

Description des traitements, localisation des données et sous-traitants

Plateforme Odres.io (ERP HORECA : ODRS ERP, OdStaff, OdKiosk, OdStock, OdClock, OdLabels) — Document technique à l'appui de l'annexe de traitement des données (DPA), des mentions légales et de la politique de cookies.

Responsable de la plateforme : ODRS GROUP SRL, Place Verte 20, 6000 Charleroi (Belgique) — BE 0802.601.160 — contact@odres.io

Version : 3.0 — **Date :** 21 octobre 2026 — **Remplace :** la version 2.0 du 8 octobre 2026

Ce document complète la Politique de confidentialité (version 5.1) publiée sur <https://odres.io>. En cas de divergence, la Politique de confidentialité prévaut.

Établi par : l'équipe technique ODRS, sur la base du code et de la configuration déployés à cette date

Adresse de la plateforme : <https://app.odres.io>

Sommaire

1. Objet et périmètre
2. Rôles des parties
3. Personnes concernées et catégories de données
4. Localisation des données et hébergement
5. Sous-traitants ultérieurs et accords de traitement
6. Traitements par intelligence artificielle
7. Cookies et stockage dans le navigateur
8. Messages automatiques et actions marketing
9. Durées de conservation
10. Mesures de sécurité
11. Droits des personnes
12. Périmètre non couvert

1. Objet et périmètre

Ce document décrit, pour la plateforme Odres.io, où les données sont hébergées, quels prestataires y ont accès et sous quel accord, quels traitements sont réalisés (y compris par intelligence artificielle), quels cookies sont déposés, quels messages sont envoyés automatiquement, et pendant combien de temps chaque catégorie de données est conservée.

Il couvre les six applications de la plateforme :

- **ODRS ERP** — back-office des propriétaires, gérants et comptables ;
- **OdStaff** — application des employés : plannings, pointages, congés, documents RH, avertissements, évaluations, formations, annonces ;
- **OdKiosk** — tablette de cuisine et d'hygiène (HACCP, checklists, nettoyage, étiquettes DLC) ;
- **OdStock** — tablette de stock (réceptions, inventaires) ;
- **OdClock** — pointeuse ;
- **OdLabels** — application iOS (App Store) d'impression d'étiquettes DLC. L'employé s'identifie par son code PIN, choisit un produit et imprime l'étiquette ; l'application échange avec la plateforme par une API dédiée et ne conserve sur l'appareil que le jeton de connexion.

Il couvre également les modules destinés aux consommateurs du restaurant (fidélité, roulette, avis en ligne). Il ne couvre pas le site vitrine odres.io (section 12).

L'application, sa base de données et les fichiers envoyés sont hébergés dans l'Union européenne. Trois fonctions font appel à des prestataires établis aux États-Unis : les notifications push, la lecture et la réponse aux avis Google, et les fonctions d'intelligence artificielle, dans les conditions décrites aux sections 4, 5 et 6.

2. Rôles des parties

Traitement	Responsable du traitement	Rôle d'ODRES
Données des employés, plannings, pointages, RH, HACCP, stock, finances, communication interne du restaurant	Le client (exploitant du restaurant)	Sous-traitant, agissant sur instruction du client via la plateforme
Données des consommateurs du restaurant (fidélité, roulette, avis)	Le client	Sous-traitant ; ODRES fournit les mentions d'information et les mécanismes de consentement, adaptables par le client
Données de compte, de facturation et de support du client (propriétaire, gérants, contacts)	ODRES GROUP SRL	Responsable du traitement
Journaux de sécurité de la plateforme (connexions, audit)	ODRES GROUP SRL	Responsable du traitement (intérêt légitime : sécurité)

3. Personnes concernées et catégories de données

Personnes	Données traitées
Propriétaires, gérants, comptables (utilisateurs ERP)	Identité, e-mail, téléphone, rôle, mot de passe (haché), secret de double authentification, photo de profil, langue, établissements rattachés, journal des actions
Employés (OdStaff, OdClock, OdLabels)	Identité, coordonnées, poste, contrat et documents RH, planning, disponibilités, congés, pointages (horodatage, et selfie de preuve conservé 24 h), code PIN (haché), évaluations, avertissements, formations, réponses aux annonces
Consommateurs du restaurant	Fidélité : nom, e-mail, téléphone, date de naissance (facultative), visites, points, préférences d'opt-in. Roulette : nom, e-mail, téléphone, note attribuée, adresse IP. Avis : nom public, note et texte tels que publiés sur Google
Fournisseurs et contacts professionnels	Coordonnées professionnelles, conditions commerciales, coordonnées bancaires de l'entreprise
Contacts de facturation du client (côté ODRES)	Nom, e-mail de facturation, adresse et numéro de TVA de l'entreprise, état des factures ; le moyen de paiement (mandat SEPA ou carte) est saisi directement chez Stripe et n'est jamais détenu par ODRES
Tous les visiteurs	Adresse IP, navigateur, identifiant de session, prise de connaissance du bandeau d'information

Selfie de pointage. Le selfie pris à la pointeuse est une photographie simple, destinée à un contrôle visuel par le gérant. Aucun traitement biométrique n'est effectué : pas d'extraction de gabarit, pas de reconnaissance faciale, pas de comparaison automatique. Il est supprimé automatiquement 24 heures après la prise. Aucune donnée dite sensible (santé, opinions, biométrie) n'est collectée par conception.

Date de naissance au programme de fidélité. Elle est facultative et sert exclusivement au bonus d'anniversaire du programme (points offerts le jour anniversaire, montant paramétrable par le client). Un client qui n'utilise pas ce bonus n'a pas à la collecter.

4. Localisation des données et hébergement

Élément	Prestataire	Lieu du traitement	Contenu
Serveur de l'application	Railway	Union européenne — Pays-Bas (région Europe-Ouest), point d'entrée réseau à Bruxelles	Le code de la plateforme, les sessions en cours, les traitements planifiés
Base de données PostgreSQL	Neon	Union européenne — Allemagne, Francfort (AWS eu-central-1)	L'ensemble des données métier : sociétés, établissements, employés, plannings, pointages, HACCP, stock, factures, conversations avec l'assistant
Fichiers envoyés	Cloudinary	Union européenne (centre de données européen du prestataire)	Photos de preuve, selfies de pointage, logos, documents RH, pièces jointes, PDF
E-mails sortants	Mailjet (groupe Sinch)	Union européenne	Adresse, nom et contenu de chaque e-mail envoyé par la plateforme
Encaissement des abonnements	Stripe Payments Europe	Irlande (Union européenne) ; certaines fonctions du groupe Stripe aux États-Unis	Identité et coordonnées de facturation du client, moyen de paiement (détenu par Stripe uniquement), factures et état des paiements
Notifications push	Google (FCM), Apple, Mozilla	États-Unis	Texte de la notification et jeton d'appareil ; aucune donnée de la base
Polices et bibliothèques des pages	ODRES (fichiers statiques de la plateforme)	Union européenne (serveur de l'application)	Aucune ressource tierce chargée ; l'adresse IP du visiteur n'est transmise à aucun réseau de diffusion

Polices et bibliothèques. Les polices de caractères (Inter, Manrope, Sora, Plus Jakarta Sans), la bibliothèque d'icônes Font Awesome, Chart.js, SortableJS et Bootstrap Icons sont des copies locales servies par la plateforme elle-même. Aucune page ne charge de ressource depuis Google Fonts, cdnjs ou jsDelivr.

Fichiers privés. Les fichiers contenant des données personnelles ou confidentielles (cartes d'identité, contrats et documents RH, signatures manuscrites, selfies de pointage, photos de profil, justificatifs d'absence, exports de paie, pièces jointes de factures, de notes de frais, de tickets et de support) sont stockés en mode privé : le prestataire de stockage refuse toute adresse non signée, et la plateforme ne communique jamais l'adresse du stockage. Les pages reçoivent un lien ODRES signé, valable quelques heures, servi uniquement à un utilisateur connecté ou à une tablette configurée. Les autres fichiers (logos, images de produits et de recettes, photos de preuve HACCP à conservation courte) sont servis par adresse directe, sans données personnelles identifiantes par conception.

Cadre des transferts. Les données de la base et les fichiers ne quittent pas l'Union européenne. Les transferts vers les États-Unis concernent les notifications push (texte de la notification et jeton d'appareil), les avis Google (données publiques), les fonctions d'intelligence artificielle (section 6) et, pour Stripe, les fonctions du groupe assurées depuis les États-Unis. Ils reposent sur les clauses contractuelles types de la Commission européenne (décision 2021/914) intégrées aux accords de traitement des prestataires et, lorsque le prestataire y est certifié, sur le cadre de protection des données UE-États-Unis (Data Privacy Framework, DPF). Le fondement retenu pour chaque prestataire figure à la section 5.

Siège des prestataires. Railway, Neon et Cloudinary ont leur siège hors de l'Union européenne, bien que le traitement ait lieu dans l'Union. Un prestataire américain reste soumis aux injonctions de son droit national quel que soit le lieu du serveur ; ce point est pris en compte dans l'analyse d'impact des transferts annexée au DPA.

5. Sous-traitants ultérieurs et accords de traitement

5.1 Sous-traitants actifs

Liste arrêtée au 14 octobre 2026 ; elle reprend la numérotation de la section 7.3 de la Politique de confidentialité et de l'Annexe 2 du DPA.

Liste des prestataires qui traitent effectivement des données pour le compte d'ODRES à la date du document (lignes 1 à 12), et des prestataires à désigner avant activation (lignes 13 et 14), à annexer au DPA. Les prestataires non listés ici n'ont accès à aucune donnée. Pour chacun figurent l'accord de traitement applicable et le fondement du transfert hors Union européenne lorsqu'il y en a un.

#	Prestataire et siège	Lieu du traitement	Finalité et données	Accord de traitement	Transfert hors UE
1	Railway Corporation 548 Market St PMB 68956, San Francisco, CA 94104, États-Unis	Pays-Bas	Hébergement de l'application. Toutes les données transitant par l'application	Data Processing Addendum railway.com/legal/dpa	Traitement dans l'UE. Le DPA intègre les clauses contractuelles types (CCT 2021/914) pour tout accès depuis les États-Unis
2	Neon, LLC (groupe Databricks, Inc.) San Francisco, États-Unis	Allemagne (Francfort)	Base de données. Toutes les données métier	Data Processing Agreement neon.com/dpa Sous-traitants : neon.com/subprocessors	Traitement dans l'UE. CCT 2021/914 intégrées au DPA pour tout accès depuis les États-Unis
3	Cloudinary Ltd. Israël (filiale Cloudinary Inc., États-Unis)	Union européenne	Stockage et diffusion des fichiers. Photos, documents RH, pièces jointes, PDF, selfies	Data Processing Agreement (nov. 2023) cloudinary.com/trust/privacy	Traitement dans l'UE. Israël bénéficie d'une décision d'adéquation (2011/61/UE). Cloudinary participe au DPF (UE, Royaume-Uni, Suisse)
4	Mailjet SAS (Sinch Email) Paris, France	Union européenne	Envoi d'e-mails. Adresses, noms, contenu des e-mails	Data Processing Agreement Sinch Email sinch.com/data-protection-agreement	Aucun

5	Stripe Payments Europe, Limited 1 Grand Canal Street Lower, Dublin 2, Irlande	Irlande ; fonctions du groupe aux États-Unis (Stripe, LLC)	Encaissement des abonnements ODRS : client Stripe, mandat SEPA ou carte, factures, portail client. Identité et coordonnées de facturation, numéro de TVA, montants et état des factures. Le moyen de paiement est saisi et conservé chez Stripe uniquement	Data Processing Agreement stripe.com/legal/dpa Politique DPF : s stripe.com/legal/privacy-shield-policy	Stripe, LLC est certifié DPF ; CCT 2021/914 intégrées au DPA. Pour les données de paiement, Stripe agit en responsable de traitement indépendant au titre de ses obligations réglementaires
6	Anthropic Ireland Limited (services dans l'UE) / Anthropic PBC Dublin, Irlande / San Francisco, États-Unis	États-Unis	Assistant conversationnel et aide à la réponse aux avis. Voir section 6	Data Processing Addendum anthropic.com/legal/data-processing-addendum Sous-traitants : anthropic.com/subprocessors	CCT 2021/914, modules 2 et 3, intégrées au DPA ; Anthropic PBC est certifié DPF
7	Google LLC — Business Profile Mountain View, CA, États-Unis	États-Unis	Lecture des avis Google et publication des réponses. Avis publics, réponses, jeton de connexion de l'établissement	Business Profile API Terms developers.google.com/my-business/content/terms Cadre RGPD : business.safety.google/gdpr	Google LLC est certifié DPF. Pour Business Profile, Google agit en responsable de traitement indépendant (données publiques)
8	Google LLC — Firebase Cloud Messaging	États-Unis	Acheminement des notifications push. Texte des notifications, jeton d'appareil	Firebase Data Processing and Security Terms firebase.google.com/terms/data-processing-terms	Google LLC est certifié DPF ; CCT intégrées aux conditions
9	Apple Inc. One Apple Park Way, Cupertino, CA 95014, États-Unis	États-Unis	Acheminement des notifications push (APNs) vers les appareils Apple. Texte des notifications, jeton d'appareil	Apple Developer Program License Agreement ; Politique de confidentialité apple.com/legal/privacy	CCT (Apple déclare fonder ses transferts depuis l'EEE sur les clauses contractuelles types). Apple ne figure pas au DPF
10	Mozilla Corporation San Francisco, CA, États-Unis	États-Unis	Acheminement des notifications push vers Firefox. Texte des notifications (chiffré de bout en bout, illisible par Mozilla), jeton d'appareil	Firefox Privacy Notice mozilla.org/privacy/firefox	CCT (mécanisme déclaré par Mozilla). Le service ne conserve aucune donnée utilisateur ; les messages sont chiffrés et supprimés dès remise

11	Vimeo Inc. New York, NY, États-Unis	États-Unis	Lecture des vidéos du module Formation. Adresse IP et cookies du lecteur, uniquement lorsqu'une vidéo est lancée	Politique de confidentialité vimeo.com/privacy	Vimeo et ses filiales participent au DPF (UE, Royaume-Uni, Suisse). Vimeo agit en responsable de traitement pour les données du lecteur
12	Google LLC — YouTube (mode sans cookie)	États-Unis	Lecture des vidéos du module Formation. Adresse IP, uniquement lorsqu'une vidéo est lancée	Règles de confidentialité Google policies.google.com/privacy	Google LLC est certifié DPF
13	Prestataire de connexion bancaire (service d'information sur les comptes) — non désigné	À inscrire avant activation ; agrément ou inscription DSP2 dans l'EEE exigé	Connexion des comptes bancaires du Client	À conclure avant activation	Statut : aucune connexion bancaire n'est opérée avant la désignation du prestataire, la vérification de son agrément et l'information préalable du Client
14	Service de reconnaissance de documents (OCR) — non identifié	À inscrire avant activation du module	Lecture automatique des documents comptables importés	À conclure avant activation	Statut : aucun traitement automatisé de documents comptables avant l'identification du prestataire et l'information préalable du Client

Les accords et certifications ci-dessus ont été relevés sur les pages officielles des prestataires le 8 octobre 2026. ODRES vérifie leur maintien, et l'inscription au registre officiel du Data Privacy Framework (dataprivacyframework.gov), à chaque révision du présent document.

5.2 Intégrations prévues, non activées

Les intégrations suivantes existent dans la plateforme mais ne sont pas activées à la date du document : aucune clé d'accès n'est configurée, aucun appel n'est émis, aucune donnée n'est transmise. Elles sont annoncées dès maintenant afin d'obtenir l'autorisation générale du client prévue à l'article 8 du DPA. Leur activation donnera lieu à une mise à jour de ce document et à une information du client.

Intégration	Prestataire et siège	Finalité	Données qui seront traitées à l'activation
Ibanity / Ponto	Ibanity (Isabel Group), Belgique	Liaison bancaire : lecture des transactions du compte professionnel du client	Transactions bancaires de l'entreprise cliente (libellé, montant, contrepartie)
e-invoice.be	e-invoice.be, Belgique	Facturation électronique Peppol	Factures clients de l'entreprise cliente (émetteur, destinataire, lignes, montants)

Meta WhatsApp Business	Meta Platforms Ireland Ltd., Irlande	Messages aux fournisseurs et aux employés via WhatsApp	Numéros de téléphone, contenu des messages
Twilio (SMS)	Twilio Inc., États-Unis	Envoi de SMS (rappels, codes)	Numéros de téléphone, contenu des SMS
Perplexity	Perplexity AI Inc., États-Unis	Fournisseur d'intelligence artificielle alternatif	Identiques à celles décrites à la section 6

6. Traitements par intelligence artificielle

Deux fonctions de la plateforme font appel à un modèle de langage fourni par Anthropic (modèle Claude, via son interface de programmation, hébergée aux États-Unis). Aucune autre fonction de la plateforme n'utilise l'intelligence artificielle. L'usage est plafonné en volume (par utilisateur et globalement par mois).

6.1 L'assistant ODRS (back-office ERP)

L'assistant est accessible aux utilisateurs autorisés par leur rôle. À chaque question, les éléments suivants sont transmis à Anthropic :

Élément transmis	Détail
Contexte de l'utilisateur	Son nom, son rôle, le nom de l'établissement en cours et la liste des modules auxquels il a accès
La question et l'historique	Le texte saisi par l'utilisateur et les échanges précédents de la même conversation
Pièces jointes	Une image jointe est transmise telle quelle ; un PDF joint est converti en texte (nombre de pages et longueur limités) et seul ce texte est transmis
Base de connaissances	Des documents rédigés par ODRS (modes d'emploi, procédures), sans données personnelles
Résultat des actions	Lorsque l'utilisateur demande une action (voir ci-dessous), son résultat revient dans la conversation et est transmis avec elle

L'assistant peut exécuter des actions dans l'ERP, uniquement après confirmation explicite de l'utilisateur, dans le périmètre de ses propres droits : créer un service ou une demande de congé, valider des pointages, préparer un export de paie, créer une facture ou un rapport TVA, enregistrer une température, une livraison ou une étiquette DLC, créer un produit, un fournisseur ou une perte, ouvrir un ticket de support, envoyer un e-mail depuis un modèle. Le résultat de ces actions peut contenir des noms d'employés, des heures, des montants et des noms de fournisseurs.

Des règles de sécurité fixes encadrent l'assistant : il ne peut pas révéler ses instructions, produire de code exécutable, divulguer d'information technique sur la plateforme, ni agir sans confirmation. L'utilisateur ne peut obtenir que les données des établissements auxquels il a accès.

6.2 Aide à la réponse aux avis Google (module Réputation)

Pour proposer ou évaluer une réponse à un avis, la plateforme transmet à Anthropic : le nom public de l'auteur de l'avis, sa note, le texte de l'avis, le nom de l'établissement et le brouillon de réponse du gérant. Ces avis sont des données publiques issues de Google Business Profile. La réponse n'est publiée qu'après validation par le gérant.

6.3 Garanties

- Les données transmises via l'interface de programmation d'Anthropic ne sont pas utilisées pour entraîner ses modèles.
- Anthropic conserve les entrées et sorties pour une durée limitée à des fins de détection d'abus, puis les supprime ; ODRES applique l'accord de traitement des données d'Anthropic (section 5.1), qui intègre les clauses contractuelles types pour le transfert UE-États-Unis.
- Ne sont jamais transmis à l'IA : les mots de passe, les codes PIN, les coordonnées bancaires, les selfies de pointage, et toute donnée d'un établissement auquel l'utilisateur n'a pas accès.
- Ce qui est conservé par ODRES : le texte des conversations (dans la base de données, section 4) et un journal d'usage par appel (utilisateur, établissement, modèle, volume, durée, succès), sans le contenu.

7. Cookies et stockage dans le navigateur

La plateforme ne dépose aucun cookie publicitaire ni de mesure d'audience : aucun outil d'analyse de trafic, aucun pixel, aucun traceur tiers déposé par ODRES. Tous les cookies déposés par la plateforme sont strictement nécessaires au fonctionnement du service et ne requièrent pas de consentement ; le bandeau affiché a une fonction d'information et enregistre la prise de connaissance. Les seules ressources tierces chargées sont les lecteurs vidéo du module Formation, et uniquement lorsqu'une vidéo est lancée (7.3).

7.1 Cookies déposés par app.odres.io

Nom	Finalité	Contenu	Durée	Protection
sessionid	Maintien de la connexion de l'utilisateur	Identifiant aléatoire ; les données de session restent sur le serveur	7 jours ; 90 jours glissants sur les tablettes OdKiosk, OdStock et OdClock	HttpOnly, Secure, SameSite=Lax
csrftoken	Protection contre les requêtes forgées (anti-CSRF)	Jeton aléatoire	1 an	Secure, SameSite=Lax
odres_device	Reconnaissance d'une tablette configurée (kiosque, boutique, stock)	Jeton aléatoire propre à la tablette	1 an glissant	HttpOnly, Secure, SameSite=Lax
rcl_<campagne>	Roulette : limitation à une participation par personne et par campagne. Nécessaire au service demandé par le consommateur qui participe	Marqueur « a déjà participé »	30 jours	HttpOnly, Secure, SameSite=Lax
django_language	Langue d'affichage choisie (FR, NL, EN)	Code de langue	Session du navigateur	SameSite=Lax
messages	Affichage d'un message de confirmation après une action	Texte du message	Supprimé dès l'affichage	SameSite=Lax

7.2 Stockage local du navigateur

Les éléments suivants sont enregistrés dans le navigateur de l'utilisateur pour son confort d'usage. Ils ne sont jamais transmis au serveur et ne permettent aucun suivi. La plateforme horodate chaque visite et efface ces clés après 12 mois sans visite.

Clé	Finalité	Durée
<code>erp_sidebar_collapsed</code> , <code>erp_nav_open</code> , <code>erp_nav_scroll</code> , <code>staffSidebarScrollTop</code>	État du menu de navigation	12 mois d'inactivité (localStorage) ou jusqu'à la fermeture de l'onglet (sessionStorage)
<code>profileTab</code> , <code>ph_view</code>	Dernier onglet ou dernière vue affiché	12 mois d'inactivité
<code>posAutoSyncTs</code>	Heure de la dernière synchronisation de caisse	12 mois d'inactivité
<code>staff_onboarding_done</code> , <code>rcv_help_seen</code> , <code>odres_demo_tour_*</code>	Guide de démarrage ou aide contextuelle déjà consulté	12 mois d'inactivité
<code>odres_cookie_consent_v1</code>	Prise de connaissance du bandeau d'information, pour ne pas le réafficher	Jusqu'à effacement par l'utilisateur
<code>odres_ls_last_seen</code>	Date de la dernière visite, qui sert à faire expirer les clés ci-dessus	12 mois d'inactivité

7.3 Autres éléments

- **Notifications push** : activées par l'utilisateur lui-même, désactivables à tout moment dans son profil ou dans le navigateur. La plateforme conserve alors l'adresse de l'appareil fournie par Google, Apple ou Mozilla.
- **Bandeau d'information** : chaque prise de connaissance est enregistrée avec l'horodatage, la version du bandeau, l'identifiant de session et l'utilisateur s'il est connecté. Ni l'adresse IP ni le navigateur ne sont enregistrés.
- **Vidéos de formation** (Vimeo, YouTube en mode « sans cookie ») : le lecteur vidéo ne dépose ses propres cookies qu'au lancement d'une vidéo par l'utilisateur. Ce sont des traceurs tiers, déclarés dans la politique de cookies.

8. Messages automatiques et actions marketing

La plateforme envoie trois familles de messages. Les deux premières sont des messages de service liés au contrat ou à la relation de travail ; seule la troisième relève de la prospection et repose sur le consentement des personnes.

8.1 ODRES vers le client (propriétaire ou gérant)

Déclencheur	Message (e-mail et notification dans l'application)
Période d'essai : 7 jours, 3 jours et 1 jour avant la fin, puis fin de l'essai	Rappel de fin d'essai ; conversion ou suspension

Abonnement souscrit à l'inscription	Confirmation et invitation à commencer la configuration
80 % puis 100 % d'une quantité incluse ; limite de dépenses atteinte	Alerte de consommation
Utilisation dépassant la formule, ou compatible avec une formule inférieure	Information de changement de formule
Facture émise ; facture échue ; paiement refusé	Facture (avec lien de paiement Stripe) ; rappel de paiement
40 jours avant la date anniversaire du contrat	Rappel d'échéance de l'abonnement
Annonce publiée par ODRES (nouveauautés, maintenance)	Bandeau dans l'application
Intervention du support ODRES sur le compte	Notification d'accès au compte

8.2 Le client vers ses employés

Déclencheur	Message (notification push, e-mail, application OdStaff)
Création du compte	Bienvenue, code PIN, mot de passe temporaire, dossier employé à compléter
Planning confirmé ; veille d'un service ; 15 minutes avant ; pointage oublié	Rappels de planning et de pointage
Tâche, checklist ou nettoyage à faire ou en retard	Rappels de tâches
Congé accepté ou refusé ; échange de service	Réponse à la demande
Avertissement, évaluation ou règlement à signer ; document RH arrivant à expiration	Demande de signature ou de mise à jour
Annonce du gérant	Annonce, avec confirmation de lecture lorsque le gérant l'exige

8.3 Le client vers ses consommateurs (prospection)

Outil	Données collectées	Déclencheur	Base légale
Roulette	Nom, e-mail, téléphone, note attribuée, adresse IP (anti-rejeu)	Participation du consommateur ; invitation identique pour tous à publier un avis Google ; e-mail d'annonce du gain ; alerte au gérant pour une note de 1 à 3 étoiles (voir ci-dessous)	Consentement recueilli au moment de la participation
Programme de fidélité	Nom, e-mail, téléphone, date de naissance (facultative, bonus anniversaire), visites, dépenses, points	Passages en caisse ; récompenses	Exécution du programme ; consentement (opt-in) pour les messages

Campagnes	Liste des membres du programme de fidélité avec leurs opt-in e-mail	Envoi manuel ou planifié par le gérant, par e-mail ou notification push	Consentement (opt-in)
Avis Google	Nom public de l'auteur, note, texte	Réponse rédigée avec l'assistant puis publiée par le gérant	Intérêt légitime (données publiques)

Pour cette troisième famille, le client est responsable du traitement et ODRES agit comme sous-traitant. Les textes d'information et de recueil du consentement affichés aux consommateurs sont fournis par la plateforme et adaptables par le client.

Avis Google et roulette. Après sa participation, le consommateur attribue une note de 1 à 5 étoiles. Quelle que soit cette note, il est ensuite invité, par le même écran et avec le même bouton, à publier son avis sur le formulaire Google de l'établissement, puis il accède à la roue. Aucun avis n'est filtré, retenu ou réorienté selon la note. Lorsque la note est de 1 à 3 étoiles, le gérant reçoit en plus une alerte par e-mail, complétée des coordonnées que le client laisse pour recevoir son cadeau, afin de pouvoir le recontacter. Cette alerte s'ajoute à l'invitation à publier ; elle ne s'y substitue jamais. La Politique d'Usage Acceptable interdit au client d'utiliser la plateforme pour filtrer les avis selon leur note.

9. Durées de conservation

Données	Durée	Mécanisme
Selfies de pointage (OdClock)	24 heures	Suppression automatique horaire
Photos de preuve (checklists, nettoyage, étiquettes DLC, réceptions)	7 jours par défaut, réglable par le client (0 = conservation)	Suppression automatique horaire
Journal des connexions (réussies et échouées, adresse IP, navigateur)	180 jours	Purge quotidienne
Contrôles techniques de disponibilité de la plateforme (résultats des sondes)	95 jours	Purge quotidienne
Sauvegardes de la base de données	90 jours (engagement du SLA et du DPA)	Assurées par le prestataire de base de données, dans l'Union européenne (restauration à un instant donné)
Sessions de connexion	7 jours ; 90 jours glissants sur les tablettes	Expiration et purge des sessions expirées
Événements de paiement reçus de Stripe (identifiant, type, date, traitement)	Durée du contrat	Trace d'idempotence ; suppression avec le compte
Conversations avec l'assistant, journal d'usage de l'IA	Durée du contrat	Suppression avec le compte
Preuves de prise de connaissance du bandeau	Durée du contrat	Suppression avec le compte
Journal d'audit (qui a fait quoi, quand)	Durée du contrat	Suppression avec le compte

Données métier (pointages, plannings, RH, HACCP, stock, factures)	Durée du contrat, puis 30 jours de lecture seule pour export après résiliation	Blocage puis suppression ; les données soumises à une obligation légale de conservation (paie, facturation, traçabilité alimentaire) sont conservées le temps requis par la loi belge, sous forme anonymisée lorsque c'est possible
Données de compte et de facturation du client (côté ODRES)	Durée du contrat + délais légaux comptables (7 ans)	Archivage restreint

10. Mesures de sécurité

10.1 Contrôle des accès

- Double authentification (TOTP) obligatoire pour l'ensemble de l'équipe ODRES ayant accès au back-office ; disponible pour tous les utilisateurs clients depuis leur profil.
- Blocage temporaire après 5 échecs de connexion en 5 minutes ; journal des connexions avec signalement automatique des anomalies (nouvel appareil, nouvelle adresse IP, rafale d'échecs).
- Mots de passe et codes PIN stockés uniquement sous forme hachée (PBKDF2-SHA256), jamais lisibles. Le code PIN est obligatoire pour pointer.
- Cloisonnement par société et par établissement : chaque utilisateur ne voit que les établissements qui lui sont rattachés ; des rôles (propriétaire, gérant, employé, comptable) limitent les modules accessibles.
- Accès du support ODRES au compte d'un client : session d'assistance limitée dans le temps, en lecture seule par défaut, tracée dans le journal d'audit et notifiée au client.

10.2 Protection des échanges et de l'application

- Chiffrement TLS de bout en bout (HTTPS obligatoire, HSTS avec préchargement) ; cookies marqués Secure, HttpOnly et SameSite.
- Protection anti-CSRF, protection contre le détournement de clic (X-Frame-Options: DENY), contrôle du type et de la taille des fichiers envoyés.
- Secrets (clés d'API, certificats, secrets de webhooks) stockés exclusivement dans les variables d'environnement de l'hébergeur, jamais dans le code. Les webhooks entrants (Stripe, e-mails fournisseurs, WhatsApp) vérifient la signature de l'émetteur et rejettent les appels non signés, expirés ou rejoués.
- Fichiers privés (section 4) : envoi au stockage en livraison « authenticated », adresse de stockage jamais exposée, lien ODRES signé par la clé secrète de la plateforme, expirant après 4 heures, servi uniquement à une session valable, sans mise en cache partagée et avec interdiction d'indexation.
- Paiements : ODRES ne voit ni ne stocke jamais de numéro de carte ni d'IBAN ; la saisie se fait sur les pages hébergées par Stripe, et ODRES ne conserve que des identifiants techniques.
- Chiffrement au repos assuré par les prestataires d'hébergement (base de données et fichiers).

10.3 Traçabilité

- Journal d'audit des créations, modifications et suppressions, des changements de formule, des accès du support et des acceptations de conditions contractuelles (nom, e-mail, date, adresse IP).
- Liste des sessions actives, consultable et révoque depuis le back-office ; purge automatique des sessions expirées.
- Journal des webhooks reçus (identifiant, type, date, traitement), consultable par l'équipe ODRES.

11. Droits des personnes

Droit	Où l'exercer	Mise en œuvre
Accès et portabilité	Espace « Mes données » de l'ERP et de l'application OdStaff	Export immédiat des données personnelles au format JSON ou CSV, tracé dans le journal
Rectification	Profil de l'utilisateur ; fiche employé (par le gérant)	Modification directe
Effacement	Espace « Mes données » : demande de suppression	Demande enregistrée et traitée par le back-office ODRES ; le compte est anonymisé (identité, e-mail et téléphone remplacés), les consentements supprimés ; les données soumises à obligation légale sont conservées anonymisées
Opposition aux notifications	Profil ou paramètres du navigateur	Retrait immédiat de l'appareil
Information	Fiche société du client	Chaque client renseigne son délégué à la protection des données (nom, e-mail, téléphone) et l'adresse de sa politique de confidentialité, affichés à ses employés dans l'application

Les demandes qui ne peuvent être traitées en libre-service sont adressées à contact@odres.io et traitées dans le délai d'un mois prévu par le RGPD. ODRES assiste le client, en sa qualité de sous-traitant, pour répondre aux demandes des personnes concernées.

12. Périmètre non couvert

Le présent document décrit la plateforme app.odres.io. Le site vitrine odres.io (présentation commerciale, formulaire de contact, assistant de site, liste de diffusion) est une application distincte, déployée séparément ; il fait l'objet d'une fiche technique propre, qui précise son hébergeur, l'assistant de site et la gestion des prospects.

Règle de mise à jour. Ce document est la source technique de référence du corpus contractuel d'ODRES. Toute modification du code ou de la configuration qui touche à la liste des sous-traitants, aux lieux de traitement, aux cookies, aux durées de conservation ou aux fonctions d'intelligence artificielle donne lieu à une nouvelle version, datée et numérotée, et à une information préalable du client conformément au DPA.

ODRES GROUP SRL — Place Verte 20, 6000 Charleroi (Belgique) — BE 0802.601.160 — contact@odres.io — Document établi le 21 octobre 2026 à partir du code et de la configuration déployés à cette date. Version 3.0, remplace la version 2.0 du 8 octobre 2026.