

Webcruiter og GDPR

Navn på systemet	Webcruiter
Leverandør	Webcruiter AS Nydalsveien 12b 0484 OSLO Org. nr.: 985 360 421 Telefon: +47 22 30 11 50 E-post supportnorge@webcruiter.no
Hva er Webcruiter	En skybasert tjeneste/programvare som understøtter rekrutteringsprosesser. Alle kunder er på én og samme instans, med logisk segmenterte databaser – såkalt "multi tenant"-løsning. Det er ikke gjort spesialtilpasninger for den enkelte kunde. Alle kunder benytter følgelig samme skytjeneste hvor de samme reglene gjelder for alle.
Formålet med bruk	Ta imot nødvendige opplysninger fra jobbsøker for å kunne gjennomføre rekrutteringsprosesser. Kunne søke i CV-databasen etter kandidater som åpner for dette. Kommunisere med jobbsøkere i hele rekrutteringsprosessen.
Hvilke opplysninger hentes inn?	Jobbsøkers navn, adresse, epost, mobiltelefon, (ev kjønn, nasjonalitet, fødselsdata) Jobbsøkers CV, søknad og vitnemål/attester Aktivitetslogg og kommunikasjon på epost Det lagres ikke personsensitive data.
Personsensitive opplysninger	Nei – det oppbevares ikke personsensitive data.
Samtykke	Generell og kundespesifikk.

	Det kreves ikke samtykke for å registrere søknad og CV, registrering baserer seg på «berettiget interesse». Jobbsøker vil informeres om formålet med behandlingen. Formålsbeskrivelsen er kundespesifikk. Jobbsøker vil måtte samtykke ved gjennomføring av personlighetstester eller dersom de ønsker å lagre sin CV i en kundes CV-database.
<i>Sletting og retting av data fra jobbsøkers side</i>	Jobbsøker kan selv slette og rette egne data. Rekrutterer har fått utvidede muligheter til å feilrette på vegne av jobbsøker som en konsekvens av GDPR. Arbeidsgiver kan også åpne for at jobbsøker kan korrigere feil selv etter søknadsfrist.
<i>Sletting av data i kundens egen rekrutteringsløsning</i>	Kunden er selv ansvarlig for egne data, også for å slette disse. Data bør slettes når en rekrutteringsprosess er avsluttet og klagefrist er utløpt. Anbefalingen fra HR Norge er at data bør slettes innen ett år etter avsluttet rekrutteringsprosess – lagring utover dette krever samtykke fra jobbsøker. Det er mulig å bestille en slettejobb hos Webcruiter som sletter alle jobbsøkerdata for prosesser som er av eldre dato. Det er også mulig å bestille denne sletting av data med ønskede intervaller. Kunden kan også selv benytte en innebygget funksjon som gjør det mulig for kunden selv å anonymisere/slette søkerdata per rekrutteringsprosess. Funksjonaliteten kan kun benyttes på avsluttede rekrutteringsprosesser og gjøres av en med administratorrettigheter. Det vil ikke bli mulig å masse-slette data fra kundens grensesnitt.
<i>Hva blir slettet når du bestiller en sletting fra Webcruiter?</i>	Sletterutinen sletter data knyttet til jobbsøkers søknad og tilhørende CV og logger/vedlegg tilknyttet den enkelte søknadsprosess. Dette innbefatter blant annet søknadstekst, svarbrev, svar på screening, kommunikasjon, notater, vedlegg, samt koblinger til eventuelle tester og bakgrunnssjekk. Statistikk-relaterte data bevares, men det vil ikke være mulig å koble enkeltindivider mot disse data. Stillinger som ikke var avsluttet da sletterutinen ble startet blir autoavsluttet i det at prosessen kjøres.

	Jobbsøkere kan fortsatt velge å legge igjen en åpen CV i den enkelte kundes CV-database. Denne blir ikke påvirket av sletterutinen. <u>Begrepsavklaringer</u> MasterCV Jobbsøkerens sist oppdaterte CV på tvers av kunder. Oppbevares av Webcruiter, ikke kunden. Jobbsøker logger seg på sin jobbsøkerportal og håndterer denne. Det er bare jobbsøkeren selv som har innsyn i denne. Åpen CV CV som ligger i CV-basen til den enkelte kunde. Søknads-CV søknadstekst + Søknads-CV knyttet til den spesifikke stillingen
Sletting av data etter henvendelse fra jobbsøker	Scenario 1 <i>Jobbsøker ønsker å bli slettet fra databasen. Prosessen vedkommende har søkt på, er fortsatt åpen.</i> Dersom rekrutteringsprosessen ikke kan avsluttes nå, må man begynne med å slette vedkommendes søknad fra prosessen. Når søknaden er slettet må man slette personens CV fra CV-databasen under «CV-administrasjon». Scenario 2 <i>Jobbsøker ønsker å bli slettet fra CV-databasen. Prosessen som vedkommende har søkt på er avsluttet og arkivert.</i> Når man sletter personens CV fra CV-administrasjon, blir vedkommendes søknads-CV(er) anonymisert på stillingen(e). Statistiske data vil ikke bli slettet, men CV-data som knyttes til jobbsøkeren blir borte. Vedkommendes åpne CV blir borte fra CV-databasen. Scenario 1 og 2 kan bare gjøres på én og én CV.
Uthenting av data	Det er utviklet en funksjon i jobbsøkernes grensesnitt der de selv kan hente ut egenregistrerte opplysninger som PDF eller i et maskinlesbart format – XML.
Innkommende data	• Ved arkivintegrasjon: Ingen data

	• Ved Dossierintegrasjon: CV-data (om toveisintegrasjon er påslått) • Ved testintegrasjoner: Kandidat-ID, poengsum (score), lenke til rapporter. • Ved bakgrunnssjekk: Kandidat-ID, lenke til rapport • Ved integrasjon med Personalportalen: alle ansatte får en «tom» CV automatisk opprettet og brukere blir opprettet. • Ved toveisintegrasjon med Agresso/Unit 4 Business World: Organisasjonsstruktur og brukere
<i>Utgående data</i>	• Ved arkivintegrasjon: arkivverdig data • Ved Dossierintegrasjon: CV-data • Ved testintegrasjoner: Kandidat-ID, språk, valgt test • Ved bakgrunnssjekk: Personalia, CV. Krever særskilt samtykke. • Ved toveisintegrasjon med Agresso/Unit 4 Business World: CV for den som ansettes
<i>Tredjepart / samarbeidspartner</i>	Disse produktene/tjenestene er opsjoner/tilvalg • Arkiv: Acos, P360, ePhorte • Kompetanse: Dossier, Competence • Testverktøy: Assessio, cut-e • Bakgrunnssjekk: Semac • Kalenderdeling: Cronofy • Videointervju: RecRight • Printannonser: Papirfly
<i>Datalagring</i>	All lagring og prosessering av data skjer innenfor EU/EØS: • Evry – Gjøvik (Norge) • Microsoft Azure – Amsterdam/Dublin (Nederland/Irland)
<i>Tilgang til data</i>	Tilgang til data hos kunden styres av organisasjonstilhørighet og roller. Webcruiters Servicedesk, Produktavdeling og Utviklingsavdeling har tilgang til kundedata.
<i>Konfidensialitet</i>	Ansatte og innleide i Webcruiter AS må signere på selskapets standard ansettelses-/innleieavtaler som inkluderer avsnitt om konfidensialitet knyttet til data om jobbsøkere, kunder og partnere. Alle ansatte gjennomgår “Dine første dager i Webcruiter” - opplæring hos Webcruiter, hvor de blir informert om alle Webcruiters områder og får opplæring og oppfølging i sine arbeidsoppgaver.

Ansatte har kun tilgang til administrasjonsverktøy gjennom egne brukere, passord og roller, og kan kun aksessere disse pålogget Webcruiters nettverk på klient satt opp i henhold til selskapets standardmal. Data fra kunder og kandidater lagres sentralt i Webcruiters driftsmiljø og lagres kun i svært spesielle tilfeller midlertidig lokalt på klienter. Alle klienter har kryptert harddisk i henhold til selskapets standardmal.

Underleverandører og samarbeidspartnere av Webcruiter AS som potensielt kommer i kontakt med person- og kundeopplysninger i forbindelse med Webcruiters rekrutteringsløsninger, signerer avtaler som ivaretar hensyn knyttet til konfidensialitet.

Kundenes rekrutteringsbrukere har kun tilgang til data i henhold til de rettigheter og organisasjonstilhørigheter vedlikeholdt gjennom kundens sentrale brukeradministrasjonsløsning, eller som kundens superbrukere har gitt tilgang til. Det foreligger standard kundeavtale som regulerer bruk av løsninger.

Jobbsøkere har kun tilgang til sine egne data, og må ved registrering av CV-profil i den enkelte Webcruiterkundes CV-database aktivt bekrefte/akseptere vilkår for oppbevaring og bruk av data.

Integritet

I utviklingen av løsninger sikres det integritet av data. Under utvikling benyttes det sentrale utviklingsbiblioteker som ivaretar datakontroll på input og lagring/sletting som forhindrer lagring i feil dataformater og uønsket slettinger, samt sikrer begrensning av datatilgang. Statistiske data låses etter registrering, og hendelser som skal kunne utføres i rekrutteringsprosess blir loggført ved hendelsestidspunktet.

Webcruiters rutiner for utvikling og release ivaretar, dokumenterer og prioriterer følgende: Innspill, utvikling, endringer, tester og releaser.

Eventuelle behov for feilrettinger som blir rapportert inn fra support er ivare tatt av samme rutiner som ved vanlig utvikling, men med umiddelbar vurdering av alvorlighet / verifisering av rapportert feil.

Tilgjengelighet

Alle rekrutteringsløsningskunder driftes av Webcruiters driftsleverandører fra samme driftsmiljø. Driftsmiljøene er bygget opp med fokus på redundans og skalerbarhet i alle ledd for å sikre høy oppetid og god respons for brukere. Miljøet består av flere fysiske driftslokasjoner med egne separate kommunikasjonslinjer ut mot

	omverden, i tillegg til redundante fiberdirekteforbindelse mellom lokasjoner. Lastbalansert driftsmiljø med redundans på adskilte lokasjoner gir redusert risiko for driftsforstyrrelser ved katastrofe eller større infrastrukturhendelser. Driftsleverandørene har døgntkontinuerlig overvåking av egen infrastruktur, herunder også internett-tilkoblingene, samt alt utstyr tilknyttet Webcruiters driftsmiljø inklusive selve applikasjonstjenestene. I tillegg til driftsleverandørenes døgntkontinuerlige overvåkning, overvåker Webcruiter kontinuerlig tilstand på servere, kapasitet og respons. I jevnlig driftsmøter vurderer og analyserer driftsleverandør og Webcruiter overvåkningshendelser samt logger av respons-, belastnings- og kapasitetsutvikling. Ved hendelser følges fastlagte rutiner "Håndtering av driftsforstyrrelser/katastrofeplaner og gjenopprettingsplaner"
<i>Årlig sårbarhets- og sikkerhetsanalyse</i>	Webcruiter gjennomfører årlig en sårbarhets- og sikkerhetsanalyse i regi av spesialisert sikkerhetsselskap. I forbindelse med årlig risikoanalyse har underleverandør workshop i forkant med Webcruiters tekniske personell for å identifisere risikoområder. I etterkant har underleverandør og Webcruiter gjennomgang av funn, og eventuelle uønskede svakheter som er funnet blir korrigert og verifisert rettet.
<i>Kontroll av sårbarhet og sikkerhet ved releaser</i>	Webcruiter har tre hovedreleaser årlig. I forkant av disse gjennomføres sårbarhets- og sikkerhetsvurdering av underleverandør. Det gjennomføres full sjekk i forbindelse med første release, og kontrollsjekk ved de to øvrige hovedreleasene.
<i>Fortløpende kontroll av sårbarhet og sikkerhet</i>	I tillegg til kontroller gjennomført av spesialisert sikkerhetsselskap, gjennomfører Webcruiter internt månedlig test av utviklet innmeldt kode målt opp mot blant annet OWASP top 10-liste. I forbindelse med driftsmøter Webcruiter har med EVRY som benyttes som underleverandør av driftstjenester, er sikkerhet og sårbarhet et fast punkt på driftsmøtene. I tillegg til Webcruiters eksterne analyser av sårbarhet og sikkerhet, gjennomfører EVRY ved hjelp av en annen underleverandør årlig analyse av EVRYs driftsmiljø.
<i>Test- og utviklingsdata</i>	Det benyttes anonymiserte data i test- og utviklingssammenheng.

	Det kan forekomme at man i noen tilfeller må teste med replikerte produksjonsdata, spesielt ved integrasjoner mot kundenes interne systemer.
<i>Oppbevaring av Back-up-data</i>	Back-up-data slettes etter én måned.
<i>Kryptering av passord</i>	Passord blir hashet og saltet.
<i>Krypterte linjer</i>	All kommunikasjon mellom nettleser og servere skjer over kryptert linje SSL/TLS 1.2
<i>Personvernombud</i>	Webcruiters personvernombud er Monica Sederholm.
<i>Spørsmål om GDPR?</i>	Kontakt oss på: gdpr@webcruiter.no eller gdpr@webcruiter.se