HSB – där möjligheterna bor

RUTINER FÖR INCIDENTRAPPORTERING

INTRODUKTION

[Bostadsrättsförening] måste för att efterleva Dataskyddsförordningen ha rutiner och processer på plats för att upptäcka, rapportera och utreda personuppgiftsincidenter.

ALLMÄNNA KRAV

Enligt Dataskyddsförordningen ska den personuppgiftsansvarige utan onödigt dröjsmål och inte senare än 72 timmar efter att ha fått vetskap och den, anmäla personuppgiftsincidenten till Datainspektionen. Detta gäller dock inte om det är *osannolikt* att personuppgiftsincidenten medför risk för enskildas rättigheter och friheter.

VAD ÄR EN PERSONUPPGIFTSINCIDENT?

En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av de personuppgifter som behandlas. Det kan också vara fråga om en säkerhetsincident som leder till obehörigt röjande av eller obehörig åtkomst till de behandlade personuppgifterna.

- Olaglig förstöring – innebär att personuppgifter förstörts eller inte längre existerar i ett format som kan användas av personuppgiftsansvarige.
- Förlust – innebär att personuppgifter fortfarande kan existera, men att den personuppgiftsansvarige har förlorat kontrollen eller åtkomsten till personuppgifterna, eller att personuppgifterna inte längre är i personuppgiftsansvariges besittning.
- Olaglig eller obehörig behandling - innebär att det kan innefatta utlämnande av personuppgifter till (eller åtkomst av) mottagare som inte är behöriga att ta emot (eller få tillgång till) uppgifterna, eller annan behandling som strider med GDPR.

Generellt ska vi dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Se nedan vad som steg för steg bör göra vid en personuppgiftsincident.

VAD SKA GÖRAS VID EN PERSONUPPGIFTSINCIDENT?

1. **Anteckna datum och tid** för när personuppgiftsincidenten upptäcktes.

2. **Gör en utredning av personuppgiftsincidenten** - Ta anteckningar löpande om incidentshanteringen och skriv datum på anteckningarna.

3. **Vidta lämpliga åtgärder** - Informera de som är ansvariga för personuppgiftsfrågor i verksamheten. Fördela vem som ska hantera vad. I de undantagsfall när vår verksamhet är personuppgiftsbiträde: se till att personuppgiftsansvarig underrättas utan onödigt dröjsmål efter att ni har fått vetskap om en personuppgiftsincident.

4. **Bedöm om det är osannolikt att personuppgiftsincidenten medför risk för fysiska personers rättigheter och friheter.** Informera de berörda registrerade utan onödigt dröjsmål om personuppgiftsincidenten kan leda till en hög risk för deras rättigheter och

friheter. Vem i verksamheten som informerar den registrerade bör diskuteras för att kunna hantera incidenten på bästa sätt för den registrerade.

Om det är osannolikt att personuppgiftsincidenten medför risk för enskildas rättigheter och friheter behöver vi inte kontakta Datainspektionen. Bedömning av risken, innebär att den personuppgiftsansvarige ska bedöma en kombination av i) hur allvarligt den potentiella påverkan är för individens rättigheter och friheter och ii) sannolikheten att det inträffar. Det innebär att om konsekvenserna är stora innebär det att risken är högre. Nedan beskrivs faktorer som ska tas i beaktande när den potentiella påverkan bedöms:

- Typ av överträdelse
  Vilken typ av överträdelse som har inträffat kan påverka vilken risk som inträffar för individen. Om det föreligger känsliga personuppgifter, är det sannolikt högre risk för individens rättigheter och friheter om uppgifterna har läckts till obehöriga jämfört med om uppgifterna förstörts.
- Karaktär, känslighet och volym av personuppgifter
  Känsligheten av personuppgifter påverkar risker för individens rättigheter och friheter. Till exempel är namn och adresser ofta publik information och anses ofta inte som känslig karaktär, men skulle en individ ha skyddade personuppgifter skulle risken för påverkan av individens rättigheter och friheter anses hög. Ett annat exempel är om en mängd information om individen hamnar i obehörigas händer, kan t.ex. kapning av identiteter inträffa.
- Enkelhet att identifiera individer
  Avser hur enkelt motparter som obehörigt har fått tillgång till personuppgifterna kan identifiera enskilda individer. Identifikation kan i vissa fall göras på direkten medan i andra fall kan det vara svårare eftersom data är skyddat med krypteringsnycklar eller pseudonymisering.
- Konsekvenser för individen
  Skadorna för individen beror bl.a. på vilka personuppgifter som förekommer i överträdelsen och vilka konsekvenser som inträffar. Konsekvenserna anses större om individen t.ex. utsetts för identifikationsstöld, bedrägeri, psykologisk stress, förnedring eller skada av sitt rykte.
- Individen
  Hänsyn bör tas till om personuppgifterna är kopplade till barn eller andra utsatta personer, vilket kan innebära en högre risk för individen.
- Personuppgiftsansvarige
  Den personuppgiftsansvariges typ av inriktning och aktiviteter kan påverka nivån av risken.
- Antal individer
  Antalet individer som påverkas av överträdelsen. Generellt anses det vara en större risk om många individer påverkas än få. Men beroende på typ av personuppgifter kan även överträdelse som är kopplat till få individer innebära en hög risk för individens rättigheter och friheter.

Om det inte är osannolikt att personuppgiftsincidenten medför risk för enskildas rättigheter och friheter, ska incidenten anmälas till Datainspektionen så snart som möjligt, dock ***inte senare än 72 timmar*** från att vi fått vetskap om incidenten. Anmälan ska ske i helst en, men om nödvändigt, i flera omgångar.

Anmälan om personuppgiftsincident görs via Datainspektionens e-tjänst.

Följande information ska rapporteras till Datainspektionen (denna information kan ändras över tid, vänligen verifiera på Datainspektionens hemsida):

Personuppgiftsansvarig
- Organisationens namn, kontaktuppgifter
- Namn på personuppgiftsbiträden, underbiträden

Kontaktperson för anmälan
- Kontaktuppgifter till den person som Datainspektionen kan kontakta

Personuppgiftsincidenten
- Har personuppgiftsincidenten medfört en risk för de registrerades fri- och rättigheter?
- När inträffade personuppgiftsincidenten?
- När upptäckte ni personuppgiftsincidenten?
- Vad har hänt vid personuppgiftsincidenten?
- Hur upptäckte ni personuppgiftsincidenten?
- Varför inträffade personuppgiftsincidenten enligt din eller organisationens uppfattning?
- Inom vilket verksamhetsområde inträffade personuppgiftsincidenten?

Personuppgifterna och de registrerade
- Hur många registrerade har påverkats?
- Hur många personuppgiftsposter har personuppgiftsincidenten påverkat?
- Vilka grupper tillhör de registrerade?
- Vilken sorts personuppgifter berörs av personuppgiftsincidenten?
- Var personuppgifterna krypterade?

Konsekvenser
- Vad kan bli konsekvenserna av personuppgiftsincidenten?
- Hur allvarlig bedömer ni att personuppgiftsincidenten är?

Information till de registrerade
- Har ni informerat de registrerade om personuppgiftsincidenten? När?
- Kommer ni att informera de registrerade? När? Om inte, varför kommer ni inte att informera de registrerade?

Sen anmälan
- Om anmälan kommer in senare än 72 timmar efter att ni upptäckte personuppgiftsincidenten ska ni beskriva varför.

Komplettering
- Om ni kommer att komplettera anmälan, beskriv varför.

Sekretess
- Om du har skrivit något som du anser bör omfattas av sekretess, beskriv det.

Vid en personuppgiftsincident är det viktigt att också informera alla relevanta parter såsom underbiträden, applikationsleverantörer och att arbeta tillsammans med juridik och IT-avdelningen för att minimera skador.

HSB – där möjligheterna bor

Information från Datainspektionens hemsida (1:e maj 2018)

Datainspektionen håller på att ta fram en e-tjänst för att du ska kunna anmäla personuppgiftsincidenter till oss. E-tjänsten kommer att finnas på denna sida senare i vår. Genom att använda e-tjänsten förenklas hanteringen både för dig och för oss, och vi hoppas därför att du använder dig av den.

Ovan text kan tas bort vid implementering av instruktion – är inkluderad för kännedom.