

# **Tjänstebeskrivning: Kuntarekry-tjänsten**

FCG Finnish Consulting Group Oy

Anne-Mari Mourukoski

## Innehållsförteckning

<b>1 ALLMÄN BESKRIVNING AV TJÄNSTEN .....</b>	<b>3</b>
<b>2 TJÄNSTENS INNEHÅLL.....</b>	<b>3</b>
<b>3 SUPPORT .....</b>	<b>4</b>
<b>4 LEVERANTÖRENS UNDERLEVERANTÖRER .....</b>	<b>5</b>
<b>5 PLATS FÖR PRODUKTION AV PROGRAMTJÄNSTER.....</b>	<b>5</b>
<b>7 SERVICEPERIODER OCH UPPDATERINGAR .....</b>	<b>5</b>
<b>9 BEHANDLING AV PERSONUPPGIFTER .....</b>	<b>7</b>
<b>10 TEKNIK OCH DATASÄKERHET.....</b>	<b>8</b>
<b>11 ÄNDRINGAR AV TJÄNSTEN ELLER TJÄNSTEBESKRIVNINGEN.....</b>	<b>17</b>

Anne-Mari Mourukoski

## 1 ALLMÄN BESKRIVNING AV TJÄNSTEN

Kuntarekry är en webbläsarbaserad Programtjänst avsedd att användas av arbetsgivare inom kommunsektorn, kommunägda företag och arbetsgivare inom välfärdsområden för att rekrytera medarbetare, publicera platsannonser och hantera vikarier. Kuntarekry förbättrar rekryteringsprocessen och förbättrar platsannonsernas exponering.

Kuntarekry underlättar rekryterarnas arbete och erbjuder redskap för utveckling av arbetsgivarimagen. Med Kuntarekry kan du även hantera kommunikation med sökande och se rekryteringsstatistik.

## 2 TJÄNSTENS INNEHÅLL

Tjänsten Kuntarekry består av följande tre funktionella enheter:

### Komponent: Rekryteringssystem

Beskrivning: Kuntarekry hanterar hela rekryteringsprocessen från att ansöka om rekryteringstillstånd till att lämna ett urvalsförslag. Systemet innehåller även funktioner för hantering av korttidsvikarier.

Centrala funktioner, riktade rekryteringar:

- Rekryteringstillstånd
- Rekryteringens grunduppgifter
- Publicering av platsannonser, externa och interna sökningar
- Handläggning och jämförelse av ansökningar
- Sammanfattningar av sökande
- Kommunikation med sökande
  - E-post
  - SMS
- Videointervjuer
- Anonym rekrytering
- Statistiska rapporter

Centrala funktioner, hantering av vikarier och vikariat

- Publicering av vikarieannonser
- Handläggning av ansökningar
- Hantering av vikariepoolen
- Kommunikation
- Sökning av vikarier
  - SMS-sökning
  - Jobbkalender
- Statistiska rapporter

### Komponent: Webbplatsen Kuntarekry.fi

www.kuntarekry.fi är en rikstäckande webbplats för rekrytering.

Centrala funktioner:

- Publiceringskanal för platsannonser

Anne-Mari Mourukoski

- Underhåll av webbplatsen för arbetsgivarpresentation
- Bildning av platsannonsflöden
- Positiv utveckling av imagen hos arbetsgivare

Tillgänglighetsutlåtande:

<https://www.kuntarekry.fi/se/tillg%C3%A4nglighetsrapport/>

### **Komponent: Gränssnitt**

Kunden kan på egen bekostnad utföra konvertering (överföring) av data till rekryteringssystemet eller till webbplatsen kuntarekry.fi från sitt eget rekryteringssystem eller annat system, och/eller införa dataöverföringsgränssnitt mellan sina egna datasystem och rekryteringssystemet. Kunden ansvarar för alla kostnader för konvertering eller anslutning, samt för underhåll och för eventuella ändringar.

Kunden ansvarar själv för den påverkan som datakonverteringar och/eller dataöverföringsgränssnitt som Kunden beställt och infört kan ha på driften och användbarheten av rekryteringssystemet eller webbplatsen.

Det finns ett gränssnitt mellan Kuntarekry och Intro, som lägger in nya rekryterade medarbetare via Kuntarekry som användare av Intro, så att en introduktionsplan kan påbörjas. Intro-gränssnittet kan aktiveras genom att skicka en begäran till vår supporttjänst.

### **3 SUPPORT**

Den av Kunden utsedda administratören har rätt att kommunicera med den av Tjänsteleverantören utsedda administratören om fel eller problem uppkommer vid användningen av tjänsterna, på vardagar kl. 9.00–15.00. Supporten till Kunden är inte avsedd att ersätta utbildning i användningen av Tjänsten.

Kontaktuppgifterna för Tjänsteleverantörens supporttjänst:

telefon: 044 4314 999

e-post: [tuki@kuntarekry.fi](mailto:tuki@kuntarekry.fi)

Tjänsteleverantören svarar på felmeddelanden och andra tjänsteförfrågningar som lämnas via det elektroniska systemet, utan onödigt dröjsmål efter mottagandet av meddelandet. Rådgivningen omfattar inte kundspecifik utbildning. Kunden kan beställa systemutbildning och driftsättningskonsultation från Tjänsteleverantören.

### **Stöd till arbetssökande**

De arbetssökande erbjuds användarstöd om inloggning, inloggningsuppgifter och den egna profilen, samt vid tekniska problem. Frågor om det arbete som ansökan gäller överförs till arbetsgivaren.

### **Instruktionsmaterial**

Tjänsteleverantören underhåller instruktionerna för användningen av Tjänsten.

Anne-Mari Mourukoski

#### 4 LEVERANTÖRENS UNDERLEVERANTÖRER

Tjänsteleverantören använder underleverantörer och externa tjänsteföretag vid genomförandet av Tjänsten. Tjänsteleverantören ansvarar för sina underleverantörers och externa tjänsteföretags verksamhet på samma sätt som för sin egen verksamhet.

#### 5 PLATS FÖR PRODUKTION AV PROGRAMTJÄNSTER

Rekryteringssystemets maskinhall och data finns i Finland. [Kuntarekry.fi](https://www.kuntarekry.fi) -webbplatsens maskinhall och data finns i Finland.

Programtjänsten produceras i Finland. De tekniker och tekniska miljöer som används vid produktionen av Tjänsten beskrivs i avsnittet Teknik och datasäkerhet samt Behandling av personuppgifter.

FCG får också överföra personuppgifter till organisationer som är verksamma utanför EU eller Europeiska ekonomiska samarbetsområdet, alltså till så kallade tredjepartsländer. Sådana dataöverföringar får utföras om något av följande villkor är uppfyllt:

- EU-kommissionen har beslutat att detta land har en tillräcklig nivå på dataskyddet.
- Andra nödvändiga skyddsåtgärder har införts, till exempel genom tillämpning av de standardavtalsklausuler som antagits av EU-kommissionen, eller genom att företaget som behandlar data har lämpliga bindande företagsregler.

#### 6 SÄKERHETSKOPIERING

Tjänsteleverantören ansvarar för säkerhetskopiering av Kundens data och material i Tjänsten minst en gång per arbetsdag. Tjänsteleverantören ansvarar inte för förstörelse av eller skador på Kundens data, om detta har inträffat som en följd av Kundens egna åtgärder. Kundens egna åtgärder anses till exempel vara verksamhet som utförs med Kundens användarnamn och lösenord.

Tjänsteleverantören har rätt att debitera kostnader och utgifter för att återställa data som förstörts eller skadats till följd av Kundens åtgärder.

#### 7 SERVICEPERIODER OCH UPPDATERINGAR

Leverantören ska ha rätt att avbryta leveransen av Programtjänsten under en rimlig tidsperiod från måndag till fredag mellan kl. 17.00 och 8.00 samt på lördag, söndag eller på allmän helgdag, om detta är nödvändigt beroende på installation, ändring eller underhåll av Programtjänsten och om installationen, ändringen eller underhållet inte kan utföras till rimlig kostnad utan att avbryta leveransen av Programtjänsten. Leverantören ska

- (a) i god tid informera Beställaren om eventuella avbrott i Programtjänsten och om hur länge avbrottet varar;
- (b) sträva efter att minimera de olägenheter som avbrottet medför.

Leverantören har rätt att avbryta leveransen av Programtjänsten beroende på installation, ändring eller underhåll av det allmänna kommunikationsnätet eller beroende på allvarliga datasäkerhetsshot mot Programtjänsten, om det krävs enligt lag eller myndighetsorder, eller beroende på force majeure.

Anne-Mari Mourukoski

Om Leverantören avbryter leveransen av Programtjänsten av skäl som anges i detta avsnitt, ska Leverantören i god tid innan avbrottet informera Beställaren om det kommande avbrottet och om hur länge det beräknas ta. Om detta inte rimligen är möjligt, ska Beställaren informeras omedelbart efter att Leverantören har upptäckt behovet av ett avbrott.

Leverantören har rätt att utan samråd hindra Beställaren att komma åt Programtjänsten, om Leverantören har rimliga skäl att misstänka, att Beställaren belastar eller använder Programtjänsten på ett sätt som försämrar andra användares möjligheter att använda Programtjänsten. Leverantören ska utan onödigt dröjsmål underrätta Beställaren om orsaken till att åtkomst nekats.

Anne-Mari Mourukoski

## 8 METODER FÖR ÖVERVAKNING AV BEHÖRIGHETER TILL OCH ANVÄNDNING AV TJÄNSTEN

Varje användare har ett personligt användarnamn och lösenord till rekryteringssystemet Kuntarekry. Det är inte tillåtet att använda generella inloggningsuppgifter. Kundens administratör ansvarar för användarnas inloggningsuppgifter och behörigheter. Användarnas lösenord är krypterade i rekryteringssystemet Kuntarekry och minimikraven för lösenord anges (längd, specialtecken, stora/små bokstäver).

Rekryteringssystemet Kuntarekry har olika behörighetsnivåer, som ger tillgång till olika funktioner. Användarnas behörigheter definieras vanligtvis av administratören. Utöver behörighetsnivåerna har rekryteringssystemet rekryterings-specifika behörigheter.

Leverantören övervakar kontinuerligt användningen av Kundens rekryteringssystem, för att utveckla både systemet och sin egen verksamhet.

Det går att logga in på webbplatsen Kuntarekry.fi enligt följande:

- FCG-underhåll, med inloggningsuppgifter på Admin-nivå
- FCG-kommunikation, med inloggningsuppgifter på Editor-nivå
- Kundorganisationernas representanter, med inloggningsuppgifter på Client-nivå
- Personen som besöker webbplatsen loggar inte in, utan använder webbplatsen på Guest-nivå

Admin: redigerar systeminställningar, moduler, användare, innehåll

Editor: hanterar systeminnehåll och användare

Client: redigerar den valda organisationens sida

Guest: kan läsa tillåtna sidor

Information om uppföljning av användningen av webbplatsen Kuntarekry.fi:

<https://www.kuntarekry.fi/fi/tietoa-sivustosta/>

## 9 BEHANDLING AV PERSONUPPGIFTER

Sekretess och dataskydd är viktigt för oss. FCG Finnish Consulting Group Oy har åtagit sig att skydda integriteten hos användarna av deras Tjänster och att följa gällande dataskyddslagstiftning, inklusive EU:s allmänna dataskyddsförordning (GDPR). FCG:s medarbetare och andra personer som deltar i behandlingen av personuppgifter åtar sig att följa sekretessplikten och att behandla den information som mottagits i samband med behandlingen av personuppgifter som konfidentiell.

Personuppgifterna behandlas enligt separat avtal mellan leverantör och kund.

Information om webbplatsen kuntarekry.fi <https://www.kuntarekry.fi/se/om-webbplatsen/>

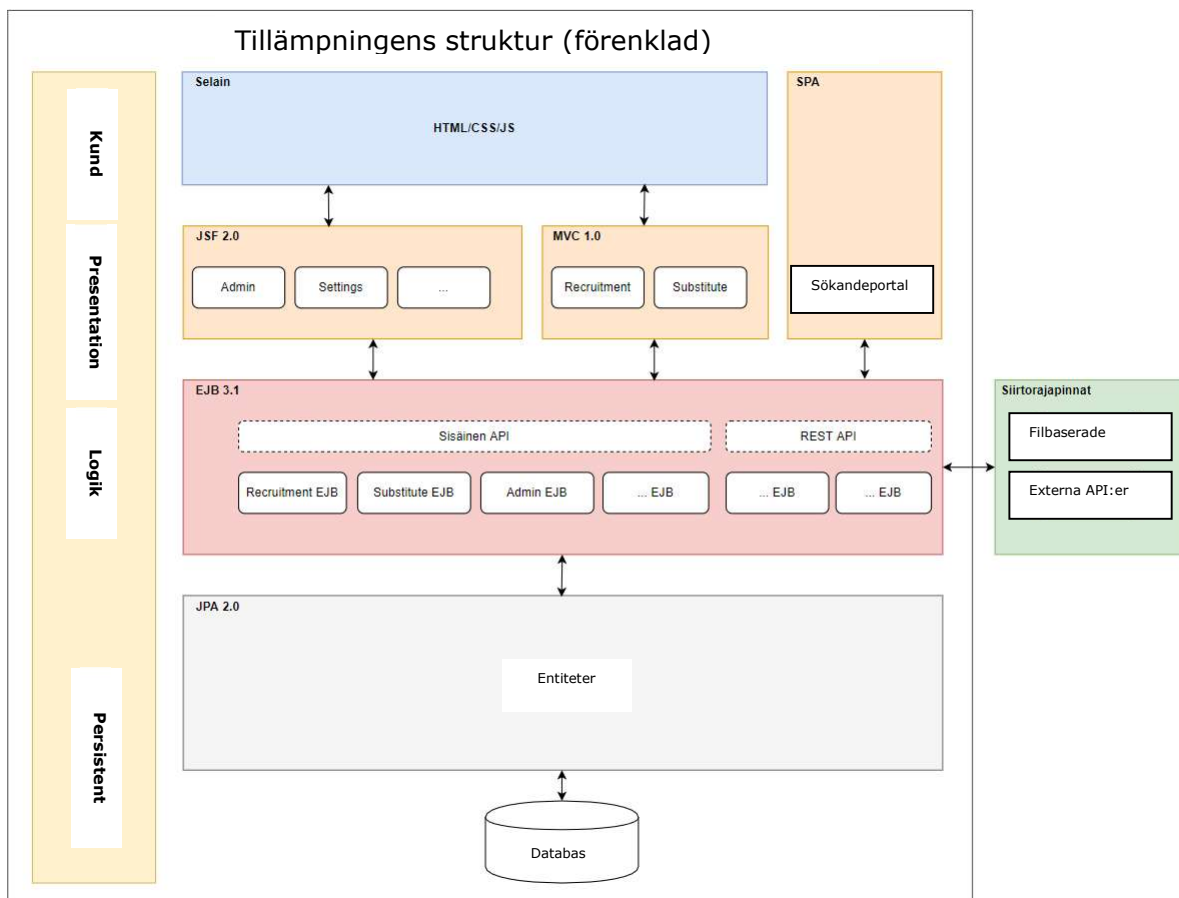
Tjänstens dataskyddsredogörelse: <https://www.kuntarekry.fi/se/dataskyddsutdrag/>

Tjänstens dataskydduttalande: <https://www.kuntarekry.fi/se/integritetsdeklaration/>

## 10 TEKNIK OCH DATASÄKERHET

### Tillämpningsarkitektur i rekryteringssystemet Kuntarekry

Rekryteringssystemet Kuntarekry används via en webbläsare, och visas för användaren som en webbsida. Kuntarekrys arkitektur är uppdelad i tre huvudskikt: presentation, logik och persistens.



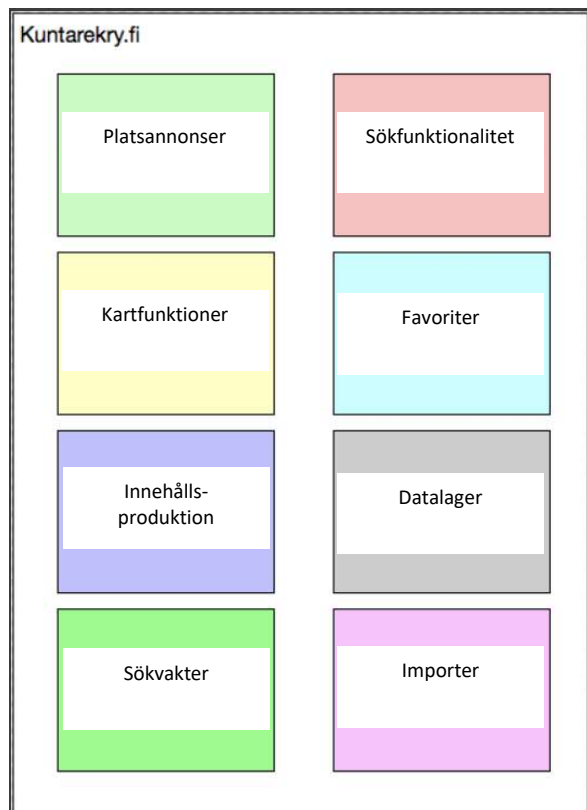


Skikt	Beskrivning
<b>Kund</b>	<p>Slutresultatet, som Kunden ser i sin webbläsare. Slutresultatet består av HTML-, CSS- och JS-filer.</p> <p>Rekryteringsportalen baseras på biblioteket AngularJS, vilket gör att tillämpningen fungerar i användarens webbläsare, och kommunicerar via Web Service med rekryteringssystemet Kuntarekry</p>
<b>Presentation</b>	<p>Presentationsskiktet är det slutresultat som användaren ser. Presentationsskiktet skapas genom samverkan mellan JSP-sidorna och JSF Beans: JSF ansvarar för presentationsskiktets logik och dess koppling till själva logikskiktet. JSP beskriver själva sidan och dess struktur.</p> <p>I rekryteringsmodulen skapas presentationsskiktet med hjälp av Java MVC-arkitektur. I praktiken baseras funktionen på samverkan mellan JSP-sidor/sidodelar och HTTP Endpoints (Controller): Controller ansvarar för mottagningen av begäran och överföring till logikskikten, och JSP beskriver sidan och dess struktur.</p>
<b>Logik</b>	<p>Logikskiktet består av ett antal gränssnitt (EJB) som skiljer programmets kärnlogik från presentationsskiktet. Logikskiktets gränssnitt kan också publiceras som Web Service (SOAP eller REST-gränssnitt)</p>
<b>Persistent</b>	<p>Persistentskikten tillåter användning av databasen</p>
<b>Överföringsgränssnitt</b>	<p>Via överföringsgränssnitten kan information från ett externt system importeras till rekryteringssystemet Kuntarekry, eller exporteras till ett externt system. Vanligtvis är överföringsgränssnitten filbaserade och definieras i samband med drifttagningen. I Kuntarekry kan överföringsgränssnitten även göras webbaserade.</p>
<b>Externa tjänster</b>	<p>Kuntarekrys externa tjänster är till exempel e-postöverföring och SMS-kommunikation. E-postmeddelanden skickas vanligtvis via Kundens egen e-postserver, och SMS skickas via en SMS-Gateway hos vår partner Kuulalaakeri.</p>

## Teknikerna bakom webbplatsen Kuntarekry.fi

Anne-Mari Mourukoski

Webbplatsen Kuntarekry.fi bygger på programmet Processwire. Processwire är ett populärt system för innehållshantering (Content Management System, CMS) med öppen källkod, vars struktur och funktionalitet kan kompletteras och utökas med olika tillägg (moduler). Processwire används i Kuntarekry som en plattform, på vilken Kuntarekry.fi-webbplatsens funktioner byggs. De centrala funktionerna presenteras i följande bild:



FUNKTION	BESKRIVNING
<b>Platsannonser</b>	Presentation, notering, sammanställning och vidarebefordran av platsannonser (RSS)
<b>Importer</b>	Funktionella schemalagda tjänster som hämtar platsannonser från olika källor.
<b>Datalager</b>	Webbplatsdata (platsannonser, sökvakter, webbplatsers innehåll och struktur)
<b>Favoriter</b>	Arbets sökande kan markera vissa jobb som favoriter. Favoriter sparas i användarens webbläsare, därför behöver användaren inte logga in för att använda favoriter.
<b>Innehållsproduktion</b>	Webbplatsens innehåll administreras med kärnfunktionerna i Processwire.
<b>Kartfunktioner</b>	Visualisering av platsannonser på karta. (Karttjänstleverantören ändras, funktionen kommer tillbaka 2023.)
<b>Sökvakter</b>	Arbets sökande kan spara sökresultat som sökvakter. Detta kan sparas antingen med en e-postadress, eller med en enhet som stöder push-meddelanden.

Anne-Mari Mourukoski

<b>Sökfunktionalitet</b>	Sökning av jobb med hjälp av olika sökkriterier och taggar
--------------------------	--

## Datasäkerhet

Datasäkerheten är en central del av Tjänsten Kuntarekry och av FCG:s verksamhetsmetoder. Vi strävar efter att ständigt förbättra datasäkerheten.

## Kuntarekrys datasäkerhetslösningar

### Arkitektur

Tjänsten Kuntarekry har en tydlig arkitektur baserad på standardiserad Java EE-arkitektur. Arkitekturen är uppdelad i olika skikt (flerskiktsarkitektur), där varje skikt har sin betydelse och avgränsning. Programvarans komponenter och nivåer kommunicerar data till varandra genom servicebegäran, där källan och innehållet i begäran kontrolleras innan begäran besvaras. Java EE-arkitekturen har flera färdiga lösningar och praxis som kan användas för att producera datasäkra och testbara lösningar.

Programmets användargränssnitt utförs med en komponentbaserad arkitektur för användargränssnitt. I en komponentbaserad arkitektur för användargränssnitt består programbilderna av komponenter som kan återanvändas i programmets olika delar. Det förenklar testningen och ger en mindre potentiell angreppsytta.

### Inloggningsuppgifter och behörigheter

Varje användare har ett personligt användarnamn och lösenord till Tjänsten Kuntarekry. Det är inte tillåtet att använda generella inloggningsuppgifter.

Tjänsten Kuntarekry har mångsidiga och anpassningsbara behörighetsprofiler.

Behörighetsprofilerna kan till exempel användas för att definiera vilken och vems data användaren har åtkomst till, samt om behörigheten gäller redigering eller läsning av uppgifterna. Behörighetsprofilerna definieras och implementeras vanligtvis under drifttagningen.

### Hantering av fel

Hantering av fel i Tjänsten Kuntarekry är en central och övergripande funktion, vilket innebär att hela den aktuella begäran avbryts vid fel. Det innebär, att man hellre avbryter systemets funktion än riskerar programmets datasäkerhet.

Vid felsituationer loggas detaljerad information om felet i den tekniska loggen, men användaren får endast en identifierare av felet för en eventuell supportbegäran. På så sätt avslöjas inte teknisk information om programmet för användarna.

### Kontroll av in- och utmatning

I Tjänsten Kuntarekry kontrolleras in- och utmatningarna för att bevara den normala funktionaliteten och användbarheten, så att in- och utmatning till eller från systemet inte kan ändras på ett sätt som är skadligt för systemet eller dess användare.

Anne-Mari Mourukoski

Vid kontrollen av in- och utmatningar beaktas bland annat följande:

- Programmets input kontrolleras formellt (längd, intervall)
- Programmets output är inte utvärderbar som standard
- Direktåtkomst till flöden förhindras genom oparametriserade databasfrågor, programomdirigeringar och hänvisningar till disksystemfiler (sökvägsmanipulation)

### **Skydd av användarsessionen**

Autentisering och sessionshantering i Tjänsten Kuntarekry baseras på Java EE-standarden och hanteras via en tillämpningsserver (Wildfly) som tillämpar standarden. Användarsessionen är cookiebaserad och sessionens giltighetstid är konfigurerbar.

### **Kryptografi och kryptering**

Data från Tjänsten Kuntarekry måste alltid krypteras. I praktiken innebär detta en säker SSL-anslutning (HTTPS) mellan webbläsaren och programmet.

### **Logghanterare och rutiner**

Tjänsten Kuntarekry tillhandahåller två olika loggar från tillämpningens drift. Den tekniska loggen kan konfigureras så att den tar emot data om tillämpningens drift och om felsituationer. I Audit Trail-loggen registreras data om programmets användning.

### **Driftsmiljö**

Datasäkerheten beaktas i programmet och i driftsmiljön. Driftsmiljön skapas av vår samarbetspartner Advania Finland Oy. Advania Finland Oy datacentertjänst har ISO27001-certifiering (beviljad 4.3.2022, gäller 17.3.2025). Tjänsterna i driftsmiljön omfattar bland annat följande:

- Övervakning av datatrafik
- Övervakning av apparater och omgivningar
- Åtkomstkontroll
- Administrationstjänster
- Centraliserad loggihantering (SIEM)
- Upptäckt av säkerhetsintrång (EDR)
- Managementcenter för informationssäkerhet (SOC)
- Dataskydd
- Palo Alto NGFW
- DDoS-trafikanalysator

### **Fysisk säkerhet**

Advania har två datacenter i huvudstadsregionen, som ligger mer än 10 km från varandra. Ur datakommunikationssynpunkt är datacenterna kopplade till varandra med fiberanslutningar dedikerade till Advania. Endast den tekniska personalen från Advania, som absolut behöver tillgång till datarummen på grund av sina arbetsuppgifter kan komma åt datarummen. Advanias egna experter, som inte arbetar i datacentret, samt extern underhållspersonal har alltid sällskap. Personer som besöker lokalerna är skyldiga att underteckna ett sekretessavtal utöver sina identitetshandlingar.

Datasalarna har 24/7 bevakning, som sköts av ett externt vaktbolag. Larmövervakning gäller larm orsakade av brottsdetektorer och passersystem. Varje väktare har den utbildning som krävs enligt lag och nödvändiga bevis, till exempel ett vaktkort.

Anne-Mari Mourukoski

## Plats

Både driftsmiljön och all data i miljön finns i Finland. Underhållspersonalen finns också i Finland och hanterar miljön från Finland.

## SIEM

Loggarna för Kuntarekry-programvaran och resurserna i operativmiljön samlas in i Logpoints Security Information and Event Management (SIEM) hanteringstjänsten. SIEM:s uppgift är att observera händelser relaterade till systemets datasäkerhet (loggar och larm) och tillhandahålla verktyg för deras bearbetning (analys). SIEM analyserar data som kommer dit och söker efter avvikelser baserat på de regler som definierats för den.

Loggkällor för SIEM är till exempel nätverksenheter, operativsystem och servrar. Larmkällor är till exempel avvikelser som upptäcks av EDR. SIEM möjliggör användning av insamlad data för informationssäkerhet-, IT-, produktion- och revision.

I SIEM-hanteringstjänsten lagras loggdata i maximalt 12 månader.

Med logghanteringstjänstens användarrättighetshantering är det möjligt att definiera de personer som har rätt till tjänstens loggdata.

## EDR

Operativmiljöns servrar använder WithSecures Elements Endpoint Protection (EDR). EDR upptäcker serverhändelser och reagerar på avvikelser. EDR möjliggör identifiering av sofistikerade och/eller riktade attacker. EDR reagerar på avvikelser autonomt och genom att generera varningar för SIEM/SOC-tjänsten.

## SOC

Informationssäkerhetshanteringscentret (Security Operations Center, SOC) i operativmiljön övervakar händelser i miljön med hjälp av SIEM-systemet. Hanteringscentralen reagerar på cybersäkerhetsavvikelser som upptäcks i driftmiljön, och när de inträffar görs en klassificering och en analys av händelsen påbörjas. Baserat på analysen vidtas nödvändiga motåtgärder och operativ förmåga återställs för att säkerställa tjänstens kontinuitet.

## Dataskydd

Kuntarekry-programvaran används alltid över en krypterad HTTP (SSL/TSL)-anslutning. I driftmiljön hanteras och skyddas datatrafik med en brandvägg och DDoS-skydd.

Anne-Mari Mourukoski

## Palo Alto NGFW

Driftmiljöns brandvägg är Palo Altos NGFW (Next-Generation Firewall), det vill säga nästa generations brandväggstjänst. NGFW-brandväggen kombinerar traditionella brandväggsfunktioner med avancerad applikationsbrandvägg och funktioner för inspektion av trafikinhåll. NGFW-brandväggen övervakar trafik som passerar genom tjänsten och filtrerar skadliga datapaket som identifieras som potentiella hot från belastningen av olika kommunikationsprotokoll.

Filtreringen av kameran mot hot sker i realtid, så virus eller skadlig kod som färdas i kommunikationspaket når inte ett potentiellt sårbart system och därmed förblir kritiska system oförorenade. Systemet försöker också upptäcka vidarebefordran av data från maskiner som eventuellt är infekterade med spionprogram. Som standard uppdateras hotdatabaser automatiskt varje timme från hårdvarutillverkarens globala källor.

Vid behov kan NGFW-brandväggen även finkornig TLS/SSL-dekryptering och undersöker därmed även krypterad trafik.

## DDoS

DDoS-reduceringstjänsten skyddar tjänsten från effekterna av distribuerade överbelastningsattacker. Reduceringsstjänsten kan identifiera de vanligaste överbelastningsattackerna och webbadresserna. Skyddet bygger på att förhindra framstegen för attackerande trafik inom tjänstens datacenter. Om omfattningen av attackerna är större än den totala bandbredden för internetanslutningstjänsten för tjänstens datacenter, kommer DDoS-reduceringstjänsten inte att helt kunna förhindra effekten av överbelastningsattacker.

Anne-Mari Mourukoski

## **Dataskyddsrutinerna på webbplatsen Kuntarekry.fi**

### **Driftsmiljö**

Datacenter Finland (DCF), som har ISO 27001-certifikat för datasäkerhet, och ansvarar för Kuntarekry-portalens driftsmiljö. Vid behov kan en mer detaljerad beskrivning av DCF:s säkerhetsrutiner (konfidentiell information) tillhandahållas.

Datasäkerheten beaktas genom en befintlig Processwire CMS (PW) plattform. Kärnan i PW innehåller färdiga lösningar för användarhantering, användarroller och lösenordsregler.

### **Övervakning**

FCG:s underhåll övervakar driften av webbplatsens platsannonserstjänster samt webbplatsens drift och svarstider. Brandväggen för webbplatsen Kuntarekry.fi blockerar IP-adresser som skapar mer trafik än normalt.

### **FCG:s dataskyddsrutiner**

#### Organisation

På FCG styrs arbetet med datasäkerhet och dataskydd av datasäkerhetschefen. Datasäkerhetschefen samordnar, fastställer, definierar och övervakar datasäkerhets- och dataskyddsrutinerna i koncernens företag, och främjar en datasäker arbetskultur. Dataskyddschefen ansvarar för koncernens datasäkerhetsrutiner (byggnader, personal).

FCG:s datasäkerhetspolicy beskrivs i koncernens personalhandbok och underhålls av FCG:s ICT-avdelning.

FCG:s enhet för rekrytering och HR-program har ett datasäkerhetsteam som träffas regelbundet för att identifiera och utveckla datasäkerhetsfrågor i samband med rekrytering och HR-program. Varje teammedlem har ett eget ansvarsområde inom datasäkerhet, som personen ansvarar för att utveckla. Ansvarsområdena är följande:

- Utveckling. Främjande och övervakning av datasäkra metoder för utvecklingsarbetet.
- Testning. Främjande och övervakning av testmetoder för datasäkerhet.
- Hårdvara/Infra/Plattformar/Nät. Uppföljning och drifttagning av datasäkerhetsfrågor i driftsmiljön.

Anne-Mari Mourukoski

- Sårbarheter i datasäkerheten. Övervakning av datasäkerhetsnivån på de plattformar och gränssnitt som används.
- Kultur & medvetenhet. Främja och lyfta fram datasäkerhetstänkande, organisera utbildning och informera FCG:s rekryterings- och HR-programvaruenhet.

## Utbildning

FCG anordnar datasäkerhetsutbildning för all personal. Som exempel kan nämnas dataskyddsutbildning som anordnas för alla medarbetare, och som varje medarbetare ska delta i.

FCG:s rekryterings- och HR-programmenhet anordnar regelbundet utbildningar i datasäkerhet för medarbetare som arbetar med produktutveckling eller motsvarande. Utbildningen är organiserad som interna kurser, externa kurser och olika former av självstudiematerial (videokurser, böcker). Dessutom deltar personalrepresentanterna aktivt i produktutvecklingsorienterade konferenser och evenemang där datasäkerhet behandlas (JFokus, Disobey, GeekOut).

Utöver de organiserade utbildningar ägnar de som arbetar med produktutveckling två timmar i veckan åt att utveckla sina tekniska färdigheter.

## Hänsyn till datasäkerhet i produktutvecklingen

### Definition

Datasäkerheten beaktas redan i förstudierna för nya funktioner. Typen av och känsligheten hos de data som behandlas i funktionen ska identifieras. Typen av information kan skapa särskilda datasäkerhetskrav, vilket ska uppmärksammas i utvecklings- och testfasen.

### Utveckling

Under utvecklingen ska datasäkerheten beaktas genom de krav som skapas i specifikationen och genom instruktioner, inspektioner och granskningar relaterade till datasäkerheten. De flesta datasäkerhetskrav är inte kopplade till funktionella krav, och därför bidrar olika riktlinjer och revisioner till att utvecklaren kan ta hänsyn till datasäkerheten.

### Testning

Programmet testas enligt testplanen. Testning av datasäkerheten är en del av denna testplan. Datasäkerhetstestningen omfattar både manuella och automatiska testrutiner. Testningen kan göras enligt checklistor (oftast automatiskt) eller undersökande (oftast manuellt).

### Underhåll

Underhållteamet ansvarar för kundsupport i produktutveckling och för att klara ut felsituationer. Därför har underhållteamet vanligtvis tillgång till kundmiljön och ibland behörighetsnivån administratör i programmet.



Anne-Mari Mourukoski

## Kvalitetsrevisioner

I EU:s dataskyddsutredning konstaterades att det finns ett behov av tekniska revisioner från tredje part. Tidigare har revisionerna utförts av kunderna i samband med drifttagningen. Vår säkerhetspartner är elfGROUP Kyberturvallisuuspalvelut Oy.

## Miljöskanningar

Vi övervakar testmiljöerna enligt systembeskrivningen med produkten F-Secure Radar, för att fånga upp eventuella sårbarheter i datasäkerheten och kommunikation så tidigt som möjligt.

## Miljön och beroenden

Produktutvecklingen är starkt kopplad till de plattformar och bibliotek som programmet är utvecklat på. Plattformar och bibliotek övervakas med avseende på deras livscykel, datasäkerhetsbrister och utveckling.

## Åtkomstkontroll

FCG:s personal ska under sin anställningstid endast ha tillgång till sådana system och miljöer som de har ett väsentligt behov. Om en medarbetares anställningsförhållande till FCG ändras eller avslutas, tas deras behörigheter till alla system och miljöer bort.

## 11 ÄNDRINGAR AV TJÄNSTEN ELLER TJÄNSTEBESKRIVNINGEN

Detta dokument beskriver Leverantörens verksamhet vid tidpunkten för dokumentationens utfärdande. Leverantören förbehåller sig rätten att vidareutveckla sin egen verksamhet och att ändra de tjänster, tekniker och metoder som beskrivs i dokumentet.

Leverantören har alltid rätt att utföra en ändring av Tjänsten som påverkar Programtjänstens produktionsmiljö, men som inte påverkar Tjänstens innehåll eller servicenivå, eller om det är nödvändigt för att förhindra ett allvarligt hot mot datasäkerheten (inklusive ett allvarligt hot mot tillgängligheten), eller om en tvingande lag eller ett myndighetsbeslut som berör produktionsmiljön kräver en sådan ändring. Om ändringen påverkar tjänstebeskrivningen, ska Leverantören informera Beställaren om den kommande ändringen i god tid. Om detta inte rimligen är möjligt, till exempel beroende på ett akut allvarligt säkerhetshot, ska Beställaren informeras omedelbart efter att Leverantören upptäckt behovet av ändringen.

Även i andra fall än de som nämns ovan är Leverantören skyldig att informera Beställaren om ändringar i Programtjänsten. Om den avsedda ändringen väsentligt påverkar Tjänstens innehåll eller servicenivå, så att innehållet eller servicenivån för den tjänst som Kunden använder minskar, ska Leverantören skriftligen underrätta Kunden om ändringen senast tre (3) månader före den dag då ändringen träder i kraft, och Beställaren har då rätt att säga upp avtalet med tre (3) månaders uppsägningstid. Uppsägning ska ske inom tre (3) månader från meddelandet om ändringen. Om behandlingen av personuppgifter överförs till en annan underleverantör, eller till en plats utanför EES, anses det vara en väsentlig ändring av Tjänstens innehåll.

Den aktuella tjänstebeskrivningen finns i Kuntarekry-systemet.