Revisionsrapport 2023:5

Nacka Energi AB

Granskning av bolagets hantering av skyddade personuppgifter

Nacka kommun

Building a better working world

Innehåll

1. Sammanfattande bedömning och rekommendationer

EY har på uppdrag av Nacka kommuns lekmannarevisorer granskat Nacka Energi AB:s (NEAB) hantering av skyddade personuppgifter. Syftet med granskningen har varit att bedöma hur styrelse och VD för NEAB säkerställer att skyddade personuppgifter inte röjs till obehöriga samt om bolagets rutiner är ändamålsenliga och tillämpade. Detta har avsett skyddade personuppgifter för både kunder och anställda i bolaget. Vår övergripande bedömning är att styrelsen och VD har säkerställt att skyddade personuppgifter inte röjs till obehöriga, men att det finns ytterligare åtgärder att vidta.

Det finns en tydlig organisation och ansvarsfördelning för hantering av kunder och framtida medarbetare eller ansökningshandlingar med skyddade personuppgifter. Det finns en riktlinje och två rutinerna upprättade, vilka säkerställer en tillräcklig vägledning på såväl övergripande som detaljerad nivå för bolagets medarbetare. Dokumenten är inte antagna av bolagets styrelse eller VD med hänvisning till att framtagande och implementering av riktlinjer som berör daglig operativ verksamhet ej ska antas av styrelsen. Vi bedömer dock att riktlinjen bör antas av styrelsen eller VD givet områdets komplexitet och medföljande risker som kräver insyn i hanteringen samt regelbunden uppföljning. Vi noterar även att riktlinjen och rutinerna nyligen är upprättade och behöver således implementeras i hela organisationen, även bland de medarbetare som sällan kommer i kontakt med skyddade personuppgifter.

Nya medarbetare ska introduceras till bolagets riktlinje och rutiner gällande hantering av skyddade personuppgifter och ingår således i den obligatoriska utbildningsplanen vilket vi ser positivt på. Däremot bedömer vi att det finns ett behov av att utbilda samtliga medarbetare i hanteringen av skyddade personuppgifter specifikt och att det bör ske regelbundet i syfte att hålla kunskapen vid liv över tid. Det skulle stärka grundkunskaperna bland de medarbetare som sällan kommer i kontakt med skyddade personuppgifter i syfte att undvika fel orsakade av den mänskliga faktorn vilket enligt oss är den största risken i hanteringen av skyddade personuppgifter.

Risk- och väsentlighetsanalyser kring hanteringen av skyddade personuppgifter har upprättats inom ramen för bolagets systematiska internkontrollarbete. Skyddade personuppgifter utgör sedan årsskiftet en del av bolagets systematiska dataskyddsarbete genom att följa ett årshjul, vilket bland annat innefattar uppföljning av efterlevnad av rutiner och att dessa vid behov revideras en gång per år. Vi ser positivt på att det har påbörjats en förändringsprocess och genomlysning av bolagets dataskyddsarbete i allmänhet och hantering av skyddade personuppgifter i synnerhet.

Bolaget har vidtagit åtgärder för hanteringen av skyddade personuppgifter. Vi bedömer dock att det finns vissa brister och svagheter i nuvarande hantering, däribland avsaknad av automatiska behörighets- och åtkomstbegränsningar inbyggda i verksamhetssystemen, att vissa nuvarande arbetsprocesser delvis kräver manuell hantering samt att det inte genomförs loggkontroller. Bolaget är medvetna om bristerna och har eller ska utifrån genomförd risk- och väsentlighetsanalys vidta ytterligare åtgärder.

Det finns ett avvikelsehanteringssystem som omfattar skyddade personuppgifter i och med att det går att identifiera skyddade personuppgifter från övriga avvikelser. Vi ser positivt på att det finns en framtagen mall med en särskild kategori som omfattar skyddade personuppgifter som används för att riskbedöma en eventuell personuppgiftsincident. Nuvarande rutiner för avvikelsehantering möjliggör att erfarenheter från avvikelser tillvaratas och kan skapa

systematisk för att åtgärda eventuella brister kopplat till hanteringen av skyddade personuppgifter.

Utifrån granskningens iakttagelser rekommenderar vi styrelsen och VD i Nacka Energi AB att:

- Fastställa riktlinjen för hanteringen av skyddade personuppgifter.
- Genomföra obligatoriska utbildningar för samtlig personal i tillämpning av styrande dokument samt hanteringen av skyddade personuppgifter regelbundet.
- Säkerställa att pågående upphandling av ett nytt kundinformationssystem, som säkerställer en mer ändamålsenlig hantering av skyddade personuppgifter och minskar manuell hantering, implementeras skyndsamt.
- Säkerställa att det inköpta system för säkra meddelanden skyndsamt implementeras.
- Genomföra kontroller av användarloggar som en organisatorisk säkerhetsåtgärd för att kompensera påtalade brister i systemstödens avsaknad av behörighet.

2. Inledning

2.1 Bakgrund

Den som är utsatt för hot kan i vissa fall få skyddade personuppgifter. Från 2011 till 2021 har personer i Sverige med skyddade personuppgifter fördubblats från drygt 12 000 personer till knappt 24 000 personer. Den 1 januari 2019 skärptes lagstiftningen i syfte att öka skyddet för hotade och förföljda personer.

Personer med skyddade personuppgifter riskerar allvarliga problem om kommunens nämnder och bolag röjer skyddade uppgifter. Kommunen och bolagen bör därför ha säkra rutiner och riktlinjer för att säkerställa korrekt hantering av dessa uppgifter. Det är väsentligt att dessa arbetssätt och metoder är välkända hos samtliga medarbetare då i princip samtliga kan komma i kontakt med skyddade personuppgifter via kundkontakter eller som kollega.

Lekmannarevisionen har beslutat genomföra en fördjupad granskning av Nacka Energi AB:s arbete med rutiner, kunskapsspridning och säkerhetsfrågor vad gäller hanteringen av skyddade personuppgifter.

2.2 Syfte och revisionsfrågor

Granskningen syftar till att bedöma hur styrelse och VD för Nacka Energi AB säkerställer att uppgifter som rör skyddade personuppgifter inte röjs till obehöriga samt om bolagets rutiner är ändamålsenliga och tillämpade. Granskningen avser skyddade personuppgifter för såväl anställd personal som för kunder.

I granskningen besvaras följande revisionsfrågor:

- Finns styrande dokument och rutiner för hantering av skyddade personuppgifter?
- Hur görs styrdokument och rutinbeskrivningar kända för medarbetare?
- Finns ett tillräckligt stöd för medarbetare i vars ansvar det ligger att hantera skyddade personuppgifter?
- Genomförs fortlöpande kompetensutveckling kring skyddade personuppgifter?
- Har styrelse och VD tillsett tillräcklig uppföljning och kontroll av styrdokumentens och rutinbeskrivningarnas efterlevnad?
- Har styrelse och VD analyserat risken för att skyddade personuppgifter röjs?
- Har säkerhetsfrågor kopplade till skyddade personuppgifter analyserats och trygghetsskapande åtgärder vidtagits?
- Har styrelse och VD vidtagit åtgärder för att minska risken för röjning av skyddade personuppgifter?
- Finns avvikelsehanteringssystem som omfattar skyddade personuppgifter?
- Hur tillvaratas erfarenhet från avvikelser?
- Råder det samsyn inom Nacka kommun och Nacka Energi AB kring hur skyddade personuppgifter ska hanteras?

2.3 Ansvarig bolagsstyrelse

Granskningen avser Nacka Energi AB.

2.4 Metod och genomförande

Granskningen baseras på dokumentstudier och intervjuer. Samtliga intervjuade funktioner och granskade underlag framgår av källförteckningen.

Granskningen har följt god revisionssed och har kvalitetssäkrats internt, bland annat genom avstämning mot revisionsfrågor, faktagranskning och strukturerad dokumentation. Utöver intern kvalitetssäkring har samtliga intervjuade haft möjlighet att komma med synpunkter på rapportutkastet, detta för att säkerställa att revisionsrapporten bygger på korrekta uttalanden.

2.5 Revisionskriterier

Med revisionskriterier avses bedömningsgrunder som används i granskningen för analyser, slutsatser och bedömningar. Revisionskriterierna kan hämtas från lagar och förarbeten eller interna regelverk beslutade av fullmäktige och bolagsstämma. Kriterier kan också ha sin grund i jämförbar praxis eller erkänd teoribildning. I denna granskning utgörs de huvudsakliga revisionskriterierna av:

- Offentlighets- och sekretesslagen (2009:400)
- Folkbokföringslagen (1991:481)
- Folkbokföringsfördordning (1991:749)
- SFS 2018:695 Lag om ändring i folkbokföringslagen
- Av fullmäktige antagna styrdokument eller relevanta riktlinjer
- Ägardirektiv
- COSO-ramverket för intern kontroll
- Best practice kring bedömning av rutiner och intern kontroll vid hantering av skyddade personuppgifter

Dessa beskrivs närmare i bilaga och i kapitel 3.

3. Kontrollmiljö

Kontrollmiljö består exempelvis av etiska värderingar, ledarskapsresurser och ansvarsfördelning inom organisationen. Kontrollmiljö utgör en betydande del av den kultur som finns i organisationen: Är de anställda medvetna om det interna regelverket? Kan de lyfta etiska frågor? Hur agerar de i avsaknad av regler? Här är ledningens riskhanteringsfilosofi, integritet och etiska värderingar viktiga. Utöver organisationskultur består kontrollmiljön även av styrdokument, till exempel rutiner och riktlinjer.

3.1 Nacka Energi AB är personuppgiftsansvarig inom sitt verksamhetsområde

Nacka Energi AB (NEAB) är ett av Nacka kommuns helägda bolag genom Nacka Stadshus AB. Den primära verksamheten är drift och förvaltning av elnätet. NEAB har dotterbolaget Nacka Energi Försäljning AB (NEFAB). Kommunfullmäktige har gett i uppdrag till NEAB att förvalta och ansvara för drift och underhåll av lokalnätet för el. NEAB:s verksamhet täcker hela Nacka exklusive Boo församling och distribuerar el till ca 30 000 anslutna kunder inom koncessionsområdet. I samband med att Nacka växer, tunnelbaneutbyggnaden och allt fler bostäder och verksamheter byggs, arbetar bolaget även med att säkerställa att investeringar i elnätet skapar möjligheter för ett framtida hållbart Nacka.

Enligt NEAB:s ägardirektiv ska bolaget bidra till kommunens vision om ”öppenhet och mångfald” och kommunens övergripande mål samtliga följa kommunens övriga styrande dokument. Bolaget ska följa Nacka kommuns fyra styrprinciper, vilket innebär att:

- bolaget genom en öppen och transparent redovisning av sina intäkter och kostnader ska bidra till att kommunfullmäktige har ett rättvisande underlag för fastställande av nätavgifter och delårsrapporter,
- bolaget uppnår samma kvalitet på levererade tjänster som övriga leverantörer i kommunen,
- bolaget genom kunskapsdelning samverkar med andra utförare av liknande tjänster,
- bolaget genom varje ansvarsnivå säkerställer att beslut fattas så nära slutkunden som möjligt.

Personuppgiftsansvaret följer kommunkoncernens ansvarsfördelning; varje nämnd/styrelse är personuppgiftsansvarig för de personuppgifter som behandlas inom sitt verksamhetsområde. Det innebär att NEAB:s styrelse har ansvaret för att kundernas personuppgifter behandlas lagligt, säkert och i övrigt korrekt i bolaget.

3.2 Organisation och ansvarsfördelning för hanteringen av skyddade personuppgifter

Ansvarig för hanteringen av skyddade personuppgifter är bolagets dataskyddssamordnare, däribland meddela om nya lagar eller regler som påverkar hanteringen av skyddade personuppgifter. Ytterst ansvarig är bolagets VD/styrelsen. Avdelningschefen för avdelningen Kund & Marknad har det övergripande ansvaret för hanteringen av skyddade personuppgifter på avdelningsnivå, samt ska säkerställa att nya medarbetare utbildas i att hantera uppgifter om skyddade personuppgifter enligt gällande rutin och riktlinje (se avsnitt 3.3 och 3.4). Inom Kund & Marknad finns tre seniora rådgivare med särskilt ansvar för hanteringen av kunder med skyddade personuppgifter. Hanteringen av arbetsorder ansvarar behörig mättekniker och behörig montör för. HR-chefen har det övergripande ansvaret för hanteringen av skyddade

personuppgifter på avdelningsnivå, samt säkerställer att nya medarbetare utbildas i att hantera sekretessmarkerade uppgifter enligt medarbetarrutinen (se avsnitt 3.3). Kommunens centrala dataskyddsombud kan också indirekt genom att påtala brister i personuppgiftshantering i de årliga granskningsrapporterna påverka bolagets hantering av skyddade personuppgifter, men saknar dock formellt ansvar.

3.3 Styrande dokument och bolagsspecifika rutiner

Nacka kommuns *Informationssäkerhetsstrategi*, fastställd av kommunfullmäktige den 11 december 2017, utgör det styrande dokumentet för kommunens informationssäkerhetsarbete och är därmed av relevans för hanteringen av skyddade personuppgifter även i bolaget. Av strategin framgår att informationssäkerhetsarbetet ska präglas av förtroende för medarbetares och leverantörers förmåga att hantera informationstillgångar på ett säkert sätt. Varje nämnd/bolag ansvarar för att informationstillgångar inom sitt ansvarsområde hanteras enligt gällande lagstiftning och strategin. Informationssäkerhetsarbetet ska vara uppbyggt så det är lätt att hantera information korrekt, vilket innefattar bland annat att det finns lättillgänglig kunskap om informationssäkerhetsarbetet och att det finns utbildning som är tillgänglig gör alla.

Vid granskningstillfället pågår en revidering av informationssäkerhetsstrategin. Av utkast till den nya strategin framgår fyra strategiska inriktningar som informationssäkerhetsarbetet ska bygga på:

- Identifiera och analysera tillgångar, krav och risker
- Utforma informationssäkerhetsarbetet efter säkerställda behov
- Arbeta aktivt, inkluderade och framåtlutat
- Systematisk uppföljning, lärande och förbättringar

Detta innefattar bland annat att respektive enhet eller bolag regelbundet ska följa upp efterlevnaden av sina mål, handlingsplaner, säkerhetsåtgärder och prioriteringar för att säkerställa att avsedd verkan uppnåtts. Enligt uppgift är en målsättning i framtagandet av den nya strategin att tydliggöra struktur för uppföljning och det förbättrande arbetet.

Det finns inget koncernövergripande styrdokument för hantering av skyddade personuppgifter specifikt. Vid intervju har detta kopplats till styrmodellen i Nacka. Upplevelsen bland intervjuade är att riktlinjer och/eller rutiner för arbetet med skyddade personuppgifter inte behöver beslutas på övergripande nivå, utan att frågan med fördel kan hanteras mer verksamhetsnära i bolaget.

I NEAB finns en riktlinje och två rutiner för hantering av skyddade personuppgifter. Skillnaden mellan policy, riktlinje och rutin fastställs av bolagets *Riktlinje för styrdokument*. En riktlinje kan klassas som både publik och intern samt gälla för hela bolaget eller flera verksamhetsområden. En rutin avser ett enskilt verksamhetsområde och klassas som intern, i särskilda fall som känslig eller hemlig. Styrande dokument som överlappar alla verksamhetsområden ska godkännas av VD och i vissa fall styrelsen. Styrande dokument för enskilt verksamhetsområde godkänns av avdelningschef, gruppledare eller processägare. Alla riktlinjer/rutiner finns tillgängliga på intranätet.

Ansvarig för riktlinjen är bolagets dataskyddssamordnare och den är godkänd av informationssäkerhetsansvarig. Den är säkerhetsklassad som intern. Riktlinjen reviderades i februari 2023 och utgör ett stöd och vägledning för anställda inom NEAB vid hantering av

skyddade personuppgifter. NEAB:s målsättning är att verksamheten ska ha erforderliga kunskaper i hur skyddade personuppgifter hanteras för att på så sätt minska risken för att uppgifter röjs och att antalet personer med åtkomst till dem begränsas. Bolagets vision är att hantering av skyddade personuppgifter ska vara tydlig och säker samt att uppgifter ej röjs. I riktlinjen beskrivs bland annat:

- olika typer av sekretessmarkering,
- NEAB:s systematiska dataskyddsarbete,
- hantering av skyddade personuppgifter inom NEAB,
- förfrågan om allmän handling,
- behandling av skyddade personuppgifter i IT-system,
- behörighet och åtkomst,
- hantering och kommunicering,
- efterlevnad av rutiner samt incidenthantering.

De två rutinerna upprättades i mars 2023. En rutin riktad till enheten Kund & Marknad och en riktad till eventuella medarbetare eller ansökningshandlingar. I de två rutinerna utvecklas respektive område mer detaljerat (se vidare i kapitel 5). Rutinerna ska revideras och uppdateras minst vartannat år. Ansvarig för rutinen för Kund & Marknad är gruppchef och den är godkänd av avdelningschef. Ansvarig för rutinen för medarbetare och ansökningshandlingar är avdelningschef som även har godkänt rutinen. De båda rutinerna klassas som interna.

Intervjuade beskriver att riktlinjen/rutinerna har upprättats/reviderats i samband med pågående förändringsprocess inom ramen för bolagets hantering av skyddade personuppgifter som dataskyddsombudet har initierat (se vidare i avsnitt 4.1 och 5.1.1). Riktlinjen och de två rutinerna är inte antagna av bolagets styrelse med hänvisning till att framtagande och implementering av riktlinjer som berör daglig operativ verksamhet ej ska antas av styrelsen.

3.4 Det finns behov av ytterligare kompetensutveckling

Avdelningschef för respektive avdelning ansvarar för att rutiner och tillhörande regler för hantering av skyddade personuppgifter följs. Nya medarbetare ska alltid introduceras till bolagets riktlinje och rutiner gällande hantering av skyddade personuppgifter. Respektive avdelningschef ansvarar för att medarbetarna har goda kunskaper om hanteringen av skyddade personuppgifter och sekretessbestämmelserna samt för att kunskapsnivån bibehålls över tid genom utbildningar.

HR-chefen ansvarar för verkställandet och utförandet av utbildning av nyanställda på avdelningsnivå. Dataskyddssamordnare ansvarar för utbildningar kring hanteringen av skyddade personuppgifter och incidenthantering. Inom Kund & Marknad ansvarar avdelningschefen för verkställandet av utbildning av nyanställda i hanteringen av skyddade personuppgifter, som sedan utförs av de seniora rådgivarna. Utbildning av nyanställda ingår i den obligatoriska utbildningsplanen. Innehållet i utbildningarna anpassas och baseras på resultatet av bolagets internkontroller.

Intervjuade beskriver dock dels att arbetet med att sprida rutinerna kan stärkas, dels att det finns ett behov av att utbilda samtliga medarbetare i hanteringen av skyddade personuppgifter specifikt och att det bör ske årligen. Framförallt framhävs behovet av att stärka grundkunskaperna bland de medarbetare som sällan kommer i kontakt med skyddade

personuppgifter i syfte att undvika fel orsakade av den mänskliga faktorn. Samtidigt framkommer att hanteringen känns tryggare i och med de nyligen framtagna/reviderade rutinerna/riktlinjen.

3.5 Bedömning

Vår bedömning är att NEAB har säkerställt en god kontrollmiljö avseende risken för röjning av skyddade personuppgifter. Det finns en tydlig organisation och ansvarsfördelning för hantering av kunder och framtida medarbetare eller ansökningshandlingar med skyddade personuppgifter. Vi bedömer det finnas en riskmedveten kultur där hanteringen av skyddade personuppgifter behandlas inom ramen för bolagets dataskyddsarbete. Riktlinjen och de två rutinerna bedömer vi vara ändamålsenliga och säkerställer en tillräcklig vägledning på såväl övergripande som detaljerad nivå för bolagets medarbetare. Stödet för medarbetarna bedömer vi således vara tillräckligt, både genom riktlinjen och två rutinerna samt genom bolagets dataskyddssamordnare. Dokumenten är inte antagna av bolagets VD eller styrelse. Vi bedömer att riktlinjen bör antas av VD eller styrelsen givet områdets komplexitet och medföljande risker som kräver insyn i hanteringen samt regelbunden uppföljning av det arbete som bedrivs för hanteringen av skyddade personuppgifter i bolaget.

Vi noterar även att riktlinjen och rutinerna nyligen är upprättade och behöver således implementeras i hela organisationen, även bland de medarbetare som sällan kommer i kontakt med skyddade personuppgifter. Enligt nuvarande rutiner ska nya medarbetare introduceras till bolagets riktlinje och rutiner gällande hantering av skyddade personuppgifter och ingår således i den obligatoriska utbildningsplanen. Däremot bedömer vi att det finns ett behov av att utbilda samtliga medarbetare i hanteringen av skyddade personuppgifter specifikt och att det bör ske regelbundet i syfte att hålla kunskapen vid liv över tid. Det skulle stärka grundkunskaperna bland de medarbetare som sällan kommer i kontakt med skyddade personuppgifter i syfte att undvika fel orsakade av den mänskliga faktorn vilket enligt oss är den största risken i hanteringen av skyddade personuppgifter.

4. Riskbedömningar

Riskanalys handlar om att identifiera interna och externa risker som en organisation riskerar att utsättas för. Till analysen hör också att kvantifiera hur stor sannolikhet det är att identifierad risk inträffar samt vilka konsekvenserna skulle bli för organisationen. Utifrån verksamhetens behov kan det finnas anledningar att göra riskanalyser på olika nivåer och i olika omfattning i organisationen för att hantera risker på ett ändamålsenligt sätt.

4.1 Risken har analyserats men inte inom ramen för bolagets internkontrollarbete

I dataskyddsombudets årliga granskningsrapport för 2022 identifieras ett antal förbättringar. Däribland konstateras att vissa behandlingar och viss information i bolagets registerförteckning saknas och behöver kompletteras för att registerförteckningen ska räknas som helt komplett. Vidare konstateras att bolaget endast delvis har genomfört riskbedömningar för att bedöma om konsekvensbedömning i syfte att identifiera om det finns en hög risk för enskildas fri- och rättigheter när personuppgifter behandlas, krävs eller ej. Det saknas konsekvensbedömningar för sociala medier, kamerabevakning, Office 365 och HR/personal-processen där känsliga personuppgifter hanteras eller enskilda medarbetare kartläggs. Bolaget har genomfört konsekvensbedömningar av identifierade risker sedan årsskiftet. Därutöver rekommenderar dataskyddsombudet att ta in gallring och arkivering av personuppgifter som en (minst) årlig aktivitet i respektive enhets/bolags verksamhetsplan eller liknande. Känsliga och extra skyddsvärda personuppgifter bedöms hanteras enligt bolagets särskilda rutiner.

Det har genomförts en riskanalys kring hanteringen av skyddade personuppgifter. Riskanalysen genomfördes i februari-mars 2023. I riskanalysen analyserades 13 risker, varav sju risker klassificerades med risken 12 av 16. Riskerna rör bland annat bristande behörighet i IT-system, bristande följsamhet mot arbetsrutiner samt systematisk felhantering av uppgifter på grund av bristande uppföljning och kontinuitet i arbetet med dataskydd. Utifrån identifierade risker har rutiner uppdaterats eller upprättats, workshopar har anordnats och ett nytt kundinformationssystem ska upphandlas (se avsnitt 5.1.1). Vid dessa workshopar har de som hanterar skyddade personuppgifter deltagit och ämnena som berörts har bland annat varit bolagets rutiner, systemstöd och lagstiftning. I arbetet ingår också att göra en översyn av de processer som fått anmärkningar i dataskyddsombudets granskningsrapport då det till viss del berör hanteringen av skyddade personuppgifter. Enligt intervjuade är hanteringen av skyddade personuppgifter sedan årsskiftet en del av bolagets systematiska dataskyddsarbete och följer ett årshjul genom att exempelvis uppföljning av efterlevnad av rutiner och att dessa vid behov revideras en gång per år.

4.2 Bedömning

Vi ser positivt på att det har påbörjats en förändringsprocess och genomlysning av bolagets dataskyddsarbete i allmänhet och hantering av skyddade personuppgifter i synnerhet. I processen har bolagsspecifika risker och brister identifierats som antingen har åtgärdats eller ska åtgärdas i närtid. Risk- och väsentlighetsanalyser kring hanteringen av skyddade personuppgifter har upprättats inom ramen för bolagets systematiska internkontrollarbete. Skyddade personuppgifter utgör sedan årsskiftet en del av bolagets systematiska dataskyddsarbete genom att följa ett årshjul, vilket bland annat innefattar uppföljning av efterlevnad av rutiner och att dessa vid behov revideras en gång per år. Vi bedömer därför att

styrelsen och VD har analyserat risken för att skyddade personuppgifter röjs i bolaget samt att de har tillsett tillräcklig uppföljning och kontroll av rutinbeskrivningarnas efterlevnad.

5. Kontrollaktiviteter – Bolagets rutiner och arbetssätt

Åtgärder eller "kontrollaktiviteter" utgörs av de aktiviteter som en organisation företar för att minska eller eliminera risker. Kontrollaktiviteter anges ofta i en internkontrollplan och syftar då till att följa upp att verksamhetens kontroller fungerar ändamålsenligt (se avsnitt 4.1). Verksamhetens åtgärder/kontroller finns ofta integrerade i verksamhetens olika processer och kan se olika ut, till exempel inom ramen för dataskyddsarbetet/informationssäkerhetsarbetet, stöd och behörighet i IT- och verksamhetssystem, interna och externa kommunikationskanaler samt hanteringen av medarbetare. Gemensamt är att aktiviteterna syftar till att reducera risker.

5.1 Skyddade personuppgifter behandlas inom ramen för bolagets systematiska dataskyddsarbete

Det systematisk dataskyddsarbete är en del av bolagets informationssäkerhetsarbete och syftar till att säkerställa lagefterlevnad enligt gällande dataskyddslagstiftning. Bolagets skydd och hantering av personuppgifter och skyddade personuppgifter säkerställs genom gällande riktlinjer och rutiner för bland annat skyddade personuppgifter, de registrerades rättigheter, registerförteckningar, risk- och konsekvensbedömningar, incidenthantering och personuppgiftsbiträdesavtal.

Skyddade personuppgifter ska enligt intervjuade hanteras med mycket stor försiktighet. För de system och processer som hanterar skyddade personuppgifter i bolaget ska det finnas rutiner för hur en korrekt hantering säkerställs. Av riktlinjen framgår att risken att uppgifterna felaktigt lämnas ut ökar med antalet handläggare som kan ta del av uppgifterna. Kretsen av personer som har behörigheten att ta del av skyddade personuppgifter ska därför begränsas så långt som möjligt.

Som kommunalt bolag omfattas NEAB av den grundlagsstadgade offentlighetsprincipen. Denna princip medför en skyldighet att på begäran tillhandahålla, genom kopia eller på plats, allmänna handlingar. Oavsett om en sekretessmarkering eller skyddad folkbokföring finns ska respektive avdelning alltid göra en prövning vid en begäran om utlämnande av allmän handling. Finns det sekretessmarkering eller skyddad folkbokföring ska dessa fungera som en varningssignal, samt utgöra en del av underlaget vid bedömningen om en handling ska lämnas ut.

5.1.1 Behandling av skyddade personuppgifter i IT- och verksamhetssystem

Behandling av skyddade personuppgifter i IT-system ska följa Skatteverkets vägledning för hantering av skyddade personuppgifter. Det ska på ett tydligt och enhetligt sätt framgå för de användare som har åtkomstbehörighet till skyddade personuppgifter att uppgifterna är markerade för skyddad folkbokföring eller har sekretessmarkering, både i IT-system och på utskrifter. Åtkomst till skyddade personuppgifter ska loggas för att i efterhand kunna kontrollera vilka som tagit del av uppgifterna.

I NEAB används två system som hanterar skyddade personuppgifter. I ett hanteras administration av kunduppgifter, fakturering och arbetsorder. Systemet markerar sekretessbelagda uppgifter och endast behöriga medarbetare handlägger ärenden med skyddade personuppgifter. Användarloggar genereras av systemet och möjliggör för kontroll av vem som tagit del av skyddade personuppgifter. Användarloggar har inte genomförts i det syftet. Det andra systemet är bolagets verktyg för dokumentation, planering och drift av

elnätet. Kundimport görs från kundinformationssystemet och de skyddade personuppgifterna förs över maskerade. Systemet genererar ändringsloggar men saknar stöd för användarloggar.

Enligt bolagets policy ska enbart de användare som har behov av uppgifterna kunna ta del av skyddade personuppgifter. Det finns dock inga behörighets- och åtkomstbegränsningar inbyggda i systemen. Enligt intervjuade är det därför av vikt att säkerställa att samtliga medarbetare har tagit del av bolagets tystnads- och sekretesspolicy. Därutöver ingår att säkerställa att berörda leverantörer har tecknat avtal gällande personuppgiftsbiträde (PUB-avtal) och att entreprenörer och inhyrd personal har skrivit under ett tystnadspliktsavtal. En åtgärd för att minimera misstag är att det tydligt ska framgå att en person har skyddade personuppgifter i systemet. Det är därför viktigt att markeringar om skyddade personuppgifter syns vid alla sökningar i systemregistret. På avdelningen Kund & Marknad har behörigheten till hanteringen av skyddade personuppgifter begränsats till avdelningens tre seniora rådgivare i bemärkelsen att övriga handläggare alltid lämnar över samtliga ärenden som involverar hantering av skyddade personuppgifter till de seniora rådgivarna.

Enligt intervjuade finns det brister i nuvarande systemstöd vilket resulterar i att behandling av skyddade personuppgifter i viss utsträckning kräver manuell hantering. En av bristerna är att det inte finns behörighets- och åtkomstbegränsningar inbyggda i systemen. En annan brist är att utskick av fakturor till kunder, däribland de med skyddade personuppgifter, måste ske manuellt via Skatteverkets postförmedling vilket kräver hantering av fysiska papper med mycket känsliga uppgifter. Hanteringen av pappersutskrifter beskrivs vara ett extra riskfyllt orosmoment som kräver varsam hantering.

Det pågår vid granskningens tidpunkt en upphandlingsprocess av ett nytt kundinformationssystem där förhoppningen är att bolaget som kravställare har möjlighet att ställa krav på en mer ändamålsenlig hantering av skyddade personuppgifter, uppger intervjuade. Enligt nuvarande tidplan ska det nya kundinformationssystemet implementeras under våren 2024.

5.2 Hantering och kommunicering av skyddade personuppgifter

Det finns ett ansvar hos den enskilde att upplysa om att man har skyddade personuppgifter. Markering för skyddad folkbokföring och sekretessmarkering kan aviseras från Skatteverket till NEAB eller direkt från den enskilde. Det framgår av rutinerna och av intervjuer att den som har skyddade personuppgifter själv måste vara mycket noggrann med hur denne hanterar sina personuppgifter.

Kommunicering med en kund sker via brev eller personliga besök om den enskilde har legitimerat sig. Ett system för säkra meddelanden, det vill säga elektronisk kommunikation med hjälp av elektronisk legitimation, är inköpt men ännu inte implementerat av okänd anledning. Kommunikation via e-post ska aldrig tillämpas vid hantering av skyddade personuppgifter. Brev till skyddade personuppgifter skickas via Skatteverkets postförmedling. Det finns därutöver mer detaljerade rutiner kring kommunicering med kund i syfte att minska risken för röjning av skyddade personuppgifter, exempelvis att personnummer aldrig ska ges ut.

Hantering av arbetsorder, exempelvis då ett fel upptäckts som kräver fysiskt besök hos kund med skyddade personuppgifter, följer särskild rutin. Samtliga arbetsorder rörande personer med skyddade personuppgifter handläggs av behörig mättekniker och montör. Dessa arbetsorder markeras av systemet med ”skyddad identitet” för att urskilja dem från övriga ärenden och innehåller inte uppgifter om namn, utan endast anläggningens id och adress.

Arbetsorder rörande person med skyddad id skrivs ut samma dag som ärendet handläggs. Utskriften görs av behörig mättekniker som förvarar den i fysisk mapp och delger ärendet till behörig montör.

5.3 Hantering av medarbetare med skyddade personuppgifter följer särskild rutin

Rutinen för hantering av medarbetare eller ansökningshandlingar med skyddade personuppgifter upprättades i mars 2023 i samband med revideringen av bolagets riktlinjer för hanteringen av skyddade personuppgifter. Enligt intervjuade fanns ett behov av en särskild rutin för hantering av ansökningshandlingar och medarbetare. Enligt rutinen ska antalet personal med insyn i ärendet begränsas så långt det går och ska i efterhand noggrant kontrollera vilka som har tagit del av de skyddade personuppgifterna. När bolaget kommer i kontakt med en anställd eller ansökningshandlingar med skyddade personuppgifter ska alltid en riskbedömning göras i syfte att kartlägga säkerhetsrisken och komma fram till åtgärder för att minimera informationsspridning av uppgifterna. Rutinen innehåller detaljerade uppgifter om fysisk överlämning av handlingar och information, begränsningar, förvaring, kommunikation via mejl, hantering av skyddade personuppgifter i personalsystemet och rekryteringssystemet, tilldelning av konton i IT-system, ansvarsfördelning, utbildning av personal samt incidenthantering.

Det finns inga medarbetare med skyddade personuppgifter. Bolaget har i praktiken inte testat bolagets rutiner för hantering av ansökningshandlingar eller medarbetare med skyddade personuppgifter.

5.4 Bedömning

Vår bedömning är att NEAB har vidtagit vissa åtgärder för att minska risken för röjning av skyddade personuppgifter, men att åtgärderna kan bli fler och skarpare.

NEAB har utifrån genomförd risk- och väsentlighetsanalys upprättat bolagsspecifika arbetsrutiner för hanteringen av skyddade personuppgifter i syfte att minska risken för röjning av skyddade personuppgifter inom ramen för bolagets dataskyddsarbete. Däribland specifika arbetsrutiner kring förfrågan om allmän handling, behandling av skyddade personuppgifter i IT- och verksamhetssystem, vissa begränsningar i behörighet och åtkomst, säkra rutiner för hantering och kommunicering av skyddade personuppgifter samt rutiner för incidenthantering.

Vi bedömer dock att det finns vissa brister i nuvarande hantering. En allvarlig brist är att det inte finns några automatiska behörighets- och åtkomstbegränsningar inbyggda i systemen vilket innebär att antalet personer med tillgång till de skyddade personuppgifterna är fler än vad som är önskvärt. En annan brist är att utskick av fakturor till kunder med skyddade personuppgifter måste ske manuellt via Skatteverkets postförmedling vilket kräver hantering av pappersutskrifter. Den typ av manuell hantering är riskfyllda moment vilket ökar risken för felhantering och röjning orsakad av den mänskliga faktorn. Den pågående upphandlingen av ett nytt kundinformationssystem som skulle kunna resultera i en mer säker och ändamålsenlig hantering av skyddade personuppgifter bör därför implementeras skyndsamt enligt vår uppfattning.

Därutöver bedömer vi det vara väsentligt att skyndsamt implementera det inköpta system för säkra meddelanden, det vill säga elektronisk kommunikation med hjälp av elektronisk legitimation i syfte att minska risken för röjning av skyddade personuppgifter vid intern och extern kommunikation. NEAB har inte genomfört kontroller av användarloggar med anledning

av risken för röjning av skyddade personuppgifter. Loggkontroller är ett effektivt verktyg för att säkerställa att obehöriga inte får tillgång till skyddade personuppgifter i IT- och verksamhetssystemen. Vi bedömer att sådana bör genomföras som en organisatorisk säkerhetsåtgärd för att kompensera påtalade brister i systemstödens avsaknad av behörighetsbegränsningar.

6. Avvikelsehantering

6.1 Det har skett en avvikelse avseende skyddade personuppgifter

Samtliga personuppgiftsincidenter rörande skyddade personuppgifter ska rapporteras enligt särskild rutin för personuppgiftsincident. Samtliga incidenter ska dokumenteras med en beskrivning av incidenten och dess konsekvenser, samt vidtagna åtgärder och uppföljning i syfte att förebygga framtida incidenter och stärka dataskyddet. Dokumentationen görs i särskild mall som innehåller en riskbedömning av personuppgiftsincidenten. Mallen uppdaterades senast i februari 2023. I mallen finns en särskild kategori som omfattar skyddade personuppgifter. Dataskyddssamordnaren fattar beslut om ärendet ska anmälas till Integritetsskyddsmyndigheten (IMY). Ytterst ansvarig är VD/styrelse vilket innebär att ansvaret är delat. För att framtida incidenter ska kunna förhindras på ett effektivt sätt måste orsaken till incidenten utredas, nya risk- och konsekvensanalyser genomföras, samt en konkret åtgärdsplan upprättas. Detta görs för varje enskilt fall av personuppgiftsincident enligt rutinen.

I Nacka kommuns dataskyddsombuds granskningsrapport konstateras att två incidenter rapporterats under 2022, vilket enligt rapporten 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. Ingen av de rapporterade incidenter rörde skyddade personuppgifter. NEAB:s dataskyddsamordnare instämmer i att de få rapporterade personuppgiftsincidenterna kan tyda på att bolagets medarbetare antingen saknar kunskap om vad en personuppgiftsincident är eller om hur en sådan anmälan ska upprättas. Orsaken är dock inte utredd och fastställd. Samtidigt finns bland de intervjuade en tilltro till att en eventuell röjning eller incident kopplat till skyddade personuppgifter skulle anmälas och hanteras skyndsamt enligt gällande rutiner.

Det har historiskt rapporterats en incident avseende hanteringen av skyddade personuppgifter. Incidenten skedde i samband med utskrivning av en faktura till kund, där kunden med skyddade personuppgifter fick ta del av en annan kunds personuppgifter. Kunden anmälde incidenten och det rapporterades till dataskyddsombudet och rutinerna stärktes därefter.

6.2 Bedömning

Enligt vår bedömning finns det ett ändamålsenligt avvikelsehanteringssystem som omfattar skyddade personuppgifter i och med att det går att identifiera skyddade personuppgifter från övriga avvikelser. Vi ser positivt på att det finns en framtagen mall med en särskild kategori som omfattar skyddade personuppgifter som används för att riskbedöma en eventuell personuppgiftsincident. Det möjliggör att erfarenheter från avvikelser tillvaratas och kan skapa systematisk för att åtgärda eventuella brister kopplat till hanteringen av skyddade personuppgifter i tillräcklig utsträckning. Vi noterar att en incident har rapporterats avseende hanteringen av skyddade personuppgifter och att rutinerna stärktes därefter.

7. Svar på revisionsfrågor

Fråga	Svar
Finns styrande dokument och rutiner för hantering av skyddade personuppgifter?	Nej. Styrelse eller VD har inte beslutat om ett styrande dokument för hantering av skyddade personuppgifter. Däremot har olika avdelningar upprättat en riktlinje och två rutiner, klassade som interna arbetsdokument, vilka vi bedömer vara ändamålsenliga och säkerställer en tillräcklig vägledning på såväl övergripande som detaljerad nivå för bolagets medarbetare. Vi bedömer att styrelse eller VD bör anta bolagets övergripande riktlinje i syfte att säkerställa tillräcklig insyn och uppföljning i bolagets arbete kring hanteringen av skyddade personuppgifter.
Hur görs styrdokument och rutinbeskrivningar kända för medarbetare?	Nya medarbetare introduceras till bolagets riktlinje och rutiner gällande hantering av skyddade personuppgifter och ingår således i den obligatoriska utbildningsplanen. Respektive avdelningschef ansvarar för att medarbetarna har goda kunskaper om hanteringen av skyddade personuppgifter och sekretessbestämmelserna samt för att kunskapsnivån bibehålls över tid genom utbildningar. HR-chefen ansvarar för verkställandet och utförandet av utbildning av nyanställda på avdelningsnivå. Dataskyddssamordnare ansvarar för utbildningar kring hanteringen av skyddade personuppgifter och incidenthantering.
Finns ett tillräckligt stöd för medarbetare i vars ansvar det ligger att hantera skyddade personuppgifter?	Ja. Det finns en tydlig organisation och ansvarsfördelning för hantering av kunder och framtida medarbetare eller ansökningshandlingar med skyddade personuppgifter. Vi bedömer det finnas en riskmedveten kultur där hanteringen av skyddade personuppgifter behandlas inom ramen för bolagets dataskyddsarbete. Vi bedömer vidare att tillgängligt stöd till medarbetare genom riktlinjen och de två rutinerna samt genom bolagets dataskyddssamordnare är tillräckligt.
Genomförs fortlöpande kompetensutveckling kring skyddade personuppgifter?	Nej. Det sker ingen fortlöpande kompetensutveckling vilket vi bedömer vara en brist. Det finns ett behov av att utbilda samtliga medarbetare i hanteringen av skyddade personuppgifter specifikt och att det bör ske regelbundet i syfte att hålla kunskapen vid liv över tid. Det skulle stärka grundkunskaperna bland de medarbetare som sällan kommer i kontakt med skyddade personuppgifter i syfte att undvika fel orsakade av den mänskliga faktorn vilket enligt oss är den största risken i hanteringen av skyddade personuppgifter.
Har styrelsen och VD tillsett tillräcklig uppföljning och kontroll av styrdokumentens och rutinbeskrivningarnas efterlevnad?	Ja. Skyddade personuppgifter utgör sedan årsskiftet en del av bolagets systematiska dataskyddsarbete genom att följa ett årshjul, vilket bland annat innefattar uppföljning av efterlevnad av rutiner och att dessa vid behov revideras en gång per år. Vi noterar samtidigt att riktlinjen och rutinerna är nyligen upprättade och behöver således implementeras i hela organisationen. Styrelsen har tidigare inte genomfört någon uppföljning av det arbete som bedrivs för hanteringen av skyddade personuppgifter.
Har styrelsen och VD analyserat risken för att skyddade personuppgifter röjs?	Ja. Styrelsen har i februari-mars 2023 genomfört risk- och väsentlighetsanalyser kring hanteringen av skyddade personuppgifter inom ramen för bolagets systematiska internkontrollarbete. Utifrån identifierade risker har bolaget påbörjat en förändringsprocess och genomlysning av bolagets dataskyddsarbete i allmänhet och hantering

	av skyddade personuppgifter i synnerhet. I processen har bolagsspecifika risker och brister identifierats som antingen har åtgärdats eller ska åtgärdas i närtid.
Har säkerhetsfrågor kopplade till skyddade personuppgifter analyserats och trygghetsskapande åtgärder vidtagits?	Ja. I genomförd risk- och väsentlighetsanalys har säkerhetsfrågor kopplade till skyddade personuppgifter analyserats. Utifrån identifierade risker och brister har åtgärder vidtagits eller ska vidtas i närtid.
Har styrelsen och VD vidtagit åtgärder för att minska risken för röjning av skyddade personuppgifter?	Ja. Bolaget har innan genomförd risk- och väsentlighetsanalys vidtagit vissa åtgärder för att minska risken för röjning av skyddade personuppgifter, men vi noterar samtidigt att åtgärderna kan bli fler och skarpare. Däribland avsaknad av automatiska behörighets- och åtkomstbegränsningar inbyggda i verksamhetssystemen, att vissa nuvarande arbetsprocesser delvis kräver manuell hantering samt att det inte genomförs loggkontroller. Bolaget är medvetna om bristerna och har eller ska utifrån genomförd risk- och väsentlighetsanalys vidta ytterligare åtgärder.
Finns avvikelsehanteringssystem som omfattar skyddade personuppgifter?	Ja. Enligt vår bedömning finns det ett ändamålsenligt avvikelsehanteringssystem som omfattar skyddade personuppgifter i och med att det går att identifiera skyddade personuppgifter från övriga avvikelser. Vi ser positivt på att det finns en framtagen mall med en särskild kategori som omfattar skyddade personuppgifter som används för att riskbedöma en eventuell personuppgiftsincident.
Hur tillvaratas erfarenhet från avvikelser?	Nuvarande rutiner för avvikelsehantering möjliggör att erfarenheter från avvikelser tillvaratas och kan skapa systematisk för att åtgärda eventuella brister kopplat till hanteringen av skyddade personuppgifter. Vi noterar att en incident har rapporterats avseende hanteringen av skyddade personuppgifter och att rutinerna stärktes därefter.
Råder det samsyn inom Nacka kommun och Nacka Energi AB kring hur skyddade personuppgifter ska hanteras?	Nej. Det råder inte samsyn gällande arbetsrutiner och det operativa arbetet med skyddade personuppgifter. Exempelvis har olika enheter i kommunen och bolagen gjort olika bedömningar gällande digital kontra manuell hantering och gällande behörighetsbegränsningar. Detta speglar också avsaknaden av kommunövergripande styrdokument, vilket gör att saknas en gemensam inriktning för hanteringen av skyddade personuppgifter.

Stockholm den 24 maj 2023

David Leinsköld
Verksamhetsrevisor, EY

Daniel Larsson
Verksamhetsrevisor, EY

Bilaga 1 Källförteckning

Intervjuade funktioner

- VD
- HR-chef
- Redovisningsekonom/Lön/HR
- Senior rådgivare Kund & Marknad
- Senior rådgivare Kund & Marknad
- Dataskyddssamordnare

Granskad dokumentation

- Ägardirektiv för Nacka Energi AB
- Bolagsordning Nacka Energi AB
- Informationssäkerhetsstrategi (dnr KFKS 2017/990)
- Riktlinje för allmänna handlingar
- Rutin för utlämnande av allmän handling
- Riktlinje för hanteringen av skyddade personuppgifter
- Rutin för hanteringen av skyddade personuppgifter (kund och marknad)
- Dataskyddsombudets granskningsrapport 2022
- Rutin för hantering av skyddade personuppgifter (medarbetare och ansökande)
- Rutin för personuppgiftsincidenter
- Riskanalys – Skyddade personuppgifter
- Riskbedömning av personuppgiftsincident (bedömningsmall)

Bilaga 2 Revisionskriterier

COSO-ramverket för intern kontroll

Det finns varken för kommuner, kommunala bolag, företag eller andra organisationer en formellt fastställd standard för hur den interna kontrollen ska hanteras. I praktiken har dock en amerikansk standard blivit dominerande: The Committee of Sponsoring Organizations of the Treadway Commission (COSO). Målet med COSO och intern kontroll är att säkerställa att risker undviks och ge en trygghet i att organisationens mål uppfylls. COSO-modellens huvudmål är att garantera en ändamålsenlig och kostnadseffektiv verksamhet, tillförlitlig finansiell rapportering och information om verksamheten samt att lagar följs.

COSO-modellen består av fem huvudkomponenter: kontrollmiljö, riskanalys, kontrollaktiviteter, information och kommunikation samt uppföljning. Dessa perspektiv beaktas i revisionsfrågorna samt rapportens analys och bedömningar.

Om begreppet skyddade personuppgifter

Det har blivit vanligare att människor lever med skyddade personuppgifter. De senaste tio åren har antalet i Sverige dubblerats från drygt 12 000 till knappt 24 000 personer. Enligt Skatteverket utgörs dessa till 59 procent av kvinnor. Vanligast förekommande är sekretessmarkering, som är den minst ingripande formen av skydd, med 82 procent av ärendena medan skyddad folkbokföring, som är ett starkare skydd, utgör 18 procent.

Antalet personer med skyddade personuppgifter motsvarar ca 0,22 procent av befolkningen och matematiskt motsvarar det ca 240 invånare. Siffran är inte exakt men visar att det statistiskt handlar om ett fåtal individer. Konsekvensen vid felaktig röjning av dessa personuppgifter kan emellertid vara mycket allvarlig för var och en.

Jämställdhetsmyndigheten har på regeringsuppdrag genomfört kunskapshöjande insatser gällande våldsutsatta personer som lever med skyddade personuppgifter med fokus på kvinnor och barn. I en delrapport[1] intervjuas 86 kvinnor och 15 barn om deras erfarenheter där närmare tre fjärdedelar av de intervjuade uppger att deras identitet har röjts.

I rapporten konstateras att det i många fall handlar om kvinnor och barn som tvingats flytta på grund av våld och hot från närstående man och att målgruppen är extra utsatt. I princip samtliga kvinnor i Jämställdhetsmyndighetens intervjustudie har fått skyddade personuppgifter röjda av myndigheter.

Det finns omfattande lagstiftning som skyddar individen

Skyddade personuppgifter är ett samlingsbegrepp för olika åtgärder som kan vidtas för att skydda personer som riskerar att utsättas för hot, våld eller förföljelse. Beroende på hotets allvarlighetsgrad finns tre grader av skydd av personuppgifter; sekretessmarkering, skyddad folkbokföring och fingerade personuppgifter. Därutöver finns ytterligare bestämmelser om sekretess som kan aktualiseras för hotade och förföljda personer, bland annat inom offentlighets- och sekretesslagen (2009:400).

Sekretessmarkering är den vanligaste och minst ingripande formen av skydd

[1] *Skyddade personuppgifter – oskyddade personer* (Jämställdhetsmyndigheten 2022:10).

Sekretessmarkering är den minst ingripande formen av skydd av personuppgifter som innebär att Skatteverket gör en sekretessmarkering av enskild persons uppgifter i folkbokföringen (se 5 kap. 5 § offentlighets- och sekretesslagen [2009:400], OSL). Syftet är att förhindra att hotande eller förföljande person med hjälp av personuppgifter kan hitta och utsätta person för brott, förföljelse eller trakasserier.

Sekretessmarkeringen är dock inte ett bindande beslut, endast en indikation på att folkbokföringssekretess enligt 22 kap. 1 § OSL kan gälla för uppgifterna. Den fungerar alltså som en påminnelse eller varningssignal hos alla myndigheter om att det finns behov att göra en noggrann sekretessprövning innan personuppgifter lämnas ut.

I praktiken registrerar Skatteverket en sekretessmarkering som aviseras tillsammans med personuppgifterna till alla myndigheter som får grundläggande personuppgifter från Skatteverkets folkbokföringsverksamhet. Det är den enskilde som ansöker om sekretessmarkering hos Skatteverket. Det finns inga formella krav för att beviljas skyddsåtgärden men den enskilde behöver motivera varför den behöver sekretessmarkering med någon form av handling som stödjer att det föreligger ett aktuellt och konkret hot. Det kan till exempel vara en utredning eller ett utlåtande från Polismyndigheten eller socialtjänsten. Sekretessmarkeringen gäller ofta i två år och kan förlängas.

Skyddad folkbokföring ger starkare skydd än sekretessmarkering

Skyddad folkbokföring ger starkare skydd än sekretessmarkering och innebär att en person kan vara folkbokförd på sin gamla folkbokföringsort efter att ha flyttat. De gamla adressuppgifterna tas bort och den nya adressen registreras inte i folkbokföringen och sprids därmed aldrig till andra myndigheter. Uppgifterna om skyddad folkbokföring skickas till andra myndigheter och annan samhällsservice som personen har kontakt med, till exempel sjukvården, Försäkringskassan och kommunen. Det betyder att dessa instanser kan se att personen har skyddad folkbokföring.

Skyddad folkbokföring medges för person som av särskilda skäl kan antas bli utsatt för brott, förföljelser eller allvarliga trakasserier på annat sätt, om åtgärden med hänsyn till den enskildes förmåga och övriga förutsättningar kan antas tillgodose behovet av skydd. Skyddad folkbokföring kan kombineras med andra skyddsåtgärder som exempelvis kontaktförbud om det bedöms lämpligt utifrån den enskildes specifika situation. Skyddad folkbokföring medges efter ansökan från den enskilde. För barn under 18 år får ansökan enbart göras av den ena vårdnadshavaren i det fall syftet är att skydda från den andra vårdnadshavaren.

Fingerade personuppgifter är den starkaste och mest ingripande formen av skydd

År 2015 fanns i Sverige ungefär 160 personer med fingerade personuppgifter. Fingerade uppgifter betyder att personen använder andra personuppgifter än de verkliga. Detta medför dock inte någon rättslig förändring av personens namn eller andra förhållanden. Kopplingen mellan den verkliga och den fingerade identiteten är sekretessbelagd. Med den nya identiteten kan personen vara öppen med sina personuppgifter utan risk att bli hittad. Fingerade personuppgifter har inget skydd i de systemstöd som används i en region eller kommun eftersom de hanteras som vilken person som helst.

Offentlighets- och sekretesslagen reglerar utlämning av allmänna handlingar

Offentlighets- och sekretesslagen (OSL) innehåller bestämmelser för hur myndigheter[2] ska registrera, lämna ut och hantera allmänna handlingar. Det finns också regler om tystnadsplikt och förbud att lämna ut allmänna handlingar.

Utöver de tre skyddsformerna (sekretessmarkering, skyddad folkbokföring och fingerade personuppgifter) finns en särskild generell sekretessbestämmelse som gäller för vissa personuppgifter om det av särskild anledning kan antas att den enskilde eller någon närstående till denne kan komma att utsättas för hot eller våld eller lida annat allvarligt men om uppgiften röjs (21 kap. 3 § första stycket OSL).

Sekretessen gäller uppgift om en enskilds

- bostadsadress eller annan jämförbar uppgift som kan lämna upplysning om var den enskilde stadigvarande eller tillfälligt bor,
- telefonnummer,
- e-postadress eller annan jämförbar uppgift som kan användas för att komma i kontakt med personen.

Sekretessen gäller även för motsvarande uppgifter om personens anhöriga. Bestämmelsen gäller oavsett sammanhang som uppgiften förekommer i.

[2] I och med att ett kommunalt bolag i regel är ett aktiebolag betraktas det inte vara en myndighet. De kommunala bolagen är dock att jämställa med myndighet om kommunen utövar ett rättsligt bestämmande inflytande över bolaget, vilket Nacka kommun gör över NEAB.