PERSONAL DATA PROCESSING POLICY FOR CUSTOMERS, SUPPLIERS AND SERVICE PROVIDERS

TRIANGLE'S COMPLIANCE

TABLE OF CONTENTS

I. INTRODUCTION

At Triangle's, the protection of the personal data of our customers, suppliers, and service providers is a priority. This Policy clearly and transparently describes which personal data is processed, for what purposes, on which legal bases, for how long it is retained, with whom it may be shared, and the rights of the respective data subjects.

This Policy must be read in conjunction with Triangle's Integrated Information Security and Digital Systems Policy and the Information Classification, Retention and Sharing Policy, ensuring a consistent approach between privacy, confidentiality, integrity, availability, and resilience of information systems.

Whenever the provision of data constitutes a legal or contractual requirement, or a necessary condition for entering into or performing a contract, failure to provide the strictly necessary data may prevent Triangle's from entering into contracts, issuing invoices, making payments, providing services, responding to requests, or granting access to facilities, platforms, or systems.

II. DATA CONTROLLER

The personal data covered by this Policy is processed by Triangle's - Cycling Equipments, S.A., holder of corporate registration and legal entity number 513 406 603, with registered office at Parque Empresarial do Casarão, Avenida das Duas Rodas, no. 1146, 3750-860 Águeda, Portugal (hereinafter "Triangle's").

For the purposes of Regulation (EU) 2016/679 of 27 April 2016 ("GDPR"), Triangle's acts as the data controller of the personal data of the external data subjects covered by this Policy.

Without prejudice to the provisions of this Policy, certain processing operations may be carried out with the support of duly selected and contractually bound processors, subject to obligations regarding confidentiality, security, assistance in the exercise of rights, and deletion or return of personal data at the end of the provision of services.

Triangle's is not legally required to appoint a Data Protection Officer (DPO). Nevertheless, Triangle's ensures compliance with legal obligations relating to personal data protection and provides a contact point for questions related to privacy and personal data processing through the email address: privacidade@triangles.pt.

III. SOURCE OF PERSONAL DATA

The personal data processed by Triangle's is provided directly by the respective data subjects within the context of commercial, contractual, or pre-contractual relationships.

However, in certain situations, data may be obtained from third parties, namely entities represented by the data subjects, business partners, processors, professional platforms, or legally

permissible sources, where this is necessary for the purposes described in this Policy and where there is a valid legal basis for doing so.
Whenever the data is not collected directly from the data subject, Triangle's ensures compliance with its duty to provide information within the deadlines and under the terms legally applicable, unless this proves impossible or would involve a manifestly disproportionate effort, in the legally provided cases.

IV. CATEGORIES OF DATA PROCESSED

In accordance with the GDPR and Law no. 58/2019, Triangle's processes only personal data that is adequate, relevant, and limited to what is necessary for specified, explicit, and legitimate purposes. Within the context of relationships with customers, suppliers, and service providers, the following categories of personal data may be processed, depending on the case:

- Identification data (e.g., name, signature, identification document number where necessary, tax identification number when the data subject is na individual, position, and represented entity);
- Contact data (e.g., email address, telefone number, business address, and billing or delivery address);
- Professional and representation data (e.g., role, department, powers of representation, certifications, experience, and professional qualifications relevant to the comercial or contactual relationship);
- Contractual, comercial, and operational data (e.g., proposals, orders, contracts, purchase orders, deliveries, service levels, communication history, requests, complaints, and support records);
- Banking and financial data (e.g., IBAN, account holder identification, payment terms, invoices, credit notes, and other biling and collection elements);
- Compliance and third-party assessment data (e.g., qualification documentation, legal declarations, integrity information, tax and social security compliance, conflicts of interest, and other due diligence elements appropriate to the risk and nature of the engagement);
- Technical and security data (e.g., user identifiers, professional credentials, IP addresses, access logs, activity logs, audit records, and security events);
- Physical access and protection of persons and assets data (e.g., reception records, visitor identification, vehicle registration numbers where applicable, and images captured by vídeo surveillance systems);
- Data included in requests for the exercise of rights, complaints, pre-litigation, or litigation matters; and
- Other data necessary to achieve the purposes described in Section V of this document.

As a rule, Triangle's does not process special categories of personal data or data relating to criminal convictions and offences within the context of relationships with external data subjects. If, exceptionally, such processing proves necessary, it shall only occur on the basis of an

appropriate legal ground, strict necessity, restricted access, and enhanced security and confidentiality measures.

V. PURPOSES AND LEGAL BASES FOR PROCESSING

The personal data referred to in Section IV is processed for the purposes described below, based on the legal grounds provided for under the GDPR. Triangle's applies the "need to know" principle, segregation of duties, and periodic access review mechanisms, in conjunction with the Integrated Information Security and Digital Systems Policy.

Purpose and Legal Basis

Purpose	Legal Basis
Management of business contacts, information requests, proposals, quotations, qualification processes, approvals, and contracting.	Pre-contractual diligences Legitimate interest
Management and execution of contractual or commercial relationships, including orders, supplies, deliveries, service provision, support, invoicing, payments, service level monitoring, and administrative management of the relationship.	Performance of a contract Legitimate interest
Compliance with legal, regulatory, tax, accounting, commercial, archival, audit, and reporting obligations.	Compliance with legal obligations
Risk management, fraud prevention, due diligence, conflict of interest assessment, asset protection, and business continuity.	Legitimate interest Compliance with legal obligations, where applicable
Management of physical and logical access, information security, monitoring of security events, logging, incident response, and service recovery.	Legitimate interest Compliance with legal obligations, where applicable
Management of complaints, debt collection, credit recovery, and the exercise and defense of rights in administrative, arbitration, or judicial proceedings.	Legitimate interest Compliance with legal obligations

Purpose	Legal Basis
Capture of images for the protection of persons and assets and facility security, where applicable.	Legitimate interest Compliance with legal obligations, where applicable
ther specific purposes compatible with the above or independent thereof, provided they are duly communicated to the data subject.	Consent, where necessary Legitimate interest, where applicable

Within the framework of alignment with the Integrated Information Security and Digital Systems Policy, Triangle's implements technical and operational measures appropriate to the risk, including information classification, access control, strong authentication where applicable, encryption in transit and/or at rest where justified, event logging and monitoring, vulnerability management, backups, recovery testing, confidentiality obligations, and security incident and personal data breach notification and management processes.
As a rule, Triangle's does not adopt decisions based exclusively on automated processing, including profiling, that produce legal effects or similarly significantly affect external data subjects. Should this occur in specific situations, the legally required information will be provided separately and appropriately.

VI. DATA RECIPIENTS

Whenever necessary for the purposes described above, personal data may be shared, strictly on a need-to-know and proportionate basis, with:

- Internal Triangle's departments that require access to the data for comercial, contractual, financial, operational, technological, security, audit, quality, or compliance purposes;
- Triangle's processors and service providers, namely providers of information technology, hosting and cloud services, ERP/CRM systems, invoicing, accounting, auditing, consultancy, legal support, cybersecurity, archiving, logistics, transport, maintenance, and document management services;
- Financial institutions, insurers, payment operators, and collection entities, whenever necessary for payment processing, insurance, guaranees, or debt recovery;
- Administrative, judicial, law enforcement, regulatory, or tax authorities whenever disclosure is legally required or necessary for the exercise or defense rights;
- Other entities that must receive the data pusuant to law, contractual obligation, or Triangle's prevailing legitimate interest, duly assessed and coumented.

Whenever acting through processors, Triangle's ensures the execution of appropriate contractual arrangements regulating, among other aspects, the subject matter and duration of the processing, the nature and purposes of processing, the categories of data and data

subjects, security measures, confidentiality obligations, rules regarding onward subcontracting, and assistance to the data controller.

VII. INTERNATIONAL DATA TRANSFERS

Should Triangle's transfer personal data to a third country or to an international organization outside the European Economic Area, such transfer shall only take place where there is a valid legal basis and appropriate safeguards as provided under Chapter V of the GDPR, namely an adequacy decision by the European Commission, standard contractual clauses, binding corporate rules, or another legally admissible mechanism.

Where applicable, Triangle's shall provide data subjects with additional information regarding the international transfer, including the legal basis used to legitimize the transfer and the means to obtain a copy of the appropriate safeguards, except where legally applicable limitations exist.

VIII. DATA RETENTION PERIODS AND CRITERIA

Triangle's retains personal data only for the period necessary for the purposes for which it was collected and processed, without prejudice to legally established retention periods, applicable limitation periods, and the need to preserve evidence for the exercise or defense of rights. Once the applicable retention periods expire, the data will be securely deleted, anonymized where possible, or blocked in cases legally required.

The retention periods indicated below may be suspended or extended where litigation, audit, investigation, security incident, obligation to preserve evidence, order from a competent authority, or another legally valid reason requires the data to be retained for a longer period.

Categories of Data, Purposes, Legal Bases and Retention Periods

Categories of Personal Data	Legal Basis	Processing Purposes	Retention Period / Criteria
Identification data Contact data Professional and representation data	Pre-contractual diligences Legitimate interest	Management of business contacts, proposals, quotations, qualification, approval, and pre-contractual negotiations	Up to 2 years after the last relevant contact or closure of the process, unless a contract is entered into or there is a legal obligation requiring longer retention
Identification data Contact data Contractual, commercial, and operational data Professional and representation data	Performance of a contract Legitimate interest	Management of the commercial and contractual relationship, deliveries, service provision, support, and administrative and operational management	During the contractual or commercial relationship and up to 3 years after termination or the last relevant operational contact, without prejudice to legal invoicing, evidence, and archiving requirements
Identification data Banking and financial data Invoicing and collection data Relevant contractual and commercial data	Compliance with legal obligations	Compliance with tax, accounting, commercial, invoicing, bookkeeping, and reporting obligations	During the relationship and, as a rule, up to 10 years after the end of the relevant financial year or after termination, where required by law
Identification data Contact data Professional data Compliance and third-party assessment data	Legitimate interest Compliance with legal obligations, where applicable	Due diligence, qualification, risk assessment, fraud prevention, conflict of interest assessment, and document validation	During the relationship and up to 5 years after termination or the decision not to contract, unless a different legal obligation or preservation of evidence applies

Categories of Personal Data	Legal Basis	Processing Purposes	Retention Period / Criteria
Technical and security data Access logs Audit records Professional credentials	Legitimate interest Compliance with legal obligations, where applicable	Access management, information security, monitoring, technical auditing, incident detection, and incident response	Up to 1 year, unless longer retention is required for incident investigation, audit, defense of rights, or legal obligation
Physical access data Visitor identification Vehicle registration number, where applicable	Legitimate interest Compliance with legal obligations, where applicable	Facility access control, protection of persons and assets, and visitor management	Up to 1 year after the visit record, unless there is a security incident, investigation, or specific legal obligation
Images captured through video surveillance	Legitimate interest Compliance with legal obligations, where applicable	Protection of persons and assets and facility security	30 days after image capture, unless longer retention is necessary for the investigation of unlawful acts or by determination of a competent authority
Data included in requests, complaints, communications, debt collection, pre-litigation, and litigation matters	Legitimate interest Compliance with legal obligations	Management of complaints, data subject rights requests, debt recovery, and the exercise or defense of rights in administrative, arbitration, or judicial proceedings	Up to 3 years after closure of the request or complaint; in case of litigation or debt collection, until final judicial decision, fulfillment of the obligation, or expiry of the applicable limitation periods
Consent records and communication preferences, where applicable	Consent	Proof of consent collection and management of the data subject's preferences	Until withdrawal of consent and, thereafter, for the period strictly necessary to demonstrate compliance and defend rights

IX. DATA SUBJECT RIGHTS

Under the applicable legislation, data subjects may request from Triangle's, at any time and within the legally established limits:

- Access to their personal data and to information relating to its processing;
- Rectification of their personal data where inaccurate, outdated, or incomplete;
- Erasure of their personal data, where legally admissible;
- Restriction of processing, in the situations provided for by law;
- Data portability, where applicable;
- Objection to processing, where such processing is based on legitimate interest or another legal basis subject to objection under the GDPR;
- Withdrawal of consent, whenever processing is based on consent, without affecting the lawfulness of processing carried out prior to such withdrawal; and
- The right to lodge a complaint with the Portuguese Data Protection Authority (*Comissão Nacional de Proteção de* Dados – CNPD).

Requests for the exercise of rights shall be analyzed diligently and responded to within the terms and deadlines established by law. Triangle's undertakes to respond within a maximum period of 30 days from the date of receipt of the request.

In cases of particular complexity or where there is a high number of requests, this period may be extended by up to an additional two months, and the data subject shall be duly informed of such extension and its respective grounds.

In certain circumstances, Triangle's may also request additional information to confirm the identity of the requester or may refuse, with proper justification, a request where there is a legal basis for doing so, namely due to overriding legal obligations, retention duties, professional secrecy, defense of rights in judicial proceedings, or protection of third parties.

X. CONTACT FOR QUESTIONS

If you wish to exercise your rights, clarify any questions related to this Policy, or obtain additional information regarding the processing of your personal data, you may contact Triangle's through the email address: privacidade@triangles.pt.

Document control
Document issued by: 7 May 2026
Version no. 1
Effective date: 11 May 2026
Prepared by: Compliance
Approved by: Executive Board