Sécurité, données et RGPD

Vous saurez qui traite quelles données, où elles sont hébergées, comment les accès sont protégés et comment mener la revue fournisseur de bloo.Cards.

NL Beveiliging, gegevens en AVG

DE Sicherheit, Daten und DSGVO

EN Security, data and GDPR

Français p. 2 | Nederlands p. 10 | Deutsch p. 17 | English p. 25

Sécurité, données et RGPD

Vous saurez qui traite quelles données, où elles sont hébergées, comment les accès sont protégés et comment mener la revue fournisseur de bloo.Cards.

Pour : services achats, informatique (DSI), juridique et DPO d'un client entreprise.

DANS CE GUIDE

01 L'essentiel en une page 3
02 Qui est responsable de quoi 3
03 Où sont les données et qui y accède 4
04 Sécurité des comptes et des accès 5
05 Contacts collectés et consentement 6
06 Conservation et suppression 6
07 Droits des personnes 7
08 Revue fournisseur : checklist et FAQ 8

01 L'essentiel en une page

Ce guide résume ce que votre service juridique et votre DSI demandent en premier. Les textes qui font foi restent la Politique de confidentialité, les Conditions générales (CGU) et les Mentions légales publiées sur bloo.cards.

Éditeur

bloo.Cards est édité par Molderez-Consult SRL, société de droit belge établie à Bruxelles (Ixelles), numéro d'entreprise 0842.262.084.

Hébergement

Les données du service sont hébergées dans l'Union européenne. Les Mentions légales nomment l'hébergeur : Falcon Internet, sur l'infrastructure OVHcloud de Gravelines (France).

Rôles RGPD

Molderez-Consult SRL est responsable du traitement pour les comptes clients. Pour les contacts que vos équipes collectent, votre entreprise est responsable et bloo.Cards agit comme sous-traitant.

Engagements

Aucune vente de données, aucune publicité, aucun entraînement de modèle d'IA sur vos contacts. Aucune certification externe n'est revendiquée.

bloo.Cards applique les bonnes pratiques de sécurité reconnues (référentiel OWASP) et mène des audits internes réguliers. Nous ne revendiquons ni ISO 27001 ni SOC 2 : si votre politique d'achat exige une certification, signalez-le dès le début de la revue.

> Les exemples de personnes et de sociétés cités dans ce guide sont fictifs.

02 Qui est responsable de quoi

Le RGPD distingue celui qui décide du traitement (le responsable) de celui qui l'exécute pour son compte (le sous-traitant). bloo.Cards occupe les deux rôles, selon les données.

Données	Responsable du traitement	Rôle de bloo.Cards
Compte, connexion, facturation des titulaires	Molderez-Consult SRL	Responsable
Contenu publié sur les cartes	Le titulaire ou votre entreprise	Hébergeur et éditeur du service
Contacts collectés (échanges, scans, formulaires)	Votre entreprise ou le titulaire de la carte	Sous-traitant
Statistiques de visite des cartes	Molderez-Consult SRL	Responsable, données agrégées

Molderez-Consult SRL n'a pas désigné de délégué à la protection des données, cette désignation n'étant pas obligatoire pour son activité. Un point de contact vie privée répond à vos questions et à celles de vos collaborateurs.

Accord de traitement (DPA)

L'accord de sous-traitance est annexé aux CGU et s'applique à tous les comptes. Pour un compte Corporate, une version à signer est disponible sur demande auprès de hello@bloo.cards.

03 Où sont les données et qui y accède

Les serveurs du service sont situés dans l'Union européenne. Quelques fonctions s'appuient sur des prestataires spécialisés, listés nommément dans la Politique de confidentialité.

Fonction	Localisation	Garantie
Hébergement du service et des fichiers	Union européenne	Contrat de sous-traitance
Paiement des abonnements (Mollie)	Pays-Bas (UE)	Aucun numéro de carte bancaire conservé par bloo.Cards
Envoi des e-mails de service	Royaume-Uni	Décision d'adéquation et clauses contractuelles types
Traduction automatique des contenus	Union européenne	Seul le texte à traduire est transmis
Lecture par IA des cartes papier scannées	Hors UE	Clauses contractuelles types, photo non conservée
Connexion Google, LinkedIn ou Apple, cartes Google Maps	États-Unis ou Irlande	Data Privacy Framework, usage facultatif

- Toutes les pages et tous les échanges avec le service passent par une connexion chiffrée (HTTPS).
- Les mots de passe ne sont jamais stockés en clair : seule une empreinte calculée par un algorithme moderne est conservée.
- La mesure d'audience du site ne se charge qu'après l'accord du visiteur, et Google Maps ne s'affiche sur une carte qu'après un clic.
- Les clés d'intégration sont en lecture seule, révocables à tout moment, et bloo.Cards n'en garde qu'une empreinte.

04 Sécurité des comptes et des accès

La plupart des incidents commencent par un compte mal protégé. bloo.Cards vous donne plusieurs verrous ; c'est à votre entreprise de les activer et de les faire respecter.

Double authentification

Chaque utilisateur peut activer la vérification en deux étapes depuis la sécurité de son compte. Un compte protégé ne s'ouvre jamais avec le seul mot de passe, y compris dans le Wallet.

Connexion par passkey

Face ID, Touch ID, Windows Hello ou l'empreinte Android remplacent le mot de passe et valent double authentification. Les appareils enregistrés sont listés et peuvent être retirés.

Téléphones autorisés

Le Wallet s'associe par un QR code ou un code à usage unique valable 5 minutes, puis l'appareil est mémorisé 90 jours. Vous révoquez un appareil perdu depuis le back-office.

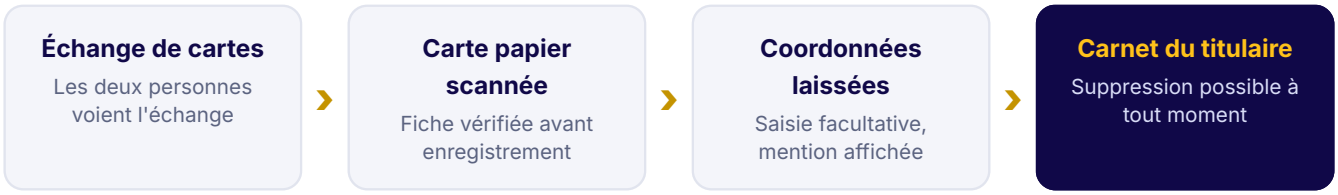
Droits par carte

Le propriétaire et les administrateurs de la société voient toutes les cartes. Un collaborateur ne voit que les siennes et celles qui lui sont confiées, en rôle Admin ou Lecteur.

1. **Nommez deux administrateurs**
   Un propriétaire et un administrateur de secours évitent qu'un départ bloque la gestion des cartes.
2. **Exigez la double authentification**
   Demandez à chaque administrateur de l'activer avant d'accéder aux cartes de l'équipe.
3. **Attribuez des rôles précis**
   Le rôle Lecteur permet de modifier le contenu (coordonnées, textes) sans toucher au design, aux modules ni aux langues.
4. **Revoyez les appareils**
   Une fois par trimestre, vérifiez la liste des téléphones et des passkeys et retirez ceux qui ne servent plus.

05 Contacts collectés et consentement

Une carte digitale sert à créer des contacts. Chaque contact entre dans le carnet du titulaire par un geste volontaire, et votre entreprise reste responsable de leur usage.



- Lors d'un échange entre deux utilisateurs bloo.Cards, l'échange est visible des deux côtés : chacun sait quelle identité a enregistré sa carte, et chacun peut supprimer le contact ou masquer l'échange.
- Un visiteur peut laisser son prénom, son nom et son e-mail au titulaire d'une carte. Cette étape est facultative (bouton « Passer »), et un texte l'informe de la transmission avec un lien vers la Politique de confidentialité.
- Pour une carte papier scannée, la photo sert uniquement à la lecture et n'est pas conservée. Le titulaire contrôle chaque champ avant d'enregistrer la fiche.
- Votre entreprise doit disposer d'une base légale pour recontacter ces personnes, en général l'échange volontaire ou l'intérêt légitime, et respecter leurs demandes d'opposition.

06 Conservation et suppression

Les données ne sont pas gardées plus longtemps que nécessaire. Voici les règles appliquées par le service.

Élément	Règle de conservation
Compte clôturé	Cartes hors ligne immédiatement, 15 jours pour exporter ou annuler, suppression des données au bout de 30 jours
Compte ou carte supprimé	Passage par une corbeille de 30 jours, puis effacement définitif
Factures	Conservées pendant la durée légale comptable, même après la clôture
Compte jamais confirmé et vide	Supprimé automatiquement après 48 heures
Données d'une société	Anonymisées 30 jours après la suppression de son dernier compte, les factures restant au nom d'origine
Statistiques de visite	Agrégées, conservées jusqu'à 24 mois
Journaux techniques	Jusqu'à 90 jours

Élément	Règle de conservation
Photo d'une carte scannée	Non conservée

Pour un compte Corporate, la clôture du compte d'un collaborateur efface aussitôt sa carte professionnelle (coordonnées, photo, contenus) et libère la carte pour votre société, qui peut l'attribuer à un autre collaborateur. Les sauvegardes expirent selon leur propre cycle.

07 Droits des personnes

Vos collaborateurs, vos contacts et les visiteurs des cartes disposent des droits prévus par le RGPD : accès, rectification, effacement, limitation, portabilité, opposition et retrait du consentement.

1. **Exporter ses données**
   Dans le back-office, la rubrique « Mes données & mon compte » propose un export complet (JSON) ainsi que les contacts en CSV ou vCard, quelle que soit l'offre.

2. **Corriger**
   Le titulaire modifie lui-même ses informations et le contenu de ses cartes, à tout moment.

3. **Demander l'effacement**
   La clôture du compte se fait en ligne, sans pénalité. Les données sont supprimées 30 jours plus tard, sauf les pièces que la loi impose de garder.

4. **Écrire à bloo.Cards**
   Pour toute autre demande, écrivez à hello@bloo.cards. Une réponse est donnée dans un délai d'un mois, prolongeable de deux mois pour une demande complexe.

Une personne enregistrée dans votre carnet

Si une personne dont vos équipes ont gardé les coordonnées exerce ses droits, elle s'adresse d'abord à votre entreprise, responsable de ce contact. Si elle écrit à bloo.Cards, nous vous transmettons sa demande et vous aidons à y répondre.

> Toute personne peut aussi introduire une réclamation auprès de l'Autorité de protection des données (APD), à Bruxelles.

08 Revue fournisseur : checklist et FAQ

Utilisez cette liste pour constituer votre dossier d'achat et vérifier les réglages avant le déploiement.

- [ ] Lire la Politique de confidentialité, les CGU et les Mentions légales en vigueur sur bloo.cards.
- [ ] Vérifier la liste des sous-traitants et leurs garanties de transfert.
- [ ] Demander l'accord de traitement signable si votre compte est Corporate.
- [ ] Désigner un propriétaire et un administrateur de secours pour la société.
- [ ] Activer la double authentification pour tous les administrateurs.
- [ ] Attribuer les rôles Admin et Lecteur carte par carte.
- [ ] Définir la base légale de vos contacts et l'inscrire dans votre registre des traitements.
- [ ] Prévoir la procédure de départ d'un collaborateur (export, clôture, réattribution de la carte).
- [ ] Noter le contact vie privée : hello@bloo.cards.

bloo.Cards est-il certifié ISO 27001 ?

Non. Aucune certification externe n'est revendiquée. Le service suit les bonnes pratiques OWASP et fait l'objet d'audits internes réguliers.

Nos données quittent-elles l'Union européenne ?

Le service est hébergé dans l'UE. Certaines fonctions facultatives (connexion par Google, LinkedIn ou Apple, lecture IA des cartes scannées) et l'envoi des e-mails de service font appel à des prestataires hors UE, encadrés par les garanties prévues par le RGPD.

Pouvons-nous récupérer toutes nos données ?

Oui. L'export complet est disponible depuis le compte, en JSON, et les contacts en CSV ou vCard.

Que devient la carte d'un collaborateur qui part ?

Sur un compte Corporate, la clôture de son compte efface sa carte professionnelle et la libère pour votre société, qui l'attribue à son successeur.

Utilisez-vous nos contacts pour entraîner une IA ?

Non. bloo.Cards ne vend pas vos données, n'affiche pas de publicité et n'entraîne aucun modèle sur vos contacts.

Pouvons-nous nous rétracter après une souscription ?

Pour un abonnement, un délai de rétractation de 14 jours s'applique aux consommateurs, dans les conditions des CGU. Une carte PVC NFC personnalisée en est exclue, car elle est fabriquée à votre nom.

Beveiliging, gegevens en AVG

U weet wie welke gegevens verwerkt, waar ze gehost worden, hoe de toegang beveiligd is en hoe u de leveranciersbeoordeling van bloo.Cards uitvoert.

Voor: aankoop, IT-afdeling, juridische dienst en DPO van een zakelijke klant.

IN DEZE GIDS

01 Het belangrijkste op één pagina 11
02 Wie is waarvoor verantwoordelijk 11
03 Waar de gegevens staan en wie er toegang toe heeft 12
04 Beveiliging van accounts en toegang 13
05 Verzamelde contacten en toestemming 14
06 Bewaring en verwijdering 14
07 Rechten van betrokkenen 15
08 Leveranciersbeoordeling: checklist en FAQ 15

01 Het belangrijkste op één pagina

Deze gids vat samen wat uw juridische dienst en uw IT-afdeling als eerste vragen. De bindende teksten blijven het Privacybeleid, de Algemene Voorwaarden en de Wettelijke vermeldingen op bloo.cards.

Uitgever

bloo.Cards wordt uitgegeven door Molderez-Consult SRL, een vennootschap naar Belgisch recht gevestigd in Brussel (Elsene), ondernemingsnummer 0842.262.084.

Hosting

De gegevens van de dienst worden in de Europese Unie gehost. De Wettelijke vermeldingen noemen de hostingpartner: Falcon Internet, op de OVHcloud-infrastructuur in Gravelines (Frankrijk).

Rollen onder de AVG

Molderez-Consult SRL is verwerkingsverantwoordelijke voor de klantaccounts. Voor de contacten die uw teams verzamelen, is uw onderneming verantwoordelijk en treedt bloo.Cards op als verwerker.

Engagementen

Geen verkoop van gegevens, geen reclame, geen training van AI-modellen op uw contacten. Er wordt geen externe certificering geclaimd.

bloo.Cards past erkende goede beveiligingspraktijken toe (OWASP-referentiekader) en voert regelmatig interne audits uit. We claimen geen ISO 27001 of SOC 2: vereist uw aankoopbeleid een certificering, meld dat dan bij het begin van de beoordeling.

> De personen en bedrijven die in deze gids als voorbeeld dienen, zijn fictief.

02 Wie is waarvoor verantwoordelijk

De AVG maakt een onderscheid tussen wie over de verwerking beslist (de verwerkingsverantwoordelijke) en wie ze in zijn opdracht uitvoert (de verwerker). bloo.Cards vervult beide rollen, afhankelijk van de gegevens.

Gegevens	Verwerkingsverantwoordelijke	Rol van bloo.Cards
Account, aanmelding en facturatie van houders	Molderez-Consult SRL	Verantwoordelijke
Inhoud die op de kaarten verschijnt	De houder of uw onderneming	Host en uitgever van de dienst
Verzamelde contacten (uitwisselingen, scans, formulieren)	Uw onderneming of de kaarthouder	Verwerker
Bezoekstatistieken van de kaarten	Molderez-Consult SRL	Verantwoordelijke, geaggregeerde gegevens

Molderez-Consult SRL heeft geen functionaris voor gegevensbescherming aangesteld, omdat die aanstelling voor haar activiteit niet verplicht is. Een aanspreekpunt voor privacy beantwoordt uw vragen en die van uw medewerkers.

Verwerkersovereenkomst (DPA)

De verwerkersovereenkomst is als bijlage bij de Algemene Voorwaarden gevoegd en geldt voor alle accounts. Voor een Corporate-account is op verzoek een te ondertekenen versie beschikbaar via hello@bloo.cards.

03 Waar de gegevens staan en wie er toegang toe heeft

De servers van de dienst staan in de Europese Unie. Enkele functies steunen op gespecialiseerde partners, die bij naam in het Privacybeleid vermeld staan.

Functie	Locatie	Waarborg
Hosting van de dienst en de bestanden	Europese Unie	Verwerkersovereenkomst
Betaling van abonnementen (Mollie)	Nederland (EU)	bloo.Cards bewaart geen bankkaartnummers
Verzending van service-e-mails	Verenigd Koninkrijk	Adequaatheidsbesluit en modelcontractbepalingen
Automatische vertaling van inhoud	Europese Unie	Alleen de te vertalen tekst wordt doorgegeven
AI-lezing van gescande papieren kaartjes	Buiten de EU	Modelcontractbepalingen, foto niet bewaard
Aanmelding via Google, LinkedIn of Apple, Google Maps	Verenigde Staten of Ierland	Data Privacy Framework, optioneel gebruik

- Alle pagina's en alle uitwisselingen met de dienst verlopen via een versleutelde verbinding (HTTPS).
- Wachtwoorden worden nooit leesbaar opgeslagen: alleen een hash, berekend met een modern algoritme, wordt bewaard.
- De bezoekersmeting van de website laadt pas na toestemming van de bezoeker, en Google Maps verschijnt op een kaart pas na een klik.
- Integratiesleutels zijn alleen-lezen, op elk moment intrekbaar, en bloo.Cards bewaart er enkel een hash van.

04 Beveiliging van accounts en toegang

De meeste incidenten beginnen bij een slecht beveiligd account. bloo.Cards biedt u meerdere sloten; uw onderneming moet ze inschakelen en het gebruik ervan opvolgen.

Tweestapsverificatie

Elke gebruiker kan tweestapsverificatie inschakelen in de beveiliging van zijn account. Een beveiligd account opent nooit met alleen het wachtwoord, ook niet in de Wallet.

Aanmelden met een passkey

Face ID, Touch ID, Windows Hello of de Android-vingerafdruk vervangen het wachtwoord en gelden als tweestapsverificatie. Geregistreerde toestellen staan in een lijst en kunnen worden verwijderd.

Toegestane telefoons

De Wallet wordt gekoppeld met een QR-code of een eenmalige code die 5 minuten geldig is; daarna blijft het toestel 90 dagen onthouden. Een verloren toestel trekt u in vanuit de back-office.

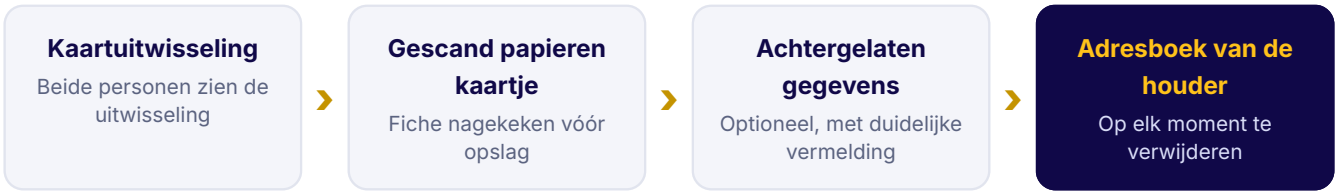
Rechten per kaart

De eigenaar en de beheerders van het bedrijf zien alle kaarten. Een medewerker ziet alleen zijn eigen kaarten en die welke hem zijn toevertrouwd, met de rol Admin of Lezer.

1. **Duid twee beheerders aan**
   Een eigenaar en een reservebeheerder voorkomen dat een vertrek het beheer van de kaarten blokkeert.
2. **Verplicht tweestapsverificatie**
   Vraag elke beheerder om ze in te schakelen voordat hij de kaarten van het team beheert.
3. **Ken nauwkeurige rollen toe**
   Met de rol Lezer past men de inhoud aan (contactgegevens, teksten) zonder het ontwerp, de modules of de talen te wijzigen.
4. **Controleer de toestellen**
   Overloop elk kwartaal de lijst van telefoons en passkeys en verwijder wat niet meer gebruikt wordt.

05 Verzamelde contacten en toestemming

Een digitale kaart dient om contacten te leggen. Elk contact komt in het adresboek van de houder via een vrijwillige handeling, en uw onderneming blijft verantwoordelijk voor het gebruik ervan.



- Bij een uitwisseling tussen twee bloo.Cards-gebruikers is die aan beide kanten zichtbaar: iedereen weet met welke identiteit zijn kaart werd opgeslagen, en iedereen kan het contact verwijderen of de uitwisseling verbergen.
- Een bezoeker kan zijn voornaam, naam en e-mailadres achterlaten bij de houder van een kaart. Die stap is optioneel (knop « Overslaan »), en een tekst meldt de doorgifte met een link naar het Privacybeleid.
- Bij een gescand papieren kaartje dient de foto alleen om het te lezen en wordt ze niet bewaard. De houder controleert elk veld voordat hij de fiche opslaat.
- Uw onderneming heeft een rechtsgrond nodig om deze personen opnieuw te contacteren, meestal de vrijwillige uitwisseling of het gerechtvaardigd belang, en moet hun bezwaar respecteren.

06 Bewaring en verwijdering

Gegevens worden niet langer bewaard dan nodig. Dit zijn de regels die de dienst toepast.

Element	Bewaarregel
Afgesloten account	Kaarten meteen offline, 15 dagen om te exporteren of te annuleren, gegevens na 30 dagen verwijderd
Verwijderd account of verwijderde kaart	Eerst 30 dagen in een prullenbak, daarna definitief gewist
Facturen	Bewaard gedurende de wettelijke boekhoudkundige termijn, ook na afsluiting
Nooit bevestigd en leeg account	Na 48 uur automatisch verwijderd
Gegevens van een bedrijf	Geanonimiseerd 30 dagen na verwijdering van het laatste account; facturen blijven op de oorspronkelijke naam
Bezoekstatistieken	Geaggregeerd, tot 24 maanden bewaard
Technische logbestanden	Tot 90 dagen
Foto van een gescand kaartje	Niet bewaard

Bij een Corporate-account wist de afsluiting van het account van een medewerker meteen zijn professionele kaart (contactgegevens, foto, inhoud) en komt de kaart vrij voor uw bedrijf, dat ze aan een andere medewerker kan toewijzen. Back-ups vervallen volgens hun eigen cyclus.

07 Rechten van betrokkenen

Uw medewerkers, uw contacten en de bezoekers van de kaarten hebben de rechten die de AVG voorziet: inzage, rectificatie, wissing, beperking, overdraagbaarheid, bezwaar en intrekking van toestemming.

1. **Gegevens exporteren**
   In de back-office biedt de rubriek « Mijn gegevens & mijn account » een volledige export (JSON) en de contacten in CSV of vCard, ongeacht de formule.

2. **Corrigeren**
   De houder past zijn gegevens en de inhoud van zijn kaarten op elk moment zelf aan.

3. **Wissing vragen**
   Het account sluit u online af, zonder boete. De gegevens worden 30 dagen later verwijderd, behalve de stukken die de wet laat bewaren.

4. **bloo.Cards contacteren**
   Voor elke andere vraag schrijft u naar hello@bloo.cards. U krijgt binnen een maand antwoord, te verlengen met twee maanden bij een complexe aanvraag.

Een persoon in uw adresboek

Wil iemand van wie uw teams de gegevens bewaren zijn rechten uitoefenen, dan richt hij zich eerst tot uw onderneming, die voor dat contact verantwoordelijk is. Schrijft hij naar bloo.Cards, dan sturen we zijn vraag naar u door en helpen we u ze te beantwoorden.

> Iedereen kan ook een klacht indienen bij de Gegevensbeschermingsautoriteit (GBA) in Brussel.

08 Leveranciersbeoordeling: checklist en FAQ

Gebruik deze lijst om uw aankoopdossier samen te stellen en de instellingen te controleren vóór de uitrol.

- [ ] Het geldende Privacybeleid, de Algemene Voorwaarden en de Wettelijke vermeldingen op bloo.cards lezen.

- [ ] De lijst van verwerkers en hun doorgiftewaarborgen nakijken.
- [ ] De te ondertekenen verwerkersovereenkomst aanvragen als uw account Corporate is.
- [ ] Een eigenaar en een reservebeheerder voor het bedrijf aanduiden.
- [ ] Tweestapsverificatie inschakelen voor alle beheerders.
- [ ] De rollen Admin en Lezer per kaart toekennen.
- [ ] De rechtsgrond voor uw contacten bepalen en opnemen in uw register van verwerkingen.
- [ ] Een procedure voorzien voor het vertrek van een medewerker (export, afsluiting, nieuwe toewijzing van de kaart).
- [ ] Het privacycontact noteren: hello@bloo.cards.

Is bloo.Cards ISO 27001-gecertificeerd?

Nee. Er wordt geen externe certificering geclaimd. De dienst volgt de goede praktijken van OWASP en wordt regelmatig intern geaudit.

Verlaten onze gegevens de Europese Unie?

De dienst wordt in de EU gehost. Enkele optionele functies (aanmelding via Google, LinkedIn of Apple, AI-lezing van gescande kaartjes) en de verzending van service-e-mails doen een beroep op partners buiten de EU, met de waarborgen die de AVG voorziet.

Kunnen we al onze gegevens terugkrijgen?

Ja. De volledige export is beschikbaar vanuit het account, in JSON, en de contacten in CSV of vCard.

Wat gebeurt er met de kaart van een vertrekkende medewerker?

Bij een Corporate-account wist de afsluiting van zijn account zijn professionele kaart en komt ze vrij voor uw bedrijf, dat ze aan zijn opvolger toewijst.

Gebruikt u onze contacten om een AI te trainen?

Nee. bloo.Cards verkoopt uw gegevens niet, toont geen reclame en traint geen enkel model op uw contacten.

Kunnen we ons herroepen na een inschrijving?

Voor een abonnement geldt voor consumenten een herroepingstermijn van 14 dagen, onder de voorwaarden van de Algemene Voorwaarden. Een gepersonaliseerde PVC NFC-kaart is uitgesloten, omdat ze op uw naam wordt gemaakt.

Sicherheit, Daten und DSGVO

Sie wissen, wer welche Daten verarbeitet, wo sie gehostet werden, wie der Zugang geschützt ist und wie Sie die Lieferantenprüfung von bloo.Cards durchführen.

Für: Einkauf, IT-Abteilung, Rechtsabteilung und Datenschutzbeauftragte eines Firmenkunden.

IN DIESEM LEITFADEN

01	Das Wichtigste auf einer Seite	18
02	Wer wofür verantwortlich ist	18
03	Wo die Daten liegen und wer Zugriff hat	19
04	Sicherheit von Konten und Zugängen	20
05	Erfasste Kontakte und Einwilligung	21
06	Aufbewahrung und Löschung	21
07	Rechte der betroffenen Personen	22
08	Lieferantenprüfung: Checkliste und FAQ	23

01 Das Wichtigste auf einer Seite

Dieser Leitfaden fasst zusammen, was Ihre Rechtsabteilung und Ihre IT zuerst fragen. Maßgeblich bleiben die Datenschutzerklärung, die Allgemeinen Geschäftsbedingungen (AGB) und das Impressum auf bloo.cards.

Herausgeber

bloo.Cards wird von der Molderez-Consult SRL herausgegeben, einer Gesellschaft belgischen Rechts mit Sitz in Brüssel (Ixelles), Unternehmensnummer 0842.262.084.

Hosting

Die Daten des Dienstes werden in der Europäischen Union gehostet. Das Impressum nennt den Hoster: Falcon Internet, auf der OVHcloud-Infrastruktur in Gravelines (Frankreich).

Rollen nach DSGVO

Für die Kundenkonten ist die Molderez-Consult SRL Verantwortlicher. Für die Kontakte, die Ihre Teams erfassen, ist Ihr Unternehmen verantwortlich, und bloo.Cards handelt als Auftragsverarbeiter.

Zusagen

Kein Verkauf von Daten, keine Werbung, kein Training von KI-Modellen mit Ihren Kontakten. Eine externe Zertifizierung wird nicht beansprucht.

bloo.Cards wendet anerkannte Sicherheitspraktiken an (OWASP-Referenzrahmen) und führt regelmäßig interne Audits durch. Wir beanspruchen weder ISO 27001 noch SOC 2: Verlangt Ihre Einkaufsrichtlinie eine Zertifizierung, sagen Sie es bitte zu Beginn der Prüfung.

> Die in diesem Leitfaden genannten Personen und Unternehmen sind frei erfunden.

02 Wer wofür verantwortlich ist

Die DSGVO unterscheidet zwischen dem, der über die Verarbeitung entscheidet (Verantwortlicher), und dem, der sie in seinem Auftrag durchführt (Auftragsverarbeiter). bloo.Cards hat je nach Daten beide Rollen.

Daten	Verantwortlicher	Rolle von bloo.Cards
Konto, Anmeldung und Abrechnung der Karteninhaber	Molderez-Consult SRL	Verantwortlicher
Auf den Karten veröffentlichte Inhalte	Der Inhaber oder Ihr Unternehmen	Hoster und Herausgeber des Dienstes
Erfasste Kontakte (Austausch, Scans, Formulare)	Ihr Unternehmen oder der Karteninhaber	Auftragsverarbeiter
Besuchsstatistiken der Karten	Molderez-Consult SRL	Verantwortlicher, aggregierte Daten

Die Molderez-Consult SRL hat keinen Datenschutzbeauftragten benannt, da dies für ihre Tätigkeit nicht vorgeschrieben ist. Eine Ansprechstelle für Datenschutz beantwortet Ihre Fragen und die Ihrer Mitarbeitenden.

Auftragsverarbeitungsvertrag (AVV)

Der Auftragsverarbeitungsvertrag ist den AGB als Anlage beigefügt und gilt für alle Konten. Für ein Corporate-Konto erhalten Sie auf Anfrage unter hello@bloo.cards eine unterschriftsfähige Fassung.

03 Wo die Daten liegen und wer Zugriff hat

Die Server des Dienstes stehen in der Europäischen Union. Einige Funktionen nutzen spezialisierte Dienstleister, die in der Datenschutzerklärung namentlich aufgeführt sind.

Funktion	Standort	Garantie
Hosting des Dienstes und der Dateien	Europäische Union	Auftragsverarbeitungsvertrag
Zahlung der Abonnements (Mollie)	Niederlande (EU)	bloo.Cards speichert keine Kartennummern
Versand der Service-E-Mails	Vereinigtes Königreich	Angemessenheitsbeschluss und Standardvertragsklauseln
Automatische Übersetzung der Inhalte	Europäische Union	Nur der zu übersetzende Text wird übermittelt
KI-Erkennung gescannter Papierkarten	Außerhalb der EU	Standardvertragsklauseln, Foto wird nicht gespeichert
Anmeldung über Google, LinkedIn oder Apple, Google Maps	USA oder Irland	Data Privacy Framework, freiwillige Nutzung

- Alle Seiten und jeder Austausch mit dem Dienst laufen über eine verschlüsselte Verbindung (HTTPS).
- Passwörter werden nie im Klartext gespeichert: Es wird nur ein mit einem modernen Verfahren berechneter Hash aufbewahrt.
- Die Reichweitenmessung der Website lädt erst nach Zustimmung des Besuchers, und Google Maps erscheint auf einer Karte erst nach einem Klick.
- Integrationsschlüssel sind schreibgeschützt, jederzeit widerrufbar, und bloo.Cards speichert davon nur einen Hash.

04 Sicherheit von Konten und Zugängen

Die meisten Vorfälle beginnen mit einem schlecht geschützten Konto. bloo.Cards bietet Ihnen mehrere Sicherungen; Ihr Unternehmen muss sie aktivieren und ihre Nutzung durchsetzen.

Zwei-Faktor-Authentifizierung

Jeder Nutzer kann die Bestätigung in zwei Schritten in der Sicherheit seines Kontos aktivieren. Ein geschütztes Konto öffnet sich nie allein mit dem Passwort, auch nicht im Wallet.

Anmeldung per Passkey

Face ID, Touch ID, Windows Hello oder der Android-Fingerabdruck ersetzen das Passwort und gelten als Zwei-Faktor-Authentifizierung. Registrierte Geräte werden aufgelistet und lassen sich entfernen.

Zugelassene Telefone

Das Wallet wird per QR-Code oder Einmalcode gekoppelt, der 5 Minuten gilt; danach bleibt das Gerät 90 Tage gespeichert. Ein verlorenes Gerät widerrufen Sie im Back-Office.

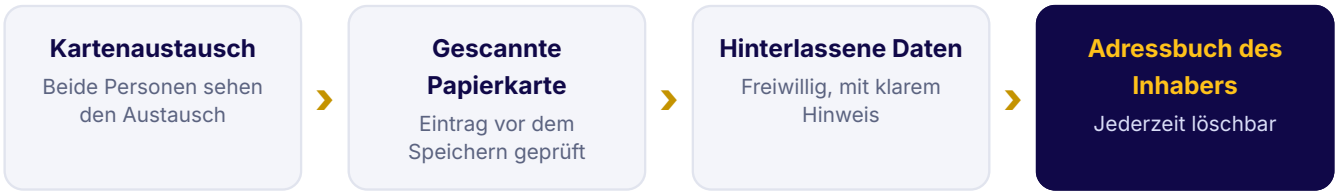
Rechte pro Karte

Eigentümer und Administratoren des Unternehmens sehen alle Karten. Ein Mitarbeitender sieht nur seine eigenen und die ihm anvertrauten Karten, mit der Rolle Admin oder Betrachter.

1. **Zwei Administratoren benennen**
   Ein Eigentümer und ein Ersatzadministrator verhindern, dass ein Weggang die Verwaltung der Karten blockiert.
2. **Zwei-Faktor-Authentifizierung verlangen**
   Bitten Sie jeden Administrator, sie zu aktivieren, bevor er die Karten des Teams verwaltet.
3. **Rollen gezielt vergeben**
   Mit der Rolle Betrachter lassen sich Inhalte (Kontaktdaten, Texte) ändern, ohne Design, Module oder Sprachen anzutasten.
4. **Geräte überprüfen**
   Prüfen Sie einmal im Quartal die Liste der Telefone und Passkeys und entfernen Sie, was nicht mehr genutzt wird.

05 Erfasste Kontakte und Einwilligung

Eine digitale Karte dient dazu, Kontakte zu knüpfen. Jeder Kontakt gelangt durch eine freiwillige Handlung in das Adressbuch des Inhabers, und Ihr Unternehmen bleibt für dessen Nutzung verantwortlich.



- Bei einem Austausch zwischen zwei bloo.Cards-Nutzern ist dieser auf beiden Seiten sichtbar: Jeder weiß, mit welcher Identität seine Karte gespeichert wurde, und jeder kann den Kontakt löschen oder den Austausch ausblenden.
- Ein Besucher kann dem Inhaber einer Karte Vorname, Name und E-Mail-Adresse hinterlassen. Dieser Schritt ist freiwillig (Schaltfläche « Überspringen »), und ein Hinweis informiert über die Weitergabe mit einem Link zur Datenschutzerklärung.
- Bei einer gescannten Papierkarte dient das Foto nur dem Auslesen und wird nicht gespeichert. Der Inhaber prüft jedes Feld, bevor er den Eintrag speichert.
- Ihr Unternehmen braucht eine Rechtsgrundlage, um diese Personen erneut zu kontaktieren, meist den freiwilligen Austausch oder das berechtigte Interesse, und muss Widersprüche beachten.

06 Aufbewahrung und Löschung

Daten werden nicht länger als nötig aufbewahrt. Diese Regeln wendet der Dienst an.

Element	Aufbewahrungsregel
Geschlossenes Konto	Karten sofort offline, 15 Tage zum Exportieren oder Widerrufen, Löschung der Daten nach 30 Tagen
Gelöschtes Konto oder gelöschte Karte	Zuerst 30 Tage im Papierkorb, danach endgültig gelöscht
Rechnungen	Während der gesetzlichen Buchhaltungsfrist aufbewahrt, auch nach der Schließung
Nie bestätigtes, leeres Konto	Nach 48 Stunden automatisch gelöscht
Daten eines Unternehmens	30 Tage nach Löschung des letzten Kontos anonymisiert; Rechnungen bleiben auf den ursprünglichen Namen
Besuchsstatistiken	Aggregiert, bis zu 24 Monate aufbewahrt
Technische Protokolle	Bis zu 90 Tage

Element	Aufbewahrungsregel
Foto einer gescannten Karte	Nicht gespeichert

Bei einem Corporate-Konto löscht die Schließung des Kontos eines Mitarbeitenden sofort seine berufliche Karte (Kontaktdaten, Foto, Inhalte) und gibt die Karte für Ihr Unternehmen frei, das sie einer anderen Person zuweisen kann. Sicherungskopien laufen nach ihrem eigenen Zyklus ab.

07 Rechte der betroffenen Personen

Ihre Mitarbeitenden, Ihre Kontakte und die Besucher der Karten haben die Rechte nach der DSGVO: Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch und Widerruf der Einwilligung.

1. **Daten exportieren**
   Im Back-Office bietet der Bereich « Meine Daten & mein Konto » einen vollständigen Export (JSON) sowie die Kontakte als CSV oder vCard, unabhängig vom Tarif.

2. **Berichtigen**
   Der Inhaber ändert seine Angaben und die Inhalte seiner Karten jederzeit selbst.

3. **Löschung verlangen**
   Die Schließung des Kontos erfolgt online und ohne Vertragsstrafe. Die Daten werden 30 Tage später gelöscht, außer den Unterlagen, die das Gesetz aufzubewahren verlangt.

4. **bloo.Cards schreiben**
   Für alle anderen Anliegen schreiben Sie an hello@bloo.cards. Sie erhalten innerhalb eines Monats eine Antwort, bei komplexen Anfragen verlängerbar um zwei Monate.

Eine Person in Ihrem Adressbuch

Möchte eine Person, deren Daten Ihre Teams gespeichert haben, ihre Rechte ausüben, wendet sie sich zuerst an Ihr Unternehmen, das für diesen Kontakt verantwortlich ist. Schreibt sie an bloo.Cards, leiten wir die Anfrage an Sie weiter und helfen Ihnen bei der Antwort.

> Jede Person kann außerdem Beschwerde bei der belgischen Datenschutzbehörde (DSB) in Brüssel einlegen.

08 Lieferantenprüfung: Checkliste und FAQ

Nutzen Sie diese Liste, um Ihre Einkaufsunterlagen zusammenzustellen und die Einstellungen vor der Einführung zu prüfen.

- [ ] Die geltende Datenschutzerklärung, die AGB und das Impressum auf bloo.cards lesen.
- [ ] Die Liste der Auftragsverarbeiter und ihre Übermittlungsgarantien prüfen.
- [ ] Bei einem Corporate-Konto den unterschriftsfähigen Auftragsverarbeitungsvertrag anfordern.
- [ ] Einen Eigentümer und einen Ersatzadministrator für das Unternehmen benennen.
- [ ] Die Zwei-Faktor-Authentifizierung für alle Administratoren aktivieren.
- [ ] Die Rollen Admin und Betrachter Karte für Karte vergeben.
- [ ] Die Rechtsgrundlage für Ihre Kontakte festlegen und in Ihr Verarbeitungsverzeichnis aufnehmen.
- [ ] Ein Verfahren für den Weggang von Mitarbeitenden vorsehen (Export, Schließung, Neuzuweisung der Karte).
- [ ] Den Datenschutzkontakt notieren: hello@bloo.cards.

Ist bloo.Cards nach ISO 27001 zertifiziert?

Nein. Eine externe Zertifizierung wird nicht beansprucht. Der Dienst folgt den OWASP-Praktiken und wird regelmäßig intern geprüft.

Verlassen unsere Daten die Europäische Union?

Der Dienst wird in der EU gehostet. Einige freiwillige Funktionen (Anmeldung über Google, LinkedIn oder Apple, KI-Erkennung gescannter Karten) und der Versand der Service-E-Mails nutzen Dienstleister außerhalb der EU, abgesichert durch die Garantien der DSGVO.

Können wir alle unsere Daten zurückerhalten?

Ja. Der vollständige Export steht im Konto als JSON bereit, die Kontakte als CSV oder vCard.

Was geschieht mit der Karte eines ausscheidenden Mitarbeitenden?

Bei einem Corporate-Konto löscht die Schließung seines Kontos seine berufliche Karte und gibt sie für Ihr Unternehmen frei, das sie seiner Nachfolge zuweist.

Nutzen Sie unsere Kontakte, um eine KI zu trainieren?

Nein. bloo.Cards verkauft Ihre Daten nicht, zeigt keine Werbung und trainiert kein Modell mit Ihren Kontakten.

Können wir nach dem Abschluss widerrufen?

Für ein Abonnement gilt für Verbraucher eine Widerrufsfrist von 14 Tagen zu den Bedingungen der AGB. Eine personalisierte PVC-NFC-Karte ist ausgenommen, da sie auf Ihren Namen gefertigt wird.

English GUIDE 07

Security, data and GDPR

You will know who processes which data, where it is hosted, how access is protected and how to run your supplier review of bloo.Cards.

For: procurement, IT, legal and DPO teams at a business customer.

IN THIS GUIDE

01 The essentials on one page 26
02 Who is responsible for what 26
03 Where the data lives and who can access it 27
04 Securing accounts and access 28
05 Collected contacts and consent 29
06 Retention and deletion 29
07 Individuals' rights 30
08 Supplier review: checklist and FAQ 30

01 The essentials on one page

This guide sums up what your legal team and your IT department usually ask first. The binding texts remain the Privacy Policy, the Terms and Conditions and the Legal Notice published on bloo.cards.

Publisher

bloo.Cards is published by Molderez-Consult SRL, a company incorporated under Belgian law and based in Brussels (Ixelles), company number 0842.262.084.

Hosting

Service data is hosted in the European Union. The Legal Notice names the host: Falcon Internet, on OVHcloud infrastructure in Gravelines (France).

GDPR roles

Molderez-Consult SRL is the controller for customer accounts. For the contacts your teams collect, your organisation is the controller and bloo.Cards acts as processor.

Commitments

No sale of data, no advertising, no training of AI models on your contacts. No external certification is claimed.

bloo.Cards follows recognised security good practice (the OWASP framework) and runs regular internal audits. We do not claim ISO 27001 or SOC 2: if your procurement policy requires a certification, please say so at the start of the review.

> The people and companies used as examples in this guide are fictitious.

02 Who is responsible for what

The GDPR separates the party that decides on the processing (the controller) from the party that carries it out on its behalf (the processor). bloo.Cards holds both roles, depending on the data.

Data	Controller	Role of bloo.Cards
Cardholders' account, sign-in and billing	Molderez-Consult SRL	Controller
Content published on the cards	The cardholder or your organisation	Host and publisher of the service
Collected contacts (exchanges, scans, forms)	Your organisation or the cardholder	Processor
Card visit statistics	Molderez-Consult SRL	Controller, aggregated data

Molderez-Consult SRL has not appointed a data protection officer, as its activity does not require one. A privacy contact point answers your questions and those of your staff.

Data processing agreement (DPA)

The data processing agreement is annexed to the Terms and Conditions and applies to every account. For a Corporate account, a version for signature is available on request from hello@bloo.cards.

03 Where the data lives and who can access it

The service's servers are located in the European Union. A few features rely on specialist providers, each named in the Privacy Policy.

Function	Location	Safeguard
Hosting of the service and files	European Union	Data processing agreement
Subscription payments (Mollie)	Netherlands (EU)	bloo.Cards stores no card numbers
Sending service emails	United Kingdom	Adequacy decision and standard contractual clauses
Machine translation of content	European Union	Only the text to translate is sent
AI reading of scanned paper cards	Outside the EU	Standard contractual clauses, photo not kept
Sign-in with Google, LinkedIn or Apple, Google Maps	United States or Ireland	Data Privacy Framework, optional use

- Every page and every exchange with the service uses an encrypted connection (HTTPS).
- Passwords are never stored in readable form: only a hash computed with a modern algorithm is kept.
- Website analytics only load once the visitor agrees, and Google Maps only appears on a card after a click.
- Integration keys are read-only, can be revoked at any time, and bloo.Cards only keeps a hash of them.

04 Securing accounts and access

Most incidents start with a poorly protected account. bloo.Cards gives you several locks; your organisation needs to switch them on and make sure they are used.

Two-factor authentication

Each user can turn on two-step verification in their account security settings. A protected account never opens with the password alone, including in the Wallet.

Passkey sign-in

Face ID, Touch ID, Windows Hello or Android fingerprint replace the password and count as two-factor authentication. Registered devices are listed and can be removed.

Authorised phones

The Wallet is paired with a QR code or a one-time code valid for 5 minutes, after which the device is remembered for 90 days. You revoke a lost device from the back office.

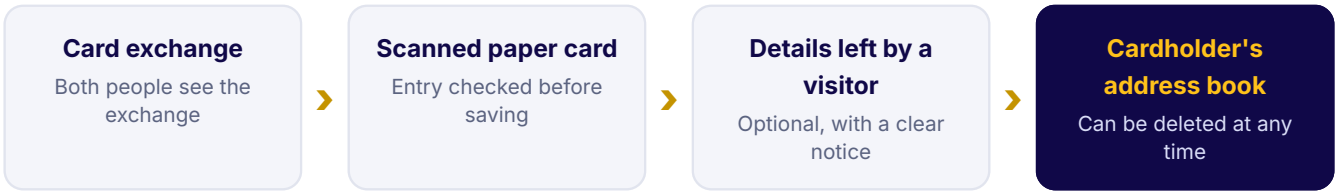
Per-card rights

The company owner and administrators see every card. A team member only sees their own cards and those entrusted to them, with the Admin or Viewer role.

1. **Appoint two administrators**
   An owner and a backup administrator stop a departure from blocking card management.
2. **Require two-factor authentication**
   Ask every administrator to turn it on before managing the team's cards.
3. **Assign precise roles**
   The Viewer role lets someone edit content (contact details, text) without touching the design, modules or languages.
4. **Review devices**
   Once a quarter, check the list of phones and passkeys and remove any that are no longer in use.

05 Collected contacts and consent

A digital card exists to create contacts. Every contact enters the cardholder's address book through a deliberate action, and your organisation remains responsible for how it is used.



- When two bloo.Cards users exchange cards, the exchange is visible on both sides: each person knows which identity saved their card, and either can delete the contact or hide the exchange.
- A visitor can leave their first name, last name and email with a cardholder. This step is optional (a « Skip » button), and a notice explains the transfer with a link to the Privacy Policy.
- For a scanned paper card, the photo is used only for reading and is not kept. The cardholder checks every field before saving the entry.
- Your organisation needs a lawful basis to contact these people again, usually the voluntary exchange or legitimate interest, and must honour any objection.

06 Retention and deletion

Data is not kept longer than necessary. These are the rules the service applies.

Item	Retention rule
Closed account	Cards go offline immediately, 15 days to export or cancel, data deleted after 30 days
Deleted account or card	Held in a 30-day bin, then permanently erased
Invoices	Kept for the statutory accounting period, even after closure
Empty account never confirmed	Deleted automatically after 48 hours
Company data	Anonymised 30 days after its last account is deleted; invoices stay in the original name
Visit statistics	Aggregated, kept for up to 24 months
Technical logs	Up to 90 days
Photo of a scanned card	Not kept

On a Corporate account, closing a team member's account immediately erases their professional card (contact details, photo, content) and frees the card for your company, which can assign it to someone else. Backups expire on their own cycle.

07 Individuals' rights

Your staff, your contacts and card visitors have the rights set out in the GDPR: access, rectification, erasure, restriction, portability, objection and withdrawal of consent.

1. **Export the data**
   In the back office, the « My data & my account » section offers a full export (JSON) and the contacts as CSV or vCard, whatever the plan.

2. **Correct it**
   Cardholders update their own details and card content at any time.

3. **Request erasure**
   The account is closed online, without penalty. Data is deleted 30 days later, except records the law requires us to keep.

4. **Write to bloo.Cards**
   For any other request, write to hello@bloo.cards. You will receive a reply within one month, extendable by two months for a complex request.

Someone in your address book

If a person whose details your teams have kept wants to exercise their rights, they should first contact your organisation, which is the controller for that contact. If they write to bloo.Cards, we forward the request to you and help you respond.

> Anyone can also lodge a complaint with the Belgian Data Protection Authority in Brussels.

08 Supplier review: checklist and FAQ

Use this list to build your procurement file and check the settings before roll-out.

- [ ] Read the current Privacy Policy, Terms and Conditions and Legal Notice on bloo.cards.
- [ ] Check the list of processors and their transfer safeguards.
- [ ] Request the signable data processing agreement if your account is Corporate.

- [ ] Appoint an owner and a backup administrator for the company.
- [ ] Turn on two-factor authentication for every administrator.
- [ ] Assign Admin and Viewer roles card by card.
- [ ] Define the lawful basis for your contacts and record it in your register of processing activities.
- [ ] Set out a leaver procedure for staff (export, closure, reassignment of the card).
- [ ] Note the privacy contact: hello@bloo.cards.

Is bloo.Cards ISO 27001 certified?

No. No external certification is claimed. The service follows OWASP good practice and is audited internally on a regular basis.

Does our data leave the European Union?

The service is hosted in the EU. Some optional features (sign-in with Google, LinkedIn or Apple, AI reading of scanned cards) and the sending of service emails use providers outside the EU, covered by the safeguards the GDPR provides.

Can we get all our data back?

Yes. The full export is available from the account as JSON, and the contacts as CSV or vCard.

What happens to a leaver's card?

On a Corporate account, closing their account erases their professional card and frees it for your company, which assigns it to their successor.

Do you use our contacts to train an AI?

No. bloo.Cards does not sell your data, show advertising or train any model on your contacts.

Can we withdraw after subscribing?

For a subscription, consumers have a 14-day withdrawal period under the Terms and Conditions. A personalised PVC NFC card is excluded, as it is made in your name.

bloo.cards

Une question ? Écrivez-nous.
Een vraag? Schrijf ons.
Eine Frage? Schreiben Sie uns.
A question? Write to us.

hello@bloo.cards

bloo.cards

bloo.Cards est une solution de Molderez-Consult SRL, Bruxelles, Belgique. · bloo.Cards is a solution by Molderez-Consult SRL, Brussels, Belgium.