Styrelseärende
Diarienummer NVAAB 2018/32

Styrelsen för Nacka vatten och avfall AB

Informationssäkerhetspolicy och Integritetspolicy

Förslag till beslut

Styrelsen beslutar att:

- anta Nacka vatten och avfall AB:s *Informationssäkerhetspolicy* enligt bilaga 1.
- anta Nacka vatten och avfall AB:s *Integritetspolicy* enligt bilaga 2.

Ärendet

Informationshanteringen och vikten av densamma ökar ständigt i vårt samhälle. En av styrelsen uppgifter är att säkra bolagets hantering av dess kunders och medarbetares personuppgifter och därmed värna om deras integritet. *Informationssäkerhetspolicyn* **och** *Integritetspolicyn* ligger till grund för VD, ledningsgruppens och alla anställdas fortsatta arbete med dataskyddsförordningen och informationssäkerhetsarbetet i sin helhet inom NVOA samt dess samarbetspartners och leverantörer.

Mats Rostö
Verkställande direktör

Linda Herkommer
IT- och digitaliseringsansvarig

Bilagor

1. Informationssäkerhetspolicy
2. Integritetspolicy

Informationssäkerhetspolicy

Syfte

Syftet med denna *informationssäkerhetspolicy* är att tydliggöra Nacka vatten och avfalls prioriteringar och principiella förhållningssätt till informationssäkerhet för att uppnå en hög säkerhet för den information som bolaget hanterar i sin verksamhet (informationstillgångar).

Grundsyn

Information är en av Nacka vatten och avfalls (nedan bolaget) viktigaste tillgångar och hanteringen av den är därför av avgörande betydelse för bolagets arbete. Med informationstillgångar avses all information oavsett om den behandlas manuellt eller med informationsteknologi.

Det är centralt att den som hanterar information kan avgöra när den är skyddsvärd, till exempel på grund av sekretess eller att den omfattar personuppgifter.

Utifrån bolagets *värdegrund* ska informationssäkerhetsarbetet präglas av förtroende för medarbetares och leverantörers förmåga att hantera informationstillgångar på ett professionellt och därmed säkert sätt. Det innebär också förtroende för att verksamheten skapar förutsättningar för ett hållbart och effektivt informationssäkerhetsarbete.

Vår ambition av nytänkande omsätts genom intryck från omvärlden, vilket för informationssäkerhetsarbetet innebär en lyhördhet för kundernas intressen samt hög kvalitet i hantering av information.

Bolaget tar ansvar för sina informationstillgångar genom att säkerställa att den egna verksamheten och leverantörer uppfyller ställda säkerhetskrav.

Styrning, stöd och samordning

- *Bolagsstyrelsen* har det övergripande ansvaret för bolagets informationssäkerhet.
- *VD* har ansvar för att hålla ihop, stödja, samordna och följa upp. Ledningsgruppen ska säkerställa att det finns funktioner som har förmåga att stötta, samordna och följa upp informationssäkerhetsarbetet samt att det finns ett användarnära stöd

- *Varje enhet* har ansvar för att informationstillgångar inom dess ansvarsområden hanteras enligt gällande lagstiftning och informationsstrategin.
- *Leverantörer* ansvarar för att leverans sker i enlighet med lagar och avtal.

Informationssäkerhetsarbetet ska vara uppbyggt så att det är lätt att hantera information korrekt. Det innebär följande:

- Det är säkerställt att det finns en förmåga att upprätthålla säker informationshantering och krishanteringsförmåga och att detta kontinuerligt övas och följs upp.
- Det sker en löpande utvärdering och uppföljning av system och rutiner.

Roller inom informationssäkerhetsarbetet

Alla verksamheter som hanterar informationstillgångar har ett ansvar för att informationssäkerheten upprätthålls.

- *Informationsägarna* har det övergripande och yttersta ansvaret för den information som används av ett eller flera system. Informationsägaren fattar de avgörande besluten om hur, av vem och vilken information som ska registreras samt om informationen behöver revideras eller gallras.
- *Systemägarna* har övergripande ansvar för respektive system och dess användning. Systemägaren ansvarar för att system uppfyller informationssäkerhetskraven i förhållande till verksamheten behov och för att dess innehåll klassificeras. Systemägaren är vanligtvis den person som har det övergripande ansvaret för ett system.
- *Systemförvaltarna* har det funktionella (dagliga) helhetsansvaret för ett system. Systemförvaltaren fungerar som systemägarens utförare och ser till systemets funktionalitet samt att planerade och beslutade aktiviteter genomförs och upprätthålls.

Säker informationshantering

För informationssäkerhetsarbetet i bolaget gäller följande.

- Alla informationstillgångar klassificeras utifrån fyra aspekter. Vid klassificeringen ska konsekvenserna av en oönskad påverkan på informationens kvalitet bedömas.
    - ✓ *Tillgänglighet*: Information ska kunna nyttjas efter behov, i förväntad utsträckning och av rätt person med rätt behörighet.
    - ✓ *Riktighet*: Information ska vara korrekt, tillförlitlig och

fullständig.
- ✓ *Konfidentialitet*: Endast den med rätt behörighet ska kunna ta del av viss information.
- ✓ *Spårbarhet*: Aktiviteter som rör informationen, till exempel bearbetning eller ändringar, ska kunna spåras.

- Systemsäkerhetsanalyser görs för att säkerställa att system uppfyller kraven för rätt nivå av skydd för informationstillgångar.
- Tekniska analyser, så som till exempel penetrationstester, genomförs kontinuerligt.
- Kontinuitetsplanering genomförs för att analysera hotbilden mot informationstillgångar och därmed förebygga händelser som kan leda till negativa konsekvenser för verksamheten och den enskilda individen.
- Riskanalyser genomförs för att identifiera och bedöma risker vars konsekvenser kan leda till störningar i tillgången till information, allvarliga händelser eller extraordinära händelser.
- Alla informationssäkerhetsincidenter anmäls till utpekad funktion och hanteras enligt en definierad incidentprocess.

Nacka den 4 juni 2018
Mats Rostö
VD

Integritetspolicy

Syfte

På Nacka vatten och avfall värnar vi om din personliga integritet och eftersträvar alltid en hög nivå av dataskydd. Denna integritetspolicy förklarar hur vi samlar in och använder din personliga information. Den beskriver också dina rättigheter och hur du kan göra dem gällande. Det är viktigt att du känner dig trygg i vår behandling av dina personuppgifter.

Grundsyn

Vad är en personuppgift och vad är en behandling av personuppgifter?

Personuppgifter är all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Exempelvis kan bilder och ljudupptagningar som behandlas i dator vara personuppgifter även om inga namn nämns. Krypterade uppgifter och olika slags elektroniska identiteter är personuppgifter ifall de kan kopplas till fysiska personer.

Behandling av personuppgifter är allt som sker med personuppgifterna. Varje åtgärd som vidtas med personuppgifter utgör en behandling. Exempel på vanliga behandlingar är insamling, registrering, organisering, strukturering, lagring, bearbetning, överföring och radering.

Ansvarig för personuppgifter

Nacka vatten och avfall (org.nr. 559066-7589), nedan bolaget, är personuppgiftsansvarig för behandlingen av personuppgifter som sker inom ramen för bolagets verksamhet.

Varför behandlar vi dina personuppgifter?

Bolaget behandlar personuppgifter för att ska kunna utföra det vi ska göra enligt lagen samt Nacka kommuns ägardirektiv. Det innebär att bolaget behandlar personuppgifter för olika ändamål kopplade till verksamheten såsom att fullgöra våra åtaganden kopplat till VA och avfall, administrera avtalsrelationer och ge kundservice.

Som arbetsgivare behandlar bolaget personuppgifter om anställda och uppdragstagare i den utsträckning det är nödvändigt för att fullgöra anställnings- eller uppdragsavtalet.

Då du använder appar (kopplade till Nacka kommun och bolagets ärendehanteringssystem) för kommunikation med bolaget för att lösa ditt ärende samlas IP Adress och GPS position in, i enlighet med leverantörernas integritets- eller säkerhetspolicys som du har godkänt.

Vänligen kontakta oss för mer specifik information om på vilken laglig grund och för vilka ändamål som bolaget behandlar dina personuppgifter.

Offentlighetsprincipen och arkivering

Bolaget är ett kommunalägt aktiebolag och det innebär att handlingar såsom brev, sms, e-post, inlägg i sociala medier etc. som skickas till oss blir allmänna handlingar. Vi gör en sekretessprövning innan vi lämnar ut allmänna handlingar.

Allmänna handlingar sparas enligt gällande arkivbestämmelser.

Från vilka källor hämtar vi dina personuppgifter?

Utöver de uppgifter du själv lämnar till oss kan vi också komma att samla in personuppgifter från någon annan, så kallad tredje part. Vänligen kontakta oss för mer specifik information om vilka personuppgifter som vi samlar in från tredje part.

Vilka kan vi komma att dela dina personuppgifter med?

Personuppgiftsbiträden

I de fall det är nödvändigt för att vi ska kunna utföra vårt uppdrag som bolag och därigenom vårt åtagande gentemot dig delar vi dina personuppgifter med företag/organisation som är så kallade personuppgiftsbiträden för oss. Ett personuppgiftsbiträde är ett företag/organisation som behandlar informationen för vår räkning och enligt våra instruktioner.

När dina personuppgifter delas med personuppgiftsbiträden sker det endast för ändamål som är förenliga med de ändamål för vilka vi har samlat in informationen, exempelvis för att kunna tillhandahålla olika tjänster till dig som kund. Vi har skriftliga avtal med alla personuppgiftsbiträden genom vilka de garanterar säkerheten för de personuppgifter som behandlas och åtar sig att följa våra säkerhetskrav samt begränsningar och krav avseende internationell överföring av personuppgifter.

Företag som är självständigt personuppgiftsansvariga.

Vi delar även dina personuppgifter med vissa företag/organisation som är självständigt personuppgiftsansvariga. Att företaget/organisationen är självständigt personuppgiftsansvarig innebär att det inte är vi som styr hur informationen som lämnas ska behandlas.

Hur länge sparar vi dina personuppgifter?

Vi sparar aldrig dina personuppgifter längre än vad som är nödvändigt för respektive ändamål.
Vänligen kontakta oss för mer information om de specifika lagringsperioderna för respektive ändamål.

NACKA
VATTEN
AVFALL

Vad har du för rättigheter som registrerad?

Rätt till tillgång (registerutdrag)

Du kan du begära att få tillgång till information om vilka personuppgifter som vi behandlar om just dig. Informationen lämnas i form av ett registerutdrag med angivande av ändamål, kategorier av personuppgifter, kategorier av mottagare, lagringsperioder, information om varifrån informationen har samlats in och förekomsten av automatiserat beslutsfattande.

Rätt till radering, rätten att bli bortglömd

Beroende på omständigheter i det enskilda fallet och vilken rättslig grund som personuppgiftsbehandlingen görs kan du även ha rätt till radering av sina personuppgifter. Rättigheten har begränsad tillämpning inom bolagets verksamhet eftersom merparten av våra personuppgiftsbehandlingar vilar på en rättslig grund där rättigheten inte är tillämplig.

Rätt till rättelse

Du kan begära att dina personuppgifter rättas ifall uppgifterna är felaktiga. Inom ramen för det angivna ändamålet har du också rätt att komplettera eventuellt ofullständiga personuppgifter.

Rätt till dataportabilitet.

Beroende på omständigheter i det enskilda fallet och på vilken rättslig grund som personuppgiftsbehandlingen grundar sig på har du i vissa fall rätt att få tillgång till personuppgifterna i ett sådant format som möjliggör överförande till en annan personuppgiftsansvarig. Rättigheten har begränsad tillämpning inom bolaget eftersom merparten av våra personuppgiftsbehandlingar vilar på en rättslig grund där rättigheten inte är tillämplig.

Klagomål

Om du vill klaga på bolagets behandling av dina personuppgifter kan du vända dig till Datainspektionen som är tillsynsmyndighet inom området, adressen är Box 8114, 104 20 Stockholm, datainspektionen@datainspektionen.se, telefonnummer 08-6576100.

Ändringar av Integritetspolicyn

Bolaget förbehåller sig rätten att revidera denna Integritetspolicy. Datumet för den senaste ändringen anges i sidhuvudet på Integritetspolicyn. Om det görs ändringar i Integritetspolicyn kommer dessa att publiceras på vår hemsida. Du rekommenderas därför att regelbundet gå in på hemsidan för att uppmärksamma eventuella ändringar i policyn.

Om du har frågor rörande denna Integritetspolicy eller om bolagets behandling av personuppgifter är du välkommen att kontakta bolaget.

För kontakt med Nacka vatten och avfall ABs dataskyddsombud:
Postadress: Dataskyddsombud, Nacka kommun, 131 81 Nacka
E-post: dataskyddsombud@nacka.se

Nacka den 4 juni 2018
Mats Rostö
VD