

AIPD — Accompagnement social externalisé

Analyse d'impact relative à la protection des données (RGPD art. 35)

Impact Social — Version 1.0 validée en interne — 8 août 2026

Document de conformité opérationnelle examiné et validé en interne le 8 août 2026 par Pascal COMORASSAMY, Référent protection des données d'Impact Social.

1. Décision de réaliser une AIPD

L'accompagnement social individualisé peut porter sur des informations très personnelles : difficultés familiales, budget, logement, handicap ou santé. La CNIL indique qu'une AIPD est requise pour les traitements susceptibles d'engendrer un risque élevé et que les données sensibles ou hautement personnelles constituent un critère important. La présente AIPD est donc réalisée par prudence et comme outil de pilotage de la conformité.

2. Périmètre et acteurs

Traitement	Accompagnement social individualisé des salariés de structures clientes et production de statistiques agrégées.
Responsable de traitement envisagé	Impact Social pour le dossier social individuel et son suivi, sous réserve de validation contractuelle de la qualification des rôles.
Structure cliente / employeur	Ne dispose d'aucun accès au dossier individuel. Reçoit uniquement des indicateurs agrégés et des recommandations non identifiantes.
Personnes concernées	Salariés utilisant volontairement le service ; contacts RH/dirigeants pour la relation contractuelle.
Sous-traitants techniques identifiés	Netlify (site, fonctions serveur, authentification Identity) ; Google Workspace / Apps Script / Sheets pour le CRM.
Secret professionnel	L'assistant de service social est tenu au secret professionnel (CASF art. L411-3 ; Code pénal art. 226-13 et 226-14).

3. Finalités

- Accueillir la demande du salarié et évaluer sa situation sociale.

- Informer sur les droits et dispositifs, organiser les démarches et orientations utiles.
- Assurer la continuité du suivi et tracer les actions professionnelles strictement nécessaires.
- Produire des statistiques agrégées pour l'entreprise cliente sans révéler l'identité ni le contenu des situations individuelles.
- Assurer la sécurité, la traçabilité et la gestion des comptes de l'espace privé.

4. Données traitées et minimisation

Principe retenu : ne collecter que ce qui est nécessaire à la situation réellement accompagnée. Les catégories suivantes ne sont pas obligatoires et ne doivent être remplies que si elles sont utiles au dossier.

Catégorie	Exemples utiles	Règle de minimisation
Identité/contact	Nom, prénom, coordonnées, éventuellement date de naissance	Pas de NIR stocké. Pas de numéro allocataire CAF/MDPH stocké. Éviter le lieu de naissance et les contacts d'urgence sauf nécessité précise.
Situation sociale	Motif, besoins, plan d'action, échéances	Descriptions factuelles ; éviter les jugements et informations sans lien avec l'accompagnement.
Professionnel	Poste, service, contrat, difficultés liées au travail	Ne pas collecter d'éléments RH non nécessaires ; l'employeur ne reçoit pas le contenu.
Logement / budget / famille	Statut logement, impayés, charges, composition familiale, aide, besoin de protection	Collecter uniquement si le thème est traité. Éviter les détails concernant des tiers non nécessaires.
Santé / handicap	RQTH/MDPH si pertinent, retentissement sur le travail, aménagements nécessaires	Pas de diagnostic détaillé, nom du médecin traitant ou détail d'ALD par défaut. Données de santé uniquement si indispensables.
Entretiens et actions	Date, durée, thème, actions, prochaines échéances	Compte rendu synthétique, professionnel et proportionné.
Reporting employeur	Comptages et tendances	Seuil de confidentialité : catégories < 3 non affichées ; recommandations masquées si volume < 3 situations.

5. Bases juridiques — position de travail à valider

Pour le dossier social individuel, la base de l'article 6 doit être définie contractuellement et dans la notice d'information. Le scénario privilégié dans cette version est l'intérêt légitime (art. 6(1)(f)) à

proposer et délivrer un accompagnement social facultatif, indépendant et confidentiel, avec mise en balance documentée. Pour les données de santé, l'exception de l'article 9(2)(h) relative aux soins ou services sociaux, combinée aux garanties de l'article 9(3) et au secret professionnel de l'assistant de service social, est envisagée ; ce fondement doit être confirmé pour l'organisation exacte d'Impact Social. Le consentement explicite est réservé aux transmissions facultatives à des tiers lorsque cela est pertinent, et n'est pas utilisé comme fondement général du dossier dans la relation de travail.

6. Flux de données

- Salarié → Impact Social : prise de contact et informations nécessaires au suivi.
- Navigateur admin → Netlify Identity : authentification ; JWT vérifié côté serveur.
- Netlify Function → Apps Script : appel serveur avec secret stocké en variable d'environnement, jamais dans le client.
- Apps Script → Google Sheets : lecture/écriture du dossier social.
- Employeur → espace employeur : accès limité à son entreprise par correspondance email → company_code côté serveur.
- Impact Social → partenaire externe : seulement si nécessaire et avec information/accord du salarié, hors obligations légales spécifiques.

7. Durées de conservation

Repère opérationnel retenu pour le dossier social : conservation en base active pendant l'accompagnement, puis suppression/anonymisation au plus tard 2 ans après le dernier contact ou la clôture, sauf obligation légale, contentieux ou besoin d'archivage intermédiaire spécifiquement documenté. Ce repère s'appuie sur la recommandation CNIL du secteur social et médico-social lorsque aucun texte n'impose une autre durée. Un contrôle de conservation sans suppression automatique est intégré au CRM V7.4.6.

Dossier social actif	Pendant l'accompagnement.
Dossier clos	2 ans après dernier contact/clôture — repère interne à confirmer.
Statistiques	Anonymisation irréversible ; conservation possible sans limite RGPD si l'anonymisation est effective.
Journaux de sécurité	Proposition : 12 mois, à confirmer selon besoin de traçabilité.
Comptes employeur	Désactivation à la fin du contrat ; suppression après période technique courte documentée.

8. Droits et information

- Notice dédiée remise ou accessible avant/au premier contact.
- Droits d'accès, rectification, effacement selon conditions, limitation et opposition ; portabilité lorsque applicable.

- Réponse sous un mois, avec vérification proportionnée de l'identité.
- Réclamation possible auprès de la CNIL.
- L'employeur ne reçoit pas les demandes d'exercice de droits relatives au dossier social individuel.

9. Analyse des risques

Risque	Niveau initial	Mesures principales	Niveau résiduel	Décision
Accès de l'employeur à une fiche individuelle	Impact 4 / vraisemblance 2	Aucun endpoint individuel employeur ; company_code résolu serveur ; JWT vérifié ; rôle admin distinct	Impact 4 / vraisemblance 1	Acceptable sous contrôle
Compromission du compte admin	Impact 4 / vraisemblance 3	Identity ; rôle admin ; mot de passe robuste ; MFA à activer si disponible ; journalisation	Impact 4 / vraisemblance 2	À réduire : MFA + revue comptes
Exposition d'un secret API	Impact 4 / vraisemblance 2	Secrets en variables Netlify et Script Properties ; aucun secret côté client ; rotation	Impact 4 / vraisemblance 1	Acceptable
Ré-identification via statistiques	Impact 4 / vraisemblance 3	Seuil <3 masqué ; pas de noms ; recommandations masquées sous 3 situations	Impact 3 / vraisemblance 1	Acceptable
Collecte excessive / NIR	Impact 4 / vraisemblance 3	V7.4.6 bloque le stockage NIR, n° CAF/MDPH, médecin traitant, ALD ; écrans minimisés	Impact 3 / vraisemblance 1	Acceptable après purge éventuelle des anciennes valeurs
Conservation excessive	Impact 3 / vraisemblance 3	Repère 2 ans ; fonction de contrôle ; purge/anonymisation à formaliser	Impact 3 / vraisemblance 2	À surveiller
Fuite via zones de texte libres	Impact 4 / vraisemblance 3	Avertissements UI ; consignes rédactionnelles ;	Impact 4 / vraisemblance 2	À réduire par procédure

		sensibilisation ; pas d'identifiants sociaux/diagnostic s		
Hébergement santé non conforme HDS/EEE	Impact 4 / vraisemblance 3	Google certifié HDS v2.0 pour services couverts, dont Workspace dans certains contextes entreprise ; configuration/con trat/région à vérifier	Impact 4 / vraisemblance 3	BLOQUANT avant données santé réelles
Transfert international / sous-traitants	Impact 3 / vraisemblance 3	DPA des fournisseurs ; SCC/DPF selon fournisseur ; revue sous- traitants et transferts	Impact 3 / vraisemblance 2	À documenter
Suppression accidentelle / indisponibilité	Impact 3 / vraisemblance 2	Sauvegardes contrôlées, journalisation, restauration testée, séparation test/production	Impact 3 / vraisemblance 1	Acceptable

10. Mesures obligatoires avant production réelle

1. Vérifier l'offre Google Workspace réellement utilisée : couverture HDS v2.0 applicable, clauses contractuelles HDS, localisation EEE et services couverts.
2. Activer MFA pour le compte Google et le compte Netlify administrateur ; supprimer tout compte inutile.
3. Purger des anciennes feuilles les NIR, numéros allocataire CAF/MDPH, nom du médecin traitant et détails d'ALD éventuellement présents.
4. Adopter et remettre la notice d'information salarié.
5. Valider le registre de traitement et la qualification des rôles responsable de traitement / sous-traitant dans les contrats clients.
6. Documenter la procédure de violation de données (qualification, journal, notification CNIL sous 72 h si nécessaire).
7. Mettre en place la revue annuelle de l'AIPD ou lors de tout changement significatif.

11. Conclusion de l'AIPD

État au 8 août 2026 : architecture applicative satisfaisante pour les tests avec données fictives. Le risque résiduel reste non acceptable pour des données de santé réelles tant que la conformité de l'environnement d'hébergement HDS/EEE et les conditions contractuelles associées ne sont pas vérifiées. Après levée de ce point bloquant et purge des identifiants exclus, le traitement peut faire l'objet d'une validation de mise en production par le responsable de traitement.

12. Références

- CNIL — Analyse d'impact (AIPD) : <https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd>
- CNIL — Registre des activités de traitement : <https://www.cnil.fr/fr/RGPD-le-registre-des-activites-de-traitement>
- CNIL — Durées de conservation, secteur social et médico-social : <https://www.cnil.fr/fr/secteur-social-et-medico-social-comment-gerer-les-durees-de-conservation>
- CNIL — Décret cadre NIR, secteur social : <https://www.cnil.fr/fr/numero-dinscription-des-personnes-dans-le-secteur-social-le-decret-cadre-nir-en-questions>
- Légifrance — CASF art. L411-3 (secret professionnel des assistants de service social).
- Légifrance — CSP art. L1111-8 et R1111-8-8 (hébergement de données de santé).
- Google Cloud — HDS v2.0 : <https://cloud.google.com/security/compliance/hds>
- Netlify — DPA / Privacy : <https://www.netlify.com/privacy/> et <https://www.netlify.com/gdpr-ccpa/>

Validation interne

Statut	Validé en interne
Référent protection des données	Pascal COMORASSAMY
Fonction	Référent protection des données
Date de validation	08/08/2026
Portée de la validation	Validation de l'AIPD et des mesures organisationnelles documentées. La mise en production avec des données de santé réelles reste conditionnée à la levée des réserves HDS/EEE et contractuelles identifiées dans le document.

Cette validation est une validation interne de conformité documentaire. Elle ne constitue ni une certification, ni un avis juridique externe.