cegid

Terms of Service

Leistungsausführung

Cegid Digitalrecruiters

23.11.2023

www.cegid.com

INHALTSVERZEICHNIS

VERLAUF VON ÄNDERUNGEN UND VALIDIERUNGEN

Erstellung des Dokuments	1.0	04.04.2023

Prüfende Person(en)

24.11.2023	Alexandre Blanc & Pauline Hubert Solution Architect Cegid HCM
24.11.2023	Myriam Hétier, Leiterin Produktmarketing Cegid HCM

Freigebende Person(en)

24.11.2023	Stephan Latrille, CTO Digital Recruiters a Cegid Company

Verteiler

Person oder Gruppe
Digital Recruiters Kunden
Digital Recruiters Intern

1. EINFÜHRUNG

1.1. Zweck des Dokuments

Die Leistungsbeschreibung ist zentraler Bestandteil des Vertrags und erläutert die besonderen Bestimmungen, die für die Digitalrecruiters Services gelten.

Dieses Dokument beschreibt die ergriffenen Maßnahmen zur Sicherstellung:

- der Qualität des von Cegid geleisteten Supports
- der Qualität der Nachverfolgungs- und Eskalationsprozesse für Anfragen während der „AUSFÜHRUNGS"-Phase nach dem Projekt („Build"-Phase).
- Support RACI
- Beschreibt die technische Architektur der Cegid Talentsoft Applikation, sowohl für die gemeinsame Kunden-Infrastruktur als auch für die kundenspezifische Infrastruktur.

Dieses Dokument wird immer dann aktualisiert, wenn sich die technische Umgebung für Cegid Talentsoft ändert.

1.2. Änderung des Dokuments

Jede Änderung an dem Dokument führt zu einer neuen Version dieses Dokuments. Änderungen werden im Verlauf der Änderungen am Anfang des Dokuments vermerkt und datiert.

Eine geringfügige Änderung führt nicht unbedingt dazu, dass sofort eine neue Version des Dokuments herausgegeben wird. Diese Änderung wird in die nächste Version des Dokuments eingearbeitet.

Jede Änderung des Dokuments muss Teil des Dokuments sein und ist für die Parteien gleichermaßen verbindlich.

Im Falle einer Änderung des Dokuments gilt die auf der offiziellen Website von Cegid veröffentlichte Version als Referenz. Die dem Kundenvertrag beigefügte Version dient der Überprüfung, dass es keine Rückschritte gibt, wie im Vertrag bereits beschrieben.

Das Dokument wird mindestens einmal im Jahr überprüft. Diese Überprüfung kann zu einer neuen Version des Dokuments führen.

2. BESCHREIBUNG DES SUPPORTS

2.1. Support-Standorte

Die Support-Teams der Kundenbetreuung von Cegid Digitalrecruiters befinden sich in Frankreich (Boulogne-Billancourt), Kanada (Montreal), Rijswijk (Niederlande) und Deutschland (Köln). Support-Anfragen können auf Deutsch, Französisch, Englisch und Niederländisch erfolgen.

Support-Tickets müssen über das Help Center Zendesk erstellt werden. Hierbei handelt es sich um Ticketing-Tool, einem Support-Tool, das allen Kunden mit einem Supportvertrag über das Internet zur Verfügung steht.

2.2. Supportvertrag

Cegid Digitalrecruiters bietet dem Kunden technischen Support, um funktionale oder technische Fragen zu klären, wozu insbesondere Anfragen folgender Art gehören: Unterstützung, Beratung, Meldung von (kleineren, größeren, blockierenden) Anomalien.

Der technische Support ist in dem Angebot von Cegid Digitalrecruiters enthalten. Alle sonstigen und weiteren Unterstützungsleistungen müssen Gegenstand eines gesonderten Vertrages auf Basis eines von Cegid Digitalrecruiters erstellten Kostenvoranschlags sein.

2.3. Zugriff auf die Anwendungsressourcen

Der Support-Bereich der Cegid Digitalrecruiters Applikation bietet Nutzern zahlreiche Artikel, die ihnen bei der Nutzung der Lösung zu folgenden Themen helfen können:

- Karriere-Webseiten
- Veröffentlichung und Verbreitung von Anzeigen
- Verwaltung von Bewerbungen
- Einstellungen
- Verwaltung von Nutzern
- Rechtliches und DSGVO
- Back Office
- FAQs und Tipps

2.4. Support-Bereiche

Die Geschäftszeiten des Kundenservices sind von Montag bis Freitag 08:30 Uhr bis 18:30 Uhr MEZ und 9:00 Uhr bis 17:00 Uhr EST. Der Support ist über ein Ticketing-Tool, das Cegid Digitalrecruiters innerhalb der Lösung bereitstellt, erreichbar.

Für eine effiziente Bearbeitung muss eine festgestellte Anomalie dem Support unbedingt schriftlich über das innerhalb der Lösung bereitgestellte technische Support-Tool gemeldet werden.

In der Meldung der Anomalie sind der Kontext und das Verfahren für die Reproduktion der Anomalie (außer wenn dies unmöglich ist) zu beschreiben. Nach der Meldung wird innerhalb des vom Support-Team bei Cegid Digitalrecruiters verwendeten Follow-up-Tools automatisch ein Ticket erstellt. Das Ticket beinhaltet die Informationen des Nutzers der Lösung sowie das Datum und die Uhrzeit der Anomaliemeldung.

Sobald die Anomaliemeldung eingegangen ist, ordnet das Support-Team diese einen Kritikalitätsgrad, wie in Kapitel 2.6 beschrieben, zu.

Im Anschluss wird die Lösung der Anomalie umgesetzt:

- Analyse der Anfrage oder Anomalie und gegebenenfalls Reproduktion
- Im Falle einer technischen Anomalie, Eskalation des Tickets durch die Kundenbetreuung an das Produkt-Team von Cegid Digitalrecruiters
- Erstellung eines Jira-Tickets durch das Produkt-Team, das mit dem Zendeck-Ticket verbunden wird
- Entwicklung des Patches durch Cegid Digitalrecruiters
- Tests in einer Entwicklungsumgebung durch einen Projektmanager von Cegid Digitalrecruiters
- Tests in einer Test-Umgebung durch einen Projektmanager von Cegid Digitalrecruiters
- Online-Bereitstellung des Patches durch Cegid Digitalrecruiters

2.5. Ticket- Workflow zwischen Kunden und Cegid

Die Tabelle unten erklärt die unterschiedlichen Status von Zendesk (Ticketing-Tool) mit dem entsprechenden Verantwortlichen für die Weiterbearbeitung des Tickets.

Status	Definition	Verantwortliche Person
Neu	Das Ticket wird vom Kunden erstellt und an Cegid gesendet. Dieser Status wird von Zendesk bei der Erstellung des Tickets automatisch aktualisiert.	*Cegid*
Offen	Das Ticket wird von Cegid bearbeitet. Dieser Status wird von Zendesk aktualisiert, sobald der Mitarbeiter *Kundenbetreuung* das Ticket analysiert hat und dem Kunden eine erste qualifizierte Antwort gibt.	*Cegid*
In Wartestellung	Das Ticket wurde vom Mitarbeiter *in der Kundenbetreuung* qualifiziert, erfordert aber weitere Informationen oder eine Validierung des Kunden. Das Ticket wartet auf die Rückmeldung des Kunden. Ein Ticket in Wartestellung bleibt 5 Tage in diesem Status, bevor es in den Status ‚Geklärt' wechselt, wenn keine Rückmeldung erfolgt.	*Kunde*
Geklärt	Dem Kunden wurde eine Antwort gegeben, das Problem wird als geklärt angesehen. Der Kunde kann das Ticket erneut eröffnen. Ein geklärtes Ticket bleibt 2 Tage in diesem Status, bevor es in den Status ‚Geschlossen' wechselt, wenn keine Rückmeldung erfolgt.	*Kunde/Cegid*
Geschlossen	Das Ticket ist geschlossen und kann nicht erneut eröffnet werden. Es ist möglich, ein Follow-up-Ticket zu erstellen.	Cegid

2.6. Vertragliche Definition von Anomalien & SLA-Richtlinie

2.6.1. Definitionen

Eine Anomalie bezieht sich auf alle Ausfälle, Vorfälle, Störungen oder ungewöhnlichen Verhaltensweisen, die vom erwarteten Verhalten, wie von der Lösung dokumentiert, abweichen. Die vollständige oder teilweise Verfügbarkeit der Anwendung oder eine Verschlechterung der Leistung, die die Nutzung der Lösung stört oder unterbricht, gilt ebenfalls als Anomalie.

Es gibt drei verschiedene Schweregrade:

Blocking Anomaly (systemkritischer Fehler):

- Störungen, die es unmöglich machen, grundlegende Aufgaben durchzuführen, die zu einer Unterbrechung der HR-Geschäftstätigkeit führen
- Störungen, die nicht umgangen werden können
- Unterbrechungen bei Funktionstests und insbesondere Anomalien, die:
    - Daten oder ihre Konsistenz verändern
    - den Ablauf der Geschäftsprozesse blockieren
    - nicht nutzbare Ergebnisse für Geschäftsprozesse liefern

Major Anomaly (erheblicher Fehler):

- Störungen, die es unmöglich machen, eine Aufgabe durchzuführen, für die es aber Workaround-Lösungen gibt:
    - Das System kann auch mit verminderter Funktionsqualität verwendet werden.
    - Die Anomalie stört die Ausführung der Aktion, hält Benutzer aber nicht davon ab, die anderen Funktionen testen zu können

Minor Anomaly (kleiner Fehler):

- Störungen, für die es Workaround-Lösungen gibt und die keine anderen Funktionen beeinträchtigen:
    - Die Auswirkungen auf die Nutzung der Anwendung sind unerheblich
    - Beispiele: Anomalien, die die Ergonomie des Systems verändern

2.6.2. Cegid-Standard-SLA für Cegid Digitalrecruiters

Dauer für die Behebung von Anomalien

Für die Behebung von Anomalien gelten folgende Zeiten:

- Blocking Anomalie: maximal innerhalb von 1 Werktag
- Major Anomalie: maximal innerhalb von 2 Werktagen
- Minor Anomalie: innerhalb von 30 Werktagen oder bei einem nächsten kleineren Update der Applikation je nach Art der Störung

Cegid Digitalrecruiters kann in folgenden Fällen nicht zur Verantwortung gezogen werden, wenn die Zeit für die Klärung einer Störung überschritten wird:

- Der Kunde weigert sich, bei der Klärung von Anomalien mitzuwirken und insbesondere Fragen zu beantworten und angeforderte Auskünfte zu liefern
- Die Lösung wird nicht, wie in der Dokumentation beschrieben, genutzt
- Der Kunde hat eine nicht autorisierte Änderung der Lösung vorgenommen
- Der Kunde hat gegen seine Vertragspflichten verstoßen
- Es wurden Software-Pakete, Software oder Betriebssysteme genutzt, die mit der Lösung nicht kompatibel sind
- Die Anomalie resultiert aus einer Fehlfunktion in Zusammenhang mit einer Lösung eines Dritten oder Partners

2.6.3. Allgemeine Verfügbarkeit

Die Lösung ist monatlich zu 99,5 % rund um die Uhr an 7 Tagen pro Woche verfügbar. Die Verfügbarkeit wird außerhalb der geplanten Wartungszeiten gemessen.

Die Verfügbarkeit des Service wird anhand der Überwachung durch ein Drittunternehmens gemessen. Ein Verfügbarkeitstest für den Service wird jede Minute von verschiedenen Quellen im Internet in Netzen verschiedener Internet-Betreiber durchgeführt.

Die monatliche Nichtverfügbarkeitsdauer (Englisch: Down Time = DT) wird wie folgt berechnet:

DT (Minuten) = Kumulierte Dauer der Nichtverfügbarkeit des Service in Minuten während des Monats

Die monatliche Gesamtverfügbarkeit (Englisch: Overall Monthly Available Time = AT) wird wie folgt berechnet:

AT (%) = [1- (DT / (Anzahl Tage im Monat * 1440))] x 100

Die Verfügbarkeitsstatistiken werden dem Kunden auf Anfrage mitgeteilt.

3. WARTUNGSPROZESS IN DER RUN-PHASE

3.1. Verfahren für den Umgang mit Vorfällen (Incidents)

Support-Anfragen folgen dem nachfolgend beschriebenen Verfahren. Je nach Art der Anfragen können die Schritte 2 bis 5 die letzten Schritte des Workflows sein.

Schritt	Handlung	Maßnahme
1	Kunde	Anfrage erstellen
2	Level 1 – Kundenbetreuung	Anfrage einstufen / Weitere Informationen einholen
3	Level 1 – Kundenbetreuung	Qualifikation von komplexen Themen
4	Level 2 – Technischer Support	Technische Analyse
5	Level 3 – F&E	Korrekturmaßnahme
6	Level 1 – Kundenbetreuung	Bestätigung der Behebung

3.1.1. RACI-Matrix für Support-Aktivitäten

- **R**: *Verantwortliche Person*
- **A**: *Zuständige oder freigebende Person*
- **C**: *Hinzugezogene Person*
- **I**: *Informierte Person*

Aktivitäten/Akteure	Administrator des Kunden	Kundenbetreuung Cegid Level 1	Kunden-betreuung Cegid Level 2	Level 3: Produkt / Technischer Support / Produktion	Kundenbetreuer / Customer Success Manager
Meldung von Anfragen	R, A	I, C			
Bearbeitung des Incidents	C, I	R, A	C	C	C
Validierung der Lösung	R, A	I			
Krisenmanagement	C, I	R	C	C	R, A

3.1.2. Servicequalitätskontrolle

Mehrere Kontrollmaßnahmen bestehen, um die Servicequalität zu gewährleisten:

- Wöchentliche Prüfung der Indikatoren durch die Leitung der Kundenbetreuung mit Verbesserungsplänen und Nachverfolgung der Maßnahmen
- Prüfung von Kundenzufriedenheitsumfragen und Verbesserungsplänen

- tägliche Prüfung von Ticket-Warteschlangen
- präventive Benachrichtigungsregeln, wenn eine potenzielle Kundeneskalation oder SLA-Verletzung im Ticketing-Tool erkannt wurde

3.2. Verfahren für das Change-Management

3.2.1 Versionierung

Cegid Digitalrecruiters führt täglich ein Versions-Update der Lösung durch, zu dem die Bereitstellung von Patches und neuen Funktionalitäten gehört.

Jede Entwicklung wird getestet. Ein strenger Qualifikationsprozess wird für jede Version auf einer Vor-Produktionsplattform genutzt, bevor die Implementierung auf der Produktionsplattform erfolgt.

Cegid Digitalrecruiters verwendet zahlreiche automatische Tests, die erfolgreich bestanden werden müssen, bevor die neue Version implementiert werden kann.

3.2.2 Wartungszeiten

Cegid Digitalrecruiters verpflichtet sich vertraglich, die Wartung der Lösung während der gesamten Vertragslaufzeit zu gewährleisten. Cegid Digitalrecruiters verpflichtet sich dazu, auf eigene Kosten sämtliche notwendigen Eingriffe oder Reparaturen durchzuführen, um den einwandfreien Funktionszustand der Lösung zu erhalten.

Wartungsarbeiten, die zu einer Unterbrechung der Dienste oder zu einer Beeinträchtigung der Leistung führen, werden wie folgt durchführt:

- Ohne Vorankündigung bei absoluter Notwendigkeit
- Mit einer Vorankündigung von 7 Tagen bei Arbeiten, die möglicherweise länger als 30 Minuten dauern

3.3. Verfahren für das Krisenmanagement

Ziel des Verfahrens für das Krisenmanagement ist es, den Schaden durch die Krise zu verhindern und abzumildern, indem eine effiziente und regelmäßige Nachverfolgung von Maßnahmen eingeleitet wird, die nicht über Standardprozesse behandelt werden können, um die Krise schnell zu lösen.

Das von Cegid befolgte Verfahren für das Krisenmanagement beinhaltet die Bearbeitung aller Arten von Vorfällen, einschließlich jener, die den Service beeinträchtigen, sowie Sicherheitswarnungen. Das Verfahren umfasst einen Eskalationsprozess, der den Incident bis zur Cegid Geschäftsführung eskalieren kann. Das Verfahren für das Krisenmanagement ist um eine zentrale Schnittstelle organisiert, die vom Kundenservice-Team erstellt wurde.

Die Krisenmanagementprozesse werden unter folgenden Umständen ausgelöst:

- bei höherer Gewalt, bei blockierenden Incidents, bei denen ein Workaround oder ein Patch nicht innerhalb einer vertretbaren Zeit geliefert werden kann, oder bei länger anhaltenden Leistungsverschlechterungen von unvertretbarer Dauer;
- bei allgemeinen Blockaden oder Verschlechterungen

- bei (bekannten oder potenziellen) Sicherheitswarnungen, bei denen Kundendaten in Gefahr sind.

3.4. Vertragsende

3.4.1. Reversibilitätsplan

Der Vertrag besagt, dass Daten, die in der Datenbank des Kunden gespeichert sind, dem Kunden gehören (siehe Abonnementvertrag). Bei einer Einstellung der Vertragsbeziehungen muss der Kunde also vor dem letzten Tag des Dienstes seine Daten, die über die Funktionalitäten des Dienstes zugänglich sind, zurückholen oder Cegid um die Rückgabe seiner Daten bitten. Cegid nimmt im Rahmen der Durchführung des vorliegenden Vertrages eine Rückübertragung aller vonseiten des Kunden empfangenen Daten und Informationen an den Kunden vor. Damit der Kunde die betreffenden Daten verwerten kann, werden die Daten in einem marktüblichen Standardformat, das im Reversibilitätsverfahren beschrieben ist, zurückübertragen.

Cegid Digitalrecruiters verpflichtet sich, keine Kopien der Daten des Kunden zu behalten und die Daten zu keinerlei Zwecken zu verwenden.

3.4.2. Richtlinie zur Datenvernichtung

Bei einer Kündigung des Vertrages oder einer Änderung der Software-Plattform verpflichtet sich Cegid, alle Daten des Kunden zu löschen (einschließlich Datenbank, URL und Backups). Cegid liefert dem Kunden eine Bestätigung über die Vernichtung der Daten. Die Daten werden 3 Monate nach dem Ende des Vertrages gelöscht.

4. HOSTING

4.1. Hosting-Orte

Cegid Digitalrecruiters verfügt zurzeit über mehrere Hosting-Standorte auf dem Gebiet der Europäischen Union.

Geografische Region	Land	Hauptort	Anbieter
Europa	Frankreich	Roubaix (Strasbourg/Gravelines)	OVHCloud

4.2. Hosting-Anbieter: Sicherheit und Geheimhaltung

Unsere Hosting-Zentren werden von uns nach strengen Sicherheits-, Geheimhaltungs-, Qualitäts- und Verfügbarkeitskriterien bewertet und ausgewählt.

Der Cloud-Provider und Cegid Digitalrecruiters sind durch einen Vertrag gebunden, der eine Geheimhaltungsklausel umfasst.

Der Sitz von Cegid Digitalrecruiters befindet sich in Frankreich, und die Rechenzentren für Kunden befinden sich in der Europäischen Union (Frankreich). Cegid Digitalrecruiters garantiert, dass sich die Daten aller europäischen Kunden stets in Europa befinden. Diese Garantie gilt auch für Backups.

Unsere Hosting-Zentren haben die folgenden gemeinsamen Merkmale:

- Rechenzentren, die mit einem hohen Maß an Redundanz für extrem hochverfügbare Lösungen ausgelegt (Tier 3 oder gleichwertig) ausgelegt sind
- ein Hochgeschwindigkeits-Kommunikationssystem, das auf einem Netzwerk voll redundanter, langer Glasfaserstrecken aufgebaut ist
- die höchsten Standards an aktiver Sicherheit
- kontinuierliche Bestrebungen rund um Energieeffizienz und Verringerung jeglicher Umweltbelastungen

Die von Cegid genutzten Rechenzentren besitzen solide Zertifizierungen.

Mehr Informationen zu den Zertifizierungen von OVH-Cloud: https://www.ovhcloud.com/de/enterprise/certification-conformity/

5. TECHNISCHE ARCHITEKTUR

Die Cegid Talentsoft Anwendung basiert auf einer dreistufigen Architektur (3 Tier):

- Die Arbeitsstationen der Benutzer nutzen einen Internetbrowser und müssen über einen Internetzugang verfügen.
- Anwendungsserver antworten auf HTTPS-Anfragen.
- Die Datenserver sind nur von den Anwendungsservern aus erreichbar. Sie hosten die Datenbank-Suchmaschinen sowie die Kundendaten.

Die zugrunde liegenden Grundsätze der technischen Architektur von Cegid Talentsoft ermöglichen:

- eine Abgrenzung von Kunden für die Zwecke der Sicherheit, Geheimhaltung und Verfügbarkeit
- umfangreiche Konfigurationsmöglichkeiten jeder Kundenumgebung ohne Auswirkungen auf andere Kunden sowie die gleichzeitige Beibehaltung der Einheitlichkeit des Softwarepakets
- das Hosting in Rechenzentren, die die Cegid-Anforderungen erfüllen

5.1. Applikationsarchitektur

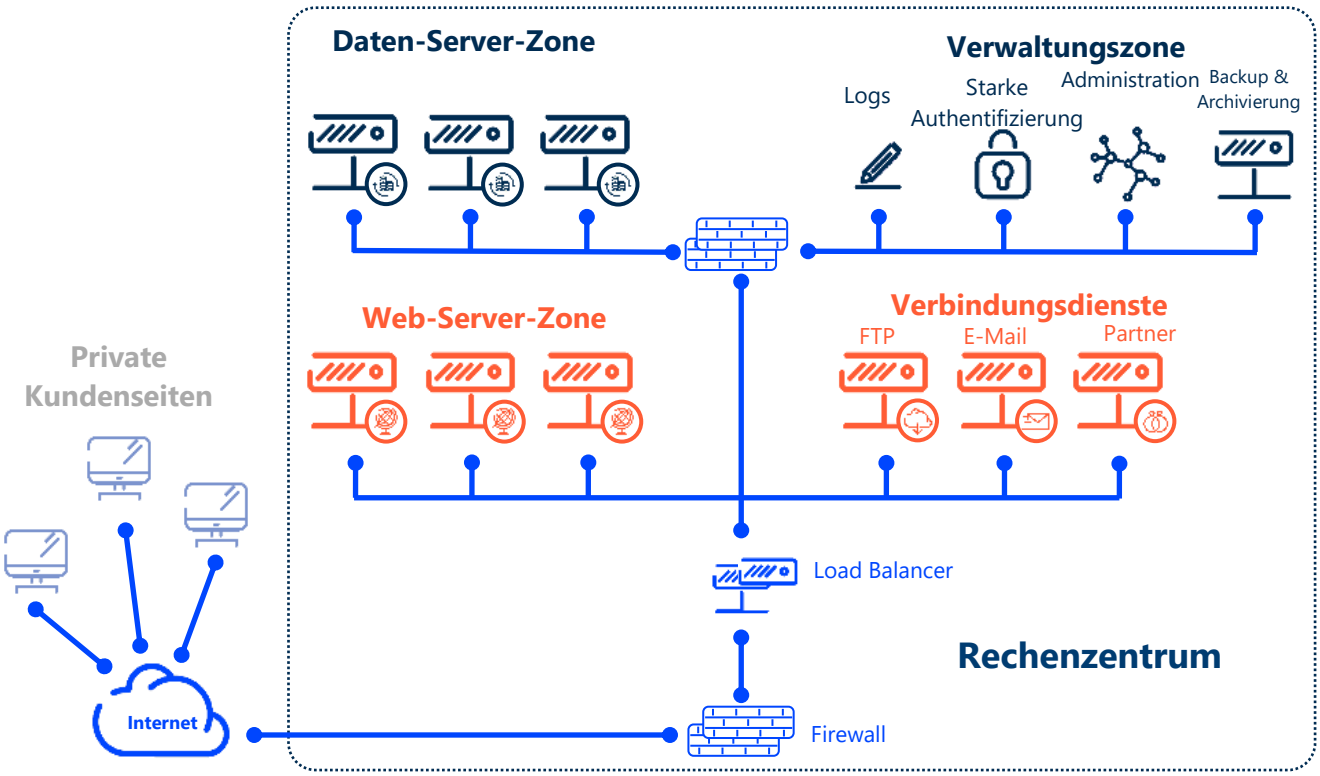
Die Cegid Digitalrecruiters Lösung setzt sich aus mehreren logischen Einheiten zusammen, die allesamt in einer einzigen Anwendung integriert sind:

- Back Office (ATS). Dieser Teil wird hauptsächlich von den HR-Teams und Führungskräften verwendet. Das Back Office wird für alle Rekrutierungsprozesse genutzt.
- Front Office (Karriereseiten). Über die Front Offices können Bewerber und Beschäftigte (interne Mobilitätsseiten) Stellenangebote einsehen, sich bewerben und ihre Lebensläufe einsenden sowie sich in Verteilerlisten eintragen. Es ist möglich, mehrere Front Offices zu implementieren, die mehreren Internet- oder Intranet-Portalen entsprechen, wobei jeweils andere Funktionalitäten und grafische Konzepte bestehen.
- Alle Informationen können innerhalb einer gemeinsamen Datenbank erstellt werden.

Das Front Office ist ein unabhängiger Block, weil es offen gegenüber dem öffentlichen Internet und Bestandteil einer Unternehmens-Website ist. Es kann daher für den Kunden umkonfiguriert und personalisiert werden. Allerdings ist das Front Office mit einem Back Office verknüpft, um Bewerber, Stellenangebote und Bewerbungen zu verwalten.

5.2. Server- und Netzwerkarchitektur

Nachfolgend findet sich eine schematische Darstellung der Architektur, die für das Hosting der Anwendungen implementiert wurde:



Die verwendete Virtualisierungstechnologie ist VMware.

Alle Web-Server sind mit einer fortschrittlichen Load-Balancing-Technologie ausgerüstet. Alle Datenbank-Server sind mit einer synchronen Replikation konfiguriert.

Die Speicher- und Archivierungszone ist physisch von der Produktionszone getrennt. Die Administrationszone ist nur für autorisierte Administratoren von Cegid Digitalrecruiters nach einem Login über einen Jump Server und eine starke Authentifizierungssequenz zugänglich. Jeder Administrator nutzt ein persönliches Konto.

Nur Web-Server haben Zugriff auf Daten-Server, die somit nicht über das Internet zugänglich sind.

5.3. Technische Software-Infrastruktur

5.3.1. Infrastrukturkomponenten

Die Cegid Digitalrecruiters Lösung wurde auf Basis der folgenden technischen Architektur entwickelt:

- Betriebssystem: Linux
- Datenbank: MySQL Server
- Anwendungs-Server: Nginx
- Programmiersprache: PHP

Nachfolgend findet sich eine Übersicht über die wichtigsten Infrastrukturkomponenten für die aktuelle Version des Produkts:

Komponente	Produkt	Version
Server-Betriebssystem	Linux Debian	10 & 11
Internet-Server	Nginx	
Datenbank-Engine	MySQL	5.7
Nicht relationale Datenbank-Engine	ElasticSearch	7.4
Cache-Engine	Redis	5.7.0.7
Queuing-Engine	RabbitMQ	3.11.5

5.4. Applikationsdatenbanken

Eine Cegid Digitalrecruiters Applikation beruht auf einem mandantenfähigen Datenbank-Cluster, der technische Daten (Konfiguration, Operationen usw.) und Kundendaten (Bewerber-Pool, Stellenangebote, Bewerbungen usw.) enthält.

Kundendaten sind logisch getrennt und werden at Rest verschlüsselt.

5.5. Multi-Client-Management

Die Cegid Digitalrecruiters Applikation ist in Form von Websites verfügbar. Für den Front Office-Teil besitzt jeder Kunde eine eigene Subdomain, die von einer eigenen Instanz des Web-Servers bedient wird. Das Produkt besitzt eine mandantenfähige Software-Architektur, und alle Subdomains verweisen auf die letzte Version der Anwendung.

5.6. Testumgebung

Je nach Vertragsbedingungen können Kunden eine Testumgebung abonnieren.

Die Testumgebung wird als eine Umgebung installiert und verwaltet, die von der Produktionsumgebung getrennt ist. Sie wird so verwaltet, als wäre es die Umgebung eines anderen Kunden.

Testumgebungen werden für das Testen einer Aktion oder einer Einstellung oder zu Schulungszwecken verwendet. Bei den Daten in der Testumgebung kann es sich um eine Kopie der Produktionsdaten zu einem bestimmten Zeitpunkt handeln. Daher sind diese Daten älter.

Testumgebungen sind nicht als Produktionsbereiche verfügbar. Darüber hinaus behält sich Cegid das Recht vor, diese Umgebungen vorübergehend zu unterbrechen, um verschiedene Aufgaben auszuführen (Installation während der Geschäftszeiten zum Beispiel).

5.7. Mobile App

Die Cegid Digitalrecruiters App ist auf zwei mobilen Plattformen verfügbar: Android und iOS. Die Applikation kann aus den jeweiligen App-Stores heruntergeladen werden. Single-Sign-On wird unterstützt, sofern der Kunde einen Identity Provider eingerichtet hat.

Die Cegid Digitalrecruiters App bietet nur eine Präsentationsschicht. Das bedeutet, dass keine Daten auf dem mobilen Gerät gespeichert werden. Die persönlichen Daten werden in den Rechenzentren von Cegid Digitalrecruiters gespeichert und können in Echtzeit über APIs abgerufen werden.

6. ZUGANGSVERWALTUNG

6.1. Anwendungszugriffssicherheit

6.1.1. Bewerber-Front Office

Per Definition sind die Bewerber-Front Office-Anwendungen öffentlich und über das Internet zugänglich.

6.1.2. Back Office und Mitarbeiter/Manager-Bereiche

Die Back Office-Anwendung ist öffentlich und über das Internet frei zugänglich.

6.2. Authentifizierung

Die Authentifizierung kann:

- Über die Cegid Digitalrecruiters Applikation verwaltet werden: Eingabe eines Logins und eines Passwortes.
- An unsere Kunden delegiert werden, wenn ein Single-Sign-On-Mechanismus aktiviert ist. In diesem Fall gilt die Richtlinie des Kunden.

6.2.1. Verantwortlichkeiten von Kunden

Wenn die Authentifizierung delegiert ist, sind Kunden für ihre eigene Passwortrichtlinie verantwortlich.

6.2.2. Authentifizierung für das Bewerber-Front Office

Der Zugang zu den Front Offices unterliegt keiner Authentifizierung.

6.2.3. Authentifizierung in Back Office

Für Nutzer, die bei dem Unternehmen arbeiten, stehen mehrere Authentifizierungsmechanismen zur Verfügung:

- Login und Passwort von Cegid Digitalrecruiters
- vom Kunden implementiertes Single-Sign-On

Die Sitzung wird komplett auf dem Server verwaltet. Auf der Arbeitsstation des Nutzers wird nur ein Sitzungs-Cookie gespeichert und in einigen Fällen ist ein Ansichtsstatus in der Seite enthalten.

6.2.4. Passwortverwaltung

Cegid Digitalrecruiters bietet im Standard die folgenden Richtlinien für die Passwortverwaltung:

- Änderung des Passworts bei der ersten Anmeldung
- Mindestlänge des Passworts von 8 Zeichen
- Mindestanzahl von nicht alphanumerischen und numerischen Zeichen sowie Klein- und Großbuchstaben im Passwort
- Zurücksetzung des Passworts über einen per E-Mail versendeten Aktivierungs-Link
- zwingend verbindliche Validierung der E-Mail-Adresse vor der Aktivierung eines Kontos

Passwörter sind in der Datenbank durch den Algorithmus Bcrypt irreversibel gesichert.

Verlorene/vergessene Passwörter: Wenn Nutzer ihr Passwort vergessen haben und kein SSO verwenden, muss folgendes durchgeführt werden:

- einen Internetbrowser benutzen, um ihre Anmeldungsseite für Cegid Talentsoft zu öffnen
- den Benutzernamen im Feld „Passwort vergessen" eingeben und dann auf „BESTÄTIGEN" klicken
- Ein Reaktivierungslink wird dem Benutzer per E-Mail gesendet. Der Benutzer muss ein neues Passwort eingeben, bevor er sich bei der Anwendung erneut anmelden kann.

6.2.5. Single-Sign-On

Wenn der Kunde einen Identity Provider implementiert hat, besteht die Möglichkeit, dass Nutzer über das Single-Sign-On auf Basis der Protokolle SAML 2.0 authentifiziert werden.

6.2.6. Dauer der Sitzung

Eine Sitzung im Back Office-Portal wird nach acht Stunden Inaktivität unterbrochen. Die Dauer der Sitzung beträgt zwanzig Stunden.

6.3. Cookies-Richtlinie

Bei der Navigation in unseren Anwendungen werden Cookies im Browser des Nutzers gespeichert. Cookies dienen dazu, Navigationsdaten zu erfassen, Nutzer zu identifizieren und ihnen den Zugang zu ihren Konten zu ermöglichen.

Bei Daten über Cookies verpflichtet sich Cegid Digitalrecruiters, die lokalen Vorschriften jedes Landes zu beachten, die Geheimhaltung der Daten zu schützen und territoriale Pflichten in Bezug auf Datenspeicherorte einzuhalten.

Der Umgang mit Cookies wird auf dieser Seite beschrieben: https://www.Digitalrecruiters.com/politique-de-confidentialite

6.4. Rollen, Rechte und Authorisierungen

Cegid Digitalrecruiters hat eine spezielle Oberfläche für die Administration von Rollen, Rechten und Autorisierungen.

6.4.1. Rollen und Rechte

Über Rollen werden Standardprofile mit bestimmten Ebenen für den Zugang zu den Funktionalitäten von Cegid Digitalrecruiters definiert. Zuerst werden die Rollen festgelegt, die dann den Nutzern von Cegid Digitalrecruiters zugeordnet werden. Bei den Rechten, die den Rollen zugeordnet sind, handelt es sich allerdings um eine im Produkt definierte Liste. Rollen können mit Hilfe des Moduls für die Rechteverwaltung komplett umkonfiguriert werden.

6.4.2. Authorisierungen

Benutzerautorisierungslisten helfen bei der Definition, wer die Berechtigung hat, auf welche Mitarbeiterdaten zuzugreifen.

7. SCHNITTSTELLEN

In Cegid Digitalrecruiters ist es möglich, Daten als Dateien im CSV-Format oder über Webservices zu importieren bzw. exportieren.

In diesem Kapitel werden die Grundsätze für den Datei- und Webservice-Austausch sowie die damit verbundenen Sicherheitsaspekte beschrieben. Angaben zu den Schnittstellen werden zu Beginn des Implementierungsprojekts gegeben.

7.1. Import/Export von Dateien

7.1.1. Import

Die Cegid Digitalrecruiters Lösung ermöglicht den Import mit Hilfe von CSV-Dateien bei folgenden Funktionalitäten:

- Import von Bewerbungen
- Import der Baumstruktur
- Import der Nutzer

Die Einrichtung dieser Importe wird in einem separaten Dokument vollständig beschrieben und wird innerhalb der Projektphase mit den Teams von Cegid Digitalrecruiters definiert.

7.1.2. Export

Die Cegid Digitalrecruiters Lösung ermöglicht den Export folgender Daten in CSV-Dateien:

- Baumstruktur
- Statistiken

7.2. Sichere FTP-Schnittstelle

Falls erforderlich, ist die Einrichtung einer Plattform für den Dateiaustausch mit den Teams von Cegid Digitalrecruiters während der Implementierung der Lösung zu organisieren.

7.3. Anwendungsprogrammierschnittstellen (API)

Cegid bietet eine Reihe von Web-Services, über die Drittanwendungen die Services von Cegid Digitalrecruiters nutzen können. Diese Web-Services erstrecken sich auf die folgenden Funktionsbereiche:

- Export von Bewerbungen
- Zusammenstellung von Anzeigen der Karriereseiten
- Export von Anzeigen
- Anzahl Anzeigen pro Dienst
- Änderung von Anzeigen
- Import von Bewerbungen
- Export von Bewerbungen

Die Einrichtung der APIs wird in einem separaten Dokument vollständig beschrieben und wird innerhalb der Projektphase mit den Teams von Cegid Digitalrecruiters definiert.

7.4. E-Mail-Schnittstelle

Die Cegid Digitalrecruiters Anwendung sendet E-Mails unter Nutzung des klassischen SMTP-Protokolls. E-Mails können im Format HTML gesendet werden.

8. NUTZUNG

8.1. Operative Verfahren

Dieses Kapitel beschreibt die operativen Verfahren, die während des Betriebs am häufigsten verwendet werden.

Löschung der System-Log-Dateien: System-Log-Dateien werden 90 Tage gespeichert.

Löschung der Anwendungs-Log-Datei: Die Anwendungs-Log-Datei enthält Daten, mit denen Aktionen von Nutzern protokolliert werden. Diese Log-Datei speichert die Daten ein (1) Jahr, ältere Daten werden gelöscht.

8.2. Datenmanagement

Dieses Kapitel gilt für Produktionsdatenbanken.

8.2.1. Organisation von Backups

Backups der verschiedenen Datenarten erfolgen auf Basis einer Strategie, bei der die optimale Sicherheit und Integrität der Daten sowie die Zeit für die Wiederherstellung berücksichtigt werden. Hierbei handelt es sich um Online-Backups, ohne dass der Datenbankbetrieb unterbrochen wird.

Daten	Maßnahme	Häufigkeit	Speicherung
Virtuelle Maschinen	Komplettes Backup	Alle 2 Stunden	14 Tage
Datenbank	Komplettes Backup	Alle 24 Stunden	30 Tage
Datenbank	Teil-Backup	Alle 2 Stunden	24 Stunden
NAS	Vollständige Replikation	1-mal am Tag	-
Logs	Komplettes Backup	1-mal am Tag	3 Monate

Die Backup-Medien und -Standorte hängen vom Cloudanbieter ab:

Anbieter	Speicherung von Backups	Replikation der Daten
OVHCloud	Object Storage	Verschlüsselte Daten werden nativ vom Object Storage-Dienst in den verschiedenen geografischen Regionen repliziert.

Nur eine sehr begrenzte Anzahl von Personen hat Zugang zu den Backups der Datenbanken. Diese Personen sind genau wie das Personal von Cegid durch eine Geheimhaltungsklausel gebunden. Gleichermaßen verfügt unser Cloud-Provider über eine begrenzte Anzahl von Personen, die Zugang zu Backups haben.

8.2.2. Verschlüsselung von Daten

Verschlüsselung von Daten-in-Transit

Um die Sicherheit von Daten bei der Übertragung zu gewährleisten, verschlüsselt Cegid den Datenfluss der Anwendungen mit dem Protokoll HTTPS in allen Domains und verlangt das Protokoll Transport Layer Security (TLS) 1.2 oder höher.

Verschlüsselung von Daten-at-Rest

Passwörter sind in der Datenbank durch den Algorithmus Bcrypt irreversibel gesichert. Cegid liefert eine Verschlüsselung der Volumes in AES XTS.

8.3. Administration und Supervision

Die Plattform wird rund um die Uhr 24/7 überwacht. Die Leistungsüberwachung und Anwendungssupervision wurden implementiert und lösen Warnungen aus, wenn Probleme erkannt werden.

Ein Prozess für die Bearbeitung und „Eskalation" wurde definiert und wird von den operativen Teams befolgt.

Die Tools, die für die Überwachung der Infrastruktur zum Einsatz kommen, sind Splunk Observability und Centreon. Unsere Hosting-Provider verfügen ebenfalls über ihr eigenes Überwachungssystem.

Die operativen Verfahren umfassen die folgenden Aufgaben (die Liste erhebt keinen Anspruch auf Vollständigkeit):

- Administration
- Wartung der Betriebssysteme (Festplattenspeicher, Log-Dateien usw.)
- Wartung der Datenbanken
- Tests, Qualifikation und Implementierung von Sicherheits-Updates
- Wartung der Anwendungen (Log-Dateien und Performance-Analyse)

Supervision:

- Überwachung der Verfügbarkeit der Anwendungen
- Überwachung der Antwortzeit
- Überwachung der Plattformauslastung (Speicher, Prozessoren, Festplatten)
- Überwachung der Netzwerkbandbreite
- Überwachung der Batch-Jobs für Anwendungen und Systeme
- Überwachung der Hardware

Hosting-Anbieter sind für folgenden Aktivitäten verantwortlich:

- physische Ausrüstung (Server-Hardware, Netzwerksausrüstung usw.)
- Hypervisoren
- Netzwerk
- Software-Updates für die Betriebssysteme, Datenbanken und Antivirus-Programme
- Nachverfolgung der obigen Elemente
- Überprüfung und Qualifikation der Backups
- Überwachung und Update der Antivirus-Systeme
- Wartung der Netzwerkausrüstung

8.4. Geschäftskontinuitätsplan

Eine Produktionsinfrastruktur mit hoher Verfügbarkeit wurde eingerichtet. Diese beruht auf einer Unterteilung der Gesamtheit in Dienste, wobei jeder Dienst durch ein Cluster unabhängiger Server gewährleistet wird. Dies garantiert die Resilienz der Infrastruktur.

Bei einer Fehlfunktion eines Rechners (oder mehrerer Rechner zur selben Zeit) übernehmen die anderen Server des Clusters vorübergehend die zusätzliche Last. Dies garantiert die Aufrechterhaltung des Betriebs.

Diese Organisation ermöglicht zudem die Skalierbarkeit der Infrastruktur, denn die Kapazität kann einfach durch die Einbindung neuer Rechner ohne Unterbrechung erweitert werden.

Aus Gründen der maximalen Effizienz werden die Tools Ansible, Chef und Terraform eingesetzt, um die Implementierung und die Konfiguration zusätzlicher Rechner zu automatisieren.

9. VERORDNUNGEN & RICHTLINIERN

9.1. Datenschutz-Grundverordnung (DSGVO)

Im Folgenden wird beschrieben, wie Cegid Digitalrecruiters die Kernelemente der DSGVO erfüllt.

Wichtig: Alle Datensicherheitselemente, werden im Sicherheitsplan oder in der Leistungsbeschreibung für die Run-Phase von Cegid Digitalrecruiters beschrieben. Deshalb finden sie hier keine Erwähnung. Sie alle betreffen jedoch die DSGVO in dem Sinne, dass Datenschutz eine wesentliche Anforderung für alle Subunternehmer (die „Auftragsverarbeiter") ist.

Für die Umsetzung der DSGVO-Anforderungen in seiner Lösung unterscheidet Cegid Digitalrecruiters als Auftragsverarbeiter zwischen zwei unterschiedlichen Personen: Bewerbern und Mitarbeitern. Einige der DSGVO -Anforderungen hängen nicht von den Personas ab, und einige von ihnen führen zu unterschiedlichen Produktverhaltensweisen, je nachdem, ob wir einen Bewerber oder einen Mitarbeiter ansprechen.

9.1.1. DSGVO-Anforderungen für alle Personas

Privacy by Design
Unser agiles Softwareentwicklungs-Verfahren umfasst Schulungen, formelle Code-Überprüfungen und Tools, mit denen kontrolliert werden kann, ob die empfohlenen Praktiken wirklich angewandt werden.
Grundsätze bezüglich der Verarbeitung personenbezogener Daten, wie im Artikel 5 der DSGVO definiert, werden durch datenschutzfreundliche Technikgestaltung bei der Produktentwicklung berücksichtigt.

Privacy by Default
Das Prinzip der „relevanten und geeigneten Daten" wird in der gesamten Digitalrecruiters - Lösung mithilfe von Rollen, Rechten und Autorisierungen umgesetzt, sodass Nutzer ausschließlich auf Daten und Funktionen in ihrem Zuständigkeits- und Aufgabenbereich zugreifen können.

Datenschutzbeauftragter
Cegid hat angesichts der Art seiner Tätigkeiten einen Datenschutzbeauftragten für Cegid Digitalrecruiters benannt.

Verzeichnis von Verarbeitungstätigkeiten
Cegid unterhält für seine Kunden als Datenverarbeiter ein Produktverarbeitungsregister.

Subunternehmer müssen alle DSGVO-Aspekte berücksichtigen
Cegid vergibt einen Teil seiner Tätigkeiten an Subauftragsverarbeiter. Sie schließen mit Cegid einen Auftragsverarbeitungsvertrag ab, der DSGVO-konforme Klauseln enthält.

Sensible Daten
Cegid erhebt keine sensiblen Daten wie in Artikel 9 der DSGVO beschrieben. Angesichts der flexiblen Möglichkeiten zum Hinzufügen von Add-ons zum Datenmodell rät Talentsoft davon ab, Zusatzfelder zu erstellen, die unter „sensible Daten" wie in Artikel 9 der DSGVO definiert fallen.

Benachrichtigung bei Datenschutzverletzungen
Cegid hat ein Verfahren für die Meldung von Datenschutzverletzungen eingerichtet. Die Festlegung, Aufrechterhaltung und Nachverfolgung dieses Verfahrens erfolgen im Rahmen des Systems für das Management der Informationssicherheit und der DSGVO.

Bei Verletzungen des Datenschutzes, die Kundendaten betreffen, verpflichtet sich Cegid dazu, den Kunden (d.h. den Verantwortlichen) so schnell wie möglich zu benachrichtigen, sodass der Kunde seinerseits die 72-Stunden-Frist gegenüber seinen eigenen Datenschutzstellen einhalten kann. Es liegt an dem Kunden zu beurteilen, ob die Aufsichtsbehörde und/oder die betroffene Person benachrichtigt werden muss.

Automatisierter Entscheidungsprozess
Cegid Digitalrecruiters verfügt über keinerlei automatisierte Profilingfunktionen oder automatisierte Funktionen für individuelle Entscheidungen. Sämtliche Entscheidungen obliegen den menschlichen Nutzern, die zwar bei ihrer Entscheidungsfindung von entsprechenden Dashboards, Indikatoren, Empfehlungen und Analytics unterstützt werden können, deren einziger Zweck jedoch darin besteht, fundierte Entscheidungen treffen zu können.

Anonymisierung von Daten
Cegid Digitalrecruiters bietet eine Anonymisierungsfunktion für die gesamte Datenbank. Letztere kommt zur Anwendung, wenn eine Produktionsumgebung im Test-, Debug- oder Schulungsmodus verwendet werden soll.

Bereitstellung von Informationen, bei der personenbezogene Daten von der betroffenen Person erfasst werden
Es liegt an dem Kunden, diese Informationen direkt seinen Bewerbern und Mitarbeitern bereitzustellen. Unsere Lösung bietet unseren Kunden die Möglichkeit, diese Informationen hochzuladen.

9.1.2. Erfüllung der DSGVO-Anforderungen bei Bewerbern

Bewerber stehen in keinem untergeordneten Verhältnis zum potenziellen Arbeitgeber, der für die Datenverarbeitung verantwortlich ist. Daher legen wir detailliert alle Verarbeitungsvorgänge dar, die vom Produkt in diesem Bereich vorgenommen werden.

Auskunftsrecht, Recht auf Berichtigung
Bewerber können eine E-Mail an den Administrator des Kunden (oder den Datenschutzbeauftragten des Verantwortlichen für die Verarbeitung) senden und die Löschung oder Berichtigung ihrer personenbezogenen Daten verlangen. Der Administrator des Kunden kann das Customer-Care Team von Cegid dazu um Unterstützung bitten. Ein Recruiter kann personenbezogene Daten eines Bewerbers ebenfalls löschen oder berichtigen, falls dies notwendig ist.

Recht auf Vergessenwerden
Löschrechte können automatisiert werden:

- Der Zeitraum der Datenspeicherung kann vom Kunden pro Land verwaltet werden.
- Am Ende dieser Frist erhält der Bewerber eine E-Mail mit der Aufforderung, seine Einwilligung zu erneuern.
- Bewirbt sich ein Bewerber in mehreren Ländern mit unterschiedlichen Speicherungsfristen, so wird die Einwilligung des Bewerbers für die jeweils kürzeste Frist eingeholt. Gibt der Bewerber seine Einwilligung, so werden die Daten im Backoffice abgespeichert. Wird die Einwilligung jedoch verweigert, so werden die personenbezogenen Daten gelöscht. Erfolgt keine Rückmeldung, so werden die Daten zum Ende der Speicherungsfrist gelöscht.

Die Datenlöschung erfolgt asynchron per nächtlichen Batch.

Rechtliche Grundlagen
Der für die Datenverarbeitung Verantwortliche ist verpflichtet, die am besten geeignete Rechtsgrundlage für die Cegid Talentsoft Lösung zu bestimmen, bevor die Lösung in Betrieb genommen wird (Art. 6.1 der DSGVO).

Jegliche Datenaustausch innerhalb der Unternehmensgruppe muss ebenfalls durch eine Rechtsgrundlage gerechtfertigt sein und muss dem Bewerber mitgeteilt werden. Cegid ermöglicht es dem Kunden (über die Produktkonfiguration), diese Informationen bereitzustellen.

9.1.3. Erfüllung der DSGVO-Anforderungen bei Mitarbeitern

Auskunftsrecht, Recht auf Berichtigung
Das Produkt bietet die notwendigen Funktionen für das Abrufen und Ändern von Mitarbeiterdaten. Der Zugriff auf diese Funktionen wird über Rollen und Rechte verwaltet, die von den Administratoren des Kunden direkt zugewiesen werden können.

Recht auf Löschung
Unternehmen erfassen und verarbeiten aus rechtlichen Gründen personenbezogene Daten ihrer Mitarbeiter. Cegid berücksichtigt insofern die Notwendigkeit, dass jegliche von Mitarbeitern geforderte Datenlöschungen zunächst vom Arbeitgeber (d.h. dem Verantwortlichen) genehmigt werden müssen.

Aus diesem Grunde bietet unser Produkt eine Löschfunktion in der Benutzeroberfläche von Cegid Digitalrecruiters. Diese Funktionalität erfordert ein bestimmtes Recht, das die Administratoren des Kunden den relevanten Nutzern zuordnen können. Zurzeit führt das Produkt eine irreversible und physische Löschung in der Datenbank durch.

Rechtliche Grundlagen

Der für die Datenverarbeitung Verantwortliche ist verpflichtet, die am besten geeignete Rechtsgrundlage für die Cegid Talentsoft Lösung zu bestimmen, bevor die Lösung in Betrieb genommen wird (Art. 6.1 der DSGVO).

In dem oben zitierten CNIL-Rahmen, stellt die CNIL in Bezug auf die Einwilligung fest, dass: "Angesichts der Abhängigkeit, die sich aus dem Verhältnis zwischen Arbeitgeber und Arbeitnehmerin/ Arbeitnehmer ergibt, können Arbeitnehmerinnen / Arbeitnehmer ihre Einwilligung nur in den seltensten Fällen frei geben, verweigern oder widerrufen. Arbeitnehmerinnen/ Arbeitnehmer können eine freie Zustimmung nur in den Fällen geben, in denen die Annahme oder Ablehnung einer vertraglichen Vereinbarung keine Auswirkungen auf ihre Situation hat."

Die CNIL schlägt also andere Rechtsgrundlagen vor, die von der Tätigkeit der Arbeitnehmerin / dem Arbeitnehmer abhängen. In diesem Rahmen steht eine Tabelle zur Verfügung, die dem für die Datenverarbeitung Verantwortlichen hilft, diese Tätigkeiten zu bestimmen.