



RAPPORT DE PROJET • 21 JUILLET 2026

SYSTÈME DE SUIVI DES CANDIDATURES

Conception, développement et mise en production d'un ATS complet pour une direction des ressources humaines du secteur transport et logistique.

LIVRABLE	Portail carrières public + back-office de recrutement
MISE EN LIGNE	https://careers.dhl.d3v-test.me
DATE	21 juillet 2026
STATUT	En production, recette complète passée

Avertissement. Ce projet est une démonstration technique déployée sur un domaine de test. Il n'est affilié à aucune entité du groupe Deutsche Post DHL, ne traite aucune donnée personnelle réelle et l'ensemble des candidats et des offres qu'il contient sont fictifs.

SOMMAIRE

TABLE DES MATIÈRES

01	Contexte et besoin	3
02	État de l'art (recherche préalable)	3
03	Périmètre livré	4
04	Architecture	5
05	Le moteur de correspondance	7
06	Sécurité	7
07	Conformité RGPD	8
08	Déploiement	9
09	Recette	9
10	Volumétrie	10
11	Limites connues	11
12	Feuille de route	11
13	Accès	11

CHAPITRE 01

CONTEXTE ET BESOIN

Le recrutement dans la messagerie et la logistique se distingue de celui des fonctions tertiaires sur quatre points, qui commandent toute la conception :

1. **Le volume.** Une plateforme de tri recrute par dizaines, pas par unités. Un poste d'agent de quai attire couramment plusieurs dizaines de candidatures, souvent peu différenciées.
2. **Les prérequis réglementaires.** Permis C ou CE, FIMO/FCO, carte conducteur, habilitation ADR, CACES 1/3/5, habilitation électrique : ce sont des conditions d'accès à l'emploi, pas des « plus ». Un dossier sans le titre requis ne peut pas avancer, et le vérifier tardivement coûte plusieurs jours à tout le monde.
3. **Les contraintes d'organisation.** Horaires 2×8, 3×8, nuit, week-end, saisonnalité du pic de fin d'année : la disponibilité est un critère de sélection à part entière.
4. **La dispersion géographique.** Plusieurs entités, une douzaine de sites, des besoins qui se déplacent d'une agence à l'autre au fil de l'activité.

Un suivi sur tableur partagé ne tient sur aucun de ces points : pas de traçabilité des décisions, pas de vérification systématique des habilitations, pas de visibilité consolidée, et surtout aucune gestion de la durée de conservation des CV — un risque RGPD direct.

L'objectif du projet est de livrer un ATS complet et opérationnel : un portail carrières qui donne envie de postuler depuis un téléphone, et un back-office qui fait gagner du temps aux recruteurs sur le tri, le suivi et la traçabilité.

CHAPITRE 02

ÉTAT DE L'ART (RECHERCHE PRÉALABLE)

Une revue des plateformes du marché et des exigences de conformité a précédé la conception. Les constantes retenues, et ce qui en a été fait ici :

CONSTANTE DU MARCHÉ	TRADUCTION DANS LE PROJET
Analyse automatique des CV en données structurées	Extraction du texte des PDF/DOCX/RTF, détection des coordonnées et de l'ancienneté
Score de correspondance candidat/poste	Moteur pondéré par critère, avec critères éliminatoires, restitué en clair
Pipeline à étapes configurables	9 étapes en table de référence, vue kanban avec glisser-déposer
Workflow d'approbation des demandes de recrutement	6 statuts, transitions contrôlées, approbation réservée au manager
Piste d'audit des décisions	Journal en ajout seul + chronologie métier par candidature
Conformité RGPD (accès, effacement, portabilité)	Conservation 24 mois, anonymisation automatique, export ZIP normalisé
Analytique temps réel (time-to-fill, conversion)	Tableau de bord et rapports, exports CSV

CONSTANTE DU MARCHÉ	TRADUCTION DANS LE PROJET
Expérience candidat mobile	Portail responsive, dépôt en trois minutes, suivi par référence

Sources consultées

- [Modern ATS: What to Look For in 2026 — Lever](#)
- [What Is an Applicant Tracking System? — Jobscan](#)
- [How Applicant Tracking Systems Work \(8-Step Data Flow\) — Reqcore](#)
- [Applicant Tracking Systems: A Complete Guide — Bullhorn](#)
- [Building a Custom ATS Workflow — Tracker](#)
- [ATS Compliance: GDPR, EEOC & DEI Requirements — Kula](#)
- [GDPR compliance guide for recruitment — Workable](#)
- [GDPR in recruitment: what employers need to know in 2026 — Recrutee](#)

CHAPITRE 03

PÉRIMÈTRE LIVRÉ

3.1 Portail candidat

PAGE	FONCTION
/	Accueil : recherche, familles de métiers, offres du moment, chiffres en direct
/offres	Liste et filtres : mot-clé, métier, ville, contrat, horaires
/offres/{ref}	Annonce complète : missions, profil, avantages, conditions
/offres/{ref}/postuler	Candidature : coordonnées, CV, lettre, questions de présélection, consentement
/candidature/confirmation/{ref}	Référence de suivi attribuée
/suivi	Suivi par référence + e-mail, avec la progression étape par étape
/candidature-spontanee	Dépôt hors offre, orienté vers le vivier
/confidentialite	Politique de traitement des données candidat

3.2 Back-office RH

- **Tableau de bord** — offres publiées, candidatures à 30 jours, dossiers en cours, entretiens de la semaine, embauches à 90 jours, délai moyen de recrutement, taux de conversion, entonnoir, origine des candidatures, offres à surveiller.
- **Réquisitions** — création, critères pondérés, questions de présélection, workflow **brouillon → à approuver → approuvée → publiée → pourvue / annulée**.
- **Pipeline** — kanban à glisser-déposer, filtres par offre, score et profils éliminés.
- **Fiche candidature** — analyse de correspondance détaillée, CV et texte extrait, réponses de présélection, chronologie, notes, évaluations multi-évaluateurs, entretiens, envoi d'e-mails depuis modèle.

- **Base de candidats** — recherche plein texte **dans le contenu des CV**, vivier.
- **Entretiens** — planification, compte rendu, agenda.
- **Rapports** — volumes, entonnoir, performance par offre, efficacité des sources, motifs de refus, exports CSV.
- **Administration** — utilisateurs et rôles, référentiels, modèles d'e-mails, file d'envoi, console RGPD, journal d'audit.

3.3 Rôles

RÔLE	PORTÉE
Administrateur RH	Tout, y compris administration et RGPD
Chargé de recrutement	Réquisitions, pipeline, candidats, e-mails
Manager opérationnel	Ses réquisitions, évaluations, approbation
Lecture seule	Consultation et rapports uniquement

CHAPITRE 04

ARCHITECTURE

4.1 Choix techniques et justification

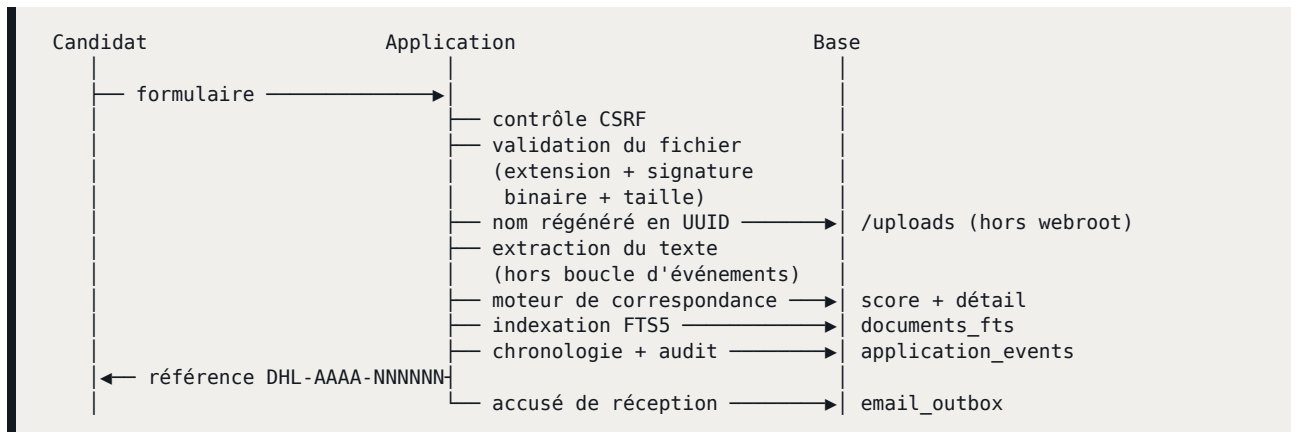
Le serveur cible impose deux contraintes : **pas de Node.js** et **pas de base PostgreSQL active**. Elles ont orienté toute la pile.

COUCHE	CHOIX	POURQUOI
Serveur	Starlette + Uvicorn	100 % Python pur. Python 3.14 étant récent, toute dépendance compilée (pydantic-core en Rust, lxml en C) exposait à une roue manquante. L'application étant en formulaires rendus côté serveur, l'apport de FastAPI aurait été marginal.
Rendu	Jinja2, CSS et JavaScript écrits à la main	Aucun outil de construction, donc aucun besoin de Node. L'application reste utilisable sans JavaScript.
Base	SQLite en mode WAL	Volumétrie cible très en deçà des limites, sauvegarde par instantané, exploitation nulle. Tous les accès passent par app/db.py : une bascule PostgreSQL ne toucherait que ce fichier.
Recherche CV	SQLite FTS5	Index plein texte natif, sans moteur externe.
Lecture des CV	pypdf + zipfile/xml.etree	pypdf est pur Python ; lire word/document.xml avec la bibliothèque standard évite python-docx et sa dépendance lxml compilée.
Génération de PDF	Écriture directe du format	Les CV de démonstration sont de vrais PDF. Quarante lignes de code ont remplacé une dépendance lourde (reportlab).
Mots de passe	hashlib.scrypt	Robuste, dans la bibliothèque standard, aucun risque de roue absente.

COUCHE	CHOIX	POURQUOI
Sessions	Cookie signé (itsdangerous) + table de sessions	Signature côté client, révocation côté serveur.

Bilan des dépendances : six paquets, tous en Python pur. L'installation ne requiert aucune chaîne de compilation.

4.2 Chaîne de traitement d'une candidature



4.3 Modèle de données

26 tables. Les principales :

DOMAINE	TABLES
Accès	users, sessions
Référentiels	business_units, sites, job_families, stages
Besoins	requisitions, requisition_criteria, screening_questions
Candidatures	candidates, applications, application_answers, documents, documents_fts
Suivi	application_events, evaluations, interviews, notes
Communication	email_templates, email_outbox
Traçabilité	audit_log, settings

L'index plein texte est tenu à jour par trois déclencheurs SQL (AFTER INSERT, AFTER UPDATE, AFTER DELETE) : aucune synchronisation applicative à maintenir.

CHAPITRE 05

LE MOTEUR DE CORRESPONDANCE

Le score est **explicable par construction**. Il ne sert pas à décider à la place du recruteur mais à trier une pile : un score bas n'écarte personne, il descend le dossier dans la liste.

Calcul

1. Le texte du CV est normalisé (minuscules, accents supprimés).
2. Chaque critère de la réquisition porte des synonymes, un poids de 1 à 5, et éventuellement un drapeau **éliminatoire**. Score de base = $\Sigma(\text{poids obtenus}) / \Sigma(\text{poids totaux}) \times 100$.
3. L'ancienneté détectée dans le CV donne un bonus de 0 à 10 points, proportionné au niveau demandé sur l'offre.
4. Une réponse non conforme à une question éliminatoire, ou un critère obligatoire absent, place le dossier en **éliminé** : son score est plafonné à 35 et le motif est affiché explicitement.

Détection. La recherche exige une frontière de mot des deux côtés, avec tolérance au pluriel : « logistique » trouve « logistiques », mais « CAP » n'est pas déclenché par « capacité ». Ce point précis a été révélé par les tests unitaires et corrigé.

Restitution. Le recruteur ne voit jamais un nombre seul, mais la liste des critères avec, pour chacun, le terme effectivement trouvé dans le CV :

✓ CACES 5	« caces 5 »	x5
✓ CACES 1 et 3	« caces 1 »	x4
✓ Expérience entrepôt	« entrepot »	x4
✓ Maîtrise WMS	« wms »	x3
✓ Travail en 3x8	« 3x8 »	x2
Score sur critères 100/100 · bonus expérience +10 · retenu 100/100		

CHAPITRE 06

SÉCURITÉ

MESURE	MISE EN ŒUVRE
Transport	HTTPS avec certificat Let's Encrypt, redirection permanente depuis HTTP, HSTS un an
Mots de passe	scrypt ($n=2^{14}$, $r=8$, $p=1$), sel aléatoire de 16 octets, comparaison à temps constant
Sessions	Cookie signé HttpOnly + Secure + SameSite=Lax, expiration 8 h, révocation en base
CSRF	Jeton signé et ancré à la session sur tous les POST, y compris les formulaires publics
Injection SQL	Requêtes exclusivement paramétrées
XSS	Échappement automatique Jinja2 ; les deux filtres produisant du HTML échappent avant d'insérer
Dépôts de fichiers	Extension et signature binaire contrôlées, 5 Mo maximum, nom régénéré en UUID, stockage hors racine web
Accès aux CV	Uniquement via une route authentifiée, avec vérification anti-traversée de chemin

MESURE	MISE EN ŒUVRE
Cloisonnement	Contrôle de rôle par décorateur sur chaque route du back-office
Suppression de compte	Réservée à l'administrateur, refusée sur soi-même et sur le dernier administrateur actif ; le travail produit survit, détaché de son auteur, et le journal d'audit conserve une trace nominative
En-têtes	CSP stricte default-src 'self', nosniff, Referrer-Policy, X-Frame-Options, Permissions-Policy
Débit	Limitation nginx spécifique sur la connexion, le dépôt de candidature et le suivi ; fail2ban actif
Énumération	La page de suivi renvoie une réponse identique que la référence existe ou non
Isolation du service	systemd : NoNewPrivileges, ProtectSystem=strict, ProtectHome=read-only, PrivateTmp
Traçabilité	Journal d'audit en ajout seul : acteur, action, objet, avant/après, IP, horodatage

Un arbitrage documenté. La snippet nginx security-headers.conf partagée par les autres sites de la machine autorise plusieurs CDN externes. L'inclure aurait produit un second en-tête CSP et affaibli la lecture de la configuration. Le vhost ne l'inclut donc pas : l'application émet sa propre CSP stricte, et nginx ne complète que le HSTS.

De même, les fichiers statiques sont servis par l'application et non par nginx : donner à www-data un droit de traversée sur /home/ubuntu pour trois fichiers aurait été un mauvais échange.

CHAPITRE 07

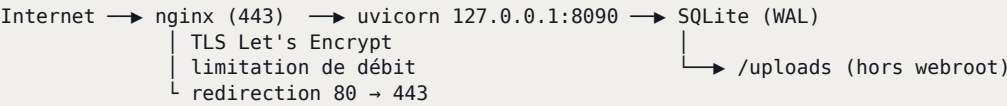
CONFORMITÉ RGPD

EXIGENCE	MISE EN ŒUVRE
Consentement	Case explicite non pré-cochée, horodatée, avec version de la politique conservée
Information	Page dédiée : qui traite, quoi, pourquoi, combien de temps, qui accède, quels droits
Durée de conservation	24 mois (recommandation CNIL), échéance calculée à la création du dossier
Effacement	Anonymisation plutôt que suppression : identité neutralisée, CV effacés du disque, notes purgées — les statistiques de recrutement restent exploitables
Automatisation	Timer systemd quotidien à 03h30 ; l'opération est tracée dans le journal d'audit
Portabilité	Export ZIP : un JSON complet (identité, candidatures, réponses, entretiens, évaluations, communications) et l'ensemble des documents
Pilotage	Console RGPD : dossiers arrivant à échéance sous 60 jours, historique des purges, registre du traitement
Minimisation	Aucune donnée sensible collectée ; pas de sous-traitant, pas de transfert hors UE

CHAPITRE 08

DÉPLOIEMENT

Cible : un serveur Ubuntu (2 vCPU, 7 Go), nginx et certbot déjà en place, en cohabitation avec d'autres applications.



COMPOSANT	DÉTAIL
Service	dhl-ats.service — uunicorn sur 127.0.0.1:8090, redémarrage automatique, durcissement systemd
Frontal	careers.dhl.d3v-test.me — TLS, en-tête HSTS, limitation de débit ciblée, corps limité à 6 Mo
Certificat	Let's Encrypt, émis le 21/07/2026, valide jusqu'au 19/10/2026, renouvellement automatique
Purge RGPD	dhl-ats-purge.timer — quotidienne à 03h30
Sauvegarde	dhl-ats-backup.timer — quotidienne à 02h00, instantané SQLite cohérent + archive des CV, rétention 14 jours
Supervision	/healthz (application), /nginx-health (frontal), journaux applicatifs séparés

Le port 8090 a été retenu après vérification : 8000 et 27017 sont déjà occupés par des conteneurs Docker sur cette machine.

CHAPITRE 09

RECETTE

9.1 Tests automatisés — 39 tests, tous passants

SUITE	COUVERTURE
tests/test_scoring.py	Pondération, critères éliminatoires, synonymes, insensibilité aux accents, frontière de mot, questions éliminatoires, bonus d'expérience, bornes du score, sérialisation, données corrompues
tests/test_scoring.py	Extraction PDF et DOCX, détection des coordonnées et de l'ancienneté, robustesse aux fichiers illisibles, hachage des mots de passe
tests/test_e2e.py	Parcours candidat complet, anti-doublon, consentement obligatoire, rejet CSRF, rejet d'un faux PDF, suivi, cloisonnement des rôles, changement d'étape, déclenchement d'e-mail, exports CSV, workflow de réquisition et transition illégale, export et anonymisation RGPD, protection des documents

```
$ .venv/bin/python -m unittest discover -s tests
Ran 39 tests in 1.287s
OK
```

Deux défauts réels détectés par ces tests et corrigés :

1. `normalize()` ne supprimait pas les espaces de bord, ce qui rendait inopérant tout synonyme placé après une virgule dans la liste des mots-clés — la majorité d'entre eux.
2. `contient()` n'exigeait une frontière de mot qu'à gauche : « CAP » était détecté dans « capacité ».

Un troisième défaut a été trouvé pendant la recette de production : le jeton CSRF était signé avec un identifiant anonyme que la réponse n'avait pas encore posé, si bien que le tout premier formulaire servi à un visiteur était systématiquement rejeté. Corrigé en fixant l'identifiant avant la signature.

9.2 Recette sur le site en production — 18/18 contrôles réussis

```
- Portail public -
OK page d'accueil rendue
OK liste des offres (13 offres)
OK filtre par mot-clé
OK détail d'une offre
OK candidature déposée avec CV PDF (DHL-2026-000079)
OK suivi de candidature par référence
- Back-office RH -
OK connexion recruteur
OK la candidature apparaît dans le pipeline
OK pages tableau de bord, réquisitions, candidats, entretiens, rapports
OK recherche plein texte dans les CV
OK export CSV (79 lignes)
- Cloisonnement des rôles -
OK un compte lecture seule est refusé sur /rh/admin
OK un visiteur anonyme est redirigé vers la connexion
OK les CV ne sont pas téléchargeables sans authentification
```

Contrôles complémentaires effectués : déplacement kanban accepté (200) et rejeté avec un jeton CSRF invalide (400) ; certificat TLS au bon nom ; en-tête CSP unique ; redirection HTTP 301 ; purge RGPD et sauvegarde exécutées avec succès.

CHAPITRE 10

VOLUMÉTRIE

Fichiers sources	69
Code Python	≈ 4 640 lignes
Gabarits HTML	≈ 3 050 lignes (30 gabarits)
CSS, JavaScript, SQL	≈ 1 170 lignes
Routes HTTP	55

Tables	26
Dépendances externes	6, toutes en Python pur

Jeu de démonstration chargé : 15 réquisitions (13 publiées), 79 candidats, 79 candidatures réparties dans le pipeline, 79 CV au format PDF réellement analysés, 29 entretiens, 259 événements de chronologie.

CHAPITRE 11

LIMITES CONNUES

- **Les e-mails ne partent pas.** Ils sont déposés dans une file consultable, telle qu'ils seraient expédiés. Brancher un SMTP consiste à implémenter une seule fonction.
- **Pas d'authentification à deux facteurs** ni de SSO d'entreprise.
- **Analyse de CV limitée aux formats textuels.** Un PDF issu d'un scan sans couche de texte n'est pas exploitable : il faudrait un moteur OCR.
- **Interface en français uniquement**, alors que le groupe est international.
- **.doc binaires anciens** mal extraits ; les formats modernes sont couverts.
- **Instance unique.** SQLite convient à la volumétrie visée mais ne permet pas de répartir la charge sur plusieurs serveurs.

CHAPITRE 12

FEUILLE DE ROUTE

HORIZON	CHANTIER
Court terme	Envoi SMTP réel ; notifications aux managers ; modèles d'e-mails par entité
Moyen terme	SSO Microsoft Entra ID et 2FA ; connecteur SIRH pour l'onboarding des embauchés ; diffusion automatique des offres vers les jobboards et France Travail
Moyen terme	Portail multilingue (anglais, allemand) ; planification des entretiens synchronisée avec les agendas
Long terme	Bascule PostgreSQL et exécution multi-instances ; OCR des CV scannés ; analyse des écarts de traitement à des fins de non-discrimination

CHAPITRE 13

ACCÈS

Portail candidat — <https://careers.dhl.d3v-test.me>

Back-office RH — <https://careers.dhl.d3v-test.me/rh>

RÔLE	IDENTIFIANT	MOT DE PASSE
Administrateur RH	admin@dhl.d3v-test.me	AdminDHL2026!
Chargé de recrutement	recruteur@dhl.d3v-test.me	Recrut2026!
Manager opérationnel	manager@dhl.d3v-test.me	Manager2026!
Lecture seule	lecteur@dhl.d3v-test.me	Lecture2026!

Ces identifiants sont ceux d'un environnement de démonstration et sont affichés sur la page de connexion. Ils devraient être supprimés avant tout usage réel.