

Politique de confidentialité Pulse myIT Mobile

Version 2026.09-R5 · En vigueur depuis le 19 octobre 2026 · Dernière mise à jour : 19 octobre 2026

Cette politique explique l'utilisation des données dans le site <https://mobile.pulsemyit.fr>, la Plateforme <https://app.mobile.pulsemyit.fr>, la souscription et les Services mobiles. Elle s'adresse aux prospects, Clients professionnels, représentants, signataires, mandants, mandataires, Gestionnaires et utilisateurs de Lignes. Elle est communiquée pour information ; l'accepter n'est pas une condition juridique générale des traitements.

01 Responsable et contact

PULSE MYIT, SAS au capital de 1 000 euros, RCS Nantes 979 954 856, SIRET 979 954 856 00014, TVA FR26979954856, siège 38 route de Saint-Hilaire, 44190 Clisson, France, est responsable des traitements qu'elle décide pour ses propres activités. Contact données personnelles : donnees.personnelles@pulsemyit.fr ou courrier au siège à l'attention du correspondant données personnelles. Ce contact ne présume pas de la désignation d'un délégué à la protection des données. PULSE MYIT n'a pas désigné de délégué à la protection des données ; elle réexamine périodiquement si les conditions de l'article 37 du règlement (UE) 2016/679 sont réunies.

Pour les traitements de gestion de flotte effectués sur instruction du Client, celui-ci est responsable du traitement et PULSE MYIT est son sous-traitant, selon l'accord RGPD. Le Client communique alors son propre contact et ses informations aux collaborateurs concernés.

02 Provenance et catégories

Les données proviennent de la personne concernée, de son entreprise ou de ses représentants, des registres et sources d'entreprise utilisés lors des vérifications, des opérateurs nécessaires au Service et des opérations réalisées dans la Plateforme.

Elles comprennent, selon le parcours : nom et coordonnées professionnelles ; entreprise, fonction et habilitations ; identifiants de compte ; lignes et numéros attribués ; commandes, offres et factures ; coordonnées bancaires et références du mandat ; échanges de support et pièces jointes ; adresses IP, horodatages, informations du navigateur et événements de sécurité.

Pour la signature et la vérification de pouvoirs peuvent être traités la date et le lieu de naissance du Signataire, les informations issues des registres, la qualité du représentant, une délégation et les justificatifs d'identité nécessaires du mandant ou du mandataire. Les pièces sont demandées en fonction de la vérification requise, et non pour une réutilisation commerciale.

Les relevés de communications ou CDR peuvent comporter un numéro de Ligne, des dates, durées, volumes, destinations et montants. Ils sont distincts du contenu des appels, messages ou pages consultées. Le Service de gestion de flotte ne réalise pas d'écoute ou de transcription du contenu des communications.

03 Finalités et bases des traitements propres à PULSE MYIT

Demandes entrantes et souscription — Finalité : Répondre, identifier l'entreprise et préparer le Service ; Base retenue selon la personne : Mesures précontractuelles ou contrat si la personne est elle-même partie ; intérêt légitime de gestion des relations professionnelles pour les représentants

Contrat et pouvoirs — Finalité : Vérifier le pouvoir, signer, conserver une preuve utile ; Base retenue selon la

personne : Intérêt légitime de sécurité des engagements ; obligation légale pour les vérifications effectivement imposées

Fourniture mobile — Finalité : Acheminer et gérer le Service et les données nécessaires à son exécution ; Base retenue selon la personne : Exécution du contrat pour l'abonné personne physique ; intérêt légitime à fournir le service professionnel demandé pour les contacts et utilisateurs qui ne sont pas parties, sous réserve de la mise en balance et des règles sectorielles ; obligation légale pour les opérations imposées

Facturation et paiements — Finalité : Établir les factures, recevoir les paiements et traiter les réclamations ; Base retenue selon la personne : Contrat pour une personne partie, intérêt légitime pour les contacts et représentants, obligations comptables et fiscales

Sécurité et prévention des abus — Finalité : Protéger les comptes, Lignes, réseaux et systèmes ; Base retenue selon la personne : Intérêt légitime, dans les limites des règles sectorielles ; obligation légale lorsqu'elle s'applique

Obligations des opérateurs — Finalité : Conserver et communiquer les seules données légalement requises ; Base retenue selon la personne : Obligation légale identifiée, notamment CPCE L34-1 dans son périmètre applicable

Assistance et incidents — Finalité : Résoudre une demande et documenter la réponse ; Base retenue selon la personne : Contrat ou intérêt légitime selon la qualité de la personne ; instruction du Client pour les données traitées pour son compte

Prospection professionnelle — Finalité : Présenter des offres en lien avec l'activité du contact ; Base retenue selon la personne : Intérêt légitime lorsque permis, avec opposition simple ; consentement lorsque requis

Le contrat conclu avec une société ne fait pas automatiquement de ses salariés des parties à ce contrat. L'intérêt légitime fait l'objet d'une appréciation de nécessité et de proportionnalité tenant compte de leurs droits. Il ne permet pas de contourner une règle spéciale de consentement ou de conservation des données de trafic.

Contacts du formulaire commercial

Lorsqu'un professionnel demande une analyse de flotte, ses nom, prénom, coordonnées, entreprise, SIREN et éléments fournis sur sa flotte, ses sites, ses zones, son besoin et son échéance sont utilisés pour traiter la demande. Une référence de dossier, l'origine de la demande et des paramètres de campagne UTM peuvent y être associés. Si la connexion Brevo est active, ces informations sont enregistrées dans l'outil de gestion des contacts et transmises au service commercial. Une demande de contact ne vaut pas consentement à toutes les campagnes ultérieures. La prospection suit sa base propre, avec opposition effective, y compris lors de la mise à jour d'un contact existant. Les messages libres et paramètres de campagne sont limités aux informations utiles. La présence de paramètres UTM ne suffit pas à qualifier l'usage réel des traceurs, qui est vérifié séparément.

04 Optimisation facultative des forfaits

Le module de recommandation compare les volumes et coûts d'une Ligne avec les offres pertinentes, sur les mois disponibles dans la durée de conservation autorisée. Il peut signaler un forfait surdimensionné, insuffisant ou une utilisation atypique. Le calcul repose sur des règles et des statistiques de consommation ; il ne nécessite pas, en lui-même, de transmettre les relevés à une IA externe.

La recommandation reste indicative : l'historique peut être incomplet et les usages futurs varier. Le Gestionnaire confirme toute modification. Aucune décision produisant automatiquement un changement de forfait ou une conséquence contractuelle n'est prise par ce module dans le périmètre décrit.

Pour le traitement facultatif de trafic, l'abonné reçoit une information spécifique et donne un consentement exprès lorsque le CPCE le requiert. Le parcours proposé recueille cet accord pour une période déterminée de douze mois au plus, sans reconduction silencieuse, et permet le retrait à tout moment. Les calculs

cessent après retrait. Ce choix de l'entreprise ne vaut pas consentement RGPD de ses salariés ; l'usage de leurs données doit aussi disposer d'une base appropriée et d'une information individuelle. Sous la responsabilité de PULSE MYIT, la finalité de recommandation est fondée sur l'intérêt légitime de fournir une optimisation facultative proportionnée, sous réserve de cette analyse et de la règle sectorielle de consentement.

Les statistiques d'aide au choix peuvent utiliser les trois mois complets les plus récents disponibles dans la fenêtre autorisée, sans qu'ils soient nécessairement consécutifs. La période disponible et les limites d'interprétation sont expliquées. Une lacune de collecte n'est pas une consommation nulle. Les choix de changement de forfait, leurs motifs utiles et les éléments de comparaison retenus peuvent être conservés avec la commande ; ils ne justifient pas l'archivage durable des relevés bruts de communications.

05 Signature électronique et identité

Yousign intervient, lorsqu'il est activé, pour la signature du cadre initial, des CGU, de l'accord RGPD et du mandat, la constitution des preuves et la vérification d'identité correspondant au niveau de signature choisi. La politique de confidentialité est jointe pour information sans signature obligatoire. Les commandes ultérieures sont prouvées par la trace figée de leur contenu et les événements d'acceptation dans la Plateforme ; elles ne nécessitent pas systématiquement une nouvelle vérification d'identité chez Yousign. Le parcours peut comporter une signature qualifiée et une vérification des pouvoirs ou d'une délégation.

Avant une vérification d'identité, la personne reçoit l'information propre au prestataire sur les justificatifs, la méthode, les destinataires et la conservation. Si une vérification biométrique est utilisée par un prestataire, son régime et l'information correspondante doivent être établis avant son déclenchement. Cette politique ne présente pas PULSE MYIT comme conservant des gabarits biométriques. Les justificatifs d'identité ne sont pas joints aux exports ordinaires de flotte ou aux factures.

06 Données nécessaires et conséquences du refus

Les champs nécessaires sont identifiés au moment de leur collecte. Sans les données indispensables à l'entreprise, à la Ligne, à la facturation ou à une vérification requise, PULSE MYIT peut ne pas pouvoir conclure ou exécuter le Service. La raison est expliquée. Le parcours d'ouverture complète du compte prévoit un mandat SEPA CORE ; les coordonnées du titulaire et de son compte sont donc nécessaires à ce parcours, même avant une première commande. Leur collecte n'autorise aucun débit sans dette et mandat valables. Les données d'un dossier abandonné suivent une durée limitée de suivi et de preuve ; elles ne sont pas conservées comme celles d'un abonnement actif. Les informations facultatives et les modules facultatifs sont distingués ; leur refus n'empêche pas l'accès aux Services qui n'en dépendent pas.

07 Destinataires

Les données sont accessibles aux seules personnes habilitées de PULSE MYIT et, selon leur besoin, aux opérateurs et fournisseurs amont, hébergeurs, prestataires de messagerie, signature, paiement, facturation et support. Les conseils, comptables et autorités reçoivent uniquement les données nécessaires à leur mission et dans les conditions applicables. PULSE MYIT ne vend pas les données personnelles.

Les intervenants à qualifier dans ce lot comprennent INIT-SYS, identifié comme émetteur d'une facture mobile, et la chaîne Alphalink, Orange et Bouygues Telecom ; Scaleway pour l'infrastructure ; les registres publics utilisés, notamment l'Annuaire des entreprises, INSEE, INPI, BODACC, VIES et éventuellement Pappers ; Scaleway TEM ou le serveur SMTP configuré pour les courriels ; OVH, Brevo ou le service REST configuré pour les SMS ; Yousign pour la signature ; Agicap pour la fonction de facturation concernée. Brevo peut aussi recevoir les contacts du formulaire commercial du site, selon son activation. Leur rôle juridique dépend du service effectivement fourni. Agicap n'est pas désigné, du seul fait de cette fonction, comme banque ou prestataire exécutant les prélèvements.

Le registre détaillé des intervenants réellement actifs, de leurs entités contractantes, des services

concernés, des lieux de traitement et des garanties applicables est annexé à la présente politique et publié avec elle. Il est daté et mis à jour lors de tout changement d'intervenant. Ce registre fait partie de l'information remise et est daté. La liste de préparation ci-dessus ne vaut pas attestation que chaque service est actif.

08 Connexion à une IA et signalement de défauts

Lorsqu'un Gestionnaire autorise une application externe par MCP, celle-ci peut recevoir les informations permises sur l'entreprise, les Lignes et SIM, les consommations synthétiques, les commandes, alertes ou factures. Les permissions sont limitées au compte et à son organisation. Ce connecteur n'expose pas, dans le périmètre décrit, les relevés bruts du fournisseur et ne permet pas de modifier les Services.

Le Client ou l'Utilisateur choisissant un outil externe vérifie ses propres responsabilités et celles du destinataire. La révocation arrête les accès futurs mais ne supprime pas automatiquement les copies déjà reçues par cet outil. Les conditions de l'outil peuvent prévoir d'autres lieux de traitement. PULSE MYIT distingue ce choix du recours à un prestataire qu'elle aurait elle-même sélectionné comme sous-traitant.

Une fonction facultative de signalement de défaut peut transmettre à GitHub, si elle est activée, une description, les étapes de reproduction et un contexte technique pouvant comprendre le nom, le courriel, le rôle, l'organisation, l'URL, le navigateur et des événements de console. Dans le parcours documenté, la capture reste dans le stockage applicatif et un lien vers un accès réservé est inséré dans le signalement ; une éventuelle autre modalité de transfert est décrite avant activation. Les données et destinataires sont indiqués avant l'envoi ; les éléments inutiles et secrets sont retirés. Le registre des intervenants précise ce service et ses lieux de traitement avant activation.

09 Lieux de traitement et transferts

Le registre joint indique les lieux de l'hébergement principal, des sauvegardes et des accès autorisés. Les ressources Scaleway facturées dans la pièce de rapprochement E01 comportent des régions françaises ; l'affectation exacte des ressources à la Plateforme doit être confirmée pour arrêter ce registre. Cette localisation ne garantit pas, à elle seule, que tout prestataire, support distant ou outil choisi par le Client traite exclusivement dans l'Espace économique européen.

Pour les transferts relevant de sa responsabilité, PULSE MYIT identifie le pays, le destinataire et le mécanisme applicable avant transfert : décision d'adéquation ou garanties appropriées, notamment clauses contractuelles types accompagnées de l'évaluation et des mesures requises. Ces informations et le moyen d'obtenir une copie des garanties, expurgée si nécessaire, figurent au registre ou sont disponibles auprès du contact données personnelles. Les transferts réalisés par un outil choisi directement par le Client sont également pris en compte dans sa propre analyse.

10 Conservation

Les données sont séparées selon leur finalité. Une archive légale n'est pas réutilisée pour la prospection, une recommandation ou le contrôle courant des collaborateurs. Une conservation exceptionnelle liée à un litige ou à une injonction porte sur le seul périmètre justifié ; elle ne prolonge pas globalement toute la base.

Données de gestion traitées pour le Client : Durée du Service puis restitution et suppression selon l'accord RGPD, sans dépasser un plafond légal plus court

Compte et contacts commerciaux actifs : Durée de la relation ; données de preuve strictement utiles isolées ensuite

Inscription abandonnée et cadre sans Service actif : Calendrier de clôture, relance et minimisation : clôture du dossier abandonné après 90 jours sans démarche utile ; cadre sans Service revu après 12 mois d'inactivité, avec avis 30 jours avant clôture ; purge des pièces non nécessaires selon leur calendrier spécifique ; les justificatifs et données bancaires ne suivent pas automatiquement la durée des prospects

Contrats et preuves d'acceptation : Cadre et commandes conservés pendant leur utilité contractuelle puis archive limitée au délai applicable ; cible de cinq ans après fin pour les pièces soumises au droit commun, sans prolonger les données de trafic. L'intégrité des documents conservés ne signifie pas une conservation indéfinie

Factures et pièces comptables : Dix ans à compter de la clôture de l'exercice concerné, conformément à l'article L. 123-22 du code de commerce

CDR nécessaires à la facturation : Au plus un an pour les données relevant du III de l'article R. 10-14 du code des postes et des communications électroniques, avec point de départ technique rattaché à la communication documenté dans le registre ; un import tardif ne remet pas le compteur à zéro, et moins si la finalité cesse ; pas de règle générale de treize mois

Données de trafic pour la sécurité du réseau : Durée nécessaire, au plus trois mois pour les données relevant du IV de l'article R. 10-14 du code des postes et des communications électroniques ; autres archives légales distinctes

Statistiques et recommandations facultatives : Fenêtre de douze mois glissants au plus, uniquement sur les données dont le traitement est autorisé ; suppression des résultats individualisés devenus inutiles après retrait, au plus trente jours

Archives opérateur relatives à l'identité civile : Cinq ans après fin du contrat dans le périmètre imposé par le 1° du II bis de l'article L. 34-1 du code des postes et des communications électroniques ; cette règle ne justifie pas toutes les copies de pièces d'identité

Autres données de souscription et paiement visées par L34-1 II bis : Un an après fin du contrat ou clôture du compte, dans le périmètre légal ; factures et preuves de mandat suivent leur régime distinct

Source de connexion et terminaux visés par L34-1 II bis : Un an après la connexion ou l'utilisation concernée, dans le périmètre légal

Journaux applicatifs de sécurité hors archives obligatoires : Six mois après l'événement, sauf incident documenté justifiant un archivage ciblé

Copies de justificatifs d'identité de vérification : Suppression après contrôle achevé, au plus trente jours après sa clôture, sauf obligation précise ou contestation justifiée ; preuves minimisées conservées séparément

Mandat et preuve bancaire : Durée d'utilisation du mandat puis durée d'archivage exigée par le régime applicable et la banque ou le prestataire chargé des prélèvements SEPA, fixée avant signature dans le registre

Tickets et échanges de support : Trois ans après clôture, avec retrait préalable des pièces devenues inutiles

Prospects professionnels : Trois ans après le dernier contact émanant du prospect ; opposition conservée au strict nécessaire pour la respecter

Demandes d'exercice de droits : Trois ans après clôture pour la preuve utile ; justificatifs d'identité supprimés dès vérification

Sessions et invitations : Session au plus sept jours ; invitation supprimée ou invalidée à expiration, purge des données inutiles sous trente jours

Sauvegardes des données traitées pour le Client : Expiration sur un cycle de quatre-vingt-dix jours au plus après suppression active, sous réserve de tout plafond légal plus court ; accès limité à la restauration et réapplication des suppressions

Une statistique reste une donnée personnelle si une personne peut être retrouvée. Seules des données effectivement anonymes, après vérification du risque de réidentification, sortent du régime des données personnelles. Le calendrier définitif est aligné sur les systèmes exploités et le registre des traitements avant

publication de la présente politique.

Les informations relatives à l'identité civile de l'utilisateur, les autres informations fournies lors de la souscription et les informations relatives au paiement, ainsi que les données techniques permettant d'identifier la source de la connexion ou relatives aux équipements terminaux, sont conservées dans les conditions et pour les durées fixées au II bis de l'article L. 34-1 du code des postes et des communications électroniques, dans sa rédaction issue de la loi n° 2025-532 du 13 juin 2025, pour les besoins des procédures pénales, de la prévention des menaces contre la sécurité publique et de la sauvegarde de la sécurité nationale. Les catégories de données concernées sont celles énumérées à l'article R. 10-13 du même code. Ces données ne sont communiquées qu'aux autorités disposant légalement d'un droit d'accès, dans les seuls cas et selon les seules modalités prévus par la loi.

11 Sécurité

Les mesures comprennent des accès nominatifs et limités par rôle, un second facteur sur les profils et opérations sensibles, des protections des sessions, la journalisation pertinente, le chiffrement des données bancaires sensibles, des accès privés aux justificatifs et la protection des échanges. Les sauvegardes, procédures d'incident et habilitations sont contrôlées périodiquement.

Les informations de session désignent ici les éléments techniques d'authentification et de sécurité ; elles ne constituent pas un enregistrement vidéo permanent des écrans. Une capture transmise volontairement au support relève d'une information distincte. Les engagements détaillés envers un Client responsable de traitement figurent dans l'accord RGPD.

12 Incidents et violations

PULSE MYIT analyse les incidents, limite leurs effets et documente les suites. Lorsqu'elle est responsable du traitement, elle effectue les notifications imposées à l'autorité et aux personnes dans les conditions et délais du RGPD. Lorsqu'elle agit pour le compte du Client, elle l'informe sans délai injustifié selon l'accord RGPD afin qu'il puisse remplir ses propres obligations.

13 Droits et demandes

Selon les conditions applicables, une personne peut demander l'accès, la rectification, l'effacement, la limitation ou la portabilité de ses données, s'opposer à certains traitements et retirer un consentement. Le retrait ne remet pas en cause les traitements antérieurs licites. L'opposition à la prospection est possible à tout moment ; pour un autre intérêt légitime, elle s'apprécie selon la situation de la personne et les motifs légitimes opposables. Des directives après décès peuvent être données dans les conditions du droit français.

Les demandes sont adressées à donnees.personnelles@pulsemyit.fr ou au siège. Une pièce d'identité n'est demandée qu'en cas de doute raisonnable et dans la mesure nécessaire. PULSE MYIT répond dans le mois suivant la réception ; une prolongation de deux mois au plus peut être nécessaire au regard de la complexité ou du nombre de demandes et est expliquée avant l'expiration du premier mois. Les droits peuvent être limités par une obligation de conservation ou les droits de tiers ; le motif est alors indiqué.

Pour un traitement décidé par son employeur, la personne peut aussi contacter celui-ci. PULSE MYIT oriente et assiste la demande lorsqu'elle agit comme sous-traitant, sans abandonner ses obligations pour ses propres traitements. Une réclamation peut être adressée à la CNIL, 3 place de Fontenoy, TSA 80715, 75334 Paris Cedex 07, ou sur cnil.fr.

14 Données des collaborateurs

L'entreprise décrit à ses collaborateurs les affectations de Lignes, les statistiques, les finalités de maîtrise des coûts et les accès des Gestionnaires. Elle respecte les obligations d'information et, lorsqu'elles s'appliquent, de consultation des représentants du personnel. Les restitutions sont proportionnées et ne servent pas à une surveillance permanente injustifiée.

Les quatre derniers chiffres des numéros appelés sont masqués par défaut sur les relevés destinés à l'employeur. Une demande exceptionnelle de numéros complets est justifiée, contrôlée et tracée, notamment au regard d'un usage manifestement abusif ; un simple rôle de facturation ne constitue pas cette justification.

15 Cookies et autres traceurs

Les traceurs nécessaires assurent l'authentification, la sécurité, les préférences indispensables et la continuité d'une opération demandée. Les traceurs facultatifs soumis au consentement ne sont activés qu'après un choix positif, révocable. Le refus n'interdit pas les fonctions qui n'en dépendent pas. Un outil d'audience n'est dispensé de consentement que si toutes les conditions d'exemption sont réunies.

Les choix de colonnes de la liste de Lignes peuvent être mémorisés dans le navigateur pour retrouver l'affichage demandé. Les sélections de changement de forfait sont conservées temporairement pendant la navigation et rattachées à l'organisation ; elles ne déclenchent aucune action sans confirmation. Ces préférences sont distinguées des traceurs de mesure ou de publicité.

La liste des traceurs effectivement déployés, leur finalité, leur éditeur et leur durée sont annexées à la présente politique et publiées avec elle, séparément pour le site public et pour la Plateforme. La durée d'un cookie et la durée d'une donnée en base peuvent différer et sont précisées séparément.

16 Information indirecte et mises à jour

Lorsque les données proviennent du Client ou d'un registre, les personnes reçoivent l'information requise dans les délais applicables, notamment lors du premier contact et, au plus tard, dans le délai légal lorsqu'aucune exception ne s'applique. Les informations relevant du Client et celles relevant de PULSE MYIT sont distinguées.

La version de la politique et sa date d'application sont indiquées dans le dossier remis. Un changement substantiel est annoncé de manière appropriée avant sa mise en œuvre ; un nouveau consentement est demandé s'il est nécessaire. Une mise à jour de cette politique ne suffit pas à autoriser un traitement incompatible avec les informations et choix antérieurs.