bnode

Legal & Compliance

Privacybeleid van de Groep

Versie 1.0
Inwerkingtreding: 1 januari 2026

Kernboodschap

Dit Privacybeleid van Bnode (het 'Beleid') legt uit hoe Medewerkers (zoals hieronder gedefinieerd) in hun dagelijks werk horen om te gaan met persoonsgegevens. Bnode hecht enorm veel belang aan gegevensbescherming en houdt zich aan de toepasselijke wetgeving, waaronder de AVG. Deze regels zorgen ervoor dat de persoonsgegevens van onze klanten, collega's en partners zorgvuldig, behoorlijk en veilig worden behandeld.

Door dit Beleid te volgen, helpen we informatie veilig te houden, blijven we transparant en winnen we het vertrouwen van iedereen met wie we samenwerken. Dit Beleid beschrijft de kernbeginselen, onze verbintenis inzake gegevensbescherming en de rollen en verantwoordelijkheden die gegevensbescherming binnen Bnode ondersteunen.

Inhoudsopgave

1. Doel en toepassingsgebied

Doel

Gegevensbescherming is een thema dat we zeer ernstig nemen bij Bnode. We verbinden ons ertoe alle wetten inzake gegevensbescherming na te leven, zoals de Algemene Verordening Gegevensbescherming ('AVG') en andere toepasselijke regels inzake gegevensbescherming die van toepassing zijn op de Bnode-entiteiten.

Dit Beleid is gebaseerd op de AVG, die als doel heeft te waarborgen dat persoonsgegevens[1] van mensen zorgvuldig en behoorlijk worden behandeld. Dat slaat onder meer op de manier waarop we omgaan met gegevens over onze klanten, collega's en iedereen met wie we in contact komen.

Het is van essentieel belang dat wij, als werknemers, deze regels strikt naleven in ons dagelijks werk. Dit betekent dat we bij alles wat we doen rekening houden met privacy en gegevensbescherming, of we nu e-mails versturen, klantgegevens opslaan of interne systemen beheren.

Door persoonlijke gegevens te beschermen, blijven we transparant, houden we gegevens veilig en bouwen we vertrouwen op, bij onze klanten, bij elkaar en bij het grote publiek. Dit weerspiegelt ook onze waarden als verantwoordelijke en privacybewuste organisatie en helpt ons om de gezondheid, de veiligheid en het welzijn van onze stakeholders te beschermen, het bedrijf te behoeden voor mogelijke reputatieschade en financiële sancties, onze reputatie als ethisch bedrijf te versterken en het vertrouwen van het publiek te sterken in ons vermogen om onze openbaredienstverplichtingen op verantwoorde wijze na te komen.

Dit **Privacybeleid van de Groep is een fundamenteel document dat een kader creëert voor de verwerking van persoonsgegevens en dat de naleving van gegevensbescherming en de vertrouwensverbintenis binnen Bnode formeel vastlegt**.

Dit Beleid geeft een gestructureerd overzicht van de volgende punten:

- Wat zijn de kernconcepten van de verwerking van persoonsgegevens? (*Titel 2*)
- Hoe bevorderen we de naleving van onze gegevensbeschermingsverbintenis binnen Bnode? (*Titel 3*)

  Wat zijn de rollen en verantwoordelijkheden voor risicobeheer op het gebied van gegevensbescherming bij Bnode? (*Titel 4*)

Dit **Beleid wordt verder ondersteund** en uitgewerkt met actuele beleidsregels, praktische richtlijnen, normen, procedures, enz. **om te verzekeren dat onze verbintenis om de gegevensbescherming na te leven ook daadwerkelijk wordt toegepast binnen Bnode**.

1 . Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon

Voornaamste overwegingen

Als we persoonsgegevens niet afdoend beschermen, kunnen onze stakeholders (onder wie, maar niet beperkt tot, onze werknemers en klanten) worden blootgesteld aan risico's van identiteitsdiefstal en gerichte fraude die rechtstreekse financiële schade en reputatieschade kunnen veroorzaken. Inbreuken op gevoelige gegevens kunnen ook leiden tot discriminatie, gemiste kansen en langdurige schade aan iemands financiële situatie.

Reikwijdte

Dit Beleid is van toepassing op:

- alle medewerkers binnen Bpost nv en zijn dochterondernemingen (gezamenlijk aangeduid als '**Bnode**' of “Groep”, voorheen aangeduid als “bpostgroup”), ongeacht hun taken of functie; en,
- personen die nauw betrokken zijn bij de (operationele) activiteiten van Bnode maar die geen werknemer zijn en aan wie dit Beleid wordt meegedeeld (dergelijke personen omvatten alle bestuurders, personen met uitvoerende, adviserende, leidinggevende of toezichthoudende functies binnen Bnode, uitzendkrachten, stagiairs en aannemers, alsook de werknemers), hierna samen de '**Medewerkers**' genoemd.

Dit Beleid is van toepassing op alle persoonsgegevens waarmee Bnode werkt, ongeacht of deze door computers worden verwerkt of handmatig worden georganiseerd (zoals gestructureerde bestanden of spreadsheets). Het is niet van toepassing op zaken zoals handgeschreven notities die niet in een formeel systeem worden opgeslagen.

Het omvat:

- persoonsgegevens van klanten, werknemers, partners en andere personen met wie we contact hebben;
- alle gedeelde tools of systemen die persoonsgegevens bevatten;
- interne uitwisseling van persoonsgegevens die nodig zijn voor een vlotte bedrijfsvoering.

Hiërarchie

Dit Beleid heeft als doel de minimumnormen vast te leggen die binnen Bnode moeten worden nageleefd.

Bij de toepassing van deze normen kunnen Dochterondernemingen waar nodig eigen normen in het leven roepen, die aansluiten bij dit Beleid. Deze normen dienen dan voor zover nodig te worden afgestemd op hun unieke behoeften, jurisdictie en lokale wettelijke vereisten en neergelegd in een zogenaamde 'Subsidiary Privacy Policy'. Op voorwaarde dat een dergelijke Subsidiary Privacy Policy rechtsgeldig is aangenomen op het niveau van de dochteronderneming en werd goedgekeurd door het Compliance-team van Bnode ('Group Compliance') en de Chief Legal Officer van Bnode (de 'Group CLO'), zal een dergelijke Subsidiary Privacy Policy van toepassing zijn op de desbetreffende Dochteronderneming in plaats van of in combinatie met dit Beleid.

2. Wat zijn de kernconcepten van de verwerking van persoonsgegevens?

2.1 Wat zijn persoonsgegevens?

Persoonsgegevens zijn alle informatie over een geïdentificeerde of identificeerbare persoon. Als bepaalde informatie, op zichzelf of in combinatie met andere gegevens, kan worden gebruikt om te achterhalen wie iemand is, dan wordt dit als persoonsgegevens beschouwd. Dit omvat voor de hand liggende zaken zoals namen en e-mailadressen, maar ook minder voor de hand liggende informatie zoals locatiegegevens of online identificatoren.

Bij Bnode zijn persoonsgegevens een cruciaal element van veel van onze dagelijkse activiteiten: van de afhandeling van zendingen en de verwerking van personeelsgegevens tot het beheer van leverancierscontracten en de verlening van digitale diensten. Daarom moet elke Medewerker begrijpen wat persoonsgegevens zijn, waarom ze belangrijk zijn en hoe ze zorgvuldig moeten worden behandeld.

Voorbeelden van persoonsgegevens:

Naam	E-mailadres	Postadres	IP-adres	Foto
Cookies	Financiële gegevens	HR-gegevens	Locatiegegevens	Gezondheidsgegevens
Personeelsnummer	Stemopnames	Videobeelden	Geboortedatum	Strafblad

2.2 Welke types persoonsgegevens verwerken wij?

In dit deel geven we een kort overzicht van wie we gegevens verwerken en welke types persoonlijke informatie we kunnen behandelen. Deze lijst is niet volledig, maar bedoeld om Medewerkers te laten inzien hoe breed onze gegevensverwerkingsactiviteiten kunnen zijn en waarom gegevensbescherming in elke rol belangrijk is.

Van verschillende personen

Wij verwerken persoonsgegevens van verschillende personen, zoals:

- klanten;
- Medewerkers en sollicitanten;
- zakenpartners en leveranciers;
- andere stakeholders en contactpersonen.

Verschillende types gegevens

We kunnen de volgende types persoonsgegevens verwerken:

- basisinformatie zoals namen, adressen en contactgegevens;
- identificatiegegevens, zoals ID-nummers of inloggegevens;
- financiële gegevens, zoals bankrekeninginformatie;
- werkgelegenheidsinformatie, zoals functies, lonen en prestatiegegevens;
- klantgegevens, inclusief bestelgeschiedenis en communicatiegegevens;
- technische gegevens, zoals IP-adressen of gebruikslogboeken;
- gegevens van pakjes, zoals het traceer- of pakjesnummer, leveringsvoorkeuren en bewijs van levering.

Uit directe en indirecte bronnen

We verzamelen persoonsgegevens uit heel wat verschillende bronnen om onze diensten te kunnen verlenen en onze activiteiten vlot te laten verlopen. Meestal krijgen we de gegevens rechtstreeks van de persoon zelf, bijvoorbeeld wanneer iemand een onlineformulier invult of een bestelling plaatst via een webshop.

Soms verzamelen we ook indirect gegevens van:

- leveranciers of klanten - zij kunnen de gegevens van hun eigen werknemers of eindgebruikers delen wanneer dat nodig is om diensten te verlenen of te ontvangen;
- partners en dienstverleners - we werken samen met andere organisaties die mogelijk gegevens met ons delen om ons te helpen bij het verlenen van diensten;
- overheidsinstanties - in sommige gevallen verzamelen we gegevens van overheidsinstanties, voor zover dit wettelijk is toegestaan;
- wervingsbureaus - tijdens wervingsprocessen kunnen we kandidaatgegevens ontvangen van headhunters of vacatureplatforms.

Meer informatie over de verwerkingsactiviteiten van elke Bnode-entiteit is te vinden in de respectieve privacyverklaringen.

2.3 Wat betekent 'verwerking' van persoonsgegevens?

Het woord 'verwerking' omvat vrijwel alles wat je met persoonsgegevens kunt doen. Het is een brede term onder de wetgeving inzake gegevensbescherming en we doen het elke dag bijna allemaal, op een of andere manier.

Verwerking omvat:

- gegevens verzamelen (bv. via formulieren of e-mails);
- gegevens gebruiken;

- gegevens opslaan of bewaren;
- gegevens organiseren of structureren;
- gegevens bekijken of doorzoeken;
- gegevens wijzigen of bijwerken;
- gegevens delen of naar iemand anders verzenden;
- gegevens verwijderen of vernietigen.

Zelfs als je gewoon een bestand met persoonlijke gegevens opslaat of iemands contactgegevens per e-mail verstuurt, geldt dat dus als verwerking. Als je op eender welke manier met persoonsgegevens werkt, hoe beperkt ook, is het jouw verantwoordelijkheid om hier zorgvuldig mee om te gaan en dit Privacybeleid na te leven.

3. Wat zijn de vereisten met betrekking tot de verwerking van persoonsgegevens?

Wij verzamelen persoonsgegevens met de nodige voorzichtigheid

Voordat we persoonsgegevens van externe bronnen verzamelen, zorgen we er altijd voor dat deze op een wettelijke en verantwoorde wijze worden verzameld en gedeeld.

Wij verwerken persoonsgegevens op een conforme manier

Als we met persoonsgegevens werken en deze verwerken, is het onze verantwoordelijkheid om deze op gepaste wijze en in overeenstemming met de toepasselijke regelgeving inzake gegevensbescherming te behandelen.

Met name voor onze entiteiten die onder het toepassingsgebied van de AVG vallen, is naleving van de volgende acht beginselen inzake gegevensbescherming van cruciaal belang:

1. **Rechtmatigheid**
   Ervoor zorgen dat we een geldige wettelijke reden (een 'rechtsgrond') hebben om persoonsgegevens te verwerken. Dit is een overzicht van de meest voorkomende redenen:

   - **Toestemming**
     We vragen iemand om zijn of haar uitdrukkelijke toestemming om zijn of haar gegevens voor een specifiek doel te gebruiken.
     Voorbeelden: een klant stemt ermee in om reclame-e-mails te ontvangen; een bezoeker accepteert niet-essentiële cookies op onze website.

   - **Overeenkomst**
     Wij verwerken gegevens omdat wij deze nodig hebben om een dienst te verlenen of een overeenkomst na te komen.

Voorbeelden: we gebruiken het adres van een klant om zijn pakje te bezorgen; we verzamelen de bankgegevens van werknemers om hun loon uit te betalen.

- **Wettelijke verplichting**
  Soms zijn we wettelijk verplicht om persoonsgegevens te verwerken.
  Voorbeelden: de identiteit van een klant verifiëren om de antiwitwaswetgeving na te leven; arbeidsongevallen registreren.

- **Gerechtvaardigd belang**
  Wij gebruiken persoonsgegevens op een manier die onze activiteiten ondersteunt, zolang dit geen afbreuk doet aan iemands privacy. Voordat we deze rechtsgrondslag gebruiken, voeren we altijd een belangenafweging uit om er zeker van te zijn dat de rechten van de betrokkenen niet zwaarder wegen dan onze gerechtvaardigde belangen.
  Voorbeelden: klantgegevens analyseren om de prijzen of diensten te verbeteren; werknemersgegevens gebruiken om te rapporteren over veiligheidskwesties.

- **Algemeen belang**

  Wij verwerken persoonsgegevens als dit nodig is voor de uitvoering van een taak van algemeen belang of in het kader van de uitoefening van het openbaar gezag dat aan Bnode of een van zijn dochterondernemingen is verleend. Deze rechtsgrond geldt enkel indien een dergelijke verwerking uitdrukkelijk bij wet is toegestaan en een legitiem maatschappelijk of openbaar doel dient.
  Voorbeelden: verwerking van persoonsgegevens om te voldoen aan wettelijk opgelegde post- of openbaredienstverplichtingen.

  - **Vitale belangen**
    Wij verwerken persoonsgegevens wanneer dit nodig is om iemands leven of fysieke integriteit te beschermen. Deze rechtsgrond wordt alleen ingeroepen in uitzonderlijke situaties waarin de betrokkene niet in staat is toestemming te geven en onmiddellijke maatregelen vereist zijn om de veiligheid of gezondheid te waarborgen.
    Voorbeelden: relevante persoonsgegevens delen met hulpdiensten tijdens een natuurramp of een ernstig incident om getroffen personen te beschermen.

2. **Behoorlijkheid en transparantie**
   Eerlijk en duidelijk zijn met mensen over waarom we hun gegevens verzamelen en hoe we deze zullen gebruiken. We informeren mensen duidelijk over hoe hun gegevens worden gebruikt, bijvoorbeeld via privacy- en cookiemeldingen die worden getoond tijdens online bestellingen, sollicitaties of bij het gebruik van onze websites.

3. **Doelbinding**
   Persoonsgegevens alleen gebruiken voor specifieke, duidelijke en legitieme doeleinden, nooit voor iets onverwachts of iets dat er geen verband mee houdt.

4. **Minimale gegevensverwerking**
   Alleen de gegevens verzamelen die we echt nodig hebben. De gegevens dienen toereikend en ter zake dienend te zijn en beperkt te blijven tot wat noodzakelijk is.

5. **Juistheid**
   Ervoor zorgen dat de gegevens juist zijn en worden geactualiseerd.

6. **Opslagbeperking**
   Persoonsgegevens niet langer bewaren dan noodzakelijk voor de doeleinden waarvoor ze worden verzameld. Zodra gegevens niet langer nodig zijn, moeten ze veilig worden verwijderd of geanonimiseerd, in overeenstemming met ons gegevensbewaringsbeleid.

Sommige gegevens moeten om wettelijke redenen (zoals belastingregels of fraudeonderzoeken) langer worden bewaard en in die gevallen hebben wettelijke vereisten altijd voorrang.

7. **Integriteit en vertrouwelijkheid**
   Passende technische en organisatorische beveiligingsmaatregelen nemen om persoonsgegevens te beschermen tegen verlies, lekken of ongeoorloofde toegang.

8. **Verantwoordingsplicht**
   We moeten kunnen aantonen dat we al deze beginselen hebben nageleefd. Daarom zijn documentatie, opleiding en veiligheidsmaatregelen zo belangrijk.

Deze beginselen weerspiegelen een breder concept dat 'Privacy door ontwerp en door standaardinstellingen' wordt genoemd, wat betekent dat privacy vanaf het begin wordt meegenomen in elk proces, systeem of project.

Wij verwerken alleen 'gevoelige' persoonsgegevens als dit is toegestaan

Gevoelige persoonsgegevens zijn types persoonsgegevensdie meer privé zijn en extra bescherming vereisen omdat ze tot discriminatie kunnen leiden. Dit omvat zaken zoals gezondheidsinformatie, raciale of etnische achtergrond, politieke opvattingen, religieuze overtuigingen, lidmaatschap van een vakbond, biometrische of genetische gegevens, seksuele geaardheid of informatie over strafbladen.

Bij Bnode verwerken we dit soort gegevens alleen als dat strikt noodzakelijk en wettelijk toegestaan is, bijvoorbeeld om te voldoen aan wettelijke verplichtingen, een arbeidsongeval aan te geven bij de verzekering of vakbondsgerelateerde activiteiten te ondersteunen. We nemen ook extra voorzorgsmaatregelen, zoals het vragen van interne goedkeuring en het uitvoeren van een gegevensbeschermingeffectbeoordelingen, voordat we deze gegevens gebruiken.

Wij verbinden ons ertoe ons register van verwerkingsactiviteiten bij te houden

Om te voldoen aan privacywetgeving zoals de AVG, houdt Bnode een gedetailleerd overzicht bij van hoe we persoonsgegevens gebruiken binnen alle entiteiten. Dit wordt het register van verwerkingsactiviteiten genoemd. Het helpt ons om transparant en verantwoordelijk te blijven in onze omgang met gegevens.

Dit register bevat informatie zoals:

- waarom we persoonsgegevens gebruiken;
- welke types gegevens we verzamelen en over wie deze gegevens gaan;
- met wie we de gegevens zouden kunnen delen;
- hoe lang we ze bewaren;
- welke veiligheidsmaatregelen we hebben getroffen.

We werken dit register regelmatig bij om eventuele wijzigingen in de manier waarop we persoonsgegevens verwerken weer te geven. Als je betrokken bent bij nieuwe of veranderende gegevensactiviteiten, volg dan altijd de interne richtlijnen over de bijwerking van ons register van verwerkingsactiviteiten.

Wij behandelen verzoeken inzake persoonsgegevens op gepaste wijze

Personen van wie Bnode persoonsgegevens verwerkt, hebben specifieke rechten op grond van de wetgeving inzake gegevensbescherming. Deze rechten worden uitgelegd in onze privacyverklaringen en omvatten aspecten als:

- inzage in de persoonsgegevens die we bewaren (toegang);
- verzoek om onjuiste gegevens te corrigeren (rectificatie);
- verzoek om hun gegevens te verwijderen (wissing of 'recht op vergetelheid');
- beperking van het gebruik van hun gegevens (beperking);
- bezwaar tegen hoe hun gegevens worden gebruikt (bezwaar);
- verzoek om hun gegevens in een bruikbaar formaat te ontvangen (overdraagbaarheid);
- weten of beslissingen automatisch worden genomen (geautomatiseerde besluitvorming);
- een klacht indienen bij een gegevensbeschermingsautoriteit.

Wanneer iemand een verzoek indient, volgen we een duidelijk intern proces om dit correct en tijdig af te handelen. Niet alle verzoeken worden geaccepteerd. Sommige kunnen worden geweigerd als er wettelijke uitzonderingen van toepassing zijn, zoals het beschermen van de rechten van anderen.

Wij handelen verantwoordelijk bij inbreuken in verband met persoonsgegevens

We spreken van een inbreuk in verband met persoonsgegevens bij toegang tot of verlies, wijziging of verstrekking van de gegevens, hetzij per ongeluk, hetzij onrechtmatig.

Bijvoorbeeld: je werklaptop kwijtraken waarop gegevens van werknemers en klanten staan, wordt beschouwd als een inbreuk in verband met persoonsgegevens. Andere voorbeelden zijn een gehackte account of een ransomware-aanval op een dienstverlener.

Bnode heeft strenge veiligheidsmaatregelen om deze incidenten te voorkomen en aan te pakken. Als er een inbreuk plaatsvindt, moeten we die snel onderzoeken, de details noteren en, afhankelijk van de ernst van de inbreuk, de gegevensbeschermingsautoriteiten en mogelijk ook de betrokken personen op de hoogte brengen.

Als je een inbreuk vermoedt, neem dan onmiddellijk contact op met de personen die onder Titel 3 worden genoemd om ervoor te zorgen dat dit correct en snel wordt afgehandeld.

Wij handelen op gepaste wijze bij het doorgeven van persoonsgegevens aan derden en binnen de Groep

Soms deelt Bnode persoonsgegevens met derden of tussen zijn eigen entiteiten om bedrijfsactiviteiten te ondersteunen.

Voorbeeld: persoonsgegevens kunnen worden gedeeld met een softwareleverancier of wanneer cookies worden gebruikt op onze websites. Persoonsgegevens kunnen tussen Bnode-entiteiten worden gedeeld voor CSRD-rapporteringsdoeleinden.

Wanneer persoonsgegevens worden verzonden naar landen buiten de Europese Economische Ruimte ('EER') of andere regio's met strikte gegevensregels, zorgt Bnode ervoor dat deze doorgiften in overeenstemming zijn met de wet en dat de gegevens naar behoren worden beschermd. Dit omvat het gebruik van speciale overeenkomsten en waarborgen om gegevens veilig te houden.

Voordat gegevens worden gedeeld met een nieuwe externe dienstverlener of een andere entiteit, moeten Medewerkers contact opnemen met de lokale Data Protection Officer,of Digital Compliance Office of Privacy Ambassador om te controleren of alles in overeenstemming is met de wetgeving inzake gegevensbescherming.

We voeren risico-evaluaties en gegevensbeschermingseffectbeoordelingen op passende wijze uit

Wanneer een nieuwe verwerkingsactiviteit wordt gepland, moet het Digital Compliance Office, het Data protection Office, de Privacy Ambassador of de lokale Data Protection Officer grondige risico-evaluaties uitvoeren om de noodzaak en evenredigheid van de verwerking te evalueren, de bijbehorende risico's tot een minimum te beperken en de nodige maatregelen te identificeren om persoonsgegevens te beschermen.

In bepaalde gevallen kan bovendien een uitgebreide 'gegevensbeschermingseffectbeoordeling' vereist zijn, met name wanneer de verwerking een hoog risico kan inhouden voor de rechten en vrijheden van personen.

Voorbeeld: de invoering van een systeem voor het beheer van gezondheidsinformatie van werknemers, zoals het registreren van medische attesten of gezondheidsscreenings, omvat de verwerking van gevoelige gezondheidsgegevens en vereist een gegevensbeschermingseffectbeoordeling om ervoor te zorgen dat deze gegevens veilig en met passende waarborgen worden behandeld.

Wij hanteren gegevensbescherming door ontwerp, zodat gegevensbescherming in alles is ingebouwd

Voor Bnode is het beschermen van persoonsgegevens en het waarborgen van de veiligheid van onze diensten en producten een topprioriteit. We zijn verplicht om gegevensbescherming in alles wat we doen in te bouwen: vanaf het prille begin van elk nieuw project of elke nieuwe verwerkingsactiviteit. Dit betekent dat we vroeg moeten nadenken over gegevensbescherming en de juiste technische en organisatorische maatregelen moeten nemen om gegevens veilig te houden en de privacy van mensen te respecteren.

Er is meer dan één manier om dit te doen en de maatregelen zijn afhankelijk van de situatie. Cruciaal is dat we belangrijke beginselen hanteren, zoals transparantie, behoorlijkheid, doelbinding, minimale gegevensverwerking, juistheid, vertrouwelijkheid en verantwoordingsplicht. We moeten ervoor zorgen dat deze beginselen ons werk sturen bij elke stap: van de aankoop van tools en diensten over de ontwikkeling en het onderhoud van systemen tot de veilige opslag en verwijdering van gegevens.

4. Wat zijn de rollen en verantwoordelijkheden met betrekking tot gegevensbescherming bij Bnode?

Bij Bnode is bescherming van persoonsgegevens **ieders verantwoordelijkheid**. Ongeacht je functie, als je met persoonsgegevens werkt, wordt van je verwacht dat je de regels in dit Beleid volgt en helpt om die gegevens veilig te houden.

Het risicobeheer op het gebied van gegevensbescherming bij Bnode is geïntegreerd in het **Enterprise Risk Management-kader (ERM)** en volgt het **'Three lines of defense'-model** (model dat voorziet in drie verdedigingslinies) om duidelijke verantwoordingsplicht en effectieve governance te waarborgen:

Eerste verdedigingslinie – Business Owners

Elk product, elke dienst of elk systeem bij Bnode heeft een verantwoordelijke; we noemen deze persoon de '**Business Owner**'. Business Owners moeten er voornamelijk voor zorgen dat alles binnen hun werkgebied voldoet aan de regels inzake gegevensbescherming. Zij vormen de eerste verdedigingslinie. De Business Owners zijn verantwoordelijk voor de dagelijkse naleving van de vereisten inzake gegevensbescherming voor hun producten, diensten en processen.

Hun belangrijkste verantwoordelijkheden zijn:

- controlemaatregelen voor gegevensbescherming en minimumnormen implementeren;
- het register van verwerkingsactiviteiten bijhouden binnen hun toepassingsgebied;
- risico-evaluaties en gegevensbeschermingseffectbeoordelingen uitvoeren als dat nodig is;
- incidenten op het gebied van gegevensbescherming afhandelen en op tijd escaleren;
- toezien op de contractuele en operationele naleving van gegevensbeschermingsverplichtingen.

Tweede verdedigingslinie – Digital Compliance Office, DPO's en Privacy Network

- **Digital Compliance Office** (zoals opgericht binnen Group Compliance):
  Het Digital Compliance Office opereert op groepsniveau. Het is een strategische partner van de onderneming om de naleving van de gegevensbeschermingsverbintenis te beheren binnen Bnode. In deze hoedanigheid moet het Digital Compliance Office in het algemeen:
  - toezicht houden op het gebied van gegevensbescherming;
  - de business adviseren, coachen, begeleiden en ondersteunen met betrekking tot de naleving van de gegevensbeschermingsverbintenis en -initiatieven en met betrekking tot het beheer van compliancerisico's, met inachtneming van geldende normen en controles;
  - de implementatie monitoren van minimale controlemaatregelen en beoordelen hoe doeltreffend deze controles zijn en in welke mate ze gedocumenteerd zijn.

  De reikwijdte van deze verantwoordelijkheden is themagebonden en kan van toepassing zijn op:
  - de hele Groep (over heel Bnode);

- een specifieke Organizational Unit[2] of dochteronderneming; of
- een specifieke activiteit uitgevoerd door een Organizational Unit van Bnode.

In het bijzonder moet het Digital Compliance Office:

- normen en governance op het vlak van gegevensbescherming binnen de Groep definiëren;
- ondersteuning bieden en toezicht houden op de naleving van gegevensbescherming;
- fungeren als aanspreekpunt voor vragen over gegevensbescherming en cyberbeveiliging;
- businessteams helpen hun verplichtingen op het gebied van gegevensbescherming te begrijpen en na te komen;
- de lancering van het gegevensbeschermingsprogramma van de Groep ontwikkelen en ondersteunen;
- helpen bij het afhandelen en rapporteren van gegevensincidenten;
- onze templates voor overeenkomsten met betrekking tot gegevensbescherming up-to-date houden en helpen bij onderhandelingen;
- diensten en projecten screenen op risico's inzake gegevensbescherming en die risico's beperken;
- de algemene inspanningen van de Groep op het gebied van gegevensbescherming aansturen;
- nauw samenwerken met het DPO Office of lokale DPO's wanneer dat nodig is;
- het Privacynetwerk creëren, onderhouden en coördineren en de entiteiten ondersteunen; en
- toezien op de naleving van dit Beleid en andere specifieke privacybeleiden en diens wettelijke vereisten.

- **De functie van lokale Data Protection Officers ('DPO's')**
  De DPO is een onafhankelijke functie die er met name voor moet zorgen dat de betreffende entiteit voldoet aan de toepasselijke vereisten inzake gegevensbescherming.
  De DPO's hebben met name de volgende verantwoordelijkheden:

  - Medewerkers van hun respectieve entiteit op de hoogte houden en opleiden over hun verantwoordelijkheden inzake gegevensbescherming;
  - controleren hoe wij omgaan met persoonsgegevens en advies geven om te blijven voldoen aan de regelgeving;
  - advies geven over gegevensbeschermingseffectbeoordelingen voor projecten met een hoger risico;
  - fungeren als belangrijkste contactpersoon voor gegevensbeschermingsautoriteiten;
  - verzoeken en bezorgdheden van personen over hun persoonsgegevens afhandelen, indien nodig.

  De functie van DPO binnen Bnode wordt als volgt vertegenwoordigd:
  - op het niveau van Bpost NV: het Data Protection Office – Bpost NV is actief op het niveau van Bpost NV en handelt onafhankelijk, zoals vereist door de wet.
  - op het niveau van de dochterondernemingen:

[2] 'Organizational Units' binnen Bnode omvatten:
- eenheden op het niveau van Bnode die zich richten op het genereren van inkomsten door producten en diensten aan te bieden ('Business Units'). De huidige business units zijn Bpost, Paxon en Landmark Cross-Border;
- lokale ondernemingen of groepen van lokale ondernemingen die actief zijn binnen een specifiek geografisch gebied en die zich richten op het genereren van inkomsten door producten en diensten aan te bieden ('Lokale Ondernemingen'). Momenteel omvatten de Lokale Ondernemingen onder meer Radial North America; Lokale Ondernemingen kunnen deel uitmaken van de Business Units;
- units die diensten verlenen en/of ondersteuning bieden aan andere units of aan Bnode in zijn geheel, waarvan de voornaamste verantwoordelijkheden niet gericht zijn op het autonoom genereren van inkomsten binnen dergelijke eenheden ('Support Units'). De huidige Support Units omvatten Finance, Human Resources, ICT & Digital, Strategy & Transformation, evenals Corporate Services die rapporteren aan de Group CEO (waaronder Legal, Compliance, Enterprise Risk Management, Corporate Audit, Communications en Public Affairs).

    - Indien vereist door de lokale wetgeving, moet de dochteronderneming een Data Protection Officer ('DPO') aanstellen. Wanneer er verplicht een DPO aangesteld moet worden, is dit een lid van het Privacynetwerk.
- Zo niet, moet de dochteronderneming een Privacy Ambassador aanstellen, iemand die de gegevensbescherming op lokaal niveau coördineert.

De verdeling van de rollen van DPO en DCO wordt verder gedefinieerd in een speciale interne verantwoordelijkheidsmatrix ('RACI').

- **Het Privacynetwerk**:
  Daarnaast wordt de naleving van de gegevensbeschermingsverbintenis ondersteund door de oprichting van het 'Privacynetwerk'. Dit netwerk, aangestuurd door het Digital Compliance Office, opereert op groepsniveau en bestaat uit de volgende leden:
    - de teamleden van het Digital Compliance Office;
    - de DPO's (incl. de Privacy Ambassadors);
    - **Privacy Champions** Elke entiteit wijst ook zgn. 'Privacy Champions' aan. Dit zijn Medewerkers in verschillende teams of afdelingen die fungeren als 'aanspreekpunten voor dagelijkse vragen over gegevensbescherming'. Ze helpen om de risico's in kaart te brengen en zorgen ervoor dat de regels voor gegevensbescherming elke dag worden nageleefd;
    - eventuele andere relevante Medewerkers, al naar gelang het geval.

  Het Privacynetwerk heeft als taak:
    - ondersteuning te bieden aan alle entiteiten (op entiteitsniveau) en tegelijkertijd te zorgen voor een consistente toepassing van gegevensbeschermingsnormen binnen Bnode;
    - te fungeren als eerste aanspreekpunt voor vragen over gegevensbescherming op entiteitsniveau om zo de risico's inzake gegevensbescherming en de nalevingsverbintenis beter te kunnen beheren;
    - de teams de weg te wijzen naar de hulp die ze nodig hebben; en
    - belangrijke kennis over gegevensbescherming te delen, waaronder richtlijnen over AI en nieuwe technologieën.

Derde verdedigingslinie – Corporate Audit op Bnode-niveau

- biedt onafhankelijke waarborgen voor het ontwerp en de operationele effectiviteit van controlemaatregelen inzake gegevensbescherming;
- voert periodieke audits uit van gegevensbeschermingsprocessen en governance;
- brengt verslag over zijn bevindingen uit aan het Audit, Risk & Compliance Comité ('ARCC') en draagt bij aan continue verbetering.

Uitvoerend toezicht op Bnode-niveau

- **Privacy, Security & AI Board**
    - volgt de interacties met de relevante toezichthoudende autoriteiten op;
    - informeert het topmanagement en biedt een platform voor de bespreking van belangrijke kwesties (waaronder kwesties die hoge risico's met zich mee kunnen brengen, zoals boetes van toezichthouders, reputatieschade of negatieve berichtgeving in de media);
    - zorgt ervoor dat het bedrijfsbudget voor naleving van de AVG en ICT-voorschriften effectief wordt toegewezen;
    - fungeert als klankbord voor beleidsregels en richtlijnen op het gebied van privacy, AI en informatiebeveiliging.
- **Executive Comité ('ExCo'):**
    - zorgt ervoor dat risicobeheer inzake gegevensbescherming wordt geïntegreerd in de strategische besluitvorming;

- valideert middelen en bevordert een cultuur van naleving.

- **Raad van Bestuur ('Raad') / ARCC**:
    - houdt toezicht op risicobeheer inzake gegevensbescherming binnen het ERM-kader;
    - beoordeelt auditresultaten en ziet toe op de naleving van de privacyverplichtingen.

5. Beschikbaarheid, updates en verduidelijkingen

Dit Beleid

- is een intern document, dat beschikbaar is voor werknemers op Bpost4me of op de toepasselijke interne Bnode-platformen die worden gebruikt door een dochteronderneming van Bnode, samen met de andere bijbehorende documenten die de gegevensbescherming binnen Bnode regelen;
- is een evolutief document dat regelmatig zal worden geëvalueerd en indien nodig bijgewerkt.
- De Medewerkers zullen in dit geval op gepaste wijze op de hoogte gebracht worden van de veranderingen.

Met vragen of opmerkingen met betrekking tot dit Beleid, kan je terecht bij je Data Protection Officer, het Digital Compliance Office of je Privacy Ambassador.