bnode

Legal & Compliance

Politique de Confidentialité du Groupe

Version 1.0
Entrée en vigueur : 1er janvier 2026

Message clé

La présente Politique de Confidentialité de Bnode (la « Politique ») explique de quelle manière les Collaborateurs (tels que définis ci-après) doivent traiter les données à caractère personnel dans le cadre de leurs tâches quotidiennes. Chez Bnode, nous prenons la protection des données très au sérieux et nous nous conformons à toutes les lois applicables, y compris le RGPD. Ces règles garantissent que les données à caractère personnel de nos clients, collègues et partenaires soient traitées avec prudence, équité et sécurité.

En appliquant la présente Politique, nous contribuons à la sécurité des informations, à la transparence et à l'établissement d'une relation de confiance avec tous nos partenaires. La présente Politique définit les principes fondamentaux, notre engagement en matière de protection des données, ainsi que les rôles et responsabilités qui soutiennent la protection des données au sein de Bnode.

Table des matières

1. Objectif et champ d'application

Objectif

Chez Bnode, nous prenons la protection des données très au sérieux. Nous nous engageons à respecter toutes les réglementations relatives à la protection des données, telles que le Règlement général sur la protection des données (« RGPD ») et les autres règles applicables en matière de protection des données qui s'appliquent aux entités de Bnode.

La présente politique est basée sur le RGPD, qui vise à garantir que les données à caractère personnel des individus [1] soient traitées avec prudence et équité. Cela inclut la manière dont nous traitons les données relatives à nos clients, nos collègues et toute autre personne avec laquelle nous sommes en relation.

En tant qu'employés, il est important que nous respections toutes ces règles dans le cadre de notre travail quotidien. En d'autres termes, nous devons penser à la confidentialité et à la protection des données dans tout ce que nous faisons, que ce soit lorsque nous envoyons des e-mails, stockons des informations sur les clients ou gérons des systèmes internes.

La protection des informations à caractère personnel nous aide à rester transparents, à garantir la sécurité des données et à instaurer un climat de confiance avec nos clients, entre nous et avec le grand public. Elle reflète également nos valeurs en tant qu'organisation responsable et soucieuse de la protection de la vie privée, et nous aide à protéger la santé, la sécurité et le bien-être de nos parties prenantes, à protéger l'entreprise contre d'éventuelles atteintes à sa réputation et sanctions financières, à renforcer notre réputation d'entreprise éthique et à maintenir la confiance du public dans notre capacité à remplir nos obligations de service public de manière responsable.

La présente **Politique de Confidentialité du Groupe est un document fondamental qui définit le cadre du traitement des données à caractère personnel et formalise l'engagement de Bnode en matière de conformité et de confiance en ce qui concerne la protection des données**.

La présente Politique est articulée selon la structure suivante :

- Quels sont les concepts clés du traitement des données à caractère personnel ? (*Titre 2*) ;
- Comment encourageons-nous l'engagement en matière de conformité à la protection des données chez Bnode ? (*Titre 3*) ; et
- Quels sont les rôles et responsabilités en matière de gestion des risques liés à la protection des données chez Bnode ? (*Titre 4*)

La présente **Politique est renforcée** et complétée par des politiques thématiques, des conseils pratiques, des normes, des procédures, etc. **afin de promouvoir notre objectif, qui consiste à garantir que l'engagement en matière de conformité à la protection des données soit réellement respecté au sein de Bnode**.

1. Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Principales considérations

Tout manquement à l'obligation de protéger les données à caractère personnel peut exposer nos parties prenantes (y compris, mais sans s'y limiter, nos employés et nos clients) à des risques d'usurpation d'identité et de fraude ciblée pouvant entraîner des préjudices financiers et réputationnels directs. Les violations de dossiers sensibles peuvent également entraîner une discrimination, des opportunités manquées et des préjudices à long terme pour la situation financière d'une personne.

Champ d'application

La présente Politique s'applique à :

- tous les collaborateurs et toutes les collaboratrices de Bpost SA et de ses filiales (dénommées conjointement « **Bnode** »), indépendamment de leur fonction ou de leur position ; et
- aux personnes étroitement liées aux activités et opérations de Bnode qui ne sont pas des employés, mais à qui la présente politique est communiquée (ces personnes incluent tous les administrateurs, les personnes occupant des postes de direction, de consultance, de gestion ou de supervision au sein de Bnode, les travailleurs intérimaires, les stagiaires et les sous-traitants), ainsi que les employés, dénommés ci-après « **Collaborateurs** ».

La présente politique s'applique à toutes les données à caractère personnel traitées par Bnode, qu'elles soient gérées par ordinateur ou organisées manuellement (comme des fichiers structurés ou des tableurs). Elle ne s'applique pas aux éléments tels que les notes manuscrites qui ne sont enregistrées dans aucun système officiel.

Elle couvre :

- les données à caractère personnel des clients, employés, partenaires et autres personnes avec lesquelles nous interagissons ;
- tout outil ou système partagé impliquant des données à caractère personnel ;
- le partage interne des données à caractère personnel nécessaires au bon fonctionnement de notre entreprise.

Hiérarchie

La Politique est destinée à fournir des normes minimales à respecter au sein de tout Bnode.

Lors de l'application de ces normes, les Filiales peuvent, le cas échéant, adopter leurs propres normes spécifiques s'alignant sur la présente Politique. Ces normes doivent être adaptées si nécessaire pour répondre à leurs besoins spécifiques, à leur juridiction et aux exigences légales locales, constituant dès lors une dite « Politique de Confidentialité de la Filiale ». À condition que cette Politique de Confidentialité de la Filiale ait été valablement adoptée au niveau de la Filiale et ait été approuvée par l'équipe Compliance de Bnode (« Group Compliance ») et le Chief Legal Officer de Bnode (« Group CLO »), cette Politique de Confidentialité de la Filiale régira la Filiale concernée à la place de la présente Politique de Confidentialité du Groupe ou coexistera avec celle-ci.

2. Quels sont les concepts clés du traitement des données à caractère personnel ?

2.1 Que sont les données à caractère personnel ?

Les données à caractère personnel sont toutes les informations qui se rapportent à une personne identifiée ou identifiable. Si une information peut être utilisée, seule ou combinée à d'autres données, pour identifier une personne, elle est considérée comme une donnée à caractère personnel. Cela inclut des informations évidentes telles que les noms et adresses e-mail, mais aussi des informations moins directes telles que les données de localisation ou les identifiants en ligne.

Chez Bnode, les données à caractère personnel sont au cœur de bon nombre de nos activités quotidiennes, qu'il s'agisse de traiter les envois des clients, de gérer les dossiers des employés, de gérer les contrats avec les fournisseurs ou de fournir des services numériques. C'est pourquoi chaque Collaborateur doit comprendre ce que sont les données à caractère personnel, pourquoi elles sont importantes et comment les traiter avec soin.

Types de données à caractère personnel :

Nom	Adresse e-mail	Adresse postale	Adresse IP	Photo
Cookies	Données financières	Données HR	Données de localisation	Données relatives à la santé
Numéros de matricule	Enregistrements vocaux	Images vidéo	Date de naissance	Casier judiciaire

2.2 Quels types de données à caractère personnel traitons-nous ?

La présente section vous donne un aperçu rapide des données que nous traitons et des types d'informations à caractère personnel que nous sommes susceptibles de traiter. Cette liste n'est pas exhaustive, mais elle vise à aider tous les Collaborateurs à comprendre l'étendue de nos activités de traitement des données et l'importance de la protection des données dans chaque fonction.

De différentes personnes

Nous traitons les données à caractère personnel de différentes personnes, telles que :

- Clients
- Collaborateurs et candidats à un emploi
- Partenaires commerciaux et fournisseurs
- Autres parties prenantes et contacts

De différents types

Les types de données à caractère personnel que nous traitons peuvent inclure :

- les informations de base telles que noms, adresses et coordonnées
- les données d'identification, telles que numéros d'identification ou identifiants de connexion
- les données financières, telles que les informations relatives aux comptes bancaires
- les informations sur l'emploi, telles que les fonctions, les salaires et les données relatives aux performances
- les données client, y compris l'historique des commandes et les enregistrements des communications
- les données techniques, telles que les adresses IP ou les journaux d'utilisation
- les données relatives aux colis, telles que le numéro de suivi ou de colis, les préférences de livraison et la preuve de livraison

De sources directes et indirectes

Nous collectons des données à caractère personnel provenant de nombreuses sources différentes afin de nous aider à fournir nos services et à gérer notre entreprise de manière optimale. La plupart du temps, nous recueillons les données directement auprès de la personne concernée, par exemple lorsqu'elle remplit un formulaire en ligne ou passe une commande dans une boutique en ligne.

Nous collectons également parfois des données indirectement auprès des :

- fournisseurs ou clients : ils peuvent partager les données de leurs employés ou utilisateurs finaux lorsque cela est nécessaire pour fournir ou recevoir des services.
- Partenaires et prestataires de services : nous travaillons avec d'autres organisations qui peuvent partager des données avec nous afin de nous aider à fournir nos services.
- Autorités publiques : dans certains cas, nous collectons des données auprès d'organismes gouvernementaux, conformément à la législation en vigueur.
- Agences de recrutement : au cours des processus d'embauche, nous pouvons obtenir des données sur les candidates et candidats auprès de chasseurs de têtes ou de plateformes d'emploi.

De plus amples informations sur les activités de traitement de chaque entité de Bnode sont disponibles dans les avis de confidentialité respectifs.

2.3 Que signifie « traitement des données à caractère personnel » ?

Le terme « traitement » couvre à peu près tout ce qu'il est possible de faire avec des données à caractère personnel. Il s'agit d'un terme général dans le cadre des lois sur la protection des données, et la plupart d'entre nous procédons chaque jour à un tel traitement d'une manière ou d'une autre.

Le traitement comprend les opérations suivantes :

- Collecte de données (par exemple, via des formulaires ou des e-mails)
- Stockage ou sauvegarde des données

- Utilisation des données
- Organisation ou structuration des données
- Visualisation ou recherche dans les données
- Modification ou mise à jour des données
- Partage ou envoi de données à autrui
- Élimination ou destruction de données

Ainsi, même si vous enregistrez simplement un fichier contenant des informations à caractère personnel ou si vous envoyez par e-mail les coordonnées d'une personne, cela est considéré comme un traitement. Si vous travaillez avec des données à caractère personnel de quelque manière que ce soit, même minime, il est de votre responsabilité de les traiter avec prudence et de respecter la présente Politique de Confidentialité.

3. Quelles sont les exigences relatives au traitement des données à caractère personnel ?

Nous collectons les données à caractère personnel avec prudence.

Avant de collecter des données à caractère personnel auprès de sources externes, nous nous assurons toujours qu'elles sont collectées et partagées de manière légale et responsable.

Nous traitons les données à caractère personnel en toute conformité.

Chaque fois que nous traitons des données à caractère personnel, nous avons la responsabilité de les traiter correctement et conformément aux réglementations applicables en matière de protection des données.

En particulier, pour nos entités relevant du champ d'application du RGPD, le respect des 8 principes suivants en matière de protection des données est essentiel :

1. **Liceité**
   Assurez-vous toujours que nous disposions d'une raison légale valable (une « base juridique ») pour traiter les données à caractère personnel. Voici une liste des raisons les plus courantes :

   - **Consentement**
     Nous demandons à la personne son autorisation expresse pour utiliser ses données à des fins spécifiques.
     Exemples : un client accepte de recevoir des e-mails promotionnels ; un visiteur accepte les cookies non essentiels sur notre site web.

   - **Contrat**
     Nous traitons les données parce que nous en avons besoin pour fournir un service ou exécuter un contrat.

Exemples : nous utilisons l'adresse d'un client pour livrer son colis ; nous collectons les coordonnées bancaires de nos employés pour leur verser leur salaire.

- **Obligation légale**
  Parfois, la loi nous oblige à traiter des données à caractère personnel.
  Exemples : vérification de l'identité des clients afin de respecter les lois anti-blanchiment d'argent ; enregistrement des accidents du travail.

- **Intérêt légitime**
  Nous utilisons les données à caractère personnel d'une manière qui soutient notre activité, à condition que cela ne porte pas atteinte à la vie privée d'autrui. Avant d'utiliser cette base juridique, nous effectuons toujours une mise en balance afin de nous assurer que les droits des personnes concernées ne l'emporte pas sur nos intérêts légitimes.
  Exemples : analyser les données clients pour améliorer la tarification ou les services ; utiliser les données des employés pour signaler des problèmes de sécurité.

- **Intérêt public**

  Nous traitons les données à caractère personnel lorsque ce traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi Bnode ou l'une de ses filiales. Cette base juridique s'applique uniquement lorsque ce traitement est clairement autorisé par la loi et sert un objectif social ou public légitime.
  Exemples : traitement des données à caractère personnel afin de respecter les obligations postales ou de service public prévues par la loi.

  - **Intérêt vital**
    Nous traitons les données à caractère personnel lorsque ce traitement est nécessaire pour protéger la vie ou l'intégrité physique d'une personne. Cette base juridique n'est utilisée que dans des situations exceptionnelles où la personne n'est pas en mesure de donner son consentement et où une action immédiate est requise pour protéger la santé ou la sécurité.
    Exemples : partager des données à caractère personnel pertinentes avec les services d'urgence lors d'une catastrophe naturelle ou d'un incident critique afin de protéger les personnes touchées.

2. **Loyauté et transparence** Soyez honnête et clair avec les gens quant aux raisons pour lesquelles nous collectons leurs données et à la manière dont nous les utiliserons. Nous informons clairement les personnes sur la manière dont leurs données sont utilisées, par exemple par le biais d'avis relatifs à la confidentialité et aux cookies affichés lors de commandes en ligne, de candidatures à un emploi ou lors de l'utilisation de nos sites web.

3. **Limitation des finalités**
   N'utilisez les données à caractère personnel que pour des raisons spécifiques, claires et légitimes — jamais pour une finalité qui n'a aucun rapport ou qui est inattendue.

4. **Minimisation des données** Ne collectez que les données dont vous avez réellement besoin. Les données doivent être adéquates, pertinentes et limitées à ce qui est nécessaire.

5. **Exactitude**
   Assurez-vous que les données soient correctes et mises à jour.

6. **Limitation de la conservation** Ne conservez les données à caractère personnel que pendant la durée nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées. Une fois que les données ne sont plus nécessaires, elles doivent être supprimées

ou anonymisées en toute sécurité, conformément à notre politique de conservation. Certaines données doivent être conservées plus longtemps pour des raisons juridiques (comme les règles fiscales ou les enquêtes pour fraude), et dans ces cas, les exigences légales priment toujours.

7. **Intégrité et confidentialité** Mettez en œuvre des mesures de sécurité techniques et organisationnelles appropriées pour protéger les données à caractère personnel contre la perte, la fuite ou l'accès par des personnes non autorisées.

8. **Responsabilité**
   Nous devons être en mesure de prouver que nous avons respecté tous ces principes. C'est pourquoi la documentation, la formation et les mesures de sécurité sont importantes.

Ces principes reflètent une idée plus large appelée « Privacy by Design and by Default » (confidentialité dès la conception et par défaut), qui consiste à prendre en compte la confidentialité dès le départ, dans chaque processus, système ou projet.

Nous traitons les « données à caractère personnel sensibles » uniquement lorsque cela est autorisé.

Les données à caractère personnel sensibles sont des types d'informations personnelles qui sont plus intimes et nécessitent une protection supplémentaire, car elles peuvent conduire à des discriminations. Ces données comprennent notamment les informations relatives à votre santé, votre origine ethnique ou raciale, vos opinions politiques, vos croyances religieuses, votre appartenance à un syndicat, vos données biométriques ou génétiques, votre orientation sexuelle ou toute information relative à votre casier judiciaire.

Chez Bnode, nous ne traitons ce type de données que lorsque cela est strictement nécessaire et légalement autorisé, par exemple pour respecter des obligations légales, traiter un accident du travail pour l'assurance ou soutenir des activités syndicales. Nous prenons également des précautions supplémentaires, telles que l'obtention d'une autorisation interne et la réalisation d'une évaluation des risques liés à la confidentialité avant d'utiliser ces données.

Nous nous engageons à tenir à jour notre registre des activités de traitement (RoPA).

Afin de rester conforme aux lois sur la protection de la vie privée telles que le RGPD, Bnode conserve un aperçu détaillé de la manière dont nous utilisons les données à caractère personnel dans toutes nos entités. Ce document s'appelle le registre des activités de traitement (RoPA). Il nous aide à rester transparents et responsables dans notre traitement des données.

Ce registre comprend des informations telles que :

- pourquoi utilisons-nous des données à caractère personnel ?
- Quels types de données collectons-nous et à qui se rapportent-elles ?
- Avec qui pourrions-nous les partager ?
- Combien de temps les conservons-nous ?
- Quelles sont les mesures de sécurité mises en place ?

Nous mettons régulièrement à jour ce registre afin de refléter tout changement dans la manière dont nous traitons les données à caractère personnel. Si vous êtes impliqué dans des activités liées à des données nouvelles ou modifiées, veillez à respecter les directives internes relatives à la mise à jour de notre RoPA.

Nous traitons les demandes relatives aux données à caractère personnel de manière appropriée.

Les personnes dont les données à caractère personnel sont traitées par Bnode disposent de droits spécifiques en vertu des lois sur la protection des données. Ces droits sont expliqués dans nos avis de confidentialité et comprennent notamment les droits suivants :

- Consulter les données à caractère personnel que nous détenons (accès).
- Demander la correction de données incorrectes (rectification).
- Demander la suppression de leurs données (effacement ou « droit à l'oubli »).
- Limiter l'utilisation de leurs données (restriction).
- S'opposer à l'utilisation de leurs données (objection).
- Demander à recevoir leurs données dans un format exploitable (portabilité).
- Savoir si les décisions sont prises automatiquement (prise de décision automatisée).
- Déposer une plainte auprès d'une autorité chargée de la protection des données.

Lorsqu'une demande est formulée, nous suivons un processus interne clair afin de la traiter correctement les données dans les délais impartis. Toutes les demandes ne seront pas acceptées — certaines peuvent être refusées si des exceptions légales s'appliquent, comme la protection des droits d'autrui.

Nous agissons de manière responsable en cas de violation des données à caractère personnel.

Une violation de données à caractère personnel se produit lorsque des données à caractère personnel sont accidentellement ou illégalement perdues, consultées, modifiées ou partagées.

Exemple : la perte de votre ordinateur portable professionnel contenant des informations sur les employés ou les clients serait considérée comme une violation de données. D'autres exemples incluent le piratage d'un compte ou une attaque par rançongiciel contre un fournisseur de services.

Bnode dispose de mesures de sécurité rigoureuses pour prévenir et gérer ces incidents. En cas de violation, nous devons rapidement mener une enquête, consigner les détails et, selon la gravité de la situation, informer les autorités chargées de la protection des données et, le cas échéant, les personnes concernées.

Si vous soupçonnez une violation de données, contactez immédiatement les personnes mentionnées au Titre 3 afin de vous assurer que le dossier soit traité correctement et rapidement.

Nous agissons de manière appropriée en matière de transferts de données à caractère personnel avec des tiers et au sein du groupe.

Parfois, Bnode partage des données à caractère personnel avec des tiers ou entre ses propres entités afin de soutenir ses opérations commerciales.

Exemple : les données à caractère personnel peuvent être partagées avec un fournisseur de logiciels ou lors de l'utilisation de cookies sur nos sites web. Les données à caractère personnel peuvent être partagées entre les entités de Bnode à des fins de reporting CSRD.

Lorsque des données à caractère personnel sont envoyées vers des pays situés en dehors de l'Espace économique européen (« EEE ») ou d'autres régions appliquant des règles strictes en matière de données, Bnode veille à ce que ces transferts soient conformes à la loi et protègent correctement vos données. Cela inclut l'utilisation d'accords spéciaux et de mesures de protection pour garantir la sécurité des données.

Avant de partager des données avec un nouveau prestataire de services externe ou une autre entité, les Collaborateurs doivent vérifier auprès du Data protection Officer local, du Digital Compliance Office ou du Privacy Ambassador local que tout est conforme aux lois sur la protection des données.

Nous effectuons de manière appropriée des analyses d'impact relatives à la confidentialité et des analyses d'impact relatives à la protection des données.

Lorsqu'une nouvelle activité de traitement est prévue, le Digital Compliance Office, le Data Protection Office, le Privacy Ambassador ou le Data Protection Officer local doit procéder à des évaluations approfondies des risques afin d'évaluer la nécessité et la proportionnalité du traitement, de minimiser les risques associés et d'identifier les mesures nécessaires pour protéger les données à caractère personnel.

Dans certains cas, une « analyse d'impact relative à la protection des données » (« AIPD ») complète peut également être requise, en particulier lorsque le traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes.

Exemple : la mise en place d'un système de gestion des informations relatives à la santé des employés, tel que l'enregistrement des certificats médicaux ou des examens de santé, implique le traitement de données sensibles relatives à la santé et nécessite une AIPD afin de garantir que ces données soient traitées de manière sécurisée et avec les garanties appropriées.

Nous agissons dans le respect de la protection des données dès la conception, en veillant à ce que celle-ci soit intégrée dans tous les aspects.

Chez Bnode, la protection des données à caractère personnel et la sécurité de nos services et produits sont des priorités absolues. Nous sommes tenus d'intégrer la protection des données dans tout ce que nous faisons, dès le début de tout nouveau projet ou traitement. Par conséquent, nous devons réfléchir dès le début à la protection des données et prendre les mesures techniques et organisationnelles appropriées pour garantir la sécurité des données et respecter la vie privée des personnes.

Il n'y a pas une seule et unique façon de procéder ; les mesures dépendent de la situation. La clé réside dans le respect de principes importants tels que la transparence, la loyauté, la limitation des finalités, la minimisation des données, l'exactitude, la confidentialité et la responsabilité. Nous devons veiller à ce que ces principes guident notre travail à chaque étape : de l'achat d'outils et de services au développement et à la maintenance des systèmes, en passant par le stockage et la suppression sécurisés des données.

4. Quels sont les rôles et responsabilités en matière de protection des données chez Bnode ?

Chez Bnode, la protection de la vie privée est **la responsabilité de toutes et tous**. Quel que soit votre rôle, si vous travaillez avec des données à caractère personnel, vous êtes tenu de respecter les règles énoncées dans la présente Politique de Confidentialité et de contribuer à la sécurité de ces données.

La gestion des risques liés à la protection des données chez Bnode s'inscrit dans le **cadre de gestion des risques d'entreprise (Entreprise Risk Management – « ERM »)** et suit le **modèle des trois lignes de défense** afin de garantir une responsabilité claire et une gouvernance efficace, comme suit :

Première ligne de défense – Business Owners

Chaque produit, service ou système chez Bnode relève de la responsabilité d'un « **Business Owner** ». Ce dernier est principalement chargé de veiller à ce que tous les aspects relevant de son domaine respectent les règles en matière de protection des données. Les Business Owners agissent en tant que première ligne de responsabilité. Les Business Owners sont responsables du respect quotidien des exigences en matière de protection des données dans le cadre de leurs produits, services et processus.
Leurs responsabilités sont notamment les suivantes :

- mettre en œuvre des contrôles et des normes minimales en matière de protection des données ;
- tenir à jour le registre des activités de traitement (RoPA) pour leur domaine de compétence ;
- réaliser des évaluations des risques et des analyses d'impact relatives à la protection des données lorsque cela est nécessaire ;
- gérer les incidents liés à la protection des données et veiller à leur escalade en temps opportun ;
- garantir la conformité contractuelle et opérationnelle avec les obligations en matière de protection des données.

Deuxième ligne de défense – Digital Compliance Office, DPO, et Privacy Network

- **Digital Compliance Office** (tel qu'établi au sein de l'équipe Group Compliance) :
  le Digital Compliance Office opère au niveau du groupe. Il s'agit d'un **partenaire stratégique de l'entreprise dans la gestion de l'engagement de conformité en matière de protection des données au sein de Bnode**.
  À ce titre, de manière générale, le Digital Compliance Office :
  - assure la supervision dans le domaine de la protection des données ;
  - **conseille, coache, encadre** et **soutient** l'entreprise dans son engagement et ses efforts de conformité en matière de protection des données et dans sa gestion des risques liés à la conformité tout en veillant au respect des normes et des contrôles ;
  - **supervise** la mise en œuvre des exigences minimales en matière de contrôle et évalue l'efficacité et la documentation de ces contrôles en rapport avec la protection des données.

  L'étendue de ses responsabilités peut varier en fonction du sujet et peut s'appliquer :
  - au **niveau du groupe** (à l'échelle de Bnode),
  - à une **Unité organisationnelle**[2] **ou une filiale** spécifique, ou

[2] Les « Unités organisationnelles » au sein de Bnode incluent :

- une **activité** spécifique menée par une Unité organisationnelle de Bnode.

En particulier, le Digital Compliance Office :

- définit les normes et la gouvernance en matière de protection des données du groupe ;
- fournit des orientations et assure la supervision en matière de conformité avec la protection des données ;
- agit en tant que personne de référence en matière de conformité pour les questions relatives à la protection des données et à la cybersécurité ;
- aide les équipes commerciales à comprendre et à respecter leurs obligations en matière de protection des données ;
- développe et soutient le déploiement du programme de protection des données du groupe ;
- aide au traitement et au signalement des incidents liés aux données ;
- tient à jour nos modèles de contrats relatifs à la protection des données et apporte son aide lors des négociations ;
- examine les services et les projets afin de repérer et de réduire les risques liés à la protection des données ;
- dirige les efforts globaux du groupe en matière de gouvernance de la protection des données ;
- travaille en étroite collaboration avec le DPO Office ou les DPO locaux en cas de besoin ;
- crée, gère et coordonne le Privacy Network et soutient les entités ; et
- contrôle le respect des politiques de confidentialité et des exigences réglementaires.

- **La fonction des Data Protection Officers (« DPO ») locaux**

Le DPO est une fonction indépendante dont la responsabilité principale est de veiller à ce que son entité respective se conforme aux exigences applicables en matière de protection des données.
Les DPO ont notamment la responsabilité de :

- tenir les Collaborateurs de leurs entités respectives informés de leurs responsabilités en matière de protection des données et de veiller à ce qu'ils soient formés en la matière ;
- surveiller la manière dont nous traitons les données à caractère personnel et donner des conseils pour assurer la conformité ;
- donner des conseils sur les AIPD pour les projets à haut risque ;
- agir en tant que contact principal pour les autorités chargées de la protection des données ;
- traiter les demandes et les préoccupations des particuliers concernant leurs données à caractère personnel, lorsque cela est nécessaire.

La fonction du DPO chez Bnode est représentée comme suit :

- au niveau de Bpost SA : le **Data Protection Office – Bpost SA** opère au niveau de Bpost SA et agit de manière indépendante, conformément à la loi ;
- au niveau des filiales :
  - **si la législation locale l'exige**, la filiale doit nommer un **Data Protection Officer (« DPO »)**. Lorsque la nomination d'un DPO est obligatoire, celui-ci est membre du Privacy Network.
- **Dans le cas contraire**, la filiale doit nommer un **Privacy Ambassador**, qui sera chargé de coordonner la protection des données au niveau local.

- les unités au niveau de Bnode qui se concentrent sur la création de revenus en offrant des produits et des services (« Business Units »). Les Business Units actuelles comprennent Bpost, Paxon et Landmark Cross-Border ;
- des entreprises locales ou des groupes d'entreprises locales opérant dans une zone géographique spécifique, qui se concentrent sur la création de revenus en offrant des produits et services (« Local Business »). Les entreprises locales actuelles comprennent Radial North America. Ces entreprises locales peuvent être incluses dans les Business Units ;
- les unités qui fournissent des services et/ou un soutien à d'autres unités ou à Bnode dans son ensemble, et qui ont des responsabilités principales autres que la création autonome de revenus au sein de ces unités (« Support Units »). Les unités de support actuelles comprennent Finance, Human Resources, ICT & Digital, Strategy & Transformation, ainsi que les services Corporate relevant du CEO du groupe (y compris Legal, Compliance, Enterprise Risk Management, Corporate Audit, Communications et Public Affairs).

La répartition des rôles DPO et DCO est définie plus en détail dans le RACI interne dédié.

- **Le Privacy Network** :
  en outre, l'engagement en matière de conformité à la protection des données est soutenu par la mise en place du « Privacy Network ». Ce réseau, piloté par le Digital Compliance Office, opère au niveau du groupe et comprend les membres suivants :
  - les membres de l'équipe du Digital Compliance Office ;
  - les DPO (y compris les Privacy Ambassadors).
  - **Privacy Champions** : chaque entité désigne également des « Privacy Champions », qui sont des Collaborateurs issus de différentes équipes ou différents départements et qui font office de « personnes de contact pour les questions quotidiennes relatives à la protection des données ». Ces personnes aident à identifier les risques et à garantir le respect des règles de protection des données dans le cadre du travail quotidien.
  - Tout autre Collaborateur concerné, selon le cas.

  Le rôle du Privacy Network est le suivant :
  - apporter un soutien à toutes les entités (au niveau de l'entité) tout en garantissant une mise en œuvre cohérente des normes de protection des données au sein de Bnode ;
  - agir en tant que premier point de contact pour les questions relatives à la protection des données au niveau de l'entité, améliorant ainsi la gestion des risques liés à la protection des données et l'engagement en matière de conformité ;
  - faciliter l'accès des équipes à l'aide dont elles ont besoin ; et
  - partager des connaissances importantes en matière de protection des données, notamment des conseils sur l'IA et les nouvelles technologies.

Troisième ligne de défense - Corporate Audit au niveau de Bnode

- Fournit une assurance indépendante sur la conception et l'efficacité opérationnelle des contrôles en matière de protection des données ;
- effectue des audits périodiques des processus et de la gouvernance en matière de protection des données ;
- rend compte des résultats au Comité d'Audit, des Risques et de Conformité (« **ARCC** ») et soutient l'amélioration continue.

Supervision exécutive au niveau de Bnode

- **Privacy, Security and AI Board**
  - Assure le suivi des interactions avec les autorités de contrôle compétentes ;
  - informe le top management et fournit une plateforme pour discuter des questions clés (y compris celles pouvant entraîner des risques élevés, tels que des amendes réglementaires, une atteinte à la réputation ou une couverture médiatique négative) ;
  - veille à ce que le budget alloué par l'entreprise à la conformité RGPD / ICT soit utilisé efficacement ;
  - sert de caisse de résonance pour les politiques et les lignes directrices en matière de confidentialité, d'IA et de sécurité de l'information.
  - **Comité exécutif (« ExCo »)** :
    - veille à ce que la gestion des risques liés à la protection des données soit intégrée dans la prise de décisions stratégiques ;
    - valide les ressources et promeut une culture de conformité.
- **Conseil d'Administration (« Conseil ») / ARCC** :
    - supervise la gouvernance des risques liés à la protection des données dans le cadre ERM ;

- examine les résultats des audits et contrôle le respect des obligations en matière de confidentialité.

5. Disponibilité, mises à jour et clarifications

La Politique de Confidentialité du Groupe

- est un document interne, disponible pour les membres du personnel sur Bpost4me ou sur les plateformes internes applicables de Bnode utilisées par une filiale de Bnode, avec les autres documents sur le sujet régissant la protection des données chez Bnode ;
- est un document évolutif qui sera régulièrement révisé et mis à jour si nécessaire.
- Les Collaborateurs seront informés de toute mise à jour.

En cas de questions ou demandes concernant la présente Politique, veuillez contacter votre Data protection officer, le Digital Compliance Office ou votre Privacy Ambassador.