Rutiner kopplat till GDPR

Rutin för rättning av uppgifter

Rättslig grund för personuppgiftsbehandlingen

Personuppgifter får endast behandlas för särskilda, uttryckligt angiva och berättigade ändamål. Varje behandling måste även stödja sig på någon av de angivna rättsliga grunderna i dataskyddsförordningen. Det är därför viktigt att redan innan en behandling påbörjas dokumentera för vilket ändamål samt på vilken rättslig grund behandlingen stödjer sig. Både personuppgiftsansvariga och personuppgiftsbiträden är skyldiga att föra ett register över de personuppgiftsbehandlingar som de utför. Vad som ska finnas i registerförteckningen föreskrivs i dataskyddsförordningen.

Vilka personuppgiftsbehandlingar som hanteras på FF finns i registerförteckningen som tas i nämnd och uppdateras varje år. Gallringsplan av personuppgifter finns angivet i fastighetsnämndens dokumenthanteringsplan och är viktiga för att säkerställa att personuppgifter inte behandlas längre än nödvändigt.

De registrerades rättigheter

De personer vars personuppgifter hanteras har ett antal rättigheter enligt dataskyddsförordningen. Rättigheterna innebär i korthet att de registrerade har rätt till information om när och hur deras rättigheter behandlas och ha kontroll över sina uppgifter. De registrerade har bland annat rätt till att få sina uppgifter rättade, raderade och flyttade samt att få ut sina uppgifter. Nedan följer exempel på dessa rättigheter.

Rätt till information

Information om personuppgiftsbehandlingen ska lämnas till den registrerade senast vid tidpunkten då personuppgifterna samlas in. Därutöver ska information lämnas till den registrerade när denne begär det, vid förändringar i personuppgiftsbehandlingen samt i särskilda fall exempelvis om det inträffar en personuppgiftsincident. Den enskilde har även rätt till information om hur denne ska göra gällande sina rättigheter.

Ansvarig för personuppgiftsbehandlingen ansvarar för ovanstående med hjälp av personuppgiftssamordnaren. Avdelning framgår av personuppgiftsförteckning och respektive avdelningschef är ansvarig.

Scenario; hyresgäst kontaktar förvaltningen för att få veta vilken information som finns registrerat om denne. (Kan även vara begäran om registerutdrag, rättelse, begränsning och radering). Avdelningschef kontrollerar tillsammans med sina medarbetare i de register som finns i sammanställningen över personuppgiftsbehandlingar och informerar hyresgästen alternativt vidtar åtgärd om korrigering. Personuppgiftssamordnaren är behjälplig när det behövs.

Registerutdrag

Den registrerade har rätt att vända sig till ett företag eller en myndighet och begära att få reda på vilka personuppgifter som företaget eller myndigheten behandlar om personen och på vilket sätt personuppgifterna behandlas. Det kallas för registerutdrag. Registerutdraget ska innehålla information om bland annat vilka personuppgifter som behandlas, hur personuppgifterna behandlas, ändamålet med behandlingen, varifrån uppgifterna kommer samt till vilka mottagare uppgifterna har lämnats ut.

Rättelse

Den registrerade har rätt att vända sig till en myndighet eller ett företag och begära att få sina personuppgifter rättade. Det innebär att den enskilde har rätt att få felaktiga uppgifter rättade men även att komplettera med sådana uppgifter som saknas eller är nödvändiga med hänsyn till ändamålet med behandlingen. Om uppgifterna rättas måste företaget eller myndigheten i regel även informera dem som de ha lämnat ut uppgifter till.

Begränsning

Den registrerade har i vissa fall rätt att begära att behandlingen av personuppgifter begränsas. Det innebär att uppgifterna markeras så att de endast får behandlas för vissa avgränsade ändamål. Rätten till begränsning föreligger bland annat när den registrerade anser att uppgifterna är felaktiga och har begärt rättelse. I en sådan situation kan en begränsning innebära att behandlingen av uppgifterna begränsas under tiden uppgifternas korrekthet utreds.

Radering

Den registrerade har rätt att vända sig till en myndighet eller ett företag och begära att dennes personuppgifter raderas. Radering ska ske i vissa i förordningen angivna fall bland annat om uppgifterna inte längre behövs för de ändamål som de samlades in för, om behandlingen vilar på den rättsliga grunden samtycke och samtycket återkallas och om personuppgifterna har behandlats olagligt. Det finns undantag från rätten till radering bland annat om det är nödvändigt för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning.

Identifiering av den registrerade

När en registrerad vill göra gällande sina rättigheter, t.ex. begär ut sina personuppgifter eller begär att personuppgifter raderas, måste det säkerställas att det är rätt person man är i kontakt med. Det är därför viktigt att det finns en process för hur identifiering av registrerade ska gå till.

Ansvarig för personuppgiftsbehandlingen ansvarar för ovanstående med hjälp av personuppgiftssamordnaren.

1. *Identifiera vilken typ av personuppgifter som avses och vi vilken grad det är känsliga uppgifter. Är det t ex en mailadress över företagskunder eller personnummer till privatperson?*
2. *Giltig legitimation måste uppvisas om det avser bostadsavdelningen eller kamerabevakning.*
3. *Säkerställ att det går att radera enligt arkivlag, myndighetsutövning etc*
4. *Informera den registrerade om rättelse, radering ej kan genomföras.*

Rutin för uppdatering av förteckningen över personuppgiftsbehandlingar

Personuppgiftssamordnaren initierar varje år en genomgång över personuppgiftsbehandlingen.

Varje ansvarig avdelningschef har tillsammans med personuppgiftssamordnaren en genomgång på avdelningens APT. Uppdateringen görs sedan av personuppgiftssamordnaren.

Rutin för personuppgiftsansvariga och personuppgiftsbiträden

Personuppgiftsansvariga (nämnd) och personuppgiftsbiträden (systemleverantörer)
Den som behandlar personuppgifter är antingen personuppgiftsansvarig eller personuppgiftsbiträde. Personuppgiftsansvarig bestämmer för vilka ändamål personuppgifterna behandlas och hur behandlingen sker. Personuppgiftsbiträdet behandlar personuppgifter för den personuppgiftsansvariges räkning. Personuppgiftsansansvarig ansvarar för personuppgifterna i alla led. Det innebär att personuppgiftsansvarig ansvarar även för att personuppgiftsbiträdet hanterar personuppgifterna på ett säkert sätt.

Innan en personuppgiftsansvarig lämnar ut personuppgifter till ett personuppgiftsbiträde ska personuppgiftsansvarig kontrollera att personuppgiftsbiträdet kan säkerställa att personuppgifterna behandlas i enlighet med dataskyddsförordningen. För att behålla kontrollen över personuppgiftsbehandlingen ska ett personuppgiftsbiträdesavtal (PUB avtal) tecknas mellan parterna där det föreskrivs hur personuppgiftsbiträdet ska behandla personuppgifterna.

Detta PUB avtal är i Helsingborgs stad framtaget av stadsledningsförvaltningen som mall och kompletteras med specifika uppgifter för respektive personuppgiftsbiträde. Det framgår av personuppgiftsbiträdesavtalet att personuppgiftsbiträdet måste ge tillräckliga garantier för att behandlingen uppfyller kraven i dataskyddsförordningen samt att personuppgiftsbiträdet måste få ett skriftligt godkännande från den personuppgiftsansvarige innan personuppgifter överförs till en underleverantör.

- ✓ Inköpscontroller skriver en uppdragsbeskrivning till inköp att upphandling ska göras.
- ✓ Säkerställ om det behövs göras en konsekvensbedömning och klassning. Framför allt gäller det nya system men kan även vara register som behandlar känsliga personuppgifter.
- ✓ Inköpscontroller eller inköpsansvarig (ex systemförvaltare) säkerställer att både huvudavtal och PUB-avtal tecknas med entreprenören/leverantören.
- ✓ Avtalen lämnas tillsammans med upphandlingshandlingar enligt rutinbeskrivning för diarieföring till registrator.
- ✓ Stickprovskontroller att PUB-avtal följs ska göras en gång/år enligt upprättad rutinbeskrivning 2024.
- ✓ Personuppgiftssamordnare och inköpscontroller/systemförvaltare säkerställer att kontrollen blir gjord enligt rutin (se nedan)

Rutin stickprovskontroller personuppgiftsbiträden

Stickprovskontroller ska göras för att kontrollera att leverantören (personuppgiftsbiträdet) följer avtalet när det gäller behandling av personuppgifter.
Det är olika frågor om det är system som är lokalt installerat eller om det system som lagras via molnet.

Nedanstående kontrollfrågor ska ingå om det är ett system som är lokalt installerat.
Vitec och Drops en idag en moltjänst (se nedan)

- ✓ Är åtkomsten i systemet begränsat till personal som behöver tillgång till systemet för att fullgöra sina arbetsuppgifter? (GDPR Artikel 25)
- ✓ Är personal informerade om vad en personuppgiftsincident är och hur den ska rapporteras? (GDPR Artikel 33.1)
- ✓ Finns det en rutin för hur en personuppgiftsincident ska rapporteras till den personuppgiftsansvarige? (GDPR Artikel 33.1-2)
- ✓ Finns det underbiträden som är lokaliserade utanför EU/EES som har tillgång till systemet? Om ja, sker det från land där lämpliga skyddsåtgärder vidtagits? (GDPR Artikel 46.1)
- ✓ Skapar systemet loggar om information som berör fel, användaraktiviteter och säkerhetshändelser?
- ✓ Granskas logginformationen regelbundet för att upptäcka incidenter och händelser där utredningstekniska åtgärder kan behövas vidtas?
- ✓ Skyddas logginformation, samt verktyg för loggning, mot obehörig åtkomst och förändring?
- ✓ Bevaras loggar från användare med högre behörigheter (priviligierade) i systemet, skyddas mot obehörig åtkomst och förändring samt granskas vid behov?

System installerat hos personuppgiftsbiträde (molnlagring):

- ✓ Har en riskanalys genomförts och dokumenterats med åtföljande åtgärdsplan? (NIS § 12)
- ✓ Har tekniska och organisatoriska åtgärder vidtagits för att hantera ev. risker? (NIS § 13)
- ✓ Är åtgärder för att förebygga och minimera driftstörningar genomförda? (NIS § 14)

Rutin för konsekvensbedömningar och klassningar

Säkerhet

Personuppgiftsansvarig är ansvarig för att vidta adekvata tekniska och organisatoriska säkerhetsåtgärder för att säkerställa en lämplig säkerhetsnivå till skydd för personuppgifterna. Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandlingen medför (riskanalys). Säkerhetsåtgärderna ska granskas regelbundet i syfte att säkerställa att de är adekvata.

Konsekvensbedömning

Om organisationen planerar att påbörja en behandling av personuppgifter som kan leda till en hög risk för de registrerade ska en konsekvensbedömning göras innan behandlingen påbörjas. Det är därför viktigt att det finns rutiner etablerade för när och hur en konsekvensbedömning ska genomföras. En konsekvensbedömning syftar till att ta reda på vilka risker som finns med att

behandla personuppgifter, vidta åtgärder för att hantera riskerna samt att visa på att man uppfyller dataskyddsförordningens krav.

Risk- och konsekvensbedömning ska göras inför varje personuppgiftsbehandling med känsliga personuppgifter.

- *Ta ställning till om detta är uppgifter som är viktiga, behöver vi samla in dem överhuvudtaget?*
- *Ta ställning till om behandlingen kan leda till en hög risk för de registrerade.*
- *Om JA, vidta åtgärder, t ex sekretessmarkera och säkerställ korrekt hantering (behörighetsbegränsning) för att minimera riskerna. Dokumentera!*
- *Klassning av systemen avseende informationssäkerheten ska genomföra i Stratsys.*

Rutin för personuppgiftsincidenter

Personuppgiftsincidenter

En personuppgiftsincident kan innebära risker för människors friheter och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över sina personuppgifter eller att rättigheterna inskränks. En personuppgiftsincident kan ha inträffat om uppgifter om en registrerad har blivit förstörda, gått förlorade på annat sätt, ändrats eller kommit i orätta händer. Det spelar ingen roll om det skett avsiktligt eller oavsiktligt. Vissa personuppgiftsincidenter måste anmälas till Integritetsskyddsmyndigheten (IMY). Anmälan ska göras inom 72 timmar efter det att händelsen har upptäckts. Ibland måste personuppgiftsansvarig även informera berörda personer om att en incident har inträffat. Det är viktigt att det finns interna riktlinjer etablerade som beskriver vad en personuppgiftsincident är samt när den registrerade och Integritetsskyddsmyndigheten (IMY) ska underrättas. Det är också viktigt att de anställda utbildas i att identifiera och rapportera en personuppgiftsincident. Om personuppgiftsansvarig har anlitat ett biträde och en personuppgiftsincident upptäcks hos biträdet, måste personuppgiftsbiträdet rapportera incidenten till personuppgiftsansvarig.

- *Alla medarbetare ska vara utbildade i personuppgiftsincidentrapportering. Ska ske årligen och i introduktionen vid nyanställning.*
- *Personuppgiftssamordnaren är behjälplig att rapportera in incidenter.*
- *Om personuppgiftssamordnaren inte är på plats hänvisas till närmsta chef eller Drops/GDPR/Rutiner så att anmälan görs omgående.*
- *Alla incidentrapporteringar diarieförs av personuppgiftssamordnaren*

Scenario; en medarbetare glömmer sin väska på bussen innehållande ett usb minne med personuppgifter. Medarbetare kontaktar omgående personuppgiftssamordnare och i dialog tar ställning till huruvida det är känsliga personuppgifter, dvs allvarlig incident. Incident rapporteras i stadens interna rapporteringsverktyg. Om allvarlig incident rapporteras även till Integritetsskyddsmyndigheten (IMY) inom 72 timmar efter upptäckt incident.

Rutin för hur personal ska utbildas samt bibehålla sina kunskaper avseende dataskyddsfrågor.

Utbildning

Det är viktigt att de anställa får kontinuerlig utbildning i dataskyddsförordningen för att dataskyddsförordningens bestämmelser ska kunna följas.

Detta gäller för 2024–2025:

1. *Riktade utbildningar i första hand för bostadsförvaltare, systemförvaltare och inköpscontroller. Detta ska ske tillsammans med stadsjuristerna hösten 2024.*
2. *Fortsätta med Information vid introduktion av nyanställda.*
3. *Digital utbildning via HBG-Learns via helsingborg.se*
4. *Genomgång i samband med den årliga inventeringen av personuppgifter på respektive avdelnings APT.*