Comment BioPoint protège vos données

Version 1.4 du 04/11/2026 — BioPoint, document de sécurité

Cette page dit ce que le service fait réellement, tel qu'il est programmé et configuré à ce jour : chaque chiffre est lu dans le code qui l'applique. Les engagements contractuels sont ceux des conditions générales de vente (art. 19 et Annexes 1 à 3).

L'ESSENTIEL

• Hébergé dans l'Union européenne : Allemagne (Francfort) ; sauvegardes chiffrées en Irlande.
• Chiffré : HTTPS, et les données sensibles chiffrées dans la base (AES-256-GCM).
• Vérification en deux temps : Obligatoire pour les gérants, les directions, les élus et l'équipe.
• Preuves scellées : Pointages et journal chaînés : une retouche se voit.
• Sauvegarde chaque nuit : Chiffrée, hors de l'hébergeur, gardée 30 jours.
• Aucune biométrie : Un badge ou un compte, jamais une empreinte ni un visage.

1. OÙ SONT VOS DONNÉES

L'application et la base de données sont hébergées par Render Services, Inc., sur des serveurs situés en Allemagne (Francfort). Les sauvegardes, chiffrées, sont déposées chez Supabase, Inc., en Irlande, dans un espace privé distinct de l'hébergeur principal.

• BioPoint ne fait intervenir que les sous-traitants ultérieurs du tableau ci-dessous, autorisés par le contrat (Annexe 1 des CGV, point 3.1). Les fonctions facultatives ne font intervenir leur prestataire que tant qu'elles sont actives.

• Tout ajout ou remplacement d'un sous-traitant est annoncé par e-mail au moins 30 jours à l'avance ; l'établissement peut s'y opposer et, à défaut de solution, mettre fin au contrat sans frais.

• Certains prestataires sont des sociétés américaines ou appartiennent à un groupe américain : le tableau dit, pour chacun, comment le transfert est encadré.

• Les données ne sont ni revendues, ni cédées, ni exploitées à des fins publicitaires ; BioPoint n'entraîne aucun modèle d'intelligence artificielle sur elles.

Les sous-traitants ultérieurs (Annexe 1 des CGV)

Render Services, Inc.
Pays du prestataire : États-Unis
Serveurs : Allemagne (Francfort)
Rôle : Hébergement de l'application et de la base de données
Encadrement d'un transfert : Certifié au cadre de protection des données UE–États-Unis (Data Privacy Framework)

Supabase, Inc.
Pays du prestataire : États-Unis
Serveurs : Irlande
Rôle : Sauvegardes de la base, chiffrées par BioPoint avant l'envoi et conservées trente jours
Encadrement d'un transfert : Clauses contractuelles types de la Commission européenne ; chiffrement préalable, clé détenue par BioPoint seul

Sendinblue SAS (Brevo)
Pays du prestataire : France
Serveurs : Union européenne
Rôle : Envoi des e-mails et des SMS du Service
Encadrement d'un transfert : Aucun transfert

OpenAI Ireland Ltd (groupe OpenAI)
Pays du prestataire : Irlande, groupe américain
Serveurs : États-Unis
Rôle : Assistant conversationnel et aide au classement des documents déposés, tant que le Client ne les a pas désactivées (offres Complètes ; jamais dans l'offre Essentielle) ; aucun CV ne lui est transmis
Encadrement d'un transfert : Clauses contractuelles types de la Commission européenne (décision 2021/914) ; accord de traitement des données (DPA) signé avec OpenAI le 06/11/2026

The Next Path Software Consulting Inc. (Metered)
Pays du prestataire : Canada
Serveurs : France
Rôle : Relais des appels vidéo entre le salarié et son responsable (serveur TURN), lorsque la connexion directe entre leurs appareils est impossible : flux chiffrés de bout en bout (DTLS-SRTP), que le relais ne peut ni lire ni enregistrer, et adresses IP des participants (seulement pendant un appel vidéo dont la connexion directe est impossible)
Encadrement d'un transfert : Décision d'adéquation de la Commission européenne pour le Canada (décision 2002/2/CE),

maintenue en 2024 ; serveurs en France

Scaleway SAS

Pays du prestataire : France
Serveurs : France (Paris)
Rôle : Copie de sécurité du journal d'audit (Cockpit) : journaux techniques, sans donnée de santé ni secret, adresses IP tronquées
Encadrement d'un transfert : Aucun transfert

2. LE CHIFFREMENT

Vos données sont chiffrées pendant leur transport et, pour les plus sensibles, dans la base elle-même.

• Pendant le transport : le site s'utilise en HTTPS. En production, chaque réponse porte l'en-tête HSTS (un an, sous-domaines compris), qui interdit au navigateur de revenir en clair, et le cookie de session est marqué Secure, HttpOnly et SameSite.

• Dans la base : avant d'être écrites, les données les plus sensibles sont chiffrées par l'application en AES-256-GCM, avec une clé conservée hors de la base. Sont ainsi chiffrés les numéros de sécurité sociale, les IBAN, les déclarations sociales (DSN) produites, le statut de bénéficiaire de l'obligation d'emploi, la situation familiale qui ouvre un droit, les aménagements d'horaires et de poste, et leur source, la déclaration certifiée du dossier du salarié, les numéros des titres d'autorisation de travail, les documents déposés et les contrats signés, les CV déposés à la borne, les vidéos et certificats de formation, les dossiers mensuels scellés et les secrets d'authentification et les clés des bornes.

• Les textes libres sont chiffrés de la même façon : les messages entre salariés et responsables, les échanges avec l'assistant, les signalements, les mesures disciplinaires et les contenus de l'espace des élus.

• En production, le service refuse d'écrire un numéro de sécurité sociale en clair si la clé de chiffrement manque.

• Les mots de passe ne sont jamais conservés : seule leur empreinte (scrypt) l'est.

• Les sauvegardes sont chiffrées avec une clé dédiée, distincte de celle de la base.

Ce chiffrement protège une copie de la base, prise par une sauvegarde volée ou une intrusion dans la base. Il ne protège pas contre qui obtiendrait aussi les clés du serveur : aucun chiffrement au repos ne le fait.

3. QUI PEUT ENTRER

Chaque utilisateur a ses propres identifiants ; les espaces du CSE et des organisations syndicales s'ouvrent par un compte propre à l'instance, pour qu'aucune appartenance syndicale ne soit enregistrée. Le salarié choisit lui-même son mot de passe, que ni l'employeur ni BioPoint ne connaissent.

• La vérification en deux temps est obligatoire pour les gérants, les directions d'enseigne, les experts-comptables, l'équipe de BioPoint, les élus du CSE et le compte d'administration de BioPoint (hors comptes de démonstration, sans donnée réelle) ; elle est proposée aux salariés.

• Trois méthodes, au choix de chacun : Face ID ou empreinte ; code de l'application d'authentification ; code reçu par e-mail. La clé d'accès ne transmet à BioPoint qu'une clé publique ; le secret de l'application est chiffré ; le code reçu par e-mail vaut 10 minutes, ne sert qu'une fois et tombe après 5 essais faux. L'activation remet 10 codes de secours à usage unique.

• Depuis une même adresse, au-delà de 5 essais de connexion faux en 5 minutes, la connexion est bloquée 5 minutes.

• Une session dure au plus 10 heures depuis son ouverture, même utilisée sans arrêt. Seule exception : dans l'application BioPoint pour iPhone ou Android, salariés, gérants, élus du CSE, directions d'enseigne et experts-comptables restent connectés sans limite de durée, jusqu'à leur déconnexion : la session ne se ferme pas d'elle-même, seulement quand son titulaire la ferme, quand elle est fermée à distance ou quand son accès prend fin. Tout navigateur, et les comptes de la console d'administration de BioPoint, restent à 10 heures. Chacun voit ses appareils connectés et peut fermer une session à distance ; le gérant peut fermer celles d'un salarié, et le départ du salarié les ferme ; changer de mot de passe ferme toutes les autres.

• Le titulaire d'un compte est prévenu quand son compte bouge : connexion depuis un nouvel appareil, verrouillage après des essais faux, mot de passe changé, second facteur retiré.

4. CHACUN NE VOIT QUE CE QUI LE CONCERNE

Tous les établissements partagent l'application, jamais leurs données.

• Les données de chaque établissement sont séparées logiquement : une page ne montre que ce qui appartient à l'établissement de la session, et changer un numéro dans l'adresse ne donne pas accès à celles d'un autre. Une épreuve

d'isolation, écrite dans le code, tente d'y parvenir par chaque route, chaque rôle et chaque méthode.

• L'employeur n'accède pas à l'espace des élus du CSE.

• Les membres de l'équipe de BioPoint ont chacun leur compte et leur rôle : chacun ne voit que les établissements qui lui sont confiés ; le commercial ne voit aucune donnée de paie ni de salarié.

• L'assistance de BioPoint n'ouvre l'espace d'un établissement que s'il l'y autorise : en lecture seule, avec un motif écrit et le nom de la personne, pendant 4 heures au plus ; chaque écran ouvert est inscrit à un journal que l'établissement consulte, et il retire l'autorisation d'un bouton.

• Les formateurs de BioPoint ne voient que des taux de bonnes réponses agrégés, à partir de dix réponses, jamais un nom.

5. DES PREUVES QU'ON NE RETOUCHE PAS

Les pointages et le journal d'audit sont scellés : une retouche se voit.

• Chaque pointage est scellé et chaîné au précédent (HMAC-SHA256) : modifier, supprimer ou insérer un pointage casse la chaîne, et la vérification désigne le maillon exact. Une correction est elle-même scellée, avec son auteur et son motif : on ne gomme pas, on contrepasse.

• Le journal d'audit (connexions, accès de l'assistance, purges, suppressions) est scellé de la même façon, une chaîne par établissement, et vérifié chaque nuit.

• Chaque mois clos donne un dossier mensuel figé et scellé, vérifiable par son empreinte SHA-256. Dans les offres sans borne, le relevé mensuel clos est scellé ; ses rectifications sont tracées avec leur motif et leur auteur.

Le scellement rend une retouche détectable pour qui n'a accès qu'à la base. Ce n'est pas un horodatage qualifié au sens du règlement eIDAS : pour une preuve opposable à un tiers, le gérant peut recopier hors du service le sceau quotidien de 16 caractères de chaque journée.

6. LES SAUVEGARDES

Une archive complète, chaque nuit, hors de l'hébergeur principal.

• Chaque nuit, une archive complète de la base est chiffrée par BioPoint (AES-256-GCM) avant de partir, puis déposée chez Supabase, Inc. (Irlande) et relue ; la clé reste chez BioPoint.

• Les archives sont conservées 30 jours, puis effacées automatiquement.

• Objectifs : perte de données limitée aux 24 dernières heures, rétablissement en 4 heures.

• La restauration s'exerce réellement, dans une base temporaire supprimée ensuite ; au-delà de 90 jours sans exercice consigné, le service alerte l'exploitant.

7. VOS DROITS ET LA DURÉE DE CONSERVATION

L'établissement est responsable du traitement des données de son personnel ; BioPoint agit comme sous-traitant, dans les conditions de l'Annexe 1 des CGV, qui est le contrat exigé par l'article 28 du RGPD.

• Chaque salarié consulte ses données dans son espace (« Mes données »), en télécharge l'export, demande une rectification, s'oppose aux analyses et conteste une décision qui le concerne.

• Il peut aussi constituer son passeport professionnel : un dossier scellé de ses heures, formations et attestations, qu'il emporte (portabilité, art. 20 du RGPD).

• Les gérants, les directions d'enseigne, les salariés, les élus et les experts-comptables suppriment eux-mêmes leur compte, après confirmation de leur mot de passe ; la suppression est immédiate, sauf pour le gérant qui tient l'abonnement et pour une direction d'enseigne, pour qui elle vaut demande de clôture de l'espace. Ce que la loi impose à l'employeur de conserver (paie, temps de travail, registre du personnel) reste, pendant les durées du registre.

• L'établissement exporte à tout moment ses données : une archive ZIP, les données en JSON et les documents dans leur format d'origine (les fichiers des vidéos de formation exceptés).

• À la fin du contrat, les données sont effacées des serveurs le lendemain du dernier jour, après les rappels d'export (CGV, art. 18.2 et 18.3) ; elles subsistent au plus 30 jours dans les sauvegardes chiffrées. Le coffre de preuves de BioPoint n'en garde aucune donnée de paie : leurs seules empreintes, cinq ans (CGV, art. 18.6).

• Les données arrivées au terme de leur durée de conservation sont effacées automatiquement chaque jour ; les salariés partis depuis cinq ans sont anonymisés.

Durées de conservation (registre des traitements)

Temps de travail et pointages
Durée : 5 ans (prescription des actions en paiement de salaire)

Paie et bulletins
Durée : 5 ans (bulletins : 5 ans pour l'employeur)

Dossier du salarié
Durée : Durée du contrat, puis 5 ans (art. L1471-1, L3245-1) ; titre de séjour et sa copie : idem (art. R1221-26)

Signalements
Durée : 2 mois après clôture sans suite ; sinon 2 ans à compter du dépôt

Conversations avec l'assistant
Durée : 1 an

CV et candidatures (Complète Borne)
Durée : 2 ans après le dernier contact ; vivier : 2 ans à compter de l'accord, renouvelable (doctrine CNIL)

Journal de sécurité
Durée : 6 mois (recommandation CNIL pour les journaux)

Preuve d'une suppression de compte
Durée : 3 ans après la demande (preuve de son exécution, art. 5.2 RGPD ; prescription de l'art. L1471-1 Code du travail)

Sauvegardes chiffrées
Durée : 30 jours, puis effacées

Pièces de BioPoint après la fin du contrat
Durée : contrat et correspondance : cinq ans (CGV, art. 4.5, 18.4 et 19.4) ; pièces comptables : dix ans (art. L123-22 du code de commerce)

8. LA BORNE DE POINTAGE (OFFRE COMPLÈTE BORNE)

La borne est un appareil du magasin : elle est verrouillée, signée et continue de travailler sans réseau.

• Chaque borne a sa propre clé d'appairage (256 bits, tirée au hasard), conservée chiffrée côté serveur ; elle signe chaque trame (HMAC-SHA256). Une trame falsifiée, trop ancienne ou déjà reçue est refusée, et le serveur refuse en production toute trame arrivée sans HTTPS.

• L'application de la borne est verrouillée en mode kiosque : une borne qui se déclare non verrouillée ne se met pas en service. Pour en sortir (mise à jour, Wi-Fi), le gérant tire depuis son espace un code de 12 chiffres propre à cette borne, valable 15 minutes, à usage unique, annulé après 5 essais faux ; la sortie dure 10 minutes, et chaque code émis, utilisé ou refusé est inscrit au journal d'audit.

• Sans réseau, la borne continue d'enregistrer : chaque pointage est conservé chiffré sur l'appareil, numéroté et signé, puis transmis au retour de la connexion. Le serveur vérifie la signature, refuse un rejeu et scelle le pointage avec la mention « reçu en différé ».

• Une borne silencieuse depuis 24 heures déclenche une alerte au gérant.

L'état du verrou est déclaré par l'application de la borne ; la garantie vient de sa signature, seule à pouvoir s'installer par-dessus, et de la procédure de mise en service.

9. AUCUNE DONNÉE BIOMÉTRIQUE

BioPoint ne lit ni empreinte ni visage.

• À la borne, le salarié pointe avec un badge : un identifiant attribué, révocable et remplaçable.

• Dans les offres sans borne, le salarié émarge sur l'application, avec son compte.

• Quand un utilisateur choisit Face ID ou son empreinte pour se connecter, la vérification reste sur son appareil : BioPoint ne reçoit et ne garde qu'une clé publique.

Ce que le service ne collecte jamais

– Diagnostic, pathologie ou motif médical d'une absence
– Origine ethnique, religion, convictions, orientation sexuelle, opinions politiques (art. 9 RGPD)
– APPARTENANCE SYNDICALE : ni la qualité d'adhérent, ni le syndicat d'un élu. L'espace des élus s'ouvre par un compte collectif.
– Données biométriques : le badge est un identifiant attribué, révocable et remplaçable, jamais une empreinte ni un visage
– Coordonnées de géolocalisation : aucune coordonnée n'est transmise ni conservée. Pour le seul pointage mobile, le téléphone vérifie s'il est dans la zone du site et ne transmet que ce résultat (« dans la zone » ou « hors zone »)
– Casier judiciaire, condamnations, infractions (art. 10 RGPD)

– Nature du handicap, taux d'incapacité, diagnostic ou copie de la pièce justificative de la reconnaissance ; état de santé, handicap ou pathologie d'un proche (seuls la catégorie BOETH, ses dates, le lien avec la personne aidée, le droit invoqué et la date de présentation du justificatif sont enregistrés)
– Frappe au clavier, captures d'écran, enregistrement des appels

10. L'INTELLIGENCE ARTIFICIELLE

Ce qu'elle reçoit, et comment l'arrêter.

• Offre Essentielle : aucune fonction d'intelligence artificielle ; aucune donnée n'est transmise à un modèle de langage.

• Offres Complètes : l'assistant des salariés et des gérants et l'aide au classement des documents déposés sont actifs par défaut. L'établissement les désactive à tout moment, d'un seul interrupteur : plus rien n'est alors transmis.

• Ce que le modèle reçoit est pseudonymisé : les noms sont remplacés par des étiquettes. Un contrôle automatique bloque tout envoi qui contient un numéro de sécurité sociale, des coordonnées bancaires (IBAN), un numéro de titre de séjour, un numéro de téléphone, une adresse e-mail, une date de naissance ou un aménagement d'horaires ou de poste d'un salarié. Aucun document médical n'est transmis.

• Chaque envoi est journalisé sans son contenu (empreinte, taille, issue).

• Aucune intelligence artificielle ne lit les CV : aucun CV n'est transmis au modèle ; les candidatures déposées à la borne sont classées par une grille fixe, et une personne décide.

• Le prestataire est OpenAI Ireland Ltd (groupe OpenAI) ; les données sont traitées aux États-Unis, et le transfert est encadré par les clauses contractuelles types de la Commission européenne (décision 2021/914) ; accord de traitement des données (DPA) signé avec OpenAI le 06/11/2026. BioPoint n'entraîne aucun modèle sur vos données.

• L'assistant ne prend aucune décision à la place d'une personne.

11. SI UN INCIDENT SURVIENT

Une procédure écrite encadre la gestion des incidents et des violations de données.

• BioPoint prévient l'établissement concerné au plus tard 48 heures après avoir pris connaissance d'une violation de ses données : sa nature, les personnes et les données concernées, ses conséquences probables et les mesures prises.

• La notification à la CNIL, quand elle est due, intervient dans les 72 heures (art. 33 du RGPD) : l'établissement la fait pour les données de son personnel, dont il est responsable, et BioPoint lui fournit les éléments et l'y aide ; BioPoint la fait pour les données dont il est lui-même responsable.

• BioPoint peut intervenir à tout moment pour corriger une faille de sécurité ; il en informe les gérants dès que possible.

• Le dirigeant de BioPoint est le responsable de la sécurité : il qualifie l'incident et notifie la CNIL dans les 72 heures quand la notification est due ; un suppléant est à nommer.

• Pour signaler une faille ou un incident : securite@biopoint.fr, ou le formulaire de contact du site, sans compte.

12. LA DISPONIBILITÉ

Un engagement chiffré, et un avoir quand il n'est pas tenu (CGV, Annexe 3).

• Engagement : 99 % de disponibilité par mois civil, hors maintenance planifiée.

• Si le mois n'est pas tenu, un avoir sur l'abonnement du mois : 5 % de 98 % à moins de 99 %, 10 % de 95 % à moins de 98 % et 20 % en dessous de 95 %.

• Maintenance planifiée entre 23 h et 6 h (heure de Paris), annoncée au moins 72 heures à l'avance, 8 heures par mois au plus ; dans l'offre Complète Borne, les bornes continuent d'enregistrer les pointages.

• Si la disponibilité n'est pas tenue trois mois de suite, ou quatre mois sur douze, l'établissement peut mettre fin au contrat sans frais.

• L'état du service se lit en direct sur la page publique « État du service ».

13. LA PROTECTION DE L'APPLICATION

Les protections d'une application web, et une chaîne logicielle suivie.

• Un jeton anti-falsification (CSRF) protège chaque formulaire et chaque requête qui écrit depuis un navigateur ; les bornes et les notifications de Stripe s'authentifient par leur signature. Une politique de sécurité du contenu (CSP) n'autorise que les scripts du site, munis d'un jeton tiré à chaque affichage ; aucune page ne peut être encadrée par un autre site.

• Les composants du logiciel sont épinglés et installés sous un verrou d'empreintes.

• Les secrets techniques sont conservés hors du code source ; le développement et les essais se font sur des données fictives.

• Engagement des CGV (Annexe 2) : recette complète des tests avant chaque mise en production.

14. CE QUE BIOPOINT NE PRÉTEND PAS

BioPoint ne revendique aucune certification : ni ISO 27001, ni hébergement de données de santé (HDS).

• Les mesures de cette page sont celles que le code et la configuration du service appliquent, et que les conditions générales de vente engagent (art. 19 et Annexes 1 à 3).

• L'établissement reste responsable de ses traitements : BioPoint lui fournit, dans son espace, le registre des traitements, la notice des salariés, un modèle d'analyse d'impact et le kit de consultation du CSE.

15. CONTACT SÉCURITÉ

Une question, un doute, une faille : écrivez-nous.

• Sécurité, faille ou incident, violation de données : securite@biopoint.fr.

• Exercice d'un droit sur vos données : securite@biopoint.fr.

• Délégué à la protection des données : le dirigeant de BioPoint, joignable à securite@biopoint.fr.

• Une question sur l'utilisation du service : l'assistance, support@biopoint.fr.

• Le formulaire de contact du site, sans compte, reçoit aussi les signalements.

• Par courrier : Mohamed Baha BHOURI — BioPoint, EI, 12 rue Maurice Fonvieille, 31000 Toulouse.

• Une réclamation peut toujours être adressée à la CNIL (www.cnil.fr).