cegid

Cegid Digitalrecruiters Villkor för tjänster

2023/08/16

www.cegid.com

INNEHÅLL

1. Inledning 6

1.1. Syftet med dokumentet 6

1.2. Ändringar av detta dokument 6

2. Beskrivning av support 7

2.1. Plats för support 7

2.2. Supportavtal 7

2.3. Tillgång till applikationsresurser 7

2.4. Sektion för stöd 7

2.5. Ärendeflöde mellan kund och Cegid 9

2.6. Avtalsdefinition av buggar och SLA-policy 9

2.6.1. Definitioner 9

2.6.2. Cegid Standard SLA för Cegid Digitalrekryterare 10

2.6.3. Tillgänglighet för SaaS 10

3. Underhållsprocessen i körfasen 11

3.1. Förfaranden för hantering av incidenter 11

3.1.1. RACI-matris för stödverksamhet 11

3.1.2. Support Service Kvalitetskontroll 11

3.2. Förfarande för hantering av förändringar 12

3.2.1 Hantering av versioner 12

3.2.2 Underhållsperioder 12

3.3. Förfarande för krishantering 12

3.4. Uppsägning av avtal 13

3.4.1. Plan för reversibilitet 13

3.4.2. Policy för förstöring av data 13

4. Webbplatser för värdtjänster 14

4.1. Värdplatser 14

4 2. Säkerhet och konfidentialitet hos leverantörer av värdtjänster 14

5. Teknisk arkitektur 15

5.1. Applikationsarkitektur 15

5.2. Server- och nätverksarkitektur 15

5.3. Teknisk programvara Infrastruktur 16
5.3.1. Komponenter för infrastruktur 16
5.3.2. Databaser för applikationer 17
5.4. Hantering av flera kunder 17
5.5. Testmiljö 17
5.6. Mobilapplikation 17
6. Tillträdeshantering 19
6.1. Säkerhet för åtkomst till applikationer 19
6.1.1. Kandidatens front office 19
6.1.2. Back Office och utrymmen för anställda/chefer 19
6.2. Autentisering 19
6.2.1. Kundansvar 19
6.2.2. Autentisering för kandidatens front office 19
6.2.3. Autentisering i Back Office 19
6.2.4. Hantering av lösenord 19
6.2.5. Enkel inloggning 20
6.2.6. Sessionens längd 20
6.3. Policy för kakor 20
6.4. Roller, rättigheter och ackrediteringar 20
6.4.1. Roller och rättigheter 20
6.4.2. Ackrediteringar 20
7. Gränssnitt 21
7.1. Import/Export av filer 21
7.1.1. Import 21
7.1.2. Export 21
7.2. Säkert FTP-gränssnitt 21
7.3. Gränssnitt för applikationsprogrammering (API) 21
7.4. Gränssnitt för e-post 22
8. Verksamheter 23
8.1. Operativa förfaranden 23
8.2. Datahantering 23
8.2.1. Säkerhetskopiering av data 23
8.2.2. Kryptering av data 23

8.3. Administration och tillsyn 24
8.4. Plan för kontinuitet i verksamheten 25
9. Förordningar och standarder 26
9.1. Allmän dataskyddsförordning (GDPR) 26
9.1.1. GDPR-krav som gäller för alla personas 26
9.1.2. Svar på GDPR:s krav på kandidater 27
9.1.3. Svar på GDPR:s krav på anställda 28

Historik för modifiering och validering

Originalversion av dokumentet	01	2023/08/04

Reviderad av

2023/08/12	Alexandre Blanc, lösningsarkitekt för Cegid HCM
2023/08/12	Myriam Hétier, produktmarknadschef för Cegid HCM

Godkänd av

2023/08/16	Stephan Latrille, CTO Digital Recruiters, ett Cegid-företag

Distributionslista

Person eller grupp
Digital Recruiters, en kund till ett Cegid-företag
Digital Recruiters, ett Cegid-företag, internt

1. INLEDNING

1.1. Purpose of the document

Detta Tjänstedokument är en integrerad del av avtalet och förklarar de särskilda bestämmelser som gäller för Cegid Digitalrecruiters Tjänster.

Detta dokument syftar till att beskriva de åtgärder som vidtagits för att säkerställa följande:

- Kvaliteten på det stöd som tillhandahålls av Cegid Digitalrecruiters;
- Kvalitet på processerna för övervakning och eskalering av förfrågningar under RUN-fasen efter projektet (Build-fasen);
- Stöd RACI;
- Beskrivning av den tekniska arkitekturen för Cegid Digitalrecruiters applikation för den delade kundinfrastrukturen.

Detta dokument uppdateras närhelst den tekniska miljön för tjänsten ändras.

1.2. Modifications to this Document

Alla ändringar av detta dokument kommer att resultera i en ny version av detta dokument. Ändringar registreras och dateras i versionshistoriken i början av dokumentet.

En mindre ändring kommer inte nödvändigtvis att leda till att en ny version av dokumentet utfärdas omedelbart. Sådana ändringar kommer att införlivas i nästa version av dokumentet.

Varje ändring av dokumentet blir en del av dokumentet och är lika bindande för parterna.

Om dokumentet ändras är den version som publiceras på Cegids officiella webbplats den officiella referensversionen. Den version som bifogas kundavtalet tjänar till att verifiera att det inte finns någon tillbakagång enligt vad som anges i avtalet.

Detta dokument ses över minst en gång per år. Denna översyn kan leda till en ny version av dokumentet.

2. STÖD BESKRIVNING

2.1. Support Location

Cegid Digitalrecruiters kundtjänstteam är baserade i Frankrike (Boulogne-Billancourt). Supportförfrågningar kan göras på engelska och franska.

Supportärenden måste utfärdas via Zendesk Helpcenter, ett ärendeverktyg som är tillgängligt online från Cegid Digitalrecruiters-applikationen för alla kunder med ett supportavtal.

2.2. Support Contract

Cegid Digitalrecruiters tillhandahåller teknisk support till Kunder för alla funktionella eller tekniska frågor, inklusive följande typer av supportförfrågningar i synnerhet: Hjälp, råd, rapportering av buggar/avvikelser (mindre, större, kritiska).

Teknisk support ingår i det erbjudande från Cegid Digitalrecruiters som Kunden abonnerar på. All annan assistanstjänst är föremål för ett separat avtal, baserat på prissättning som tillhandahålls av Cegid Digitalrecruiters.

2.3. Access to Application Resources

Cegid Digitalrecruiters applikation Support erbjuder användarna ett antal resurser för att hjälpa dem att använda lösningen. Dessa resurser täcker följande ämne:

- Webbplatser för karriärer;
- Publicera och distribuera platsannonser;
- Hantering av jobbansökningar;
- Konfigurera inställningar;
- Hantera användare;
- Juridik och GDPR;
- Back Office;
- Vanliga frågor och tips .

2.4. Support Section

Support finns tillgänglig från måndag till fredag, från 9:00 till 18:00 (Paristid), via ett ärendehanteringsverktyg i Cegid Digitalrecruiters Solution eller, om detta alternativ inte är tillgängligt, via e-post på: support@Digitalrecruiters.com eller via telefon på: (+33) (0)1 71 19 77 08.

För att säkerställa en effektiv uppföljning måste alla upptäckta fel rapporteras skriftligen till supporttjänsten med hjälp av det tekniska supportverktyget som tillhandahålls (via länk) i lösningen. Om verktyget inte är tillgängligt kan felet också rapporteras direkt via e-post på: support@Digitalrecruiters.com eller via telefon.

Felrapporten måste beskriva sammanhanget och, om möjligt, processen för att reproducera felet. När rapporten har skickats skapas ett ärende automatiskt i det spårningsverktyg som används av Cegid Digitalrecruiters supportteam. Ärendet kommer att innehålla den information som användaren av lösningen har skickat in samt datum och tid för rapporten.

När felrapporten har tagits emot kommer supportteamet att tilldela en brådskande nivå baserat på de nivåer som definieras i avsnitt 2.6 i detta dokument.

Följande process tillämpas sedan för att lösa felet:

- Kundtjänstoperatören analyserar felet eller begäran och reproducerar det om tillämpligt;
- Vid tekniska buggar eskalerar kundtjänstoperatören ärendet till Cegid Digitalrecruiters produktteam;
- Produktteamet skapar ett Jira-ärende som är länkat till Zendesk-ärendet;
- Cegid Digitalrecruiters utvecklar en patch;
- Cegid Digitalrecruiters projektledare testar patch i utvecklingsmiljön;
- Cegid Digitalrecruiters projektledare testar patch i pre-produktionsmiljön;
- Cegid Digitalrecruiters laddar upp patch till produktionsmiljön (live).

2.5. Support Ticket Workflow between the Customer and Cegid

I följande tabell förklaras de olika statusarna i Zendesk (ärendehanteringsverktyget) med motsvarande prime (tilldelad aktör) för varje status.

Status	Definition	Prime
Ny	Biljetten skapas av Kunden och skickas till Cegid. Denna status tilldelas automatiskt av Zendesk när ärendet skapas.	*Cegid*
Öppna	Biljetten behandlas av Cegid. Denna status tilldelas av Zendesk när en kundtjänstmedarbetare har analyserat ärendet och gett ett första kvalificerat svar till kunden.	*Cegid*
Pågående	Ärendet har kvalificerats av kundtjänstoperatören men kräver ytterligare information eller validering av kunden. Ärendet väntar på svar från kunden. Väntande ärenden behåller denna status i 5 dagar innan de ändras till lösta om inget svar inkommer.	*Kund*
Löst	Ett svar har lämnats till kunden och problemet anses vara löst. Kunden kan öppna ärendet igen. Uppklarade ärenden behåller denna status i 2 dagar innan de ändras till stängda om inget svar har mottagits.	*Kund / Cegid*
Stängt	Ärendet är stängt och kan inte öppnas igen. Ett uppföljningsärende kan skapas.	Cegid

2.6. Contractual Definition of Bugs and SLA Policy

2.6.1. Definitioner

Ett fel definieras som en funktionsstörning som helt eller delvis kan tillskrivas Lösningen. Det finns tre nivåer av Bugs:

- **Kritisk**: Innebär ett fel som gör det omöjligt att använda en eller flera funktioner i Lösningen, såvida det inte finns en lösning;
- **Större**: Betecknar alla icke-kritiska fel som leder till försämrad funktion hos en eller flera funktioner av lösningen;
- **Mindre**: Betecknar fel som inte är kritiska eller större, som inte förhindrar användning av en funktion eller tjänst, men som har en inverkan på dess användarvänlighet.

2.6.2. Cegid Standard SLA för Cegid Digitalrecruiters

Tid för åtgärdande av fel

Tidpunkterna för felavhjälpning är följande:

- Kritisk: inom högst 1 arbetsdag;
- Större: inom högst 2 arbetsdagar;
- Mindre: inom 30 arbetsdagar eller under en kommande mindre uppdatering av applikationen, beroende på typen av fel.

Cegid Digitalrecruiters kan inte hållas ansvarigt för att bugglösningstiderna överskrids under följande omständigheter:

- Kunden vägrar att samarbeta för att lösa fel, och i synnerhet att svara på frågor och förfrågningar om information;
- Användning av lösningen för ett ändamål som den inte är avsedd för, eller på ett sätt som inte överensstämmer med dess dokumentation;
- Obehörig modifiering av Lösningen av Kunden;
- Kundens underlåtenhet att fullgöra sina skyldigheter enligt Avtalet;
- Användning av paket, programvara eller operativsystem som inte är kompatibla med Lösningen;
- Fel som beror på felaktig användning i samband med en lösning från tredje part eller partner.

2.6.3. Tillgänglighet för SaaS

Den månatliga tillgängligheten för Lösningen är 99,5% (nittionio komma fem procent), 24 timmar om dygnet, 7 dagar i veckan.

Tjänstens tillgänglighet mäts baserat på övervakning av ett tredjepartsföretag. Tester av tjänstens tillgänglighet utförs varje minut från olika källor på internet som finns i olika internetoperatörers nätverk.

Den månatliga stilleståndstiden (DT) beräknas enligt följande:

DT (minuter) = Total stilleståndstid för Tjänsten i minuter under månaden

Den totala månatliga tillgängliga tiden (AT) beräknas enligt följande:

AT (%) = [1- (DT / (antal dagar i månaden * 1,440))] x 100

Tillgänglighetsstatistik kommer att göras tillgänglig för Kunden på begäran.

3. UNDERHÅLLSPROCESS I KÖRFASEN

3.1. Procedures

Supportförfrågningar följer det förfarande som anges nedan. Beroende på typen av förfrågan kan steg 2 till 5 vara de sista stegen i arbetsflödet.

Steg	Skådespelare	Åtgärder
1	Kund	Skapa förfrågan
2	Nivå 1 - Kundservice	Lämna in begäran / samla in ytterligare information
3	Nivå 1 - Kundservice	Bedömning av komplexitet
4	Nivå 2 - Teknisk support	Utföra teknisk analys
5	Nivå 3 - FoU	Genomföra korrigerande åtgärder
6	Nivå 1 - Kundservice	Bekräfta resolution av begäran

3.1.1. RACI-matris för stödverksamhet:

- **R**: *Ansvarig person*
- **A**: *Godkännande*
- **C**: *Konsulterad*
- **I**: *Informerad*

Aktiviteter/spelare	Kundadministratör	Cegid Kundservice Nivå 1	Cegid Kundservice Nivå 2	Nivå 3: Produkt/Tekniskt stöd/Produktion	Chef för kundtjänst/chef för kundframgångar
Skicka in supportförfrågningar	R, A	I, C			
Behandling av supportförfrågningar	C, I	R, A	C	C	C
Validering av lösning på supportärenden	R, A	I			
Krishantering	C, I	R	C	C	R, A

3.1.2. Support Service Kvalitetskontroll

Följande kvalitetskontrollåtgärder har införts för att säkerställa kvaliteten på supporttjänsterna:

- Veckovis genomgång av indikatorer av Customer Care-ledningen, med förbättringsplaner och uppföljning av åtgärder;
- Granskning av omedelbara kundutvärderingar och förbättringsplaner;

- Daglig granskning av biljettköer;
- Förebyggande varningsregler i händelse av potentiell kundeskalering eller brott mot SLA som identifierats i ärendehanteringsverktyget.

3.2. Change Management Procedure

3.2.1. Hantering av versioner

Cegid Digitalrecruiters genomför dagliga uppgraderingar till Solution-versionen, inklusive implementering av patchar och nya funktioner.

All utveckling testas och en grundlig kvalificeringsprocess genomförs för varje ny version i en förproduktionsmiljö innan den lanseras i produktionsmiljön.

Cegid Digitalrecruiters genomför en rad automatiserade tester som måste vara framgångsrikt genomförda innan en ny version kan rullas ut i produktion.

3.2.2. Underhållsperioder

Cegid Digitalrecruiters åtar sig, som en del av Avtalet, att säkerställa underhållet av Lösningen under hela Avtalets löptid. Cegid Digitalrecruiters åtar sig därför att på egen bekostnad utföra alla ingrepp eller reparationer som krävs för att hålla Lösningen i perfekt funktionsdugligt skick.

Underhållsåtgärder som leder till avbrott i tjänsterna eller försämrad prestanda skall utföras:

- Utan föregående meddelande om det är absolut nödvändigt
- Med 7 dagars varsel för varje ingripande som sannolikt kommer att överstiga 30 (trettio) minuter.

3.3. Crisis Management Procedure

Syftet med krishanteringsförfarandet är att förebygga och mildra eventuella skador som orsakas av en kris genom att utlösa effektiv och regelbunden övervakning av åtgärder som inte kan hanteras med standardprocesser, för att snabbt kunna lösa krisen.

Cegids krishanteringsrutin omfattar hantering av alla typer av incidenter, inklusive sådana som påverkar tjänsten, samt säkerhetslarm. Rutinen inkluderar en eskaleringsprocess som kan eskalera incidenten till Cegids verkställande ledning. Krishanteringsförfarandet är organiserat kring ett enda gränssnitt som skapats av kundtjänstteamet.

Krishanteringsförfarandet utlöses under följande omständigheter:

- I fall av force majeure, kritiska incidenter för vilka en lösning eller patch inte har tillhandahållits inom en rimlig tidsperiod, eller om lösningens prestanda försämras under en oacceptabel tidsperiod;
- Generella blockeringsincidenter eller försämrad prestanda hos lösningen;
- Alla säkerhetsvarningar (kända eller potentiella) som äventyrar kunddata;

3.4. Contract Termination

3.4.1. Plan för reversibilitet

Avtalet föreskriver att data som lagras i Kundens databas tillhör Kunden (se abonnemangsavtalet). I händelse av uppsägning av avtalsförhållandet måste Kunden därför, före Tjänstens sista dag, återställa sina data som är tillgängliga via funktionerna i Tjänsten, eller begära från Cegid att deras data återlämnas. Cegid skickar Kunden all data och information som erhållits från Kunden som en del av genomförandet av detta avtal. För att Kunden ska kunna använda uppgifterna i fråga skickas de i ett standardiserat marknadsformat som beskrivs av reversibilitetsförfarandet.

Cegid Digitalrecruiters förbinder sig att inte lagra kopior av Kundens uppgifter och att inte använda uppgifterna för något som helst ändamål.

3.4.2. Policy för förstöring av data

Vid uppsägning av avtalet eller byte av mjukvaruplattform åtar sig Cegid att radera all kunddata (inklusive databas, URL och säkerhetskopior). Cegid ska förse kunden med ett intyg om att uppgifterna har raderats. Uppgifterna raderas 3 månader efter avtalets upphörande.

4. WEBBPLATSER FÖR VÄRDTJÄNSTER

4.1. Hosting Locations

Cegid Digitalrecruiters har för närvarande flera platser för hosting av lösningar i Europeiska unionen.

Geografiskt område	Land	Huvudläge	Tjänsteleverantör
Europa	Frankrike	Roubaix	OVHmoln
Europa	Frankrike	Strasbourg	OVHmoln
Europa	Frankrike	Gravelines	OVHmoln

4.2. Security and Confidentiality of Hosting Service Providers

Vi utvärderar och väljer våra hostingcenter baserat på strikta kriterier för säkerhet, sekretess, kvalitet och tillgänglighet.

Molnleverantören och Cegid Digitalrecruiters är bundna av ett avtal som innehåller en sekretessklausul.

Den juridiska strukturen för Cegid Digitalrecruiters är baserad i Frankrike och datacentren för våra kunder är baserade i Europeiska unionen (inklusive Frankrike). Cegid Digitalrecruiters garanterar att lösningsdata alltid kommer att finnas i Europa för alla europeiska kunder. Denna garanti gäller även för säkerhetskopior.

Våra hostingcenter har följande gemensamma egenskaper:

- Datacenter med hög redundansnivå för lösningar med hög tillgänglighet (nivå III eller motsvarande);
- Höghastighetskommunikationssystem baserat på ett helt redundant fiberoptiskt långdistansnät;
- Högsta standard för aktiv säkerhet;
- Ständigt fokus på energieffektivitet och önskan att begränsa all miljöpåverkan. De

datacenter som Cegid använder har ledande branschcertifieringar.

5. TEKNISK ARKITEKTUR

Applikationen Cegid Digitalrecruiters är baserad på en arkitektur med tre (3) nivåer:

- Användarnas arbetsstationer använder en webbläsare och måste ha tillgång till internet;
- Applikationsservrar svarar på HTTPS-förfrågningar;
- Dataservrarna är endast åtkomliga från applikationsservrarna. De är värdar för databasens sökmotorer samt kunddata.

De underliggande principerna för Cegid Digitalrecruiters tekniska arkitektur möjliggör

- Logisk separation av kunder av säkerhets-, sekretess- och tillgänglighetsskäl;
- En hög grad av anpassning av varje kunds miljö, utan att påverka andra kunder, samtidigt som programvarupaketets enhetlighet bibehålls;
- Hosting i datacenter som uppfyller Cegid Digitalrecruiters krav.

5.1. Application Architecture

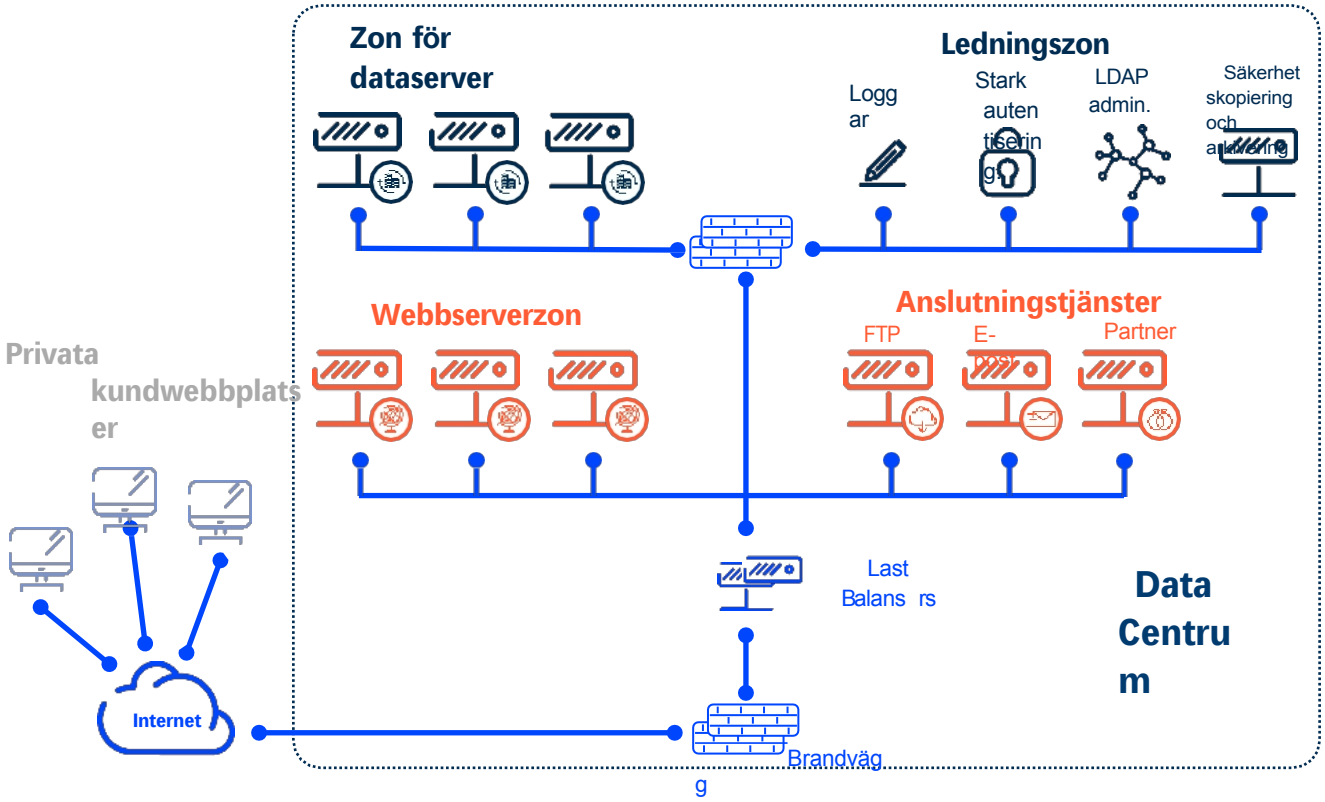
Cegids Digitalrecruiters-lösning består av flera logiska enheter som alla är integrerade i en enda applikation:

- Back Office (ATS). Detta område används främst av HR-team och chefer. Back Office används för alla rekryteringsprocesser.
- Front Offices (karriärsajter). Front Offices gör det möjligt för kandidater och anställda (via webbplatser för intern rörlighet) att se lediga jobb, ansöka och skicka in sina meritförteckningar samt registrera sig på e-postlistor. Det är möjligt att driva flera Front Offices som motsvarar flera Internet- eller Intranet-portaler, var och en med olika funktioner och grafisk profil.
- All information kan samlas i en gemensam databas.

Front Office är ett oberoende block, eftersom det är exponerat mot det publika Internet och i allmänhet utgör en del av ett företags webbplats. Som sådant kan det omkonfigureras och anpassas för kunden. Det är också kopplat till ett Back Office för att hantera kandidater, lediga jobb och ansökningar.

5.2. Server and Network Architecture

Nedan visas ett diagram över den arkitektur som används för hosting av applikationer:



Den virtualiseringsteknik som används är VMware.

Alla webbservrar är utrustade med avancerad teknik för lastbalansering. Alla databasservrar är konfigurerade med synkron replikering.

Lagrings- och arkiveringszonen är fysiskt åtskild från produktionszonen. Administrationszonen är endast tillgänglig för behöriga administratörer från Cegid Digitalrecruiters, efter en anslutning via en hoppserver och en stark autentiseringssekvens. Varje administratör använder ett namngivet konto.

Endast webbservrarna har tillgång till dataservrarna, som därför inte kan nås från Internet.

5.3. Technical Software Infrastructure

5.3.1. Infrastrukturkomponenter

Cegid Digitalrecruiters lösning har utvecklats baserat på följande tekniska arkitektur:

- Operativsystemet Linux
- MySQL Server-databas
- Nginx applikationsserver
- Programmeringsspråket PHP.

Nedan följer en sammanfattning av de viktigaste infrastrukturkomponenterna för den aktuella produktversionen:

Komponent	Produkt	Version
Operativsystem för server	Linux Debian	10 & 11
Internet-server	Nginx	
Databasmotor	MySQL	5.7
Icke-relationell databasmotor	ElasticSearch	7.4
Cache-motor	Redis	5.7.0.7
Kö-motor	RabbitMQ	3.11.5

5.3.2. Databaser för tillämpningar

En Cegid Digitalrecruiters-applikation baseras på ett kluster av multi-tenant databaser som innehåller tekniska data (konfiguration, drift, etc.) och kunddata (kandidatpool, lediga jobb, ansökningar, etc.).

Kunddata separeras logiskt och krypteras när de är i viloläge.

5.4. Multi-Customer Management

Applikationen Cegid Digitalrecruiters finns tillgänglig i form av webbplatser. För Front Office-området har varje kund sin egen subdomän, som betjänas av en enda instans av webbservern. Produkten har en multi-tenant mjukvaruarkitektur och alla subdomäner pekar på den senaste versionen av applikationen.

5.5. Test Environment

Beroende på avtalsvillkoren kan kunderna få tillgång till en testmiljö.

Testmiljön installeras och hanteras som en separat miljö från produktionsmiljön. Den hanteras som om den vore en miljö för en annan kund.

Testmiljöerna används för att testa en åtgärd eller en konfiguration, eller i utbildningssyfte. Data i testmiljön kan vara en kopia av produktionsdata från en viss tidpunkt och är i sådana fall därför äldre.

Testmiljöer har vanligtvis lägre tillgänglighet än produktionsmiljöer. Dessutom förbehåller sig Cegid Digitalrecruiters rätten att tillfälligt avbryta dessa miljöer för att utföra olika uppgifter (t.ex. installationer under arbetstid).

5.6. Mobile App

Cegid Digitalrecruiters mobilapp finns tillgänglig på två mobila plattformar: Android och iOS. Appen kan laddas ner från respektive appbutik/bibliotek.

Unik autentisering stöds så länge kunden har en identitetsleverantör på plats.

Cegid Digitalrecruiters mobilapp tillhandahåller endast ett presentationslager. Detta innebär att ingen data lagras på den mobila enheten. Personuppgifter lagras i Cegid Digitalrecruiters datacenter och kan nås i realtid via API:er.

6. TILLTRÄDESHANTERING

6.1. Application Access Security

6.1.1. Kandidatens front office

Per definition är Candidate Front Office-komponenten i lösningen tillgänglig och åtkomlig via Internet.

6.1.2. Back Office och utrymmen för anställda/chefer

Back Office-komponenten är tillgänglig och fritt åtkomlig via Internet;

6.2. Authentication

Plattformens policy för åtkomstkontroll kan vara:

- Hanteras via applikationen Digitalrecruiters: ange inloggning och lösenord.
- Delegeras till våra kunder för aktivering av en mekanism för enkel inloggning (SSO), i vilket fall kundens policy gäller.

6.2.1. Kundansvar

Om autentiseringen delegeras är kunderna ansvariga för sin egen lösenordspolicy.

6.2.2. Autentisering för kandidatens front office

Front Office-åtkomst är inte föremål för autentisering.

6.2.3. Autentisering i Back Office

Följande autentiseringsmekanismer är tillgängliga för kundanvändare:

- Använda Cegid Digitalrecruiters inloggning och lösenord;
- Använda den single sign-on (SSO) som implementerats av Kunden.

Sessionen hanteras helt och hållet på servern. Endast en sessionskaka lagras på användarens arbetsstation, och i vissa fall innehåller sidan en visningsstatus.

6.2.4. Hantering av lösenord

Cegid Digitalrecruiters rekommenderar följande policyer för lösenordshantering:

- Byte av lösenord vid första inloggningen;
- Lösenordet ska vara minst 8 tecken långt;
- Minsta antal icke-alfanumeriska, numeriska, gemener och versaler i lösenordet;
- Lösenordet återställs med hjälp av en aktiveringslänk som skickas via e-post;
- Obligatorisk validering av e-postadress innan ett konto aktiveras;

Lösenord säkras oåterkalleligt i databasen med hjälp av Bcrypt-algoritmen.

Förlorade/glömda lösenord. Användare som glömt sitt lösenord och inte använder SSO (Single Sign-On) bör gå tillväga på följande sätt:

- Använd en webbläsare för att komma åt din inloggningssida för Cegid Digitalrecruiters;
- Klicka på fältet "Glömt ditt lösenord", ange e-postadressen och klicka sedan på "BEKRÄFTA";
- Användaren kommer att få en återaktiveringslänk via e-post. Användaren måste ange ett nytt lösenord innan han/hon kan logga in i applikationen igen.

6.2.5. Enkel inloggning

Om kunden har en identitetsleverantör på plats kan användare autentiseras via single sign-on baserat på SAML 2.0-protokoll.

6.2.6. Sessionens längd

En session i Back Office-portalen avbryts efter åtta timmars inaktivitet. En session varar i tjugo timmar.

6.3. Cookie Policy

När du surfar på våra applikationer lagras cookies i användarens webbläsare. Syftet med cookies är att samla in webbläsarinformation, identifiera användare och ge dem tillgång till sina konton.

När det gäller uppgifter om cookies har Cegid Digitalrecruiters åtagit sig att följa lokala bestämmelser i varje land, skydda uppgifternas konfidentialitet och uppfylla territoriella skyldigheter när det gäller lagringsplatser för uppgifter.

Behandlingen av cookies beskrivs på följande plats:

https://www.Digitalrecruiters.com/en/privacy-policy

6.4. Roles, Rights and Accreditations

Cegid Digitalrecruiters har ett gränssnitt för administration av roller, rättigheter och ackrediteringar.

6.4.1. Roller och rättigheter

Roller används för att definiera standardprofiler med vissa nivåer av åtkomst till Cegid Digitalrecruiters funktioner. Roller definieras först och tilldelas sedan användare av Cegid Digitalrecruiters. De rättigheter som tilldelas roller är också konfigurerbara inom produkten. Roller kan omkonfigureras fullständigt med hjälp av rättighetshanteringsmodulen.

6.4.2. Ackrediteringar

Med användarackrediteringslistor kan du definiera vem som har rätt att få tillgång till informationen i en viss resurs.

7. GRÄNSSNITT

I Cegid Digitalrecruiters kan data importeras och exporteras i form av filer i CSV-format eller genom att använda Web Services.

I detta avsnitt beskrivs de bakomliggande principerna för filutbyte och Web Services, samt de säkerhetsaspekter som är involverade i dessa utbyten. Gränssnittsspecifikationer tillhandahålls i början av driftsättningsprojektet.

7.1. File Import/Export

7.1.1. Import

Cegid Digitalrecruiters lösning tillåter import med hjälp av CSV-filer för följande funktioner:

- Import av ansökningar;
- Import av organisationens trädstruktur;
- Import av användare;

Implementeringen av dessa importer beskrivs i sin helhet i särskilda dokument och avtalas med Cegid Digitalrecruiters team när lösningen rullas ut.

7.1.2. Export

Cegid Digitalrecruiters lösning tillåter export till CSV-filer för följande data:

- Organisatorisk trädstruktur;
- Statistik.

7.2. Secure FTP Interface

Om så krävs kommer implementeringen av en filutbytesplattform att arrangeras med Cegid Digitalrecruiters team när lösningen rullas ut.

7.3. Application Programming Interfaces (API)

Cegid tillhandahåller ett visst antal webbtjänster som gör det möjligt för tredje parts applikationer att använda Cegid Digitalrecruiters tjänster. Dessa webbtjänster täcker följande funktionella domäner:

- Export av rekryterade kandidatansökningar;
- Tillägg av annonser på karriärsidan;
- Export av platsannonser;
- Antal platsannonser per avdelning;
- Ändring av platsannonser;
- Import av ansökningar;
- Export av applikationer.

Implementeringen av dessa API:er beskrivs i sin helhet i särskilda dokument och avtalas med Cegid Digitalrecruiters team när lösningen rullas ut.

7.4. Email Interface

Applikationen Cegid Digitalrecruiters skickar e-post med hjälp av standardprotokollet SMTP. E-postmeddelanden kan skickas i HTML-format.

8. VERKSAMHET

8.1. Operating Procedures

I detta avsnitt beskrivs de vanligaste arbetsprocedurerna under service.

Rensning av systemloggar. Systemloggar sparas i nittio (90) dagar.

Rensning av applikationsloggen. Applikationsloggen innehåller spårningsdata för användarens åtgärder.
Denna logg lagrar ett (1) års data. Äldre data rensas bort.

8.2. Data Management

8.2.1. Säkerhetskopiering av data

Detta avsnitt gäller för produktionsdata.

Organisation av säkerhetskopiering

Säkerhetskopiering av de olika typerna av data sker utifrån en strategi som optimerar dataintegritet och säkerhet samt återställningstid. Säkerhetskopieringen sker online utan avbrott i databastjänsten.

Data	Åtgärder	Frekvens	Bevarande
Virtuella maskiner	Komplett säkerhetskopia	Varannan timme	14 dagar
Databas	Komplett säkerhetskopia	Var 24:e timme	30 dagar
Databas	Partiell säkerhetskopiering	Varannan timme	24 timmar
NAS	Fullständig replikering	En gång per dag	-
Loggar	Komplett säkerhetskopia	En gång per dag	3 månader

Medier och platser för säkerhetskopiering beror på molnleverantören:

	Lagring av säkerhetskopior	Replikering av data
OVHmoln	Objektlagring	Krypterade data replikeras av Object Storage-tjänsten i olika geografiska områden.

Endast ett mycket begränsat antal personer har tillgång till säkerhetskopiorna av databasen. Dessa personer, liksom all Cegid-personal, är bundna av en sekretessklausul. Vår molnleverantör har också ett begränsat antal personer som är behöriga att få tillgång till säkerhetskopior.

8.2.2. Kryptering av data

Kryptering av data under överföring

För att garantera säkerheten för data under överföring krypterar Cegid applikationsflödet med HTTPS-protokollet för alla domäner och kräver TLS-protokollet (Transport Layer Security) 1.2 eller högre.

Kryptering av data i vila
Lösenord säkras oåterkalleligt i databasen med hjälp av Bcrypt-algoritmen. Cegid

tillhandahåller AES-XTS-kryptering av volymer.

8.3. Administration and Supervision

Plattformen övervakas 24 timmar om dygnet, 7 dagar i veckan. Prestandaövervakning och applikationsövervakning finns på plats och kommer att utlösa varningar om problem upptäcks.

Ett förfarande för hantering och eskalering har definierats och följs av de operativa teamen.

De verktyg som används för övervakning av infrastrukturen är Splunk Observability och Centreon. Våra hostingleverantörer har också sina egna övervakningssystem.

Driftsrutinerna omfattar, men är inte begränsade till, följande uppgifter:

- Administration;
- Underhåll av operativsystemen (diskutrymme, loggar etc.);
- Underhåll av databas;
- Tester, kvalificering och lansering av säkerhetsuppdateringar;
- Underhåll av applikationer (loggar och prestandaanalys);

Övervakning:

- Övervakning av applikationernas tillgänglighet;
- Övervakning av svarstiden;
- Övervakning av plattformens belastning (minne, processorer, enheter);
- Övervakning av nätverkets bandbredd;
- Övervakning av batchuppgifter för applikationer och system;
- Övervakning av hårdvara.

Hostingleverantörer ansvarar för de uppgifter som är förknippade med följande:

- Fysisk utrustning (serverhårdvara, nätverksutrustning etc.);
- Hypervisorer;
- Nätverk;
- Programuppdateringar för operativsystem, databaser och antivirusprogram;
- Övervakning av ovanstående;
- Verifiering och kvalificering av säkerhetskopior;
- Övervakning och uppdatering av antivirussystem;
- Underhåll av nätverksutrustning.

8.4. Business Continuity Plan

En produktionsinfrastruktur med hög tillgänglighet finns på plats, baserad på en uppdelning av tjänsterna, där varje tjänst säkerställs av ett kluster av oberoende servrar, vilket garanterar infrastrukturens motståndskraft. Om en maskin (eller flera maskiner samtidigt) skulle sluta fungera kommer de andra servrarna i klustret tillfälligt att absorbera den extra arbetsbelastningen, vilket säkerställer kontinuitet i tjänsten.

Denna organisation erbjuder också en skalbar infrastruktur med möjlighet att enkelt öka kapaciteten genom att distribuera nya maskiner efter behov. För maximal effektivitet används verktygen Ansible, Chef och Terraform för att automatisera driftsättning och konfiguration av ytterligare maskiner.

9. FÖRORDNINGAR OCH STANDARDER

9.1. General Data Protection Regulation (GDPR)

Nedan finner du en beskrivning av de tillämpliga åtgärderna enligt GDPR för att hjälpa kunder i deras GDPR-efterlevnad med Cegid Digitalrecruiters.

Viktigt: Alla datasäkerhetselement beskrivs i Security Assurance Plan eller i andra delar av detta dokument; de nämns därför inte här. De är dock alla relaterade till GDPR i den meningen att datasäkerhet är ett centralt krav för alla personuppgiftsbiträden.

För att implementera GDPR-kraven i sin lösning skiljer Cegid Digitalrecruiters, som personuppgiftsbiträde, mellan två olika personas: kandidater och anställda. Vissa av kraven i GDPR är inte beroende av personas, och vissa av dem resulterar i olika produktbeteenden beroende på om de riktas till en kandidat eller en anställd.

9.1.1. GDPR-krav som gäller för alla personas

Respekt för privatlivet redan från designstadiet

Den nuvarande agila utvecklings- och programvaruprocessen omfattar personalutbildning, formella kodgranskningar och verktyg som upptäcker behovet av att tillämpa bästa praxis.

Principerna för behandling av personuppgifter enligt definitionen i artikel 5 i GDPR beaktas av designen i produktutvecklingen.

Sekretess som standard

Som standard är dataskyddsnivån alltid inställd på den mest restriktiva nivån.

Ombud för dataskydd

Cegid har utsett ett dataskyddsombud med tanke på verksamhetens art.

Registrering av bearbetningsaktiviteter

Cegid för register över behandlingar i egenskap av personuppgiftsbiträde.

Dataskyddsmyndigheter med efterföljande personuppgiftsbiträden

Cegid delegerar en del av sin verksamhet till underleverantörer. Cegid undertecknar dataskyddsavtal med dessa underleverantörer, som innehåller klausuler som är förenliga med GDPR.

Känsliga uppgifter

Cegid Digitalrecruiters samlar inte in känsliga uppgifter, såsom de som nämns i artikel 9 i GDPR. Eftersom Cegid Digitalrecruiters erbjuder en viss flexibilitet i de tillägg som finns tillgängliga för datamodellen, rekommenderar Cegid inte sina kunder att definiera ytterligare fält som motsvarar "känsliga uppgifter", enligt definitionen i artikel 9 i GDPR.

Anmälan av dataintrång

Cegid har upprättat en rutin för anmälan av dataintrång. Detta förfarande definieras, underhålls och övervakas inom ramen för ledningssystemet för informationssäkerhet och GDPR.

I händelse av personuppgiftsincident åtar sig Cegid att så snart som möjligt underrätta kunden (den personuppgiftsansvarige) enligt GDPR, så att kunden därefter inom 72 timmar kan anmäla personuppgiftsincidenten till relevant tillsynsmyndighet och den registrerade, om sådan anmälan är obligatorisk. Det är upp till kunden att bedöma om en sådan anmälan till tillsynsmyndigheten och/eller den registrerade är nödvändig.

Automatiserad beslutsprocess

Applikationen Cegid Digitalrecruiters innehåller inte något automatiserat individuellt beslutsfattande eller någon automatiserad profileringsfunktion. Alla beslut fattas av mänskliga användare, som kan använda dashboards, KPI:er, rekommendationer och analyser för att fatta ett välgrundat beslut.

Anonymisering av uppgifter

Cegid Digitalrecruiters erbjuder en anonymiseringsfunktion för "komplett databas". Den används när en Produktionsdatabasen ska användas för testning, felsökning eller utbildning.

Information som ska tillhandahållas när personuppgifter samlas in från den registrerade

Det är kundens ansvar att tillhandahålla denna information direkt till sina kandidater och anställda. Vår lösning ger våra kunder möjlighet att tillhandahålla denna information via en konfiguration.

9.1.2. Svar på GDPR:s krav på kandidater

Kandidater har ingen hierarkisk relation till den potentiella arbetsgivaren, som är den personuppgiftsansvarige. Av denna anledning har vi definierat alla möjliga databehandlingsmetoder som används av produkten.

Rätt till tillgång, rätt till rättelse

Kandidater kan skicka ett e-postmeddelande till kundadministratören (eller dataskyddsombudet för den personuppgiftsansvarige) för att begära radering eller rättelse av sina personuppgifter. Kundadministratören (eller dataskyddsombudet) kan kontakta Cegids kundtjänstteam för hjälp. En rekryterare kan också radera eller korrigera en kandidats personuppgifter om det behövs.

Rätten att bli bortglömd

Rätten till radering kan automatiseras per organisatorisk enhet:

- Detta gör det möjligt för kunderna att hantera datalagringsperioder per land.
- I slutet av lagringsperioden får kandidaterna ett e-postmeddelande där de tillfrågas om de vill ge sitt samtycke till att förlänga lagringen av deras personuppgifter.
- Om en kandidat skickar in jobbansökningar i flera länder med olika lagringsperioder, kommer den tillämpliga lagringsperioden att vara den som gäller för den organisation som är involverad i den senaste ansökningsåtgärden. Om kandidaten ger sitt samtycke till att förlänga lagringstiden för sina personuppgifter, kommer deras personuppgifter att lagras i back office. Om den sökande inte ger sitt samtycke kommer dennes personuppgifter att raderas. Om den sökande inte svarar kommer dennes personuppgifter att raderas i slutet

av lagringsperioden.

Personuppgifter raderas asynkront under schemalagda nattprocedurer.

Rättslig grund

Den personuppgiftsansvarige är skyldig att fastställa den lämpligaste rättsliga grunden för sitt sammanhang (artikel 6.1 i GDPR) innan Cegid Digitalrecruiters-lösningen tas i produktion.

I informationssyfte, för att hjälpa till att fastställa de rättsliga grunderna, antog den franska dataskyddsmyndigheten (CNIL) ett referensdokument "*om behandling av personuppgifter som används för personalhantering*" den 21 november 2019.

I detta referensdokument föreslår CNIL 2 rättsliga grunder som rör rekrytering:

-"***Behandling av ansökningar (CV och personligt brev) och företagsledning**: Åtgärder före avtalets ingående*

***-Skapande av ett CV-bibliotek**: Berättigat intresse*"

All överföring av uppgifter inom koncernen måste också motiveras med en rättslig grund och meddelas kandidaterna.

9.1.3. Svar på GDPR:s krav på anställda

Rätt till tillgång, rätt till rättelse

Produkten tillhandahåller de nödvändiga funktionerna för att komma åt och ändra anställdas data. Åtkomsten till dessa funktioner styrs av roller och rättigheter som kan tilldelas direkt av kundadministratörerna.

Rätt till radering

Av olika skäl samlar företag in och behandlar personuppgifter om sina anställda. En begäran om radering av personuppgifter från en anställd måste godkännas av arbetsgivaren (den personuppgiftsansvarige).

Av denna anledning erbjuder vår produkt en raderingsfunktion i Cegid Digitalrecruiters användargränssnitt. Denna funktion är föremål för en specifik rättighet, som kan tilldelas av kundadministratörer till de berörda användarna. För närvarande raderar produkten databasen fysiskt och oåterkalleligt.

Rättslig grund

Den personuppgiftsansvarige är skyldig att fastställa den lämpligaste rättsliga grunden för sitt sammanhang (artikel 6.1 i GDPR) innan Cegid Digitalrecruiters-lösningen tas i produktion.

I samma *CNIL-referensdokument* som citeras ovan ("*Référentiel relatif aux traitements de données personnelles mise en œuvre aux fins de gestion du personnel*" (referensdokument om behandling av personuppgifter som används för personaladministration) av den 21 november 2019) anger CNIL följande när det gäller samtycke: "*Anställda är sällan i stånd att fritt ge, vägra eller återkalla sitt samtycke, med tanke på maktobalansen i förhållandet mellan arbetsgivare och anställd. De kan endast ge sitt fria samtycke om godkännandet eller avvisandet av ett förslag inte har några konsekvenser för*

deras situation".

CNIL föreslår därför andra rättsliga grunder för anställda beroende på verksamhet. Detta dokument innehåller en tabell som hjälper den personuppgiftsansvarige att fastställa dessa rättsliga grunder.