

PRIVACY POLICY

Version	Date	Evolution	Author
A	29 jul 2026	Original document	KVD
B			
C			
D			
E			
F			
G			

1. General

1.1. Language

The original version of this document is made in Dutch, in compliance with local regulations. This translation in English is provided for the convenience of international communication.

1.2. Document controls

Field	Reference
Policy owner	Compliance Manager
Executive sponsor	Managing Director
Approved by	Management Team
Effective date	29 jul 2026
Review cycle	Annually, and following material legal, business, or risk changes
Applies to	Suppliers, subcontractors, manufacturers, distributors, agents, consultants, labor providers, and their relevant sub-tier partners
Related documents	Sustainability Policy; Supplier Code; Speak-up Procedure

1.3. Controller & contact

Controller: Nucomat bv, Spieveldstraat 65, B-9160 Lokeren, Belgium. Privacy contact: info@nucomat.be. If Nucomat appoints a Data Protection Officer, the DPO contact details will replace or supplement this contact.

1.4. Purpose and legal framework

This Policy explains how Nucomat processes personal data as controller under Regulation (EU) 2016/679 (GDPR), the Belgian Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data, and other applicable Belgian and EU data-protection rules. Contract-specific processor obligations are addressed in data-processing agreements.

This is a general transparency policy. More specific notices may apply to recruitment, employment, CCTV, websites/cookies, events, customers, suppliers, products, or speak-up reports. The specific notice prevails for that processing.

2. Privacy Policy

2.1. Our principles

- Lawfulness, fairness, and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality.
- Accountability, privacy by design, and privacy by default.

2.2. Personal data, purposes, and legal bases

Context / data	Purpose	Primary legal basis
Customers and prospects: identity, role, contact, quotations, contracts, orders, communications, service and support records	Sales, contracting, delivery, support, relationship management, debt recovery, dispute handling, and business development	Contract or pre-contract steps; legal obligation; legitimate interests in B2B operations, service, security, and claims; consent where required for electronic marketing
Suppliers and partners: identity, role, contact, due diligence, contracts, orders, invoices, access and performance records	Procurement, onboarding, due diligence, contracting, payment, quality, compliance, and relationship management	Contract or pre-contract steps; legal obligation; legitimate interests in responsible, secure procurement and claims
Applicants: CV, identity/contact, qualifications, experience, interview/assessment notes, references, work authorisation	Recruitment, selection, communication, verification, and preparation of employment	Pre-contract steps; legal obligation; legitimate interests in fair recruitment and claims; consent only for optional talent-pool retention where appropriate
Workers: identity, contact, family/dependants where required, bank/tax/social-security, contract, attendance, pay/benefits, performance, training, access, travel, expense, safety and occupational-health administration	Employment administration, payroll, benefits, planning, performance, training, access/security, safety, legal compliance, claims, and business continuity	Employment contract; legal obligations in labor, tax, social-security and safety law; legitimate interests for proportionate security, management, fraud prevention and claims; special-category conditions under GDPR Article 9 and applicable law
Visitors and facility users: identity, company, host, time, access badge, safety acknowledgement, CCTV where separately notified	Physical security, safety, emergency response, asset protection, and incident investigation	Legitimate interests; legal obligation; vital interests in emergencies
Website and IT users: IP/device identifiers, logs, account/access data, messages, support and security events	Website/service operation, cybersecurity, authentication, logging, troubleshooting, communications, and misuse prevention	Contract where applicable; legitimate interests; legal obligation; consent for non-essential cookies or tracking
Speak-up participants: identity/contact if provided, report details, persons mentioned, evidence, investigation and outcome records	Receive, triage, investigate, follow up, protect reporters, remediate, defend claims, and meet legal duties	Legal obligation where the Belgian Whistleblower Act applies; legitimate interests in ethics/compliance; establishment, exercise or defence of legal claims; relevant GDPR Articles 9/10 conditions where needed

2.3. Sensitive and criminal-offence data

Nucomat processes special-category data - such as health, disability, trade-union, or biometric data - only where necessary and permitted, for example for employment/social-protection duties, occupational health, safety, vital interests, explicit consent where valid, or legal claims. Access is strictly limited. Criminal-offence data is processed only under official authority or where authorised by EU or Belgian law with appropriate safeguards.

2.4. Sources

We obtain data directly from individuals and from employers, customers, suppliers, recruitment agencies, professional references, public registers, public professional sources, service providers, security systems, devices and systems used for work, authorities, and persons making or participating in reports. Where GDPR Article 14 applies, required information is provided within the applicable period unless a lawful exception applies.

2.5. Recipients

- Authorised Nucomat personnel with a role-based need to know.
- Payroll, social secretariat, benefits, occupational-health, insurance, travel, IT/cloud, cybersecurity, communications, hosting, archiving, legal, audit, and other service providers under appropriate terms.
- Customers, suppliers, logistics providers, banks, insurers, professional advisers, auditors, group or transaction parties, and certification bodies where necessary and lawful.
- Tax, social-security, labor, data-protection, customs, law-enforcement, courts, regulators, and other authorities where required or permitted.
- Emergency services and other parties where necessary to protect vital interests.

Nucomat does not sell personal data.

2.6. International transfers

Where personal data is transferred outside the European Economic Area, Nucomat uses an applicable adequacy decision or appropriate safeguards such as European Commission Standard Contractual Clauses, together with supplementary measures where required. Information on the relevant safeguard may be requested through the privacy contact, subject to necessary redactions.

2.7. Retention

Nucomat keeps personal data only as long as necessary for the stated purpose, applicable limitation periods, legal duties, audits, safety, disputes, and documented legal holds. The following operational schedule applies unless a more specific law, contract, notice, or hold requires a different period.

Record category	Standard retention rule
Unsuccessful recruitment	Delete within 6 months after the process closes, unless the applicant agrees to a talent-pool period of up to 2 years or a dispute requires longer retention.
Personnel and payroll	During employment and thereafter for the period required by Belgian employment, social-security, tax, pension, safety, and limitation rules; personnel-file access remains need-to-know.

Record category	Standard retention rule
Customer/supplier contracts, orders, invoices, and accounting evidence	Contract term plus the applicable statutory accounting, tax, warranty, and limitation period; normally 10 years for core accounting/contract evidence unless counsel confirms another period.
Business contact/CRM	Relationship duration plus 3 years of inactivity; suppression information may be kept to respect objections.
Access and ordinary security logs	Normally 12 months, unless required for investigation, security, contract, or law.
CCTV, if used and separately notified	Normally no longer than 1 month, unless images evidence an incident, offence, damage, or claim.
Speak-up and investigation	Only as long as necessary and proportionate for follow-up, protection, remediation, legal duties, and claims; access is restricted and periodic deletion is documented.

2.8. Security

- Role-based access, least privilege, authentication, secure configuration, patching, malware protection, backups, logging, and network protections.
- Confidentiality duties, training, clean-desk/clear-screen practices, secure disposal, and supplier security requirements.
- Encryption or equivalent safeguards where appropriate to risk; incident detection, escalation, response, and recovery.
- Periodic risk assessment and testing proportionate to the nature, scale, context, and risk of processing.

Individuals must report suspected loss, misdirection, unauthorised access, phishing, malware, or other personal-data incidents immediately to the privacy contact. Nucomat assesses notification to the Belgian Data Protection Authority and affected individuals within applicable GDPR deadlines.

2.9. Individual rights

Subject to conditions and exceptions, individuals may request access, correction, erasure, restriction, portability, and objection; may withdraw consent without affecting prior lawful processing; and may object at any time to direct marketing. Individuals also have rights concerning decisions based solely on automated processing that produce legal or similarly significant effects.

Requests may be sent to info@nucomat.be or by post to Nucomat bv, Spieveldstraat 65, B-9160 Lokeren, Belgium, marked "Privacy". Nucomat may verify identity proportionately. It normally responds within one month; that period may be extended by up to two further months for complex or numerous requests, with notice.

Individuals may lodge a complaint with the Belgian Data Protection Authority (Gegevensbeschermingsautoriteit / Autorité de protection des données), Rue de la Presse 35, 1000 Brussels, Belgium, through its current official contact and complaint channels.

2.10. Children

Nucomat's B2B activities are not directed to children. Personal data concerning minors is processed only where necessary, lawful, proportionate, and subject to additional safeguards: for example, lawful internships, visitors, emergency contacts, or dependants for employment administration.

2.11. Cookies and direct marketing

Non-essential cookies or similar technologies are used only after valid consent where required. Recipients may unsubscribe from electronic marketing at any time. Operational and contractual communications are not marketing and may continue where necessary.

2.12. Automated decision-making and AI

Nucomat does not make employment, customer, or supplier decisions based solely on automated processing with legal or similarly significant effects unless lawful safeguards and a specific notice are in place. Personal or confidential data must not be entered into unapproved AI services.

2.13. Responsibilities and changes

The Managing Director is accountable; the Privacy Coordinator maintains records of processing, notices, processor agreements, risk assessments, breach records, rights requests, training, and review. A Data Protection Officer will be appointed if legally required or voluntarily designated. Material changes will be communicated through appropriate channels.

2.14. Legal and regulator references

- Regulation (EU) 2016/679 (GDPR).
- Belgian Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data.
- Belgian Data Protection Authority guidance on legal bases, transparency, rights, employee files, security, and retention.

<https://www.gegevensbeschermingsautoriteit.be/index.php/professioneel/avg/rechtsgronden>

3. Acknowledgement

I confirm that I have received, read and understood Nucomat's Privacy Policy; I will comply with it, complete the training provided, seek advice if in doubt and report any breaches.

Name	Role	Signature	Date