EXHIBIT

TO THE DATALOGIC GENERAL TERMS AND CONDITIONS OF PURCHASE

GUIDELINE ON CRA REQUIREMENTS

This Exhibit to the Datalogic General Terms and Conditions of Purchase: Guideline on CRA Requirements (the "**CRA Exhibit**") is issued pursuant to, and forms an integral part of, the Datalogic General Terms and Conditions of Purchase of Datalogic (the "**Terms and Conditions of Purchase**"), together with any Purchase Order issued thereunder. Capitalized terms used but not defined in this CRA Exhibit shall have the meanings ascribed to them in the Terms and Conditions of Purchase.

This CRA Exhibit sets out the additional terms and conditions applicable to the supply of Products with digital elements intended for placement on the EU market, in order to ensure compliance with Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements (the "**Cyber Resilience Act**" or "**CRA**" as defined below), as may be amended from time to time.

Datalogic and Supplier in this CRA Exhibit shall have the same meaning under the Terms and Conditions of Purchase.

ARTICLE 1 – DEFINITIONS

Capitalized terms used but not defined in this CRA Exhibit shall have the meanings given to them in the Terms and Conditions of Purchase. For the purposes of this CRA Exhibit, the following terms shall have the following meanings:

1.1 "Product(s)" means any hardware and/or software product with digital elements manufactured by the Supplier and supplied to Datalogic that is intended for placement on the EU market.

1.2 "CRA" means Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements, as may be amended from time to time, together with all related legal instruments issued thereunder or in connection therewith, including but not limited to:

(a) delegated acts and implementing acts adopted by the European Commission pursuant to the CRA;
(b) harmonized standards developed by European standardization organizations (CEN, CENELEC, ETSI) and referenced in the Official Journal of the European Union in relation to the CRA;
(c) technical specifications and common specifications adopted under the CRA;
(d) guidelines, guidance documents, recommendations and opinions issued by the European Union Agency for Cybersecurity (ENISA), the European Commission, national market surveillance authorities, or other competent authorities for the interpretation or application of the CRA; and
(e) any national transposition measures, administrative decisions or enforcement guidance issued by competent authorities of EU Member States in relation to the CRA.

1.3 "Support Period" means the support period required under the CRA, during which security updates and vulnerability handling obligations must be maintained, which shall in no event be less than five (5) years from the date of first placement of the Product on the EU market, or such longer period as may be prescribed by the CRA or applicable delegated acts for the relevant product category, and which shall be defined and agreed by the parties at the time of purchase.

1.4 "SBOM" means a Software Bill of Materials: a machine-readable inventory of software components, third-party libraries, top-level dependencies, and known associated vulnerabilities included in or forming part of the Products.

1.5 "ENISA" means European Union Agency for Cybersecurity.

1.6 “CSIRTs” means Computer Security Incident Response Teams.

ARTICLE 2 – SUPPLIER OBLIGATIONS

2.1 Secure by Design and Cybersecurity Risk Assessment

2.1.1 The Supplier shall design, develop, manufacture, and maintain the Products in accordance with the essential cybersecurity requirements of the CRA, including but not limited to:

(a) No known exploitable vulnerabilities at the time of delivery and throughout the Support Period and reasonably expected product lifecycle;
(b) Secure-by-default configurations and the ability for users to reset the Product to its original factory state;
(c) Protection against unauthorized access through appropriate authentication and access control mechanisms;
(d) Confidentiality of stored and transmitted data, including encryption where appropriate;
(e) Integrity of data, commands, programs, and configuration against unauthorized manipulation;
(f) Data minimization: collecting and processing only data necessary for the Product’s intended purpose;
(g) Protection of availability, including resilience against denial-of-service attacks;
(h) Minimization of the attack surface, including limitation of external interfaces to those necessary for the Product’s function;
(i) Security logging and monitoring capabilities;
(j) Ability to securely and permanently delete user data;
(k) Provision of security updates, including automatic update mechanisms enabled by default where technically applicable.

The Supplier shall conduct and document a cybersecurity risk assessment that informs the above requirements across the Product’s planning, design, development, production, delivery, and maintenance phases.

2.1.2 The Supplier shall establish and maintain documented procedures ensuring that series production of the Products remains in conformity with the CRA at all times. Such procedures shall adequately account for:

(a) Changes in development or production processes;
(b) Changes in product design or characteristics; and
(c) Changes in harmonized standards, European cybersecurity certification schemes, or common specifications referenced under the CRA.
(d) The Supplier shall, upon Datalogic's reasonable request, provide evidence of compliance with such ongoing conformity procedures.

2.2 Software Bill of Materials (SBOM)

2.2.1 The Supplier shall provide Datalogic with a machine-readable SBOM in CycloneDX or SPDX format (or such other format as may be mandated by the European Commission) for each Product, covering at minimum:

(a) All software components, third-party libraries, and top-level dependencies;
(b) Known vulnerabilities in the listed components at the time of delivery.

2.2.2 The Supplier shall maintain and update the SBOM throughout the Support Period and provide updated versions upon request, and in any event within thirty (30) days following any material software change or new Product release.

2.3 Security Updates

2.3.1 The Supplier shall:

(a) Provide security patches, updates, and vulnerability remediation for the full Support Period;
(b) Deliver such security updates at no additional charge to Datalogic;
(c) Support automatic update mechanisms where technically feasible;
(d) Ensure that security updates are provided in a timely manner and without adversely affecting Product functionality;
(e) Distribute security updates securely, accompanied by advisory messages describing nature, severity, and recommended actions for each update.

2.3.2 Supplier shall Ensure that each security update made available during the Support Period remains available to Datalogic and end users for at least ten (10) years after the date such update is first released, or for the remainder of the Support Period, whichever is longer.

2.4 Vulnerability Management

The Supplier shall:

(a) Identify and document vulnerabilities and Product components, including by maintaining an up-to-date SBOM in a commonly used, machine-readable format;
(b) Address and remediate vulnerabilities without delay, providing security updates free of charge;
(c) Apply effective and regular security testing and reviews throughout the Product lifecycle;
(d) Publicly disclose information about fixed vulnerabilities;
(e) Establish and enforce a coordinated vulnerability disclosure policy;
(f) Maintain a publicly accessible contact address for vulnerability reporting;
(g) Continuously monitor publicly disclosed vulnerabilities affecting the Products and any third-party or open-source components;
(h) Promptly notify Datalogic in writing of any discovered vulnerability affecting the Products;
(i) Provide remediation or mitigation measures without undue delay and within the timeframes agreed with Datalogic;
(j) Maintain records relating to all vulnerability handling activities.

2.5 Incident Reporting

2.5.1 Upon becoming aware of an actively exploited vulnerability or severe cybersecurity incident affecting any Product, the Supplier shall promptly notify Datalogic and provide all information, documentation and reasonable assistance necessary to enable Datalogic to comply with its reporting and notification obligations under the CRA. Without limiting the foregoing, the Supplier shall:

(a) Notify Datalogic in writing without undue delay and in any case immediately after becoming aware of the vulnerability or incident, providing all information then available, and shall continuously provide any additional information, updates, corrective or mitigating measures and supporting documentation as soon as they become available, so that Datalogic is able to comply with the applicable reporting deadlines under the CRA;
(b) Cooperate fully with Datalogic in relation to any notifications, reports, investigations, corrective actions, or market surveillance measures involving any CSIRT, competent authority, notified body, or other EU authority.; and in addition, prepare and provide to Datalogic — in form, content and language suitable for onward communication to end users — notifications concerning actively exploited vulnerabilities and severe incidents affecting the Products, including available corrective or mitigating measures, for dissemination to end users in accordance with the CRA.

2.6 Technical Documents

2.6.1 The Supplier shall:

(a) Specify the Product's classification under the CRA (default, Class I, Class II, or critical product) and the applicable conformity assessment module, and update Datalogic promptly upon any change in classification;

(b) Ensure each Product bears a type, batch or serial number, or other element allowing its identification, in accordance with the CRA;
(c) Prepare and maintain complete technical documentation as required under the CRA, with all such documentation retained for a period of ten (10) years after placement of the Product on the market or for the duration of the Support Period, whichever is longer;
(d) Issue an EU Declaration of Conformity in compliance with the model structure and content requirements of the CRA and applicable conformity assessment module, and affix the CE Marking to each Product prior to, or as a condition of, supplying Products to Datalogic for placement on the EU market;
(e) Cooperate fully in any conformity assessment procedure initiated by Datalogic or a notified body;
(f) Promptly inform Datalogic of any changes to the Products that may affect CRA compliance.

2.6.2 The Supplier shall provide all technical information, testing reports, cybersecurity risk assessments, security architecture descriptions, declarations, certifications, and assistance required by Datalogic.

2.6.3 The Supplier shall prepare and provide to Datalogic the Product related information and instructions required under the CRA for each Product. The Supplier shall provide such information and instructions to Datalogic in an editable format suitable for incorporation into Datalogic's own product documentation and shall retain copies thereof for at least ten (10) years after placement of the Product on the market or for the Support Period, whichever is longer.

2.7 CRA Compliance Attestation

The Supplier shall provide Datalogic with:

(a) A written attestation confirming that the Products meet the essential cybersecurity requirements of Exhibit I of the CRA, accompanied by a copy of the EU Declarations of Conformity and evidence of CE Marking; or
(b) Where full compliance has not yet been achieved (and no later than 10 December 2027), a documented compliance plan and timeline specifying the steps and milestones for achieving full CRA conformity.

The Supplier shall update such attestation or compliance plan whenever there is a material change in the compliance status or product classification.

2.8 Vulnerability Management Process Documentation

The Supplier shall provide Datalogic with evidence of an established vulnerability handling process, including:

(a) A copy of the Supplier’s coordinated vulnerability disclosure policy;
(b) The designated contact point for vulnerability reports;
(c) The defined Support Period (including end-of-support date) for each Product supplied to Datalogic;
(d) Any relevant certifications, test results, or third-party assessments evidencing the Supplier’s cybersecurity practices.

2.9 Open Source Software

The Supplier shall be responsible for the security, integrity, and licence compliance of all third-party and open-source software components included in the Products. The Supplier shall monitor publicly disclosed vulnerabilities affecting such components and promptly remediate them.

2.10 Corrective Actions, Recall and Withdrawal

If a Product presents a cybersecurity risk or fails to comply with the CRA, the Supplier shall immediately take corrective measures and, at its own cost and without undue delay:

(a) Immediately notify Datalogic in writing upon discovering or having reason to believe that any Product or process is not in conformity with the CRA;
(b) Implement corrective actions;
(c) Suspend deliveries if requested by Datalogic;
(d) Support Product withdrawal or recall activities; and
(e) Cooperate in customer communications and remediation activities.

2.11 Subcontractors and Supply Chain

The Supplier shall ensure that all subcontractors, software providers, and third-party suppliers involved in the Products comply with obligations equivalent to those set out in this CRA Exhibit. The Supplier shall implement appropriate technical and organisational measures to ensure cybersecurity protection of any personal data processed by the Products. The Supplier shall include in all subcontracts relating to the Products provisions granting Datalogic (or its authorised representative) audit rights equivalent to those set out in Article 3 of this CRA Exhibit, and shall facilitate the exercise of such rights upon Datalogic reasonable request.

2.12 Ongoing Compliance Updates

The Supplier shall provide Datalogic with timely updates as the CRA's harmonised standards, delegated acts, and implementing measures are finalised, including:

(a) Any changes to the Product's classification under the CRA;
(b) Any change in the applicable conformity assessment route;
(c) Any material changes to the Supplier's EU Declarations of Conformity or CE Marking status.

2.13 Regulatory Changes

The parties shall cooperate in good faith to amend this CRA Exhibit as reasonably necessary to reflect future changes to applicable CRA requirements, implementing acts, harmonized standards, or guidance issued by EU authorities.

2.14 Cessation of Operations

If the Supplier intends to permanently cease operations or discontinue manufacturing of any Product, the Supplier shall:

(a) Notify Datalogic in writing immediately upon making such decision and in any event no less than ninety (90) days before the cessation takes effect;
(b) Provide Datalogic with a transition plan, which shall include delivery of all outstanding security updates, release of all CRA compliance documentation (including technical documentation, SBOM, EU Declaration of Conformity, cybersecurity risk assessments, and vulnerability records), and if reasonably requested by Datalogic, deposit of source code and build environments into escrow to enable continued delivery of security updates for the remainder of the Support Period;
(c) Notify the relevant market surveillance authorities and, through Datalogic, the affected users of the Products, in accordance with the CRA; and
(d) Cooperate fully with Datalogic to ensure continuity of CRA compliance for the Products throughout the remainder of the Support Period.

2.15 Language Requirements

All CRA-required information, documentation, user instructions, EU Declarations of Conformity, and communications provided by the Supplier under this CRA Exhibit shall be in the official language(s) of the EU Member States where Datalogic intends to place the Products on the market, as agreed between the parties. In addition, all information and documentation required to be provided to market surveillance authorities shall be available in a language easily understood by the requesting authority.

2.16 Market Surveillance Cooperation

The Supplier shall:

(a) Maintain all CRA compliance documentation in a state of readiness for provision to market surveillance authorities upon reasoned request, in accordance with the CRA;
(b) Respond to any request for information or documentation from any market surveillance authority without undue delay and in any event within fifteen (15) calendar days, or within such shorter period as may be required by law;
(c) Cooperate fully with Datalogic and any market surveillance authority in any investigation, corrective action, or enforcement proceeding related to CRA compliance; and
(d) Bear all costs incurred by the Supplier in connection with such cooperation, provided that if the investigation reveals no non-compliance attributable to the Supplier, the parties shall agree on an equitable allocation of external costs.

2.17 CRA Compliance Timeline

The Supplier shall meet the following milestone schedule to fully comply the requirements of CRA:
(a) By September 11, 2026: Have vulnerability and incident reporting processes operational to support Datalogic in meeting the reporting obligations that take effect on that date, in accordance with Article 2.5. And in case that Supplier is responsible for the direct reporting obligations under the CRA, Supplier shall comply with the reporting obligations under the CRA.
(b) By Q4 2026: Provide Datalogic with CRA compliance attestations (or detailed compliance roadmaps) for all Products and components supplied for integration into Datalogic products destined for the EU market.
(c) By December 11, 2027: Achieve full CRA compliance, including completed conformity assessments, CE marking, EU Declarations of Conformity, and all required technical documentation.

ARTICLE 3 – AUDIT & INSPECTION

3.1 Upon reasonable prior notice (not less than seven (7) business days), Datalogic or its authorised representative may conduct a compliance audit of the Supplier's relevant processes, documentation, systems, and facilities.
3.2 The Supplier shall provide all reasonable cooperation, access, and assistance required for such audit.
3.3 The Supplier shall promptly remediate any non-conformities identified during the audit at its own expense.

ARTICLE 4 – REPRESENTATIONS & WARRANTIES

The Supplier represents and warrants that:
4.1 Products delivered to Datalogic shall comply with all applicable CRA cybersecurity requirements and other applicable EU cybersecurity laws;
4.2 All information provided to Datalogic regarding CRA compliance shall be accurate, complete, and not misleading; and
4.3 The Supplier has implemented and shall maintain adequate internal cybersecurity governance and compliance procedures.

ARTICLE 5 – INDEMNIFICATION

The Supplier shall indemnify, defend, and hold harmless Datalogic, its affiliates, directors, employees, and customers from and against any fines, penalties, losses, damages, liabilities, recall costs, remediation expenses, customer claims, legal fees, and regulatory sanctions arising directly or indirectly from:

(a) The Supplier's breach of this CRA Exhibit;
(b) Any CRA non-compliance attributable to the Supplier's Products, software, components, or manufacturing processes; or
(c) Any failure by the Supplier to comply with applicable cybersecurity obligations.

ARTICLE 6 – TERM & TERMINATION

6.1 This CRA Exhibit shall remain applicable to the Supplier for the duration of the Terms and Conditions of Purchase and any Purchase Order issued thereunder, and for any additional period during which the CRA remains applicable to the Products, whichever is longer.

6.2 Any breach of this CRA Exhibit that is not remedied within thirty (30) days after written notice shall entitle the non-breaching party to terminate the Purchase Order with immediate effect, without prejudice to any other rights and remedies available under the Terms and Conditions of Purchase.

6.3 The obligations relating to security updates, vulnerability handling, conformity documentation, confidentiality, indemnification, and regulatory compliance shall survive termination of this CRA Exhibit for the duration required under applicable law.

ARTICLE 7 – GOVERNING LAW & JURISDICTION

The governing law and dispute resolution provisions set out in the Terms and Conditions of Purchase shall apply to this CRA Exhibit. Without prejudice to the foregoing, this CRA Exhibit shall be governed by the laws of Italy, without prejudice to the application of mandatory EU law, including the CRA.

Any dispute arising out of or in connection with this CRA Exhibit shall be submitted to the exclusive jurisdiction of the courts of Bologna, Italy.

ARTICLE 8 – GENERAL

8.1 This CRA Exhibit supplements and forms an integral part of the Terms and Conditions of Purchase. In the event of any conflict between this CRA Exhibit and the Terms and Conditions of Purchase with respect to CRA compliance obligations, this CRA Exhibit shall prevail.

8.2 This CRA Exhibit supersedes any prior arrangements between the parties relating specifically to the subject matter hereof.

8.3 Supplier acknowledges that Datalogic may act as manufacturer, importer, distributor, or other economic operator under the CRA, and Supplier shall provide all assistance reasonably necessary for Datalogic to fulfil its regulatory obligations.

8.4 This CRA Exhibit shall automatically apply and be binding upon any Supplier that supplies Products to Datalogic which are subject to the CRA, regardless of whether such Supplier has separately executed this CRA Exhibit, and the Supplier shall be deemed to have accepted and agreed to comply with the terms and obligations set forth herein.