2.3.2023

Kunnallisen nuorisotyön dokumentointijärjestelmän (NuoDo/UngDo) kuvaus

Sisällysluettelo

1 Yleiskuvaus ja kohteen määritys

1.1 Yleiskuvaus kohteesta

Järjestelmä on valtakunnallinen, kunnallisen nuorisotyön dokumentointijärjestelmä.

Kuntaliiton nuoDo on järjestelmä, johon kunnat dokumentoivat kunnissa tehtävää nuorisotyötä ja -toimintaa. NuoDo löytyy osoitteesta www.nuodo.fi. NuoDo-järjestelmään kerätyn tiedon pohjalta voidaan tuottaa ja raportoida tietoa kunnallisen nuorisotyön järjestämisestä, resursseista, toimintaympäristöistä, työn tekemisen tavoista sekä nuorisotyön palveluista paikallisesti ja kansallisesti. Järjestelmän avulla tuotetaan myös tietoa ryhmätasolla palveluihin osallistuvista nuorista. Kuntien on mahdollista vertailla järjestelmässä omaa toimintaansa muiden kuntien tuottamaan tietoon. Yhteensä toimintoja kirjataan järjestelmään arviolta noin 250 000 kpl vuodessa.

NuoDo-järjestelmässä olevia toimintaa ja järjestämistä koskevia tietoja tullaan julkaisemaan avoimesti. Tarkoituksena on mahdollistaa ko. tietojen mahdollisimman laaja hyödynnettävyys kunnissa, alueilla ja valtakunnallisesti. Järjestelmä ei kerää eikä siinä käytetä arkaluonteista henkilötason salassa pidettävää tietoa. Järjestelmään ei tallenneta tietoja, joiden avulla yksittäinen nuori tai nuorten ryhmittymä voidaan tunnistaa suoraan tai välillisesti (tarkemmin järjestelmän sopimuksessa ”Sopijapuolten vastuut ja velvoitteet”).

NuoDo-järjestelmää kunnan puolesta käyttävistä henkilöistä (kuten pääkäyttäjät, tietoa kirjaavat ammattihenkilöt) kerätään nimi ja sähköpostitieto palvelun hallintaan liittyviin tarkoituksiin. (Tarkempi kuvaus järjestelmän sopimuksessa).

Järjestelmän toimimisella ei ole kriittisiä vaikutuksia kuntien toimintaan. Kyseessä on kunnallisen nuorisotyön tilastointi- ja dokumentointijärjestelmä, joka sisältää toimintaan ja tekemiseen liittyvää (pääsääntöisesti määrällistä) tietoa.

1.2 Käyttäjät

Järjestelmän käyttäjinä on niin kuntien nuorisotyöntekijöitä, suunnittelijoita kuin nuorisotyön esimiehiä.

Kuntaliiton työntekijä ylläpitää järjestelmää ja auttaa kuntia mahdollisissa ongelmatapauksissa.

1.3 Kielet

Järjestelmä on kaksikielinen. Käyttäjä voi kirjautumisen jälkeen vaihtaa kielensä ruotsiksi halutessaan. Kielivalinta löytyy työpöytäkokoisessa näkymässä yläpalkista ja mobiilissa "lintuikonin" alta avautuvasta pudotusvalikosta.

1.4 Raportit

Järjestelmän tarkoituksena on tuottaa helposti ymmärrettävää dataa nuorisotyön käyttöön ja raportointiin. Raportit ovat työkalu tähän tarpeeseen.
Raporttinäkymiä on kolme erilaista.

- Minun kuntani
- Nuorisotyö lukuina

- Tietokysely.

Minun kuntani ja nuorisotyö lukuina ovat näkymiä joihin käyttäjä saa määrittämillään tiedoilla valmiiksi muotoillut tiedot. Tietokyselyssä käyttäjä saa valita mitä tietoja haluaa järjestelmästä ottaa ulos, ja järjestelmä generoi käyttäjälle halutuilla tiedoilla olevan CSV-tiedoston (Comma-separated values).

2 Tekninen ympäristö

2.1 Järjestelmäarkkitehtuuri

Järjestelmä on jaettu kahteen osaan. Käyttöliittymä (frontend) on toteutettu JavaScriptilla ja React-frameworkilla. Taustajärjestelmä (backend) on toteutettu Java Spring -frameworkilla ja koodit ajetaan Mavenilla.

Käyttöliittymän ja taustajärjestelmän välinen kommunikaatio tapahtuu REST-rajapinnan yli ja autentikaatio tapahtuu käyttäjätunnuksella ja salasanalla sekä JWT-tokenilla (JSON Web Token).

Taustajärjestelmän tietovarastona toimii PostgreSQL-kanta. Kantayhteyteen käytetään JOOQ-kirjastoa.

Järjestelmässä on lisäksi bastion host, jota voidaan käyttää esim. tietokantaoperaatioihin. Bastion host on Linux-virtuaalikone.

2.2 Palvelin ja tekninen ympäristö

Ympäristö on Vincitin ylläpitämä AWS-ympäristö ja ympäristöön authorisointi tapahtuu Vincitin sisäisten prosessien mukaisesti.

- Kaikki on AWS Cloudissa (IaaS sekä SaaS (AWS RDS)).
- Palvelimen sijaintipaikka on Tukholmassa (eu-north-1)

2.3 Integraatiot

Järjestelmässä ei ole ulkoisia integraatioita.

2.4 Ulkoiset kannat ja palvelut

Järjestelmä lähettää sähköpostia ja sähköpostipalvelimena toimii FCG:n ylläpitämä ja Kuntaliiton omistama sähköpostipalvelin. Muita ulkoisia palveluita järjestelmässä ei ole.

3 Turvallisuusmekanismit ja -kontrollit

3.1 Verkkoturvallisuus ja segmentointi

Käyttöliittymä on Amazon Web Services:n sisällönjakeluverkossa (CloudFront CDN).

Verkot on segmentoitu julkiseen, yksityiseen ja tietokantasegmentteihin ja lisäksi ne jaettu Amazon Web Services:n saatavuusalueille (availability zone) toisin sanoen erillisiin konesaleihin. Julkisissa verkoissa sijaitsee taustajärjestelmän kuormantasaaja.

Yksityisissä verkoissa, mihin ei ole pääsyä Internetistä, mutta mistä on pääsy NAT gateway -palvelun kautta Internetiin, sijaitsee taustajärjestelmäsovellus. Tietokantasegmentissä, mihin ei ole pääsyä Internetistä eikä sieltä ole pääsyä Internetiin, sijaitsee tietokanta.

Pääsy tietokantaan on rajattu palomuurisäännöin ainoastaan taustajärjestelmän sovelluksesta.

Pääsy taustajärjestelmään on rajattu palomuurisäännöin ainoastaan kuormantasaajalta.

Yksityisessä verkossa on bastion host, mihin on pääsy Amazon Web Services Systems Manager Agentin avulla, jolloin julkista osoitetta ei tarvita.

3.2 Pääsynhallinta ja yhteydet

3.2.1 Autentikointiperiaatteet

Käyttäjät autentikoidaan käyttäjätunnus / salasana yhdistelmällä. Käyttäjätunnus on käyttäjän sähköpostiosoite.

3.2.2 Tunnuksien hallinnointi

Tunnuksia hallinnoi Kuntaliiton pääkäyttäjä Pauliina Lahtinen

3.2.3 Yhteydet järjestelmään

Sovelluksen käyttöliittymä on osoitteessa https://nuodo.fi, mihin ollaan yhteydessä Internet-selaimella.

3.2.4 Sähköposti

Järjestelmä lähettää sähköposteja käyttäjille seuraavissa käyttötapauksissa:

- "uusi käyttäjän salasana"
- "unohditko salasanasi?"
- käyttäjän luonti.

"Uusi käyttäjän salasana" lähettää käyttäjälle ”unohditko salasanasi” -sähköpostin, jotta hän voi asettaa itselleen uuden salasanan.
"Unohditko salasanasi" lähettää ”unohditko salasanasi” -sähköpostin käyttäjälle, jotta hän voi asettaa itselleen uuden salasanan.
Käyttäjän luonti lähettää seuraavat viestit:

- tiedoksiantoviestin uudelle käyttäjälle
- tiedoksiantoviestin uuden käyttäjän luoneelle käyttäjälle

”unohditko salasanasi” -sähköpostin uudelle käyttäjälle, jotta hän voi asettaa itselleen salasanan.

3.3 Käyttövaltuudet ja käyttäjät

Järjestelmään on määritelty seuraavat roolit:

- Järjestelmän pääkäyttäjä (Kuntaliitto/ järjestelmän tekninen ylläpitäjä)
- Kunnan pääkäyttäjä
- Kuntapäällikkö

- Organisaation pääkäyttäjä
- Kunnan työntekijä
- Organisaation työntekijä
- Vieras

Käyttöoikeudet on määritelty näiden tasojen perusteella. Jokaisen taustajärjestelmäkutsun yhteydessä vaadittavat käyttöoikeudet tarkistetaan. Käyttöliittymäpuolella on myös määritelty nämä samaiset oikeudet. Niillä määritellään mitä näkymiä, toimintoja tai komponentteja kullekin käyttäjälle näytetään.

Rooleille määritellyt oikeudet löytyvät dokumentin liitteestä.

Kunta määrittelee itse pääkäyttäjät järjestelmän käyttöönoton yhteydessä. Kuntaliitto pitää pääkäyttäjiä ajan tasalla järjestelmään liittyvistä mahdollisista muutoksista/ päivityksistä. Kuntien käyttäjät pääsevät vaikuttamaan järjestelmän kehittämiseen. Kunnat dokumentoivat tekemäänsä nuorisotyötä järjestelmän avulla, ja täten vastaavat.

Järjestelmän pääkäyttäjät kunnissa vastaavat oman kuntansa muusta käyttäjähallinnasta. Teknisissä ongelmatilanteissa yhteydenotto ensisijaisesti projektipäällikköön/järjestelmänvalvojaan (Kuntaliitto).

3.4 Hierarkiatasot ja toiminnot

- #### Kunnat
  Järjestelmän korkein hierarkiataso. Kunnan alta löytyy organisaatiot, kunnan käyttäjät, kohteet, toiminnat jne.

- #### Organisaatiot
  Kunnan pääkäyttäjät voivat luoda kuntaan organisaatiopuun. Organisaatiopuu on korkeintaan kolmen syvyinen.

- #### Kohteet
  Kunnan alle voidaan lisätä kohteita, joissa toimintaa yleensä tehdään. Nämä kohteet voivat olla mm. kouluja, nuorisotiloja, leirikeskuksia jne.

- #### Toiminnat (Event/Function)
  Toiminnat ovat järjestelmän keskeisin osa. Nuorisotyötä tekevät työntekijät lisäävät järjestelmään toimintaa toteutuneen mukaan. Toiminnan voi lisätä myös etukäteen, jolloin toiminnan osallistujamääriä ei tarvitse täyttää. Jos järjestelmään on jäänyt toiminta, joka on jo mennyt mutta siihen ei ole lisätty osallistujatietoja, järjestelmä muistuttaa käyttäjää asiasta etusivun muistutukset-osiossa.

Sisältötunnisteet
Toimintaa kategorioidaan sisältötunnisteiden avulla. Aikaisemmin valtakunnallisesti on ollut ongelmaa saada kokonaiskuvaa kuntien nuorisotyöstä, koska kuntien seurannat eivät ole olleet keskenään verrannollisia. Siksi sisältötunnisteet ovat tässä järjestelmässä määritelty valtakunnallisella tasolla. Kunnat voivat lisätä omia sisältötunnisteitaan järjestelmään, jolloin näihin (kunnallisiin) sisältötunnisteisiin pitää merkitä, minkä valtakunnallisen sisältötunnisteen "alle" nämä kuuluvat. Tällä tavoin järjestelmästä on mahdollista saada valtakunnallisesti vertailukelpoista dataa.

Ilmoitukset

Ylläpitäjät voivat luoda käyttäjille ilmoituksia, jotka näkyvät järjestelmän etusivulla määrätyn ajan. Ilmoitukset voivat olla valtakunnallisia tai kohdennettu yksittäiselle kunnalle. Ilmoitus voi olla tyypiltään ohje, info tai muistutus.

Muistutukset

Järjestelmä luo käyttäjille muistutuksia määräajoin erinäisistä tapahtumista. Muistutukset luodaan käyttäjän kirjautuessa ja ne näkyvät järjestelmän etusivulla. Muistutukset voivat olla esimerkiksi muistutuksia vaihtaa salasana tai päivittää jokin tieto.

3.5 Käyttäjän luonti järjestelmään ja ensimmäinen kirjautuminen

Käyttäjän luonti järjestelmään on prosessi, jossa osapuolina ovat (kunnan)pääkäyttäjä sekä uusi käyttäjä. Prosessissa järjestelmä lähettää sähköpostivahvistukset molemmille käyttäjille sekä uudelle käyttäjälle sähköpostin, jonka linkistä hän voi käydä vaihtamassa itselleen haluamansa salasanan.

3.6 Kryptografia ja salaus

Liikkeessä oleva tieto käyttäjän ja käyttöliittymän välillä kuljetetaan https-protokolla käyttäen ja salataan käyttäen minimissään TLSv1.2 -algoritmilla.

Liikkeessä oleva tieto sovelluksen käyttöliittymän ja taustajärjestelmän välillä kuljetetaan https-protokolla käyttäen ja salataan käyttäen minimissään TLSv1.2 -algoritmia. Järjestelmä käyttää TLS 1.3. Joten kaikki yhteydet ovat salattuja.

Liikkeessä oleva tieto taustajärjestelmän ja tietokannan välillä on salaamaton.

Tietokannan levossa oleva tieto on salattu käyttäen AES-256 salausalgoritmia.

3.7 Lokit

Järjestelmälokiin kirjautuu kaikki järjestelmässä tehtävät muutokset/ lisäykset/ poistot/ arkistoinnit. Tämä koskee kaikkia käyttäjiä, ei ainoastaan admin-käyttäjiä.

Järjestelmälokin kautta ylläpitäjät voivat palauttaa arkistoituja instansseja seuraavista kokonaisuuksista:

- Organisaatio
- Kohde
- Toiminta
- Sisältötunniste.

Tietokannan ja taustajärjestelmän sovellustason lokit talletetaan Amazon Web Services CloudWatch logs -palveluun.

Tiedot, jotka lokitetaan ovat:

- koska sisäänkirjautuminen tapahtui
- millä sähköpostilla yritettiin kirjautua sisään

Koska jokaisella käyttäjällä on oltava uniikki sähköposti, on helppoa päätellä, kuka yritti kirjautua sisään. Ainoat henkilötiedot järjestelmässä ovat käyttäjien etu- sekä sukunimet

ja sähköposti. Nämä lokitetaan niissä tapauksissa, kun niitä käsitellään, esimerkiksi sisäänkirjautumisessa ja käyttäjän lisäämisessä ja salasanan resetoinnissa.

Tietokantalokeja pystyy muuttamaan vain kirjautumalla sisään suoraan tietokantaan. Tähän pystyy ainoastaan sysadminit ja jatkokehittäjät, jotka töidensä puolesta tarvitsevat pääsyn tietokantaan. Lokeja, jotka tallennetaan AWS:ään ei pysty muuttamaan mitenkään, ainoastaan poistamaan sysadminien ja jatkokehittäjien toimesta. Täten voi sanoa, että lokien muuttaminen sekä poistaminen on estetty.

4 Ohjelmiston käyttöönotto ja elinkaaren hallinta

4.1 Varmuuskopiointi ja toipumismenettelyt

Tietokanta varmuuskopioidaan päivittäin aikaikkunassa 04:00-07:00 UTC. Tietokannan varmuuskopioita säilytetään 35 vuorokautta. Kaikki data on tietokannassa. Koko järjestelmä pyörii AWS:ssä. Käytössä on AWS RDS (relational database service) jolla on automaattisesti hoidetut päivitykset sekä varmuuskopioinnit. Testauksia voidaan tehdä asiakkaan pyynnöstä.

4.2 Järjestelmän valvonta

Järjestelmän julkista yhteyspistettä https://nuodo.fi valvotaan automaattisesti. Virheen tapahtuessa tukipalvelu selvittää ongelmaa (arkisin klo 8-16).

4.3 Päivitysten hallinta

Sovellukset (käyttöliittymä ja taustajärjestelmä) päivitetään tarvittaessa (bugikorjaukset ja tietoturvapäivitykset) käyttäen GitLabin jatkuvan julkaisun työkalulla käyttäen Terraform ja Ansible DevOps-työkaluja.

Amazon Web Services Tietokanta päivittyy automaattisesti huoltoikkunassa maanantaisin 00:00-03:00 UTC. Infrastruktuurin komponentit, kuten kuormantasaajat, päivittää Amazon Web Services.

5. Tietoturva ja päivitykset

Tietokanta ei tue suostumusten ja kieltojen hallintaa, koska sitä ei olla pidetty tarpeellisena. Ainoat henkilötiedot, jotka järjestelmä sisältää on lisättyjen käyttäjien etu- ja sukunimet sekä sähköpostiosoite. Tästä johtuen ei ole tarve kysyä henkilötietojen käytöstä. Täten salaamista ja pseudonymisointia ei olla harkittu. Kuntien käyttäjätiedot (järjestelmän käyttäjien nimet) eivät näy toisiin kuntiin.

Kaikilla järjestelmän käyttäjillä on yksilöllinen käyttäjätunnus/salasana paitsi teknisen ylläpidon järjestelmänvalvoja-käyttäjä.

- Salasanan minimipituus on 8 merkkiä, ja sen täytyy sisältää ainakin yksi numero, pieni kirjain sekä iso kirjain.

- Järjestelmässä ei ole kaksivaiheista tunnistautumista
- Järjestelmässä ei käsitellä arkaluonteisia henkilötietoja

- Käytössä olevien teknologien tietoturvatiedotteiden seuraaminen. Jos havaitaan puutteitta teknologioiden tietoturvassa, niihin reagoidaan välittömästi.
- Toimitaan GDPR:n ja muiden tietoturvaohjeistusten mukaisesti.

Järjestelmää päivitetään tarvittaessa käyttämällä CI/CD pipelinea. Automaattisia päivityksiä ei ole käytössä. Päivityksistä ei tule downtimea, joten niistä tiedottaminen ei ole tarpeellista. Jos tulee päivityksiä, jotka vaativat käyttökatkon niistä tiedotetaan etukäteen kuntien pääkäyttäjille. AWS pitää huolen siitä, että jos järjestelmä kaatuu, se uudelleenkäynnistetään automaattisesti. Tarkempaa toipumissuunnitelmaa ei ole tarkemmin dokumentoitu koska sellaista ei ole vaadittu.

6. Ylläpito

Sisällön ylläpidosta vastaa kunta. Kuntaliitto vastaa järjestelmän teknisen ylläpidon mahdollistamisesta, ja palvelun ostamisesta ulkopuoliselta toimittajalta.

6.1. Toimittaja

Järjestelmän omistaja ja toimittaja on Suomen Kuntaliitto ry
PL 200, 00101 Helsinki / Kuntatalo, Toinen linja 14, 00530 Helsinki

Kuntaliiton yhteyshenkilö:
Pauliina Lahtinen, projektipäällikkö
+358 9 771 2290, +358 50 401 9159
Pauliina.Lahtinen@kuntaliitto.fi
www.kuntaliitto.fi
https://www.kuntaliitto.fi/kunnallisen-nuorisotyon-dokumentaatio-hanke

Järjestelmän kehittämistä toteutetaan yhteistyössä järjestelmää käyttävien kuntien kanssa. Järjestelmän omistajana Kuntaliitto vastaa päätöksistä yhteistyössä järjestelmän teknisen toteuttajan/ ylläpidon kanssa.

Asiakaspalvelu ja käyttäjätuki (arkisin 8-16): pauliina.lahtinen@kuntaliitto.fi