Brf Tullen har angett är att debitera medlemmarna för användning av gemensamma lokaler.

Datainspektionen anser att denna behandling, med hänsyn till det integritetsintrång behandlingen innebär för de boende, inte är nödvändig för att uppfylla ändamålet. Vi menar att samma ändamål kan uppfyllas genom behandling av endast de loggar som avser bokningen av lokalen i fråga. En sådan behandling är att jämföra med den behandling av personuppgifter som utförs då bokning av en lokal sker på papper. En behandling av personuppgifter i bokatningsloggar får anses mindre integritetskänslig än motsvarande behandling i passageloggar.

När det gäller statistiska ändamål anser Datainspektionen att det inte kan vara nödvändigt för Brf Tullen att behandla identifierbara uppgifter, dvs. personuppgifter, under längre tid än en vecka för att rent tekniskt kunna ta ut statistiken. Därefter ska uppgifterna avidentifieras.

Brf Tullen har också uppgett att föreningen sparar uppgifter om dörrar – som Datainspektionen förstår det passageloggar – i tio dagar för att möjliggöra tekniskt underhåll. Datainspektionen har i tidigare ärenden uttalat att en passagelogg får sparas om det är nödvändigt för att få systemet att fungera tillfredställande med stöd av en intresseavvägning. I de ärendena avsågs en lagringstid om en vecka respektive 15 dagar. Mot denna bakgrund måste Brf Tullens behandling av personuppgifter i passageloggar för tekniskt underhåll under tio dagar anses uppfylla de grundläggande kraven och vara tillåten enligt personuppgiftslagen.

*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 Brf Tullen, 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.

De informationsinsatser som Brf Tullen har beskrivit i sin åtgärdsplan uppfyller, 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).

Brf Tullen har uppgett att föreningen kommer att skriva avtal med sin systemleverantör, som numera är det enda personuppgiftsbiträde som föreningen anlitat. Således kommer Brf Tullen 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.

Vid inspektionen uppmärksammades att de administrativa användarna av Brf Tullens nyckelsystem kunde se andra användares lösenord för webbaccess. Enligt Datainspektionens bedömning kan inte denna behandling vara nödvändig och bör enkelt kunna åtgärdas.

Datainspektionen bedömer att de tekniska och organisatoriska åtgärder som Brf Tullen beskrivit vid inspektionstillfället och i sin åtgärdsplan i övrigt ger ett lämpligt skydd för de personuppgifter som föreningen behandlar i det elektroniska nyckelsystemet.

#### *Slutsatser*

Hanteringsreglerna i personuppgiftslagen är tillämpliga på den behandling av personuppgifter som Brf Tullens användning av elektroniska nycklar i föreningens gemensamma utrymmen innebär.

Datainspektionen konstaterar att den behandlingen av passageloggar som Brf Tullen utför för att debitera medlemmarna för användning av gemensamma lokaler kan utföras på ett mindre integritetskänsligt sätt.

När det gäller statistiska ändamål konstaterar Datainspektionen att det inte är nödvändigt för Brf Tullen att behandla personuppgifter under längre tid än en vecka.

Datainspektionen konstaterar vidare att Brf Tullen i sitt elektroniska nyckelsystem exponerar lösenord för webbaccess mer än nödvändigt.

Sammantaget finner Datainspektionen att Brf Tullens behandling av personuppgifter enligt vad som framgår ovan inte är förenlig med 9, 10 och 31 §§ per-

sonuppgiftslagen. Datainspektionen förutsätter dock att Brf Tullen 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