Bilaga O
till ”Arbetsordning för
styrelsen i Atrium Ljungberg AB”

Policy för personuppgiftsbehandling Atrium Ljungberg AB

(Beslutad vid styrelsemöte 2024-06-12)

Syfte

Atrium Ljungberg AB med dotterbolag, nedan benämnd Bolaget, bearbetar och behandlar personuppgifter i överensstämmelse med dataskyddsförordningen samt fastställda policys och riktlinjer som berör behandlingen och skyddet av personuppgifter.

Ansvar

Atrium Ljungbergs styrelse fastställer Bolagets Policy för personuppgiftsbehandling.

Denna policy ska revideras regelbundet och minst en gång per år fastställas av styrelsen. Personuppgiftsombud är dokumentägare och ansvarar för policyn.

Organisation

Personuppgiftsombud

Atrium Ljungberg behöver ej ha ett dataskyddsombud enligt dataskyddsförordningens definition då det inte bedriver en verksamhet som väsentligen behandlar personuppgifter. Atrium Ljungberg ska ha ett Personuppgiftsombud, som ansvarar för att Bolaget utför korrekt behandling av och har ändamålsenligt skydd för personuppgifter. Personuppgiftsombudet skall alltid tillfrågas vid frågor som rör behandling och skyddet av personuppgifter.

IT-arkitekt ansvarar för Informationssäkerhetsfrågor och är Personuppgiftsombud.

Krav på personuppgiftsbehandling

Personuppgifter ska hanteras med omtanke om den registrerades integritet. Minimeringsprincipen ska tillämpas på all personuppgiftsbehandling, vid var tid ska så lite personuppgifter som möjligt användas för att uppnå syftet med personuppgiftsbehandlingen Alla personuppgifter som Bolaget samlar in ska vara riktiga, relevanta, aktuella och det ska finnas ett tydligt syfte, ändamål och rättslig grund för behandlingen.

Information

Vid varje tillfälle som Bolaget samlar in nya eller uppdaterar personuppgifter ska berörd person informeras om vem som är personuppgiftsansvarig, det fullständiga syftet och den rättsliga grunden för behandlingen. Fullständig information om Bolagets behandling av personuppgifter ska finnas tillgänglig för berörda via Bolagets hemsida.

För intern och inhyrd personal ansvarar respektive chef för att informera om behandlingen av personuppgifter för anställningen eller inhyrningen.

Känsliga personuppgifter

Känsliga personuppgifter får, utöver lagkrav, endast samlas in för att fullgöra skyldigheter eller utöva rättigheter som arbetsgivare.

Konsekvensanalys

Alla åtgärder som inbegriper ny eller ändrad behandling av personuppgifter som kan medföra risker för de registrerades integritet ska föregås av en riskanalys. Analysen ska även föreslå lämpliga rutiner och åtgärder för att bemöta identifierade risker. Initiativtagare till förändringen är ansvarig för att initiera riskanalysen och ska vid behov av stöd kontakta personuppgiftsombudet.

Avtal som innefattar hantering av personuppgifter ska alltid granskas och godkännas av personuppgiftsombudet.

Lagringstid

Alla personuppgifter ska ha en maximal lagringstid. Denna ska sättas så kort som möjligt för att skydda den registrerades integritet men ta hänsyn till Bolagets krav och behov.

Radering

Alla personuppgifter som inte lever upp till kraven i denna policy eller uppnått sin maximala lagringstid ska raderas.

Skydd

Personuppgifter ska hanteras och lagras på ett sådant sätt att de är skyddade för obehörig åtkomst, förvanskning eller radering. Vid elektronisk lagring eller överföring ska kryptering av hög standard användas.

Rättelser

Det ska finnas kontroller och rutiner som ser till att felaktiga eller vilseledande personuppgifter som upptäcks eller blir kända hanteras på ett sätt så att de omedelbart raderas eller utan dröjsmål rättas.

Registrerades rättigheter

All behandling av personuppgifter ska ske på ett sådant sätt att de registrerades rättigheter enligt dataskyddsförordningen tillvaratas. Det ska finnas en tydlig kontaktväg för de registrerade för att kontakta Bolaget.

Incidenthantering

En process för rapportering och hantering av personuppgiftsincidenter som uppfyller rapporteringsskyldigheten till Integritetskyddsmyndigheten och till registrerad ska finnas dokumenterad.

Register

Det ska finns ett centralt register över alla personuppgiftsbehandlingar i koncernen.

Leverantörer och partners

Krav på lämpligt skydd av personuppgifter ska ställas på alla leverantörer som behandlar eller lagrar personuppgifter för Bolagets räkning genom personuppgiftsbiträdesavtal.

Behandling ska ske inom EU

Personuppgiftsbehandling ska ske inom EU/EES eller inom av EU kommissionen godkända länder. Avsteg från detta får ske endast med av EU kommissionen godkända mekanismer för överföring och varje sådan behandling ska godkännas av Chef Teknikutveckling och Digitalisering.

Periodiska kontroller

Processer för rapportering och uppföljning av efterlevnaden av personuppgiftsbehandlings policyn med därtill hörande riktlinjer ska finnas.

Regelbunden övervakning, dokumentation och rapportering av uppfyllnadsgrad inom hela Koncernen ska ske som en integrerad del i det dagliga arbetet. Personuppgiftsombud är ansvarig för att uppföljning och rapportering sker minst årligen.

Rapporteringen ska som ett minimum innehålla:

- Uppföljningar av kontrollernas effektivitet med underlag för bedömningen.
- Rapportering av incidenter/avvikelser från policyn med beskrivning
- Åtgärd/er med beskrivning, åtgärdsnytta samt när incident/avvikelse ska vara åtgärdad
- Uppföljning av utestående åtgärder samt klarrapportering