Styrelseärende
Diarienummer NVAAB 2018/31

Styrelsen för Nacka vatten och avfall AB

Utkast - Rapport av den 21 maj 2018 om införande av EU:s nya dataskyddsförordning på Nacka vatten och avfall AB

Förslag till beslut

Styrelsen har tagit del av informationen.

Ärendet

Nacka vatten och avfall har genomfört ett omfattande utredningsarbete under våren för att säkerställa att hanteringen av personuppgifter behandlas i enlighet med Dataskyddsförordningen. Vidare arbete har identifierats för fortsatta förbättringar i förhållande till bolagets totala informationshantering. Rapporten har baserats på Datainspektionen, SKL och Nacka kommuns förberedande arbeten kring frågan. Ett fåtal aktiviteter kvarstår och dessa presenteras explicit under styrelsemötet.

Den slutliga rapporten kommer att lämnas på styrelsesammanträdet.

Mats Rostö
Verkställande direktör

Linda Herkommer
IT- och digitaliseringsansvarig

Bilaga

1. Utkast - Rapport av den 21 maj 2018 om införande av EU:s nya dataskyddsförordning på Nacka vatten och avfall AB

Rapport om införande av EU:s nya dataskyddsförordning på Nacka vatten och avfall AB

Innehåll

NACKA VATTEN AVFALL

Inledning

Den 25 maj 2018 kommer den nya allmänna dataskyddsförordningen (DSF, även känd som GDPR) börja gälla som lag i Sverige och ersätta den nuvarande personuppgiftslagen (PUL). Mycket av det som finns i den nya förordningen återfinns i personuppgiftslagen, men det finns också en del nya och förändrade bestämmelser som innebär stora förändringar i hanteringen av personuppgifter.

Genom den nya dataskyddsförordningen kommer den personuppgiftsansvariges ansvar och skyldigheter att förtydligas och utökas, samt de registrerades rättigheter kommer att förstärkas. Dataskyddsförordningen lägger stor vikt vid den personuppgiftsansvariges skyldighet att kunna visa att förordningen följs, vilket medför krav på ökad dokumentation och säkerhet. Som en anpassning till dataskyddsförordningen har Nacka vatten och avfall (kommer fortsättningsvis benämnas som "NVOA") sett över sin interna styrning och tagit fram riktlinjer för hur personuppgifter hanteras.

För att anpassa verksamheten är det viktigt att arbeta med de korta- och långsiktiga konsekvenser förordningen kommer få för NVOA. Rapporten innehåller en utredning av förordningens krav och innebörd, inventering av hur verksamheten ser ut just nu och vilka personuppgifter som hanteras. I arbetet har alla anställda informerats och involverats, även om merparten av jobbet gjorts av ledningspersonal och staben. All personal har blivit informerade om DSF, vilket arbete som gjorts och vad som är viktigt att tänka på. Uppdraget har till viss del omfattat planering och prioritering av framtida arbete, projekt och anpassning av verksamheten för den nya DSF. Handlingsplanen innehåller åtgärder och förslag till de åtgärder som NVOA behöver göra för att säkerställa att den nya lagen följs när den träder i kraft 25 maj 2018, samt att den därefter fortsatt efterlevs.

Arbetet har samordnats av en arbetsgrupp bestående av personer från ledningen inklusive den nytillträdde digitaliseringsansvarige och bolagsjuristen. Arbetet har att letts av NVOA:s digitaliseringsansvarige med stöd av NVOA:s dataskyddsombud samt konsulter från Grandezza Konsult AB.

Grandezza har lämnat förslag på fortsatt arbete för att ytterligare riskminimera och de är i korthet; processkartläggning, fortsatt klassning av personuppgiftshanteringen, informationshanteringsplan och rutiner (inklusive avtalsgranskning), ISO-certifiering.

Den rödmarkerade texten i rapporten är aktiviteter som vi planerar att slutföra före den 25 maj eller före styrelsemötet.

NACKA VATTEN AVFALL

Disposition

Rapporten är uppbyggd efter Integritetsskyddsmyndigheten (före detta Datainspektionens) *Vägledning till personuppgiftsansvariga*[1] som bygger på 13 frågor. Av vilka NVOA endast ska besvara 12, eftersom bolaget inte har verksamhet i andra länder. Frågorna skapar en uppfattning om vilket arbete som behöver göras inom NVOA, innan förordningen träder i kraft samt hur den påverkar NVOA:s löpande arbete. Det handlar bland annat om vilka personuppgifter NVOA hanterar, hur vi ger information till de registrerade och hur våra rutiner för hanteringen av personuppgifterna ser ut.

Nedan bild visar vilka aktiviteter som har genomförts under projektet. De flesta är avslutade nu under arbetet med den nya DSF, innan den träder i kraft, men vissa fortgår också i det fortsatta löpande arbetet efter att förordningen har börjat gälla för att effektivisera arbetsprocesser och minimera riskerna med personuppgiftshanteringen.

Bild; Aktiviteter som ingått i arbetet och ingår i handlingsplanen.

[1] Integritetsskyddsmyndigheten (f.d. Datainspektionen), Vägledning till personuppgiftsansvariga

http://www.datainspektionen.se/lagar-och-regler/eus-dataskyddsreform/forberedelser-for-personuppgiftsansvariga/

NACKA VATTEN AVFALL

1. Information om EU:s nya dataskyddsförordning

Genom seminarier, möten, information och utbildning har beslutsfattare och nyckelpersoner inom organisationen blivit väl medvetna om att personuppgiftslagen kommer ersättas av dataskyddsförordningen. NVOA är även medvetna om hur organisationen har och kommer påverkas samt inom vilka områden det behöver vidtas åtgärder.

Informationsinsatser såsom arbetsplatsträffar, frukostmöten (samtliga medarbetare) och informationsutskick (till samtliga) har genomförts i enlighet med NVOA:s organisationsstruktur.

2. Vilka personuppgifter hanteras

För att skapa en bred översyn över vilka personuppgifter som hanteras inom NVOA har en inventering gjorts och en samlad registerförteckning över samtliga personuppgifter tagits fram. Förteckningen baseras först och främst på en systemförteckning och inte en processförteckning, då företaget inte sedan tidigare har fastslagna processer. Ett kärnsystem (EDP Future) har analyserats mer ingående för ökad förståelse kring fortsatt digitalisering. Leverantörens arbete uppfyller kraven och vissa nyligen införda funktioner stödjer verksamheten väl i att följa DSF.

Nya policys och rutiner har tagits fram för hur personuppgifter ska hanteras och för hur de samlas in samt till vem de lämnas ut. I detta ingår även hanteringen av förändringar av personuppgifter i befintliga system samt när beslut om nya system och hanteringar fattas. Policy har beslutats av VD och styrelse.

Samtliga enhetschefer har gått igenom registerförteckningen för att uppdatera och korrigera information om samtliga av bolagets behandlingar av personuppgifter. Registerförteckningen uppdateras löpande och granskas via en modul i Ledningsinformationssystemet (LIS), för tillfället Stratsys. Det åligger informationsägaren att löpande uppdatera förteckningen när det sker förändring av behandlingar av personuppgifter och stöd kan ges av digitaliseringsansvarig vid inventering av systemen. VD ansvarar för att årligen rapportera en sammanställd lista till styrelsen.

Syftet med att ha en central registerförteckning är att bland annat uppfylla kravet på att rättningar av felaktiga uppgifter ska kunna genomföras inom skälig tid. Detta är svårt och tidskrävande att genomföra om det inte finns en strukturerad förteckning på vilka uppgifter som hanteras, varifrån de kommer och till vem de lämnas ut.

3. Används missbruksregeln idag

I den nuvarande lagstiftningen är missbruksregeln ett undantag så länge behandlingen inte utgör kränkning, men regeln kommer att upphöra när den nya dataskyddsförordningen träder i kraft. Missbruksregeln innefattar ostrukturerat material såsom personuppgifter i löpande text, i e-post och dokument samt på NVOA:s hemsida, intranät eller i annan löpande text.

NACKA VATTEN AVFALL

NVOA har använt missbruksregeln tidigare och efter att samtliga enheterna gått igenom sina system så är behandlingarna nu förenliga med förordningen. Viss information, t.ex. bilder och namn på hemsidan har gallrats bort. Kommunikationsenhetens rutiner har uppdaterats för att bibehålla kontroll framöver. NVOA har även kontaktat Föreningen Sambruk (organisation som arbetar med e-tjänster som skapar förutsättningar för kommunal verksamhetsutveckling) för att se om den AI lösning som tagits fram med stöd av bl.a. Nacka Kommun kan användas för en granskning. Vidare har ett filter (Forcepoint) för förhandsgranskning av personuppgifter i mail testats med gott resultat och kommer införas så snart Digitaliseringsenheten på Nacka kommun godkänt lösningen.

4. Vilken information lämnas till registrerade

När personuppgifter samlas in måste NVOA enligt personuppgiftslagen lämna viss information, bland annat ändamålen med behandlingen. Dataskyddsförordningen innehåller utökade krav på vilken information som ska lämnas till de registrerade. Mallar har tagits fram och NVOA informerar nu om ändamål, den rättsliga grunden för behandling, hur länge personuppgifterna lagras och möjligheten att lämna klagomål till tillsynsmyndigheten (som idag i Sverige är Integritetsskyddsmyndigheten (ISM) tidigare Datainspektionen). Informationen är kortfattad, lättbegriplig och utformad på med ett tydligt och enkelt språk.

Samtyckes- och modellavtalsmall har tagits fram och har implementerats i våra rutiner.

NVOA har skickat ut information till hela kundregistret via faktura. Den externa webben har uppdaterats med en text om DSF. Det har också publicerats en övergripande integritetspolicy beslutad av VD för att kunder och medarbetare ska kunna läsa mer kring hur NVOA hanterar deras personuppgifter.

5. De registrerades rättigheter

NVOA har sett över rutinerna för att säkerställa att alla rättigheter som de registrerade har enligt Dataskyddsförordningen uppfylls.

De viktigaste rättigheterna för de registrerade är att:

- få tillgång till sina personuppgifter
- få felaktiga personnummer rättade
- få sina personuppgifter raderade
- invända mot att personuppgifterna används för direktmarknadsföring
- invända mot att personuppgifterna används för automatiserat beslutsfattande och profilering
- flytta personuppgifterna (dataportabilitet)

En av de viktigast delarna i förordningen som även är ny, är rätten att flytta personuppgifter. Det innebär att uppgifter ska kunna tas ut i ett allmänt och maskinläsbart format.

NACKA VATTEN AVFALL

En inventering av de system som innehåller personuppgifter har genomförts för att säkerställa att rättigheterna ovan kan uppfyllas. Rutiner har tagits fram för hur NVOA ska hantera den registrerades rättigheter samt En e-tjänst/blankett utvecklas i skrivande stund, målet är att den ska vara publicerad till den 25/5, för att den registrerade enklare ska kunna begära ut sina personuppgifter från NVOA genom ett registerutdrag.

6. Med vilket rättsligt stöd behandlas personuppgifter

I den inventering som NVOA gjort har även det rättsliga stödet för de personuppgifterna NVOA behandlar säkerställts och dokumenterats. Rättsligt stöd finns för alla idag identifierade personuppgiftsbehandlingar. Det finns även en sammanfattning kring vilka typer av uppgifter som behandlas, vart de behandlas, hur länge de behandlas samt med vilket rättsligt stöd.

Förordningen har ett krav att redan vid insamlingen av uppgifterna informera om den rättsliga grunden. Det är därför viktigt att redan från början ha klart för sig med vilket stöd detta sker för nya verksamhetssystem.

7. Hur inhämtas samtycke

NVOA har inventerat på vilket sätt samtycke inhämtats, vilken information som lämnats och hur uppgifter om att samtycke har lämnats av den registrerade har lagrats. Rutiner har uppdaterats för hantering av samtycke.

Ett giltigt samtycke är frivilligt, specifikt och otvetydig viljeyttring genom vilken den registrerade, efter att ha fått information, godtar behandlingen av personuppgifter som rör denne. Dataskyddsförordningen ställer tydliga krav på att den som behandlar personuppgifter med stöd av samtycke måste kunna visa att ett samtycke har lämnats.

Information eller samtycke rörande NVOA:s blanketter och e-tjänster har setts över under våren 2018 av enheterna. Fortsatt kvalitetsgranskning kommer att ske under hösten för att kontrollera och säkerställa informationshanteringen i NVOA:s processer och system.

8. Behandlas personuppgifter om barn

Dataskyddsförordningen innebär ett förstärkt skydd för barns personuppgifter, särskilt när det gäller kommersiella internettjänster som sociala nätverk. NVOA tog ett beslut om att radera nuvarande personuppgifter rörande barn och ersätta med en annan bild på den externa webben.

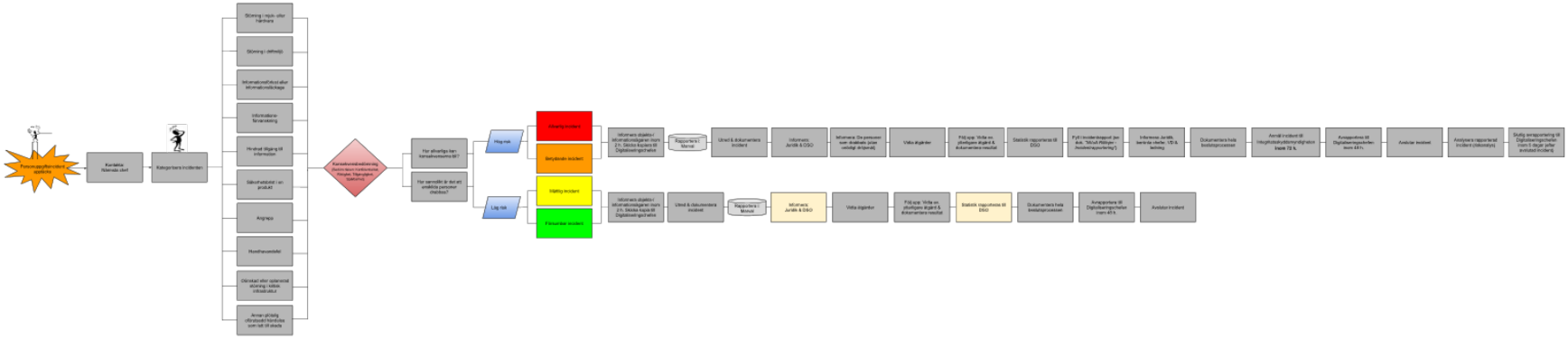
För att säkerställa de nya rutinerna för hantering av personuppgifter så genomförde NVOA en pilot vid invigningen av Älta Kretsloppscentral (KLC). NVOA dokumenterar sina aktiviteter genom fotografering och filmning i syfte att använda materialet till deras hemsida och marknadsföring. Deltagare av invigningen bestod av medarbetare, besökare, leverantörer, kunder och ett flertal skolklasser, vilket innebar att samtycke krävdes för att få hantera och lagra dessa bilder och film. Därav inhämtades skriftligt samtycke från samtliga personer som deltog samt samtycke från barnens båda vårdnadshavare. Rutinen kommer uppgraderas med en e-tjänst under hösten 2018.

NACKA VATTEN AVFALL

9. Personuppgiftsincidenter

NVOA har uppdaterat rutiner för att upptäcka, rapportera och utreda personuppgiftsincidenter i enlighet med dataskyddsförordningen.

Alla personuppgiftsincidenter måste dokumenteras och om händelsen medför risker för enskildas fri- och rättigheter måste den anmälas till integritetsskyddsmyndigheten (ISM) inom 72 timmar. I rutinen framgår också när och hur NVOA informera de registrerade.



NACKA VATTEN AVFALL

10. Särskilda integritetsrisker vid behandling

Den nya förordningen ställer särskilda krav på behandlingen av personuppgifter som kan medföra stora integritetsrisker för enskilda. Riskfyllda behandlingar kan till exempel vara storskaliga register som innehåller känsliga personuppgifter, profilering eller omfattande kameraövervakning på allmän plats.

Samtliga enhetschefer har gjort en inventering för att undersöka om NVOA hanterar riskfyllda behandlingar. I ett fåtal fall (t.ex. behovstömning för Kunder och internt för företagshälsa) finns det sådan information om än i liten omfattning och konsekvensanalyser har gjorts avseende dataskydd via DSF-modul i LIS:et. Först övervägdes att utvärderade via KLASSA (ett SKL-verktyg för informationsklassificering), men då LIS:et har likvärdig funktionalitet eller bättre, valde NVOA detta system för att kunna kontrollera hur behandlingarna hanteras och för att identifiera eventuella åtgärder.

11. Skydd för personuppgifter i IT-systemen

I nya IT-system som införskaffas och vid förändringar i befintliga system ska DSF regler förhållas till och anpassas mot. Vilket innebär att dataskydd ska byggas in i systemen genom lämpliga åtgärder, både organisatoriska och tekniska. Grundläggande principer inom integritetsskydd är att inte samla in mer information än vad som behövs, inte ha kvar information längre än nödvändigt och inte använda uppgifterna till något annat än vad som var syftet när de samlades in.

Digitaliseringsansvarig och berörda medarbetare har informerats om att dessa krav ska finnas med i upphandling av både utveckling och inköp av nya IT-system och vid förändringar i befintliga system. Riktlinjerna innehåller även ett avsnitt angående integritetsskydd.

Kontakt har tagits med nuvarande leverantörer för att se till att de bygger in dataskydd i nuvarande system. NVOA har även säkerställt att det finns biträdesavtal med Nacka kommun och alla leverantörer, personuppgiftsbiträden, som hanterar personuppgifter.

Det identifierades ett par tydliga brister i systemet EDP Future, då t.ex. medarbetare på NVOA fritt kan söka på namn och få upp information om flera Kunder inklusive personnummer. En uppdatering infördes i april dock fanns det befintliga problemet kvar. NVOA utreder och ställer krav på leverantören om att konfigurera systemet så att det inte är möjligt för medarbetarna att se flera personnummer vid en sökning på namn. Ytterligare en uppdatering i systemet kommer införas i maj och då ska problemet vara korrigerat och verifierat. NVOA arbetar aktivt med deras kundprocesser och system. Bland annat genom leverantörers kundgrupper samt branschorganisationer (bl.a. Svenskt Vatten), för att komma tillrätta med möjliga tillkortakommanden och hitta en branschstandard. Vidare ser NVOA till att systemet uppdateras kontinuerligt till senaste version i enlighet med gällande Informationssäkerhetspolicy.

12. Ansvar för dataskyddsfrågor i NVOA

Ansvariga för dataskyddsfrågor inom NVOA är VD med stöd av digitaliseringsansvarig och de agerar bland annat på inrådan av dataskyddsombudet. Det är enhetschefer och informationsägarens ansvar att tillsammans med digitaliseringsansvarig kontinuerligt definiera ändamålen och medlen för behandling av personuppgifter.

NACKA VATTEN AVFALL

Personuppgiftsbiträden, leverantörer, har även ett ansvar för dataskyddsfrågor då de behandlar personuppgifter för den personuppgiftsansvariges räkning. Vilket den personuppgiftsansvariga även behöver följa upp. Detta bör ske med 1–3 leverantörer under hösten 2018 och därefter årligen med minst en leverantör. Leverantören VA-banken bör vara först ut i en sådan granskning.

Den nya förordningen ställer krav på att offentliga myndigheter och enheter utser ett dataskyddsombud. Privata företag och organisationer som, i stor omfattning, som del av dess kärnverksamhet regelbundet och systematiskt övervakar individer (all form av profilering på internet) eller behandlar känsliga personuppgifter (som hälsodata eller biometriska data) behöver också utse dataskyddsombud. NVOA har beslutat att ha ett inhyrt dataskyddsombud. NVOA har utsett samma dataskyddsombud (DSO) som Nacka Kommun och DSO är inhyrd till 5 procent tillsvidare. Beslutet bör ses över andra halvåret 2019. Det är viktigt att Dataskyddsombudet har tillräcklig kunskap om dataskydd och får det stöd och befogenheter som krävs för att kunna utföra sitt uppdrag på ett effektivt och oberoende sätt.

Dataskyddsombudens uppdrag är att informera, ge råd, inventera, dokumentera, följa efterlevnaden av förordningen, ge råd vid konsekvensbedömningar avseende dataskydd och övervaka genomförandet av informationssäkerhetsaspekter, samarbeta med tillsynsmyndigheten (Integritetsskyddsmyndigheten), fungera som en kontaktpunkt och ta hänsyn till de risker som förknippas vid behandling.

NACKA VATTEN AVFALL

Bilaga 1

Enhetsrapporter

Varje enhet har arbetat med sina ansvarsområden och system, med stöd från digitaliseringsansvarig, kommunikationsansvarig samt konsultbolaget Grandezza. Projektet har haft en styrgrupp som rapporterats till veckovis. Projektet planerades så att det initialt leddes av Grandezza och när sedan digitaliseringschefen kom in i organisationen så tog NVOA över projektledarrollen.

Som ingångsvärde angavs att ca 15–20 system fanns i organisationen. Nedan följer en sammanfattning av aktiviteterna som varit specifika för respektive enhet. En skattning per enhet för tidsåtgång i projektet gjordes inledningsvis till 1–4 h/per system, totalt ca. 80 system. Registerförteckningen uppgick efter kartläggning till strax över 100 system och ytterligare tre personuppgiftsbehandlingar identifierades i samband med framtagandet och den pågående utveckling av gallrings- och arkiveringspolicyn. Antalet behandlingar kommer sannolikt att utökas till hösten då en processgenomgång bör göras av hela verksamheten. Totalt behövdes ca. 11 PUB avtal upprättas med existerande leverantörer, underleverantörer samt ett med Nacka kommun. Initialt kommer bolaget använda sig utav samma avtal som Nacka Kommun fram tills att bolaget tagit fram egna avtal med samtliga leverantörer. I vissa fall har bolaget efter granskning valt att acceptera leverantörens PUB-avtal.

I. Ledning & Staben

Arbetet med registerförteckningen har uppskattats till 20 h för ledningens olika system. Ett antal policys, riktlinjer och mallar har dessutom tagits fram (t.ex. informationssäkerhetspolicy, integritetspolicy, gallrings- och arkiveringsriktlinjer och incidenthantering). Utgångspunkten baserades på Nacka Kommuns (NK) tillgängliga mallar och granskades sedan av Grandezza som gett förslag på ändringar. Om det saknats mallar från NK har SKL:s mallar använts och jämförelser har även gjorts från andra referensobjekt framtagna av Grandezza. Dessutom har beslutats hur och vem som tar beslut om vilka dokument relaterat till DSF.

Efter möte med Stratsys (NVOAs leverantör av verksamhetsstyrningssystem) och samråd med NK beslutades att Stratsys DSF-modul skall användas för löskoppling mellan LIS och det kontinuerligt kvalitetssäkrade DSF-arbetet. Det ger en säkrare och bättre koppling till verksamheten över tiden än en fristående registerförteckning.

Grundavtal för samarbete med NK finns i samarbetsavtalet, dock har förslag skickats till NK på PUB-avtal samt annex för de tjänster som köps in direkt från Nacka kommun. Beslut togs att inte arbeta fram ny prisstruktur för respektive tjänst utan i det fall detta fattades hänskjuta detta till hösten.

Det tillsatta Dataskyddsombudet (DSO) är inhyrt från Nacka Kommun på 5 procent ca. 90h. DSO har granskat denna rapport och registerförteckningen i LIS:et under maj månad.

II. Ekonomi

Arbetet med registerförteckningen uppskattades till 16 h. Ekonomienhetens kärnsystem UBW saknar i viss mån tillräckliga autentiseringsmekanismer för att fullt ut uppfylla DSF. En mer utvecklad rollbaserad åtkomstkontroll behöver införas, för att inte alla medarbetare ska kunna ta del av

samtliga personuppgifter. Detta anses bero delvis på att det saknas unika anställningsnummer i NK. Enhetschefen arbetar med leverantören för att få till fler roller i systemet. Risken idag är att en kunnig användare kan komma åt mer information än nödvändigt, dock inte i budgetarbetet men i utfallet.

Ekonomienheten har ett flertal personuppgiftshanteringar tillsammans med personalenheten, dessa kopplingar bör granskas mer ingående under hösten 2018. För att se vad som kan systematiseras i verksamhetssystemen.

Majoriteten av avtalen på NVOA finns idag lagrade på flera olika ställen (Platina, UBW, EDP, Q, N). Detta ledde till att det var svårt eller nästintill omöjligt att finna vissa avtal. Detta bör ses över omgående för att minimera datalagring av personuppgifter samt för att få bättre kontroll på informationsflödet och dokumenthanteringen.

III. HR

Arbetet med registerförteckningen uppskattades till 24 h. En första intervju gjordes med HR-ansvarig. Hanteringen av personuppgifter mellan ekonomi och HR identifierades initialt som de enheterna som historiskt varit mest problematiskt, när det gäller delning av information i form av personuppgifter som skickas över e-post (ostrukturerade data). Detta fungerar nu tillfredställande, men en fortsatt översyn av kopplingarna mellan HR- och ekonomifunktionens aktiviteter bör genomföras till våren 2019.

Olika enheter använder idag olika system vid tillbud. Systemen används dock inte så ofta så situationen är hanterbar men en konsolidering baserat på systemet Abou bör ske när nya HR-ansvarige anser att det är lämpligt, dock senast till oktober.

En genomgång av gallrings- och arkiveringsplan med den nya HR-ansvarige gjordes och gav resultatet att ytterligare tre mindre system/hanteringar adderades till registerförteckningen.

IV. Kommunikation

Arbetet med registerförteckningen uppskattades till 40 h. En ordentlig inventering och korrigering av externa webben behövde genomföras för att kartlägga hantering av personuppgifter på webben (namn, fotografier och filmer) och därefter ta bort eller byta ut visst innehåll. En tidsuppskattning kring webben var att en sida som enbart innehöll DSF-godkända personuppgifter tog ca. 30–45 sekunder samt en sida med tveksamheter kring personuppgifter tog ca. 0,5–2 h att korrigera. Utöver det tillkommer 8 h för KLC (Kretsloppscentral) eventet som blir NVoA första pilot-event under DSF lika förhållanden. En mall för samtycke och modellavtal har tagit fram och den ska implementeras snarast även som online version. Till dess att online version finns skannas samtycken och originalet kastas.

Den interna webben (medarbetarwebben) kommer att få samma behandling och vara klar till utgången av oktober. Nacka Kommun är föredömligt när det kommer till öppna data kring sina verksamheter, men det ger också en effekt på personuppgiftshanteringen. En sökning på ”Mats Rostö” (bara Rostö inom parentes) ger förslag på 713 (7) sidor, 125 (2) internt och 11 958 (54) i protokoll. Åtgärd för detta, är att protokoll bör referera roll samt treställig initial istället för namn i klartext.

Vidare har lättförståelig information för webben skapats och en textmall för samtycke har tagits fram för informationsägarnas användning.

En kommunikationsplan för projektets kommunikation internt och externt togs fram. Tidigt togs ett beslut, på inrådan av kommunikationsansvarig, att inte inhämta samtycken kring gamla personuppgifter på webben utan att istället satsa på en ny etablering av personuppgifter som inhämtats på ett DSF korrekt sätt.

En första kommunikation med medarbetarna kring DSF-arbetet gjordes vid ett frukostmöte på NVOA, detta följdes sedan upp med information via mail och interna webben.

V. Digitalisering och IT

Arbetet för systeminventeringen uppskattades till 42 h, där vissa system kom att läggas över på andra enheter och en hel del system är redan detaljgranskade av Nacka Kommun, därför var det svårt att göra en rimlig skattning kring dessa.

NVOA:s har konstaterat att det finns behov att se över ärendehanteringsprocessen. Inom bolaget hanteras inga känsliga personuppgifter, bortsett från de få personuppgifter inom ärendehanteringssystem, EDP-Future, där det finns uppgift om enstaka kunders funktionsnedsättning. NVOA har därför gjort en granskning av det ärendehanteringssystemet.

Vid granskningen har det framkommit att leverantören har uppdaterat ärendehanteringssystemet utifrån DFS under april 2018 och ytterligare en ska genomföras i maj 2018. I det fall samkörning eller profilering görs sker detta endast av utbildade experter med specifika behörigheter.

En gallring av existerande (3–4) enklare enkätverktyg bör snarast (senast till sommaren 2019) konsolideras på en plattform (sannolikt Abou). Informationen kring Cookies kommer att ses över i samverkan med Nacka Kommun.

NVOA har valt att använda en modul i Stratsys för registerförteckning av bolagets personuppgiftsbehandlingar. Genom användning av det aktuella systemet ges bolaget förutsättningar att på strukturerat sätt arbeta med informationssäkerhetsklassning av system samt utföra risk- och sårbarhetsanalyser. Modulen är installerad och informationen från registerförteckningen etc. En vidare granskning av EDP-Future och VA-banken har gjorts i verktyget. Där vissa allvarliga svagheter dokumenterats och bör följas upp omgående med leverantören. En säkerhetsklassning av alla systemen ska ske i DSF modulen, de har prioriterats i 3 grupper i registerförteckningen med olika deadlines (innan utgång september 2018, innan 2019 samt innan sommaren 2019).

NVOA har vid kartläggningen konstaterat att det förekommer ostrukturerad behandling av personuppgifter på gemensamma lagringsytor. NVOA kommer att gå igenom handlingarna som är lagrade på denna yta och vid behov överföra till ärendehanteringssystem. Det finns tekniska lösningar som kan söka och identifiera förekomsten av personuppgifter i ostrukturerade data, vilket skulle underlätta bolagets arbete strukturerat gallra och arkivera information innehållande personuppgifter.

Nacka Kommun har delfinansierat ett projekt genom Sambruk för att utveckla en sådan teknisk lösning. Den *digitaliseringsansvarige* på bolaget samarbetar med Nacka kommun för att utröna om det är en möjlig väg för bolaget att nyttja denna tjänst. Grandezza anser att behovet ser ut att överväga nuvarande tillkortakommanden av produkten.

Därutöver planerar den *digitaliseringsansvarige* att införa ett verktyg som uppmärksammar och hjälper medarbetaren att hantera personuppgifter på korrekt sätt.

Även den nya tjänsten säkra meddelanden har testats och kommer fortsätta utvärderas för att se om den är lämplig för hantering av meddelanden som innehåller känsliga uppgifter eller stora mängder personuppgifter.

En rutin har införts för rapportering till Integritetsskyddsmyndigheten. Under hösten bör behovet av en rutin för incidentrapportering till MSB och cert.se ses över.

VI. Avfall och Kund

Arbetet uppskattades till 32 h för existerande system samt 8 h för e-tjänster och blanketter samt 8 h extra för KLC-event genomgången. I arbetet identifierade vi potentiellt känsliga uppgifter kring (funktionsvariation) dock i en liten omfattning som hanterades på ett tillräckligt korrekt sätt, dvs. sjukintyget sparas inte, bara en notis om att det finns. NVOA har prioriterat revision av leverantören EDP Future, samt Artvise under resten av året.

En kort information om DSF och hur NVOA hanterar personuppgifter kommer att skickas till alla Kunder på deras faktura med hänvisning till mer information på webben. Informationen bör innehålla information om att delge epost och mobiltelefonnummer (för SMS-UMS). Det viktigaste som NVOA bör informera sina Kunder om sammanfattas i nedan punkter:

- NVOA tydliggör ansvaret för att skydda sina Kunders rättigheter och integritet.
- NVOA förtydligar vilka personuppgifter som behandlas för ökad transparens enligt dataskyddslagstiftningen (GDPR).
- NVOA förklarar hur de hanterar personuppgifter som Kunderna delar med dem, för att de ska kunna erbjuda sina Kunder vatten- & avfallstjänster och ge bästa möjliga upplevelse av dem.

Samt hänvisar kunder att läsa vidare kring NVOA:s integritetspolicy på hemsidan.

Ett evenemang lett av Avfallsgruppen är invigningen av den nya KLC:n i Älta. Detta har använts som en pilot för att testa samtyckesmallen, processer m.m. Invigning av Älta KLC inkluderade elever vilket gav ett bra tillfälle att både testa den nya samtyckesprocessen såväl som att fylla på webben med ny och korrekt inhämtad information.

En medborgarundersökning utförs årligen tillsammans med en extern leverantör (Rangola) en granskning av hur detta arbete sker bör göras vid nästa tillfälle och PUB-avtal ska tecknas med leverantören. Arbete sker i samarbete med ledningen.

VII. Vattenenheten

Arbetet med registerförteckningen uppskattades till 34 h. I arbetet identifierades även här en avsaknad av vissa gallringsrutiner när det kom till bl.a. avtalshantering. Inskannade överlåtelseavtalet bör t.ex. pseudonymiseras, anonymiseras eller arkiveras så att det blir en mindre grupp människor som har direkt åtkomst till informationen.

En del behandlingar av personuppgifter, som idag ligger under NVOA på webben, görs egentligen av miljöenheten t.ex. fettavskiljare dispensansökan görs idag av NVOA men ska göras av miljöenheten. Åtgärd: Enhetschefen för VA tar kontakt med miljöenheten för att korrigera detta.

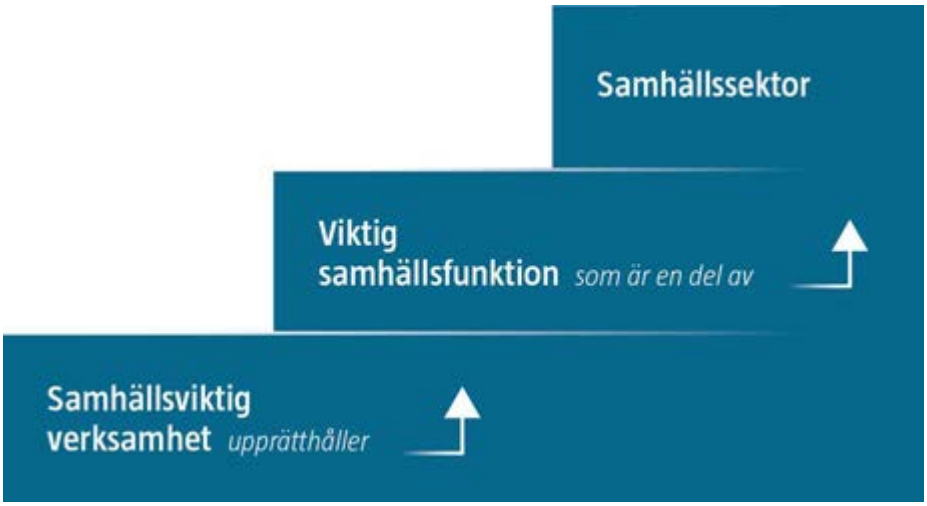
En tjänst fungerade inte på webben (reducerad avgift). Åtgärd: Enhetschefen följer upp och korrigerar.

Bolagets systemförvaltare har identifierat brister i VA-banken med modulerna VASS och Regista och dess integrationer med InternGIS och för en dialog med leverantörerna. Ingen relevant information om korrigering/återkoppling inkom innan den 25:e maj. En dokumentation av VA-banken har gjorts i Stratsys för en strukturerad uppföljning. Leverantören hävdar att de ”I arbetet med GDPR tar vi självklart hänsyn till Privacy by design, ansvarsskyldighet, dataportabilitet, arkiveringstider, anonymisering, kryptering m.m.” och att de arbetar aktivt med branschorganisationen och att ett PUB-avtal skickas ut under våren 2018. Nästa steg bör bli att anmäla leverantören till Integritetsskyddsmyndigheten (före detta Datainspektionen) senast utgången oktober 2018 om inte uppdateringar kommit NVOA tillhanda.

VIII. Drift och Underhåll

Arbetet uppskattades till 24 h. De lite svårare personuppgiftsbehandlingarna som sker av leverantörer som levererar till stora delar av den svenska marknaden för t.ex. övervakningssystem av fysiska platser och vad NVOA och Grandezza kan avgöra sker det i enlighet med DSF. Utöver dessa identifierades ett system som införts med syfte att öka den fysiska säkerheten för samtliga medarbetare. Verktyget är nu formellt en del av NVOA:s digitaliseringsresa.

En kvarvarande fråga som dök upp är om eller hur NVOA arbetar med MSB (se modell nedan), Cert.se https://www.cert.se/it-incidentrapportering/rapportera-har/ och är de eller ska de bli en aktiv del av civilförsvaret?



Exempel: Vattenverk X upprätthåller den viktiga samhällsfunktionen dricksvattenförsörjning som är en del av samhällssektorn kommunalteknisk försörjning.

Kommunikationsplan

En kommunikationsplan togs fram tidigt i projektet och fokuserade på riktad kommunikation till såväl kunder som medarbetare. NVOA arbetade med frukostträffar internt.

NACKA VATTEN AVFALL

Utbildning

Utbildning (anpassat för respektive enhet för att både inhämta och sprida information om DFS och personuppgiftsbehandlingar) om DSF har genomförts vid arbetsplatsträffar (APT) på respektive enhet. Grandezza föreslog 2-3h utbildning men detta bestämdes bli mellan 30 minuter (drift och underhåll) och 2h (staben). Det är viktigt att alla medarbetare i organisation förstår bakgrund och principer för DSF:s regelverk och börjar arbeta utifrån dessa. Därför föreslås att NVOA bör genomföra ett flertal workshops (i mindre grupper) under år 2018–2019, så att samtliga medarbetare blir involverade och kan bidra med att förbättra och säkerställa informationsströmmar och rutiner/processer i det dagliga arbetet samt minimera risker.

Hantering av Risk & Möjlighet i projektet

Risk/möjlighet	Innebörd	Åtgärd
Tidsaspekten	Alla måste vara medvetna om tidspressen	Mer personal, mer arbete på plats
Praktisk hantering av legala frågor	Avvägningar	Aktivt rådfråga DI samt delta i samarbetsrum på SKL. Bolagsjurist SS på plats i början på april
Svårt att nå alla berörda intressenter	Identifiera nya intressenter t.ex. Nacka Energi, PACTA	Kommunikation via etablerade kanaler. Inbjudningar till öppna informationsmöten ansågs inte behövas
Oro hos personalen	För mycket eller för lite information	Information 10 april, endast ett fåtal frågor. Balanserad mängd information. Internt nyhetsbrev. Nytt verktyg som kollar mail
Resursbehov	Långsiktigt och kortsiktigt	Mer tid för systemförvaltarna framöver att digitalisera istället för att digitisera.
Samtyckesinhämtning	Nytt samtycke Ja eller Nej per system	Detaljdriva frågan. Minimera antalet samtycken, tydlig informationen på webben

Identifierade processer (Kretslopp - Återanvända)

Ett antal processer har identifierats i arbetet med registerförteckningen samt informationshanteringsplan. Nedan finns ett par översiktligt beskrivna processer. Fortsatt arbete bör ske för att förenkla och automatisera NVOA verksamhet generellt och i relation till DSF.

NACKA
VATTEN
AVFALL

1. Kundprocessen; Kring t.ex. EDP-Future, VA-Banken, UBW och ärendehanteringssystemen, berör:
    a. Kundgruppen
    b. Projektering; Nybyggnation och tillbyggnad
    c. Drift och Underhåll
2. Budgetprocessen;
    a. Inköp & Upphandling
    b. Logistik & Lager
    c. Leverantör & Entreprenad
    d. Medarbetare & HR
3. HR / Rekryteringsprocessen; minimera Q och papper, maximera ”Personec”.

NACKA
VATTEN
AVFALL

Bilaga 2

Förslag till handlingsplan

I arbetet har framkommit behov av att en del projekt med kopplingar till DSF bör prioriteras eller omprioriteras. Rekommenderade och prioriterade i ordning enligt nedan;

1. Kundprocessen workshop; Uppskattas till 8x3h per enhet, ca 90h totalt intern tid
2. Informationshanteringsplan och rutiner; Ägare Kommunikation & Digitalisering
    a. avtalsgranskning
3. KLASSA alla (relevanta) system i enlighet policys i DSF modulen innan sommaren 2019
4. Processkartläggning av hela företaget; Rutiner, processer och informationsflöden
5. Fördelning reguljära arbetsuppgifter och projekt via ledningsgruppen; Ägare HR, Ledningsgruppen och facken deltar
6. ISO certifiering; Ledningen
7. Rapport rutin till MSB cert.se
8. Säkerhetsklassning av anläggningar; Pågår inom VA, koppling till ISO certifiering och MSB?