bnode

Legal & Compliance

Group Privacy Policy

Version 1.0
Entry into force: 1 January 2026

Key message

This Bnode Privacy Policy (the 'Policy') explains how Coworkers (as defined below) must handle personal data in their daily work. At Bnode, we take data protection seriously and comply with all applicable laws, including the GDPR. These rules ensure that personal data of our customers, colleagues and partners is treated carefully, fairly and securely.

By following this Policy, we help keep information safe, stay transparent, and build trust with everyone we work with. This Policy sets out the core principles, our commitment to data protection, and the roles and responsibilities that support data protection across Bnode.

Table of contents

1. Purpose and Scope

Purpose

At Bnode, we take data protection seriously. We are committed to follow all data protection laws, like the General Data Protection Regulation ("GDPR") and other applicable data protection rules that apply to the Bnode entities.

This policy is based on the GDPR, which is all about making sure people's personal data[1] is handled carefully and fairly. That includes how we work with data about our customers, colleagues, and anyone else we deal with.

As employees, it is important that we all respect these rules in our daily work. This means thinking about privacy and data protection in everything we do – whether we're sending emails, storing customer info, or managing internal systems.

Protecting personal information helps us stay transparent, keeps data safe, and builds trust – with our customers, with each other, and with the wider public. It also reflects our values as a responsible and privacy-aware organization and helps us to protect the health, safety and wellbeing of our stakeholders, shield the company from possible reputational damage and financial penalties, strengthen our reputation as an ethical company, and maintain the public's trust in our capacity to fulfill our public service obligations responsibly.

This present **Group Privacy Policy is a foundational document providing the framework around the processing of personal data formalizing this data protection compliance and trust commitment across Bnode**.

This Policy provides a structured articulation of the following:

- What are the key concepts of processing personal data? (*Title 2*);
- How do we promote the data protection compliance commitment at Bnode? (*Title 3*); and
- What are the roles and responsibilities for data protection risk management at Bnode? (*Title 4*

This **Policy is being further supported** by and elaborated with topical policies, practical guidance, standards, procedures, etc. **to promote our purpose that the data protection compliance commitment is truly being lived upon across Bnode**.

1. Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural personal information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Key considerations

A failure to protect personal data can expose our stakeholders (including, but not limited to, our employees and customers) to risks of identity theft and targeted fraud that can cause direct monetary and reputational damage. Breaches of sensitive records can also lead to discrimination, lost opportunities, and long-term harm to an individual's financial status.

Scope

This Policy applies to:

- all employees within Bpost NV/SA and its subsidiaries (collectively referred to as "**Bnode**") regardless of their duties or position and ;
- persons closely connected with Bnode's activities and operations who are not employees, but to whom this Policy is communicated (such persons include all directors, persons holding executive, consultancy, managerial or supervisory positions within Bnode, temporary workers, trainees, and contractors), together with the employees defined hereafter as "**Coworkers**".

This policy applies to all personal data Bnode works with – whether it is handled by computers or manually organized (like structured files or spreadsheets). It does not apply to things like handwritten notes that are not stored in any formal system.

It covers:

- Personal data of customers, employees, partners, and other people we interact with.
- Any shared tools or systems that involve personal data.
- Internal sharing of personal data needed for our business to run smoothly.

Hierarchy

The Policy is intended to provide minimum standards to be observed across Bnode.

When applying these standards, Subsidiaries may, where appropriate, adopt their own specific standards that align with this Policy. These standards should be adapted as necessary to address their unique needs, jurisdiction, and local legal requirements, forming a so-called "Subsidiary Privacy Policy". Provided that such Subsidiary Privacy Policy has been validly adopted on the Subsidiary level and has been approved by the Bnode Compliance team ("Group Compliance") and the Bnode Chief Legal Officer (the "Group CLO"), such Subsidiary Privacy Policy will govern the relevant Subsidiary instead of or co-exist with this Group Privacy Policy.

2. What are the key concepts of processing personal data?

2.1 What is personal data?

Personal data is any information that relates to an identified or identifiable person. If a piece of information can be used — on its own or together with other data — to figure out who someone is, it counts as personal data. This includes obvious things like names and email addresses, but also less direct information like location data or online identifiers.

At Bnode, personal data is at the core of many of our daily activities — from handling customer shipments and processing employee records to managing supplier contracts and providing digital services. Because of this, every Coworker needs to understand what personal data is, why it is important, and how to treat it with care.

Examples of personal data:

Name	Email Address	Postal Address	IP Address	Picture
Cookies	Financial Data	HR Data	Location Data	Health Data
Employee Number	Voice Recordings	Video Footage	Date of Birth	Criminal Records

2.2 Which types of personal data do we process?

This section gives you a quick overview of who's data we process and what types of personal information we might handle. This is not an exhaustive list, but it is here to help all Coworkers understand just how broad our data processing activities can be — and why data protection matters in every role.

From different individuals

We process personal data from different individuals, such as:

- Customers
- Coworkers and job applicants
- Business partners and suppliers
- Other stakeholders and contacts

Different types of data

The types of personal data we process may include:

- Basic info like names, addresses, and contact details
- Identification details, such as ID numbers or login credentials
- Financial data, like bank account information
- Employment information, such as roles, salaries, and performance data
- Customer data, including order history and communication records
- Technical data, like IP addresses or usage logs
- Parcel-related data, like tracking or parcel number, delivery preferences and proof of delivery

From direct and indirect sources

We collect personal data from many different sources to help us deliver our services and run our business smoothly. Most of the time, we get data directly from the person — for example, when someone fills out an online form or places an order in a webshop.

We also sometimes collect data indirectly from:

- Suppliers or customers – they might share the data of their own employees or end users when it's needed to provide or receive services.
- Partners and service providers – we work with other organizations that may share data with us to help deliver services.
- Public authorities – in some cases, we collect data from government bodies, as allowed by law.
- Recruitment agencies – during hiring processes, we might get candidate data from head-hunters or job platforms.

Further details on the processing activities of each Bnode entity can be found in the respective privacy notices.

2.3 What does "processing personal data" mean?

The word "processing" covers just about anything you can do with personal data. It is a broad term under data protection laws — and most of us are doing it in some way every day.

Processing includes:

- Collecting data (e.g., through forms or emails)
- Storing or saving data
- Use of data
- Organizing or structuring data
- Viewing or searching through data

- Changing or updating data
- Sharing or sending data to someone else
- Deleting or destroying data

So, even if you are just saving a file with personal details, or emailing someone's contact info, that counts as processing. If you are working with personal data in any way, no matter how small, it is your responsibility to handle it carefully and follow this privacy policy.

3. What are the requirements regarding the processing of personal data?

We collect personal data with caution

Before we collect any personal data from outside sources, we always make sure it is being collected and shared legally and responsibly.

We process personal data in a compliant manner

Whenever we work with and process personal data, we have the responsibility to handle it properly and in compliance with the applicable data protection regulations.

In particular, for our entities falling under the scope of application of the GDPR, adherence to the following 8 data protection principles is key:

1. **Lawfulness**
   Always make sure we have a valid legal reason (a "legal basis") to process personal data. Here is a breakdown of the most common ones:

   - **Consent**
     We ask someone for their clear permission to use their data for a specific purpose.
     Examples: a customer agrees to receive promotional emails; a visitor accepts non-essential cookies on our website.

   - **Contract**
     We process data because we need it to deliver a service or fulfil a contract.
     Examples: we use a customer's address to deliver their parcel; we collect employee bank information to pay their salary.

   - **Legal Obligation**
     Sometimes, the law requires us to process personal data.
     Examples: verifying customer identity to follow anti-money laundering laws; registering work-related accidents.

   - **Legitimate Interest**
     We use personal data in a way that supports our business — as long as it does not harm someone's privacy. Before relying on this legal basis, we always carry out a balancing test to

ensure that the rights of the data subjects do not override our legitimate interests.
Examples: analysing customer data to improve pricing or services; using employee data to report on security issues.

- **Public Interest**

  We process personal data when it is necessary to perform a task carried out in the public interest or in the exercise of official authority granted to Bnode or one of its subsidiaries. This legal basis applies only where such processing is clearly authorised by law and serves a legitimate societal or public purpose.
  Examples: Processing personal data to comply with postal or public service obligations assigned by law.

  - **Vital Interests**
    We process personal data when it is necessary to protect someone's life or physical integrity. This legal basis is used only in exceptional situations where the individual is unable to give consent, and immediate action is required to safeguard health or safety.
    Examples: Sharing relevant personal data with emergency services during a natural disaster or critical incident to protect affected individuals.

2. **Fairness and Transparency**
   Be honest and clear with people about why we are collecting their data and how we will use it. We inform people clearly about how their data is used — for example, through privacy and cookie notices shown during things like online orders, job applications, or when using our websites.

3. **Purpose Limitation**
   Only use personal data for specific, clear, and legitimate reasons — never for something unrelated or unexpected.

4. **Data Minimisation**
   Only collect the data you truly need. The data must be adequate, relevant, and limited to what is necessary.

5. **Accuracy**
   Make sure the data is correct and kept up to date.

6. **Storage Limitation**
   Only keep personal data as long as needed for the purpose it was collected. Once data is no longer needed, it must be safely deleted or anonymized, following our retention policy. Some data must be kept longer for legal reasons (like tax rules or fraud investigations), and in those cases, legal requirements always come first.

7. **Integrity and Confidentiality**
   implement appropriate technical and organizational security measures to protect personal data from being lost, leaked, or accessed by the wrong people.

8. **Accountability**
   We must be able to prove that we have followed all these principles. That is why documentation, training, and security measures matter.

These principles reflect a broader idea called "Privacy by Design and by Default", which means thinking about privacy from the start — in every process, system, or project.

We process “sensitive personal data” only when allowed

Sensitive personal data are types of personal information that are more private and need extra protection because they may lead to discrimination. This includes things like your health information, racial or ethnic background, political opinions, religious beliefs, union membership, biometric or genetic data, sexual orientation, or any information about criminal records.

At Bnode, we only process this kind of data when it is strictly necessary and legally allowed — for example, to meet legal obligations, handle a workplace accident for insurance, or support union-related activities. We also make sure to take extra precautions, such as getting internal approval and doing a privacy risk assessment before using this data.

We engage to maintain our Record of Processing Activities (RoPA)

To stay compliant with privacy laws like the GDPR, Bnode keeps a detailed overview of how we use personal data across all entities. This is called the Record of Processing Activities (RoPA). It helps us stay transparent and accountable in our data handling.

This record includes information like:

- Why we are using personal data
- What types of data we collect and who it’s about
- Who we might share it with
- How long we keep it
- What security measures are in place

We regularly update this record to reflect any changes in how we process personal data. If you are involved in any new or changing data activities, make sure to follow the internal guidelines on keeping our RoPA up to date.

We handle personal data requests appropriately

People whose personal data is processed by Bnode have specific rights under data protection laws. These rights are explained in our privacy notices and include things like:

- Consulting what personal data we hold (access)
- Asking to correct incorrect data (rectification)
- Requesting their data to be deleted (erasure or "right to be forgotten")
- Limiting how their data is used (restriction)
- Objecting to how their data is used (objection)
- Asking to receive their data in a usable format (portability)
- Knowing if decisions are made automatically (automated decision-making)

- Filing a complaint with a data protection authority

When someone makes a request, we follow a clear internal process to handle it correctly and on time. Not all requests will be accepted — some may be refused if legal exceptions apply, like protecting the rights of others.

We act responsibly upon personal data breaches

A personal data breach happens when personal data is accidentally or unlawfully lost, accessed, changed, or shared.

Example: losing your work laptop that contains employee or customer information would be considered a data breach. Other examples include having an account hacked or a ransomware attack on a service provider.

Bnode has strong security measures to prevent and handle these incidents. If a breach occurs, we must quickly investigate it, record the details, and depending on how serious it is, notify data protection authorities and potentially the people affected.

If you suspect a data breach, immediately contact the persons mentioned under the Title 3 to make sure it's handled properly and quickly.

We act appropriately regarding data transfers regarding personal data with third parties and intra-group

Sometimes Bnode shares personal data with third parties or between its own entities to support business operations.

Example: personal data might be shared with a software provider or when using cookies on our websites. Personal data might be shared between Bnode entities for CSRD-reporting purposes.

When personal data is sent to countries outside the European Economic Area ("EEA") or other regions with strict data rules, Bnode ensures these transfers follow the law and protect your data properly. This includes using special agreements and safeguards to keep data safe.

Before sharing data with any new external service provider or another entity, Coworkers must check with the local Data Protection Officer, the Digital Compliance Office or Privacy Ambassador to make sure everything complies with data protection laws.

We perform Privacy Impact Assessments and Data Protection Impact Assessments appropriately

When a new processing activity is planned, the Digital Compliance Office, Data Protection Office, Privacy Ambassador or local Data Protection Officer has to conduct thorough risk assessments to evaluate the necessity and proportionality of the processing, minimize associated risks, and identify necessary measures to safeguard personal data.

In certain cases, a comprehensive "Data Protection Impact Assessment" ("DPIA") may additionally be required, particularly when the processing could present a high risk to the rights and freedoms of individuals.

Example: introduction of a system to manage employee health information, such as recording medical certificates or health screenings, involves processing sensitive health data and requires a DPIA to ensure it is handled securely and with appropriate safeguards.

We act with data protection by design ensuring data protection is built into everything

At Bnode, protecting personal data and ensuring security in our services and products is a top priority. We are required to build data protection into everything we do — from the very start of any new project or processing activity. This means we must think about data protection early and use the right technical and organizational steps to keep data safe and respect people's privacy.

There's no single way to do this; the measures depend on the situation. The key is to follow important principles like transparency, fairness, purpose limitation, data minimization, accuracy, confidentiality, and accountability. We need to make sure these principles guide our work in every step: from buying tools and services, to developing and maintaining systems, to securely storing and deleting data.

4. What are the roles and responsibilities regarding data protection at Bnode?

At Bnode, protecting privacy is **everyone's responsibility**. No matter your role, if you work with personal data, you are expected to follow the rules in this privacy policy and help keep that data safe.

Data Protection risk management at Bnode is embedded within the **Enterprise Risk Management (ERM) framework** and follows the **three-lines-of-defense model** to ensure clear accountability and effective governance as follows:

First Line of Defense – Business Owners

Each product, service, or system at Bnode has someone in charge – we call them the "**Business Owner"**. That person is mainly accountable for making sure everything in their area follows data protection rules. They act as the first line of responsibility. The Business Owners are accountable for day-to-day compliance with data protection requirements within their products, services, and processes.
Their responsibilities include:

- implementing data protection controls and minimum standards.
- maintaining the Record of Processing Activities (RoPA) for their scope.
- conducting risk assessments and DPIAs when required.
- managing data protection incidents and ensuring timely escalation.
- ensuring contractual and operational compliance with data protection obligations.

Second Line of Defense – Digital Compliance Office, DPOs, and Privacy Network

- **Digital Compliance Office** (as established within Group Compliance):
  The Digital Compliance Office operates at group level. It is a **strategic partner to the business in managing the data protection compliance commitment across Bnode**.
  In this capacity, the Digital Compliance Office in general:
  - provides oversight in the data protection domain;

- **advises, coaches, mentors** and **supports** the business in their data protection compliance commitment and endeavors and in managing compliance risks while ensuring adherence to standards and controls;
- **monitors** the implementation of minimum control requirements and evaluates the effectiveness and documentation of these controls in relation to data protection.

The scope of its responsibilities may vary depending on the topic and may apply at:

- the **group level** (Bnode-wide),
- a specific **Organizational Unit**[2] **or subsidiary**, or
- a specific **activity** carried out by a Bnode Organizational Unit.

In particular, the Digital Compliance Office:

- defines group data protection standards and governance;
- provides guidance and oversight on data protection compliance;
- acts as the compliance go-to contact for data protection and cybersecurity questions;
- helps business teams understand and meet their data protection obligations;
- develops and supports the rollout of the group's data protection program;
- assists with handling and reporting data incidents;
- keeps our data protection-related contract templates up to date and helps with negotiations;
- reviews services and projects to spot and reduce data protection risks;
- leads the group's overall data protection governance efforts;
- works closely with the DPO Office or local DPOs when needed;
- creates, maintains and coordinates the Privacy Network and supports the entities; and
- monitors adherence to privacy policies and regulatory requirements.

- **The function of local Data Protection Officers ("DPOs")**

DPO is an independent function with the key responsibility to ensure that its respective entity complies with the applicable data protection requirements.
In particular, the DPOs have the responsibility to:

- keep Coworkers of their respective entities informed and trained on their data protection responsibilities.
- monitor how we handle personal data and gives advice to help stay compliant.
- advise on DPIAs for higher-risk projects.
- act as the main contact for data protection authorities.
- handle requests and concerns from individuals about their personal data, when required.

The function of DPO across Bnode is being represented as follows:

- at Bpost sa/nv level: The **Data Protection Office – Bpost sa/nv** operates at Bpost sa/nv level and acting independently, as required by law.
- at subsidiaries level:
  - **If required by local law**, the subsidiary must appoint a **Data Protection Officer** ("**DPO**"). Where mandatory to appoint DPO, the DPO is member of the privacy network.

[2] "Organizational Units" within Bnode include the following:

- units at the level of Bnode that focus on generating revenue by offering products and services ("Business Units"). Current Business Units include bpost, Paxon and Landmark Cross-Border;
- local businesses or groups of local businesses operating within a specific geographic area that focus on generating revenue by offering products and services ("Local Business"). Current Local Businesses include Radial North America. Local Businesses may be included within Business Units.
- units that provide services and / or support to other units or to Bnode as a whole, having the primary responsibilities other than autonomous revenue generation within such units ("Support Units"). Current Support Units include Finance, Human Resources, ICT & Digital, Strategy & Transformation, as well as Corporate Services reporting to the Group CEO (including Legal, Compliance, Enterprise Risk Management, Corporate Audit, Communications, and Public Affairs).

- **If not**, the subsidiary must name a **Privacy Ambassador** – someone coordinates data protection at the local level.

The DPO and DCO roles' repartition is further defined in dedicated internal RACI.

- **The Privacy Network**:
  In addition, the data protection compliance commitment is being supported by the establishment of the "Privacy Network". This network, steered by the Digital Compliance Office, operates at group level and is comprised of the following members:
    - The team members of the Digital Compliance Office;
    - The DPOs (incl. the Privacy Ambassadors);
    - **Privacy Champions**. Each entity also assign Privacy Champions, it being Coworkers in different teams or departments who act as "data protection go-to contacts for daily questions". These help identify risks and make sure data protection rules are followed in everyday work;
    - Any other relevant Coworkers as the case may be.

  The role of the Privacy Network is to:
    - provide support across the entities (at entity level) while ensuring consistent implementation of data protection standards across Bnode;
    - acts as the first point of contact for data protection questions at entity level improving the management of data protection risks and the compliance commitment;
    - make it easier for teams to get the help they need; and
    - share important data protection knowledge, including guidance on AI and new technologies.

Third Line of Defense – Corporate Audit at Bnode level

- provides independent assurance on the design and operating effectiveness of data protection controls.
- conducts periodic audits of data protection processes and governance.
- reports findings to the Audit, Risk & Compliance Committee ("**ARCC**") and supports continuous improvement.

Executive Oversight at Bnode level

- **Privacy, Security and AI Board**
    - follows-up on interactions with the relevant Supervisory authorities.
    - Inform top management and provide a platform for discussing key issues (including it may entail high risks, such as regulatory fines, reputational damage, or negative press coverage).
    - ensures the corporate GDPR / ICT compliance budget is allocated effectively.
    - acts as a sounding board for policies and guidelines on privacy, AI and information security.
    - **Executive Committee ("ExCo")**:
        - ensures data protection risk management is embedded in strategic decision-making.
        - validates resources and promotes a culture of compliance.
- **Board of Directors ("Board") / ARCC**:
        - oversees data protection risk governance as part of the ERM framework.
        - reviews audit results and monitors compliance with privacy obligations.

5. Availability, updates and clarifications

This Global Privacy Policy

- is an internal document, available to employees on Bpost4me or on applicable internal Bnode platforms used by a Bnode subsidiary together with the other related documents governing data protection within Bnode.
- is an evolutive document that will be reviewed on a regular basis and updated as necessary.
- Coworkers will be informed of any updates.

If you have any questions or queries in relation to this Policy, please contact your Data protection officer, the Digital Compliance Office or your Privacy Ambassador.