NACKA ENERGI

Granskningsrapport 2022
Styrelsemöte NEAB 2022-12-06

Personuppgiftsansvarig
Nacka Energi AB

Dataskyddsombudets granskningsrapport 2022

Dataskyddsombud
Hanna Virtanen

Datum 2022-10-28

Innehåll

Inledning

Dataskyddsförordningen (GDPR) reglerar hur myndigheter, bolag och andra organisationer får hantera personuppgifter. Som personuppgift räknas all typ av information som kan kopplas till en fysisk person. Varje organisation, oavsett verksamhet, behandlar därmed personuppgifter i någon omfattning och måste därmed förhålla sig till dataskyddsförordningens regler.

Förordningen ställer en rad krav; från säker hantering av information, till kontroll över vilka personuppgifter som hanteras, var, varför och hur samt kontinuerlig utvärdering av risker för enskildas fri- och rättigheter. Det är bolaget som är personuppgiftsansvarig för den personuppgiftsbehandling som sker inom dess verksamhet och därmed ytterst ansvarig för att förordningens krav följs.

Granskningens omfattning och metod

Denna rapport sammanfattar Nacka Energi AB:s efterlevnad av dataskyddsförordningen fördelat på nio områden. Områdena beskrivs närmare i rapporten nedan.

Rapporten lämnas av bolagets Dataskyddsombud. Dataskyddsombud är en roll som bolaget är skyldig att utse enligt dataskyddsförordningen och har i uppdrag att granska och rapportera om bolagets efterlevnad. Därutöver har dataskyddsombudet även i uppgift att ge råd och stöd om skyldigheter som följer av lagen samt fungera som kontaktpunkt gentemot enskilda och tillsynsmyndigheten, Integritetsskyddsmyndigheten (IMY). Denna rapport överlämnas till bolagets styrelse som en del av dataskyddsombudets uppdrag.

Bolagets efterlevnad av dataskyddsförordningen

I detta avsnitt sammanfattas bolagets efterlevnad av dataskyddsförordningens inom nio områden. Områdena beskrivs under respektive rubrik nedan.

1. Registrera personuppgiftsbehandlingar

Varje personuppgiftsansvarig ska enligt artikel 30 ha en förteckning över sina personuppgiftsbehandlingar (en registerförteckning) där bland annat syfte, kategorier av registrerade[1], typer av personuppgifter och lagringstid framgår. Registerförteckningen är förutsättning för att överhuvudtaget kunna efterleva dataskyddsförordningens då den anger vilka personuppgifter som behandlas, hur och varför.

Årets granskning omfattar huruvida bolagets samtliga personuppgiftsbehandlingar har registrerats och om innehåller i registerförteckningen motsvarar kraven i artikel 30.

Bolagets efterlevnad

[1] Registrerade = enskilda vars personuppgifter hanteras

Bolagets registerförteckning är i stora drag komplett och innehåller i stort nödvändig information. Vissa behandlingar och viss information saknas dock och behöver kompletteras för att registerförteckningen ska räknas som helt komplett. Därutöver rekommenderas att registerförteckningen ses över regelbundet.

2. Grundläggande principer

Grundläggande principer för behandling av personuppgifter anges i artikel 5 i dataskyddsförordningen. Principerna fungerar som vägledning för hur personuppgifter får hanteras och genomsyrar övriga krav på dataskydd. Principer handlar bland annat om att ha en rättslig grund, enbart behandla så många personuppgifter som behövs för ett visst syfte, iaktta proportionalitet, inte spara uppgifter längre än de behövs och ha tillräcklig säkerhet.

Årets granskning omfattar huruvida bolaget har rutiner för att säkerställa att de grundläggande principerna beaktas.

Bolagets efterlevnad

I samband med upprättandet av nya behandlingar i registerförteckningen, utvärderas även om behandlingen följer de grundläggande principerna. Utvärdering görs även i samband med konsekvensbedömningar (DPIA). Årets granskning har dock inte omfattat huruvida enskilda personuppgiftsbehandlingar iakttar principerna.

3. Rapportera personuppgiftsincidenter

Varje personuppgiftsansvarig ska ha processer för att upptäcka, utreda, åtgärda och anmäla vissa personuppgiftsincidenter till tillsynsmyndigheten Integritetsskyddsmyndigheten (IMY). Det innebär att medarbetare ska kunna identifiera när en personuppgiftsincident har hänt, veta hur den ska rapporteras och att det finns processer för att ta hand om en bekräftad incident. Det är även av vikt att incidenten leder till uppdaterade rutiner och arbetssätt för att förhindra nya incidenter.

Årets granskning omfattar huruvida bolaget har en process för att upptäcka, dokumentera och anmäla personuppgiftsincidenter.

Bolagets efterlevnad

Bolaget har en framtagen process som uppfyller kraven på hantering av personuppgiftsincidenter. Dock har enbart två incidenter rapporterats hittills under 2022, vilket kan bero på att inga andra incidenter skett men också på att inträffade incidenter inte rapporterats på grund av okunskap om definitionen av en incident. Orsaken till att få incidenter rapporterats har dock inte granskats närmare i årets rapport.

4. Konsekvensbedömning (DPIA)

Om det finns en hög risk för enskildas fri- och rättigheter när personuppgifter behandlas, ska den personuppgiftsansvarige göra en konsekvensbedömning. Exempel på situationer då en hög risk kan föreligga är: övervakning eller kartläggning av personer i beroendesituation,

behandling av känsliga personuppgifter eller användning av ny teknik. Konsekvensbedömningens syfte är både att säkerställa att enskildas fri- och rättigheter respekteras och är även ett sätt för den personuppgiftsansvarige att visa att dataskyddslagstiftningen följs.

Årets granskning omfattar huruvida bolaget dels genomfört en riskbedömning för att bedöma om en konsekvensbedömning krävs och om konsekvensbedömningen är gjord.

Bolagets efterlevnad

Bolaget har delvis genomfört riskbedömningar för att bedöma om konsekvensbedömning krävs eller ej. Konsekvensbedömningar har genomförts för behandlingar där personuppgifter överförs till tredjeland, men Dataskyddsombudet bedömer att konsekvensbedömningar krävs även för sociala medier, kamerabevakning, Office 365 och HR/personal-processen där känsliga personuppgifter hanteras eller enskilda medarbetare kartläggs.

5. Personuppgiftsbiträdesavtal (PUB-avtal)

Personuppgiftsbiträdesavtal ska tecknas om en personuppgiftsansvarig anlitar en extern part som behandlar personuppgifter åt den personuppgiftsansvariga. Den externa parten är då biträde till den personuppgiftsansvariga och ska genom avtalet förbindas att endast behandla personuppgifter efter instruktioner från den ansvarige. Syftet med avtalet är att säkerställa att enskildas personuppgifter skyddas även när det är någon annan än den personuppgiftsansvarige som behandlar personuppgifterna.

Årets granskning omfattar huruvida personuppgiftsbiträdesavtal tecknats där så krävs.

Bolagets efterlevnad

Bolaget har tecknat personuppgiftsbiträdesavtal med sina biträden.

6. Lagringsminimering, arkivering och gallring

Lagringsminimering är en av dataskyddsprinciperna och handlar om att personuppgifter endast behandlas får behandlas så länge de behövs för ändamålet. Inom offentlig verksamhet innebär lagringsminimering att det finns ordning och reda bland myndighetens information, att information rensas, arkiveras och gallras. Informationshanteringsplanen (IHP) är det styrdokument som ska visa vilka allmänna handlingar en verksamhet har och hur dessa ska hanteras.

Årets granskning omfattar huruvida bolaget har en uppdaterad informationshanteringsplan och om arkivering och gallring utförs enligt den.

Bolagets efterlevnad

– Bolaget har en aktuell informationshanteringsplan, dock gallras och arkiveras inte information efter den. Dataskyddsombudet rekommenderar att ta in gallring och arkivering som en (minst) årlig aktivitet i respektive verksamhets verksamhetsplan eller liknande.

7. Registrerades rättigheter

Enskilda har ett antal rättigheter i förhållande till sina personuppgifter, nämligen:

- Rätt att vända sig till en personuppgiftsansvarig för att få bekräftat om ens personuppgifter behandlas och i så fall få tillgång till dessa (Rätt till tillgång – även kallat ”registerutdrag”)
- Rätt att få information om hur personuppgifter hanteras (rätten till information)
- Under vissa förutsättningar få sina uppgifter raderade eller rättade (rätten till radering och rättelse)
- Rätt att invända, dvs. motsätta sig, mot en personuppgiftsbehandling och även begära begränsning av personuppgifternas användning (Rätten att göra invändningar och begära begränsning)
- Rätt att inte bli föremål för automatiskt beslutsfattande[2]
- Rätt att få ut sina personuppgifter på ett strukturerat sätt för att använda de hos någon annan (rätt till dataportabilitet – gäller enbart i få specifika fall inom offentlig förvaltning)

Årets granskning omfattar bolagets huruvida bolaget har processer för att hantera registrerades rättigheter som följer de grundläggande kraven i dataskyddsförordningen.

Bolagets efterlevnad

– Bolaget har rutiner för att hantera registerutdrag (rätten till tillgång), dataportabilitet och begäran om rättelse, däremot är inte processen för att hantera övriga rättigheter lika tydlig varken hur de ska hanteras internt eller kommuniceringen gentemot de registrerade. Bolaget informerar enskilda om hur deras personuppgifter hanteras, men informationen omfattar inte all den personuppgiftsbehandling som bolaget utför och behöver förtydligas i vissa delar för att helt följa kraven i dataskyddsförordningen.

8. Känsliga och extra skyddsvärda personuppgifter

Det finns ett generellt förbud mot att använda känsliga personuppgifter[3] i dataskyddsförordningen. Det är enbart tillåtet om en av undantagen är tillämpliga, därför är det viktigt att veta om eventuella känsliga personuppgifter som behandlas är laglig. Förutom känsliga personuppgifter, finns det en grupp personuppgifter kallat extra skyddsvärda[4]

---

[2] Beslut som fattas utan att en fysisk person är inblandad.

[3] För en beskrivning av känsliga personuppgifter, se: https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/personuppgifter/kansliga-personuppgifter

[4] För en beskrivning av extra skyddsvärda personuppgifter, se: https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/personuppgifter/kansliga-personuppgifter

personuppgifter som inte kräver ett undantag för att det ska vara tillåtet att hantera dem, men är samtidigt av en karaktär som kräver att de skyddas med högre säkerhet. Dessa typer av uppgifter och känsliga personuppgifter får enbart hanteras enligt säkerskilda rutiner och i system/lagringsytor som har högre säkerhet.

Årets granskning omfattar huruvida bolaget har rättslig grund för behandling av känsliga personuppgifter och huruvida rutiner finns för hantering av känsliga och extra skyddsvärda personuppgifter.

Bolagets efterlevnad

Det har inte framkommit att bolaget behandlar känsliga personuppgifter utan rättslig grund. Både känsliga och extra skyddsvärda personuppgifter hanteras enligt särskilda rutiner.

9. Informationssäkerhet

En av de grundläggande principerna är integritet och konfidentialitet som handlar om att kunna säkerställa personuppgifternas konfidentialitet (att inga uppgifter röjs för obehöriga), tillgänglighet (att uppgifterna är tillgängliga när de behövs) och riktighet (att uppgifterna är korrekta). Med andra ord handlar det om att arbeta aktivt med informationssäkerhet.

Årets granskning omfattar huruvida bolaget har ett informationssäkerhetsarbete och genomför analyser kopplat till detta, exempelvis informationsklassning och riskanalys,

Bolagets efterlevnad

Bolaget har en antagen informationssäkerhetspolicy från 2021 och infört ledningssystem för informationssäkerhet.

Sammanfattning av bolagets efterlevnad och dataskyddsombudets rekommendationer

Bolaget efterlever dataskyddsförordningen i de flesta avseenden. Inom några områden krävs åtgärder för att uppfylla kraven i sin helhet. Dataskyddsombudet ger därför följande rekommendationer:

- Färdigställa och uppdatera bolagets registerförteckning. Registerförteckningen bör ses över minst årligen och kan läggas in som en aktivitet i verksamheternas årshjul, verksamhetsplan eller liknande.
- Genomföra och dokumentera konsekvensbedömningar där dataskyddsförordningen kräver det. I dagsläget bedöms följande personuppgiftsbehandlingar kräva en konsekvensbedömning: sociala medier, kamerabevakning, Office 365 och HR/personal-processen där känsliga personuppgifter hanteras eller enskilda medarbetare kartläggs.

- Säkerställa att gallring och arkivering utförs enligt informationshanteringsplanen. Detta kan ske genom att gallring och arkivering läggs in som en aktivitet i verksamheternas årshjul, verksamhetsplan eller liknande.
- Förtydliga processen internt och för de registrerade om hur de kan utöva samtliga sina rättigheter och uppdatera informationstexterna till de registrerade så att de i sin helhet speglar hur bolaget hanterar personuppgifter.