Data processing agreement

Information section

Parties. This Data Processing Agreement (the "DPA") is entered into between:

a. The entity that (i) executes this DPA or (ii) accepts this DPA by electronic means (including click-acceptance) in connection with the Provider's services (hereinafter, the "CUSTOMER"), acting as data controller (hereinafter, the "CONTROLLER"); and

b. CHECKPOINT GROUP, acting as data processor (hereinafter, the "PROCESSOR"). For the purposes of this DPA, "CHECKPOINT GROUP" means the Provider and its affiliates involved in providing the services, as identified in the applicable Main Contract, order form or the Provider's legal notice/customer portal made available from time to time.

Main Contract. This DPA forms part of, and is incorporated into, the agreement governing the CUSTOMER's use of the services (the "Main Contract"), which consists of the agreement, order form, statement of work, purchase order, online subscription flow, click-through terms, or other ordering document accepted by the CUSTOMER, as applicable. This DPA applies to the extent the PROCESSOR processes personal data on behalf of the CONTROLLER while providing the services under the Main Contract.

Applications processing details. The subject matter, nature, and purpose of the processing, the types of personal data and categories of data subjects, and the duration of processing for each of the PROCESSOR applications are set out in APPENDIX I (SERVICES PROCESSING DETAILS), which is incorporated by reference and forms an integral part of this DPA.

Security Measures. The technical and organizational measures implemented by the PROCESSOR are described in APPENDIX II (TECHNICAL AND ORGANISATIONAL MEASURES), which is incorporated by reference and forms an integral part of this DPA.

Sub-processors. The PROCESSOR's authorized Sub-processors and related information are set out in APPENDIX III (SUB-PROCESSORS) and in the Provider's then-current online Sub-processor List made available through the Provider's privacy page, customer portal, or equivalent legal notices page. The Sub-processor List is incorporated by reference and forms an integral part of this DPA.

International Transfers. Where processing involves transfers of personal data outside the EEA (as applicable), the transfer mechanisms and safeguards are described in APPENDIX IV (INTERNATIONAL DATA TRANSFERS) and in the PROCESSOR's then-current transfer information made available through the Provider's privacy page, customer portal, or equivalent legal notices page. That transfer information is incorporated by reference and forms an integral part of this DPA.

Contact Points. The PROCESSOR's data protection contact point is the privacy contact made available in the Provider's Privacy Policy, customer portal, or equivalent legal notices page, as updated from time to time. The CONTROLLER's contact point remains the contact details associated with the CUSTOMER's account unless otherwise notified to the PROCESSOR in writing.

Terms and conditions

FIRST. - OBJECT

It is the object of this Data Processing Agreement (hereinafter, the "**Agreement**"), to regulate the processing of personal data in accordance with the provisions of the applicable legislation on the protection of personal data, especially , the provisions pursued by the Regulation (EU) 2016/679, of the European Parliament and of the Council, of April 27, 2016, regarding the protection of natural persons with regard to the processing of personal data and the free movement of these data (hereinafter, "GDPR"), as well as the provisions of the national regulations that are applicable.

In particular, by means of this clause, the PROCESSOR is authorized to process, on behalf of the CONTROLLER, the necessary personal data for the execution of the Main Contract referenced in the Information Section above.

For the purposes of this contract, all terms used shall have the meaning attributed to them by the GDPR, unless a different meaning is expressly established in this contract.

SECOND. - NATURE AND PURPOSES OF THE PROCESSING ACTIVITY

The nature and purpose of the processing activity will consist in the execution of the Main Contract specified in the Information Section above. The applicable categories of data subjects and types of personal data are those specified for the contracted Application(s) in APPENDIX I. The Applications are not intended for the processing of special categories of personal data unless the CONTROLLER configures, uploads, or otherwise makes such data available on its own documented instructions.

THIRD. - DURATION

This Agreement will be applicable from the date of its signature and will be in force during the term of the Main Contract and until the obligations contemplated in this Agreement have been fulfilled, regardless of any other legal obligation applicable to the parties upon termination of said relationship.

FOURTH. - PROCESSOR OBLIGATIONS

The PROCESSOR, in his capacity as the person in charge of the processing activity, shall use reasonable efforts to comply with the following obligations, considering the nature of the processing and the information available to the PROCESSOR. The obligations below shall apply to the extent required by applicable law and the Main Contract, and subject to the PROCESSOR's technical and

organizational capabilities:

a. use the processed personal data, or those collected for inclusion, only for the purposes established in this Agreement and the Main Contract. The PROCESSOR shall not use the data for its own purposes or outside the provision of the Services detailed in the Main Contract, except where required by law or with the prior written con sent of the CONTROLLER.

b. process personal data only following documented instructions that, at any time, the CONTROLLER indicates, committing, in any case, to carry out the processing activities (i) within the framework of the European Union, (ii) in countries declared with a level of adequate protection by the European Commission, or (iii) in third countries where appropriate safeguards have been provided, such as the subscription of the Standard Contractual Clauses approved by the European Commission (SCC), adoption of Binding Corporate Rules (BCR), or adherence to conduct codes, certification mechanisms, or ad-hoc contractual clauses , to the extent applicable.

   Where applicable and upon reasonable request, the PROCESSOR will make available to the CONTROLLER documentation evidencing the appropriate safeguards adopted. This includes resources or auxiliary services used by the PROCESSOR for normal operation, either directly or outsourced, as documented in APPENDIX III: INTERNATIONAL DATA TRANSFERS.

   If, by legal requirement of the law of the European Union or of the Member States, the PROCESSOR is required to transfer personal data to a third country or an international organization, the PROCESSOR will inform the CONTROLLER beforehand where legally permitted, unless such law prohibits it for important reasons of public interest.

   The PROCESSOR shall request the CONTROLLER for any material change in the location from which the Processing of the CONTROLLER's Personal Data is conducted. This authorization shall be requested at least six (6) months prior to the implementation of such change, which shall be subject to the CONTROLLER's approval.

c. immediately inform the CONTROLLER if, in his opinion, instruction violates the applicable data protection regulations or other provisions regarding data protection matters of the Union or Member States that may be equally applicable.

d. ensure that persons authorized to process personal data are subject to appropriate confidentiality obligations, either contractually or by law. The PROCESSOR will use reasonable efforts to ensure that such obligations are maintained during the validity of this Agreement and, where applicable, for the periods established by current legislation. The PROCESSOR will provide necessary training in the protection of personal data to authorized persons, as appropriate and reasonable.

e. Maintain a record, in writing, of processing activities carried out on behalf of the CONTROLLER, to the extent required by applicable law and as reasonably practicable, containing, at a minimum:

   i. The name and contact details of the PROCESSOR and the CONTROLLER, and, where applicable, the joint controller, the CONTROLLER's representative, and the Data Protection Officer, to the extent such information is required and available.

   ii. The categories of processing activities are carried out on behalf of the CONTROLLER, as applicable.

   iii. Where applicable, transfers of personal data to a third country or an international organization, including, where possible, the identification of that third country or international organization and the documentation of suitable safeguards.

   iv. A general description of the technical and organizational security measures implemented by the PROCESSOR, as appropriate and reasonable in relation to the risk, and in particular, those specified in APPENDIX I: TECHNICAL AND ORGANIZATIONAL MEASURES to this Agreement, taking into account the state of the art, implementation costs, the nature, scope, context and purposes of the processing, as well as risks of varying probability and severity for the rights and freedoms of natural persons.

f. undertake to keep under their control and custody, the personal data provided by the CONTROLLER to which they have access in connection with the provision of the services, and not to disclose them, transfer them or communicate them in any other way to third parties, except as required by law, with the CONTROLLER's prior written consent, or as necessary for the performance of the Services under this Agreement.

g. implement appropriate technical and organizational measures to ensure a level of safety appropriate to the risk, and in particular, those specified in APPENDIX I: TECHNICAL AND ORGANIZATIONAL MEASURES to this Agreement, taking into account the state of the art, implementation costs, the nature, scope, context and purposes of the processing, as well as risks of varying probability and severity for the rights and freedoms of natural persons. The PROCESSOR shall use reasonable efforts to comply with these measures, subject to its technical and organizational capabilities.

h. assist the CONTROLLER, as reasonably practicable, so that the CONTROLLER can comply with its obligation to respond to requests regarding the exercise of data subjects' rights, notifying and sending any request to the CONTROLLER promptly and, w here possible, within a reasonable period.

i. notify the CONTROLLER, without undue delay, about any personal data security breach affecting the CONTROLLER's data of which the PROCESSOR becomes aware. The PROCESSOR may provide initial notification with limited information and shall provide additional relevant information for the documentation and communication of the incident as it becomes reasonably available, including, where possible, the following information:

i. description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

ii. the name and contact details of the data protection officer or other contact points where further information can be obtained, if available;

iii. a description of the possible consequences of the breach of the security of personal data, to the extent such information is known or can be reasonably determined; and

iv. a description of the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects, to the extent such measures are known or can be reasonably determined.

If and to the extent that it is not possible to provide the information at the same time, the information may be provided in phases as it becomes reasonably available, without undue further delay.

j. support the CONTROLLER, as reasonably practicable, in carrying out data protection impact assessments, taking into account the nature of the processing in question and the information available to the PROCESSOR.

k. make available to the CONTROLLER information reasonably necessary to demonstrate compliance with the obligations set out in this Agreement, as well as to enable and contribute to the conduct of audits, including inspections, by the CONTROLLER or another auditor authorized by the CONTROLLER.

Specifically, the CONTROLLER reserves the right to audit the compliance of the PROCESSOR with the agreements reached in this Agreement, with prior written notice thirty (30) days in advance and, at most, once every twelve (12) months. The PROCESSOR undertakes to cooperate with the CONTROLLER and to provide reasonable assistance, as well as access to the necessary information.

To perform the audit, the CONTROLLER must submit a detailed audit plan proposal to the PROCESSOR at least two (2) weeks prior to the proposed audit date. The proposed audit plan should describe the proposed scope, duration and start date of the audit. The PROCESSOR shall review the proposed audit plan and convey to the CONTROLLER any concerns or questions (e.g. request for information that may compromise the safety or confidentiality of the PROCESSOR). The PROCESSOR will work in good faith with the CONTROLLER to agree the audit plan.

The audit shall be conducted during regular business hours at the relevant facility, subject to the agreed audit plan and in no case shall it unreasonably interfere with the normal operation of the PROCESSOR's business activities. The PROCESSOR may impose reasonable conditions to minimize disruption.

The CONTROLLER shall provide the PROCESSOR with all audit reports generated in connection with any audit conducted under this clause. The audit reports shall be treated as Confidential Information of the parties, and the PROCESSOR shall have the right to review and comment on the reports prior to their finalization.

Similarly, in the event of any action, request or inspection by a Data Protection Authority of the facilities of the CONTROLLER or of the PROCESSOR, as the case may be, in the exercise of its competences related to the services covered by this Agreement, the PROCESSOR in this act accepts and authorizes the carrying out of such visits and will allow access to the personal data owned by the CONTROLLER in its possession, subject to reasonable notice and applicable confidentiality obligations. The PROCESSOR will cooperate with the CONTROLLER and the Data Protection Authority as required by law and to an extent reasonably practicable. In the case of subcontracting, the actions, requirements or inspections may be carried out in the subcontracted entities, and the PROCESSOR will use reasonable efforts to take the necessary measures to this effect.

l. Once the provision of the services covered by the Main Contract has been completed, the PROCESSOR undertakes to destroy any information containing personal data transmitted by the CONTROLLER to the PROCESSOR in connection with the provision of the services, unless retention is required by law or for legitimate business purposes. Notwithstanding the foregoing, the PROCESSOR may retain backup copies of such data for a limited period, not exceeding ninety (90) days, solely for the purpose of defending against potential claims, after which such copies shall be securely deleted.

   Once destroyed, the PROCESSOR will issue a certificate of destruction to the CONTROLLER where the destroyed information, physical support, and documentation will be listed.

   Alternatively, and if the CONTROLLER so indicates, once the provision of the services covered by the Main Contract has been completed, the PROCESSOR undertakes to return any information containing personal data transmitted by the CONTROLLER to the PROCESSOR in connection with the provision of the services.

   The return must involve the total erasure of the existing data in the computer equipment used by the PROCESSOR.

   Notwithstanding the provisions of the preceding paragraphs, the PROCESSOR may keep the data and information processed in order to defend itself against possible legal claims or to make them available to Public Administrations, Judges and Courts, for the attention of possible responsibilities arising from the processing and only during the period of prescription of said responsibilities. Such retention shall not require strict blocking measures, provided that the data are not used for any other purpose and are subject to appropriate safeguards.

m. The PROCESSOR shall not resort to another processor ("sub-processor") to carry out part or all the processing of personal data covered by this Agreement without the prior written, specific or general authorization of the CONTROLLER.

Upon obtaining such authorization, the PROCESSOR shall inform the CONTROLLER of any envisaged changing, incorporation, or replacement of sub-processors, thereby giving the CONTROLLER the opportunity to oppose such changes. The PROCESSOR shall also indicate the processing activities to be subcontracted and shall clearly and unequivocally identify the subcontracted company and its contact details. The authorized sub-processors are detailed in APPENDIX II: SUB-PROCESSORS OF THE PROCESSING ACTIVITY.

In any event, the PROCESSOR undertakes to impose on the sub-processor, by contract or other legal act established under the law of the European Union or the Member States, data protection obligations that are substantially similar to those laid down in this Agreement, including the adoption of suitable safeguards and the implementation of appropriate technical and organizational measures so that processing complies with the provisions of the GDPR, to the extent applicable.

If the sub-processor fails to comply with its data protection obligations, the PROCESSOR shall be liable to the CONTROLLER only to the extent required by applicable law and this Agreement, and subject to any limitations of liability agreed between the parties.

j. In the event that the PROCESSOR has appointed a Data Protection Officer, the PROCESSOR shall complete APPENDIX IV: INFORMATION ON THE PROCESSOR'S DATA PROTECTION OFFICER, and shall inform the CONTROLLER in writing, within a reasonable period, of any changes.

FIFTH. - OBLIGATIONS OF THE CONTROLLER

The CONTROLLER, in its capacity as data controller, undertakes to:

a. Provide personal data to the PROCESSOR according to stablished in Clause 2 of this Agreement.

b. Carry out a data protection impact assessment of the processing operations to be carried out by the PROCESSOR.

c. Carry out the corresponding prior consultations.

d. Ensuring, prior to and throughout the processing, compliance with applicable legislation on the protection of personal data by the PROCESSOR.

e. Supervise the data processing, including inspections and audits.

f. Cooperate actively and provide the PROCESSOR with all reasonable information or assistance necessary to enable the PROCESSOR to comply with its legal and contractual obligations, particularly in relation to audits, data protection impact assessments, and incident management.

g. Provide the PROCESSOR with prior reasonable notice of any changes to the data, instructions, or services that may affect the processing, so that the PROCESSOR may adapt its technical and organizational measures accordingly.

h. Reimburse the PROCESSOR for reasonable costs incurred as a result of providing additional assistance, complying with new regulatory obligations, or implementing additional technical or organizational measures requested by the CONTROLLER.

i. Guarantee that all personal data provided to the PROCESSOR has been obtained and transferred in accordance with applicable law and hold the PROCESSOR harmless from any liability arising from non-compliance prior to the transfer of such data.

j. Acknowledge that any modification, adjustment, configuration change, or alteration made by either the CONTROLLER or the PROCESSOR to the management, configuration, or operation of the Platform (whether carried out directly by the party making the change or instructed to the other party) shall be performed entirely at the sole risk of the party initiating or requesting such modification. Accordingly, neither the CONTROLLER nor the PROCESSOR shall be liable to the other party for any impact, malfunction, security issue, degradation of performance, loss of data, or any other consequence arising from or related to such modifications.

SIXTH. - LIABILITY

The PROCESSOR's liability shall be limited exclusively to direct damage caused to the CONTROLLER because of such breach, expressly excluding any liability for indirect, consequential, special, punitive damages, or loss of profit, except in cases of willful misconduct or gross negligence.

Each party to this Agreement shall be fully responsible for the consequences arising from its own non compliance with the obligations set forth herein and shall, in such cases, compensate the other party for the damages caused by such non compliance.

The non-performing party shall indemnify the other party for all the damages caused to the latter by the breach of this Agreement and the regulations in force regarding the protection of personal data attributable to the aforementioned entity. By way of illustration, the non-performing party shall pay the other party:

a. the expenses incurred in the defense against possible sanctioning procedures initiated by the corresponding Data Protection Authority and its appeals before the competent Courts.

b. the amount of the sanction, if any, that could be imposed by the corresponding Data Protection Authority.

c. the expenses caused by their defense against possible legal actions that could be promoted by the data owners. Such expenses shall include, in any case, the fees of the lawyers involved in the defense.

d. The CONTROLLER assumes responsibility for the accuracy, integrity, and legality of the data provided to the PROCESSOR, and shall indemnify the PROCESSOR for any damage, losses, or claims arising from the provision of incorrect data or from instructions that are illegal or not in accordance with applicable law.

SEVENTH. – CHANGES AND ADJUSTMENTS

The undersigned parties undertake to revise this Agreement in the event of any regulatory changes that may occur in relation to the protection of personal data.

Any regulatory changes that materially affect the obligations of the PROCESSOR under this Agreement shall require the parties to make good faith efforts to maintain the essence of those obligations unchanged, using the mechanisms permitted under applicable principles of good faith. Regulatory changes that do not have a material impact on the PROCESSOR's obligations shall not trigger mandatory renegotiation of the Agreement. If, after good faith negotiations, the parties are unable to reach an agreement on the necessary modifications within (30) days, either party may terminate this Agreement without penalty by providing written notice to the other party.

EIGHTH. - SEVERABILITY CLAUSE

This Agreement contains and reflects all the covenants and agreements of the parties relating to its subject matter, superseding and annulling any other documents relating to the same subject matter that may have been signed or exchanged by the parties prior to this Agreement. In the event of any contradiction between the Main Agreement and this Agreement with respect to the protection of personal data, the provisions of this Agreement shall prevail.

The Appendices attached to this Agreement shall form an integral part of this Agreement for all legal purposes. Together, the Master Agreement, this Agreement and its Appendices shall constitute a single, unified contractual body.

NINTH. - MISCELLANEOUS

The personal data of the parties' representatives will be processed respectively by the entities identified in the heading, which will act independently as data controllers. Such data will be processed in compliance with the rights and obligations contained in this Agreement, without any automated decisions affecting the representatives. Consequently, the legal basis for the processing is to comply with the contractual relationship, such purpose being strictly necessary to execute this Agreement.

The data of the representatives of the parties will be maintained as long as the contractual relationship stipulated herein is in force, and will only be processed by the parties and those third parties to whom they are legally or contractually obliged to communicate them (as is the case of third party service providers who have been entrusted with any service related to the management or execution of the Main Contract).

The representatives of the parties may exercise, under the terms established by the legislation in force at any given time, the rights of access, rectification and deletion of data, as well as request that the processing of their personal data be limited, oppose the same, or request the portability of their data by sending a written communication to each of the parties, through the addresses specified in the heading. They may also file a complaint with the Spanish Data Protection Agency or another competent authority.

TENTH. - APPLICABLE LAW AND PLACE OF JURISDICTION

This Agreement shall be governed by the laws of the country where the PROCESSOR has its registered office, unless mandatory applicable law requires otherwise. Any dispute arising from this Agreement shall be submitted to the courts of the city where the PROCESSOR has its registered office.

And in proof of conformity, the parties sign this Agreement in duplicate, exemplary and to a single effect, at the place and date indicated in the heading.

CONTROLLER	PROCESSOR
	Firmado por: Sergio Soariano A1CA2A3AA03F48E... Sergio Soariano 07 de septiembre de 2026 | 12:42 PM CEST
Signed by the duly authorised representative of the CONTROLLER	Signed by the duly authorised representative of the PROCESSOR

Appendix I: Services processing details

This APPENDIX I forms an integral part of the DPA and sets out, for each Application: (i) the subject matter of the processing, (ii) the nature and purpose of the processing, (iii) the types of personal data, (iv) the categories of data subjects, and (v) the duration of the processing.

Common elements in all applications

1. Hosting environment

The Applications are provided in a Software-as-a-Service (SaaS) model and are hosted on Microsoft Azure cloud infrastructure. Access to production environments is restricted to authorized personnel on a need-to-know basis and subject to role-based access controls.

2. Nature of the processing

The processing may include: hosting; storage; access; retrieval; consultation; use; disclosure by transmission as initiated by the CONTROLLER and its authorized users; user and access administration; authentication; logging and audit trail generation; monitoring necessary for service operation and security; backup; restoration; troubleshooting; technical support; and deletion or return upon termination (as applicable).

3. Purpose(s) of the processing

To provide, operate, maintain, secure and support the Applications; manage authentication, authorizations, roles and user accounts; provide operational monitoring, dashboards and reporting (where applicable); prevent, detect and remediate security incidents, abuse and fraud; ensure business continuity (including backup and disaster recovery); and comply with applicable legal obligations to the extent required.

4. Types of personal data

Depending on the Application and the CONTROLLER's configuration, the processing may involve: user identity and professional details (e.g., name, corporate email, role, job title); account and authentication data (e.g., user IDs, access credentials or tokens, access logs); professional contact data (e.g., business phone number where enabled); and technical data (e.g., audit logs, timestamps, system logs generated by the Application).

5. Special Categories of Personal Data

The Applications are not intended for the processing of special categories of personal data as a standard feature. Where the CONTROLLER chooses to upload or otherwise make available such data, this occurs solely on the CONTROLLER's instructions and subject to the safeguards set out in this DPA.

6. Duration of the Processing

Personal data is processed for the duration of the Main Contract. User account data is retained for a maximum of twelve (12) months and, if the user does not access the Application during the following month, the corresponding Personal Data is deleted, unless a longer retention period is required by applicable law or permitted under the DPA (e.g., limited backup retention).

A. ItemOptix

1. Subject matter of the processing

Provision of "ItemOptix", a multi-tenant SaaS RFID platform enabling centralized management of operational optimization solutions, including Store Inventory Management (SIM), Supply Chain Management (SCM), EAS-Intelligence (EAS-Intel) and Asset Tracking (AT).

2. Categories of data subjects

Employees of the CONTROLLER who use ItemOptix as authorized users during their professional activities.

3. Types of personal data

User identity and professional details (including corporate email and professional profile data), and access and authentication identifiers (e.g., user IDs) provisioned via the CONTROLLER's corporate identity systems (e.g., SSO/ADFS) and/or by the CONTROLLER's designated administrators; plus, access logs and support-related technical records.

4. Processing environment

ItemOptix is hosted on Microsoft Azure. User identification and access data are centrally processed within the ItemOptix SaaS environment, with role-based access controls and need-to-know access for authorized personnel for authentication, user administration and technical support.

5. International data transfers

Support access may occur from the EU, UK, US and India, and Application-related transfers (if any) are governed by APPENDIX IV and the applicable safeguards described therein.

B. StoreOperations

1. Subject matter of the processing

Provision of "StoreOperations", a store operations platform integrating device monitoring, alarm management and multimedia services, including (i) Device Monitoring and Alarm Management, (ii) StoreOps Mobile (alarm handling via mobile devices), and (iii) Media Service for capturing, storing and viewing videos or photos associated with ORC-related operational events.

2. Categories of data subjects

Authorized users of the CONTROLLER's organization and authorized internal users of the PROCESSOR's group who access StoreOperations for operational monitoring and support.

3. Types of personal data

User identity and professional contact details (name, surname, corporate email and, depending on configuration, additional professional contact details); access or authentication data; and operational usage logs. Where Media Service is used, media content may contain personal data to the extent uploaded or captured as directed or configured by the CONTROLLER.

4. Processing environment

StoreOperations is hosted by Microsoft Azure. Centralized processing of user identification and access data occurs within the StoreOperations environment, with role-based access controls and need-to-know access for authentication, operational monitoring, reporting and support.

5. International data transfers

Support access may occur from the EU, UK and US. Any international transfers (if applicable) are governed by APPENDIX IV and the applicable safeguards described therein.

C. CheckNet

1. Subject matter of the processing

Provision of "CheckNet", a cloud solution for order management and automation, including creation of orders, automated printing, and RFID label printing or encoding; and operational workflows with suppliers and retailers.

2. Categories of data subjects

Employees of the PROCESSOR's group and authorized personnel of the CONTROLLER, administrators, and professional contacts at suppliers and retailers using CheckNet during their professional activities.

3. Types of personal data

Professional identity and contact data (e.g., name, professional email, organization, country), user roles or permissions, professional contact addresses, and activity and audit records generated by the platform in connection with orders and operational workflows.

4. Processing environment

CheckNet is hosted by Microsoft Azure. Processing is centralized for user or access management, order handling, RFID printing or encoding workflows and related audit and configuration records,

with controlled visibility and role-based access for authorized operations and customer support

5. International data transfers

Support access may occur from multiple jurisdictions (including EU, UK, US, India, Mexico, Morocco, Sri Lanka, Turkey and Vietnam). Any international transfers (if applicable) are governed by APPENDIX IV and the applicable safeguards described therein.

D. CheckLINQ

1. Subject matter of the processing

Provision of "CheckLINQ", a cloud platform enabling generation and hosting of clean QR codes linked to public web pages per product line, supporting product lifecycle traceability, sustainability and compliance information management, and consumer access to product-related information.

2. Categories of data subjects

Employees of the PROCESSOR's group and authorized personnel of retailers who use CheckLINQ during their professional activities.

3. Types of personal data

Professional identity and contact data (name, job title, professional email and corporate phone where enabled), access credentials, and platform usage and log data generated through use of the service.

4. Processing environment

CheckLINQ is hosted by Microsoft Azure. Identification data, credentials and activity logs are processed within the CheckLINQ environment, with role-based access controls and need-to-know access for authentication, service provision, support and related operational activities.

5. International data transfers

Support access may occur from the EU and UK. Any international transfers (if applicable) are governed by APPENDIX IV and the applicable safeguards described therein.

E. CheckProof

1. Subject matter of the processing

Provision of "CheckProof", a central repository for managing customer label design or artwork, enabling review, correction and approval workflows, with integrations into related internal platforms.

2. Categories of data subjects

Employees of the PROCESSOR's group and authorized retailer users who access CheckProof during their professional activities.

3. Types of personal data

Professional identity and contact data (e.g., name, job title and professional email), plus access logs and activity records associated with review or approval workflows.

4. Processing environment

CheckProof is hosted on Microsoft Azure. Processing occurs within the CheckProof environment and integrated workflows, with limited access by authorized personnel strictly on a need-to-know basis for support and maintenance, and with role-based access controls.

5. International data transfers

Access may occur from authorized internal personnel located in the EU and UK. Any international transfers (if applicable) are governed by APPENDIX IV and the applicable safeguards described therein.

Appendix II: Technical and organisational measures

The PROCESSOR shall implement technical and organizational security measures that are appropriate to the risks and context of the processing, and which provide a level of security equivalent to the measures detailed in this APPENDIX. The PROCESSOR is not required to comply literally with each specific measure, provided that the implemented measures achieve an equivalent level of protection for personal data.

In accordance with the provisions of Clause 5 of this Agreement ("Clauses"), the PROCESSOR shall adopt all necessary security measures to guarantee the full security of the personal data being processed, considering the business model, the purposes for which they will be used and the type of data. All this, in accordance with the instructions given by the CONTROLLER, as well as based on the result of the risk analysis carried out, and where appropriate, the corresponding impact assessment.

A. The PROCESSOR shall apply, as a minimum and regardless of the type of data being processed, the following security measures:

1. Organization of information security:
    a. Management should actively support security initiatives by demonstrating its support for and commitment to information security within the Organization.
    b. Have a clear definition of all information security responsibilities.
    c. Definition and establishment of an authorization management process for new information processing resources.
    d. Process of identifying risks in information processing involving the participation of third parties, with prior implementation of controls before granting access.
    e. Third party agreements involving access, processing, communication or management of the organization's information or information processing facilities should cover all relevant security requirements.
    f. A clean desk policy must be in place to ensure the confidentiality of information when it is not being used for the purpose for which it was collected.
    g. Have a code of conduct for the use of information systems by users.
    h. Guarantee that an information security management model based on some recognized standard (e.g. ISO27001, NIST Cybersecurity Framework, etc...) is complied with.

2. Asset management:
    a. All assets should be clearly identified in an inventory that should be updated regularly.
    b. The information should be classified in relation to its value, criticality, legal requirements and sensitivity to the organization.

3. Security linked to human resources:
    a. There shall be a formal user registration and termination procedure in order to guarantee and cancel access to all information systems and services.
    b. Security roles and responsibilities for employees, contractors and third parties should be defined and documented in accordance with the organization's information security policy.
    c. As part of their contractual obligation, employees, contractors and third parties must accept and sign the terms and conditions of the employment contract, in which their obligations and those of the organization for information security must be established.
    d. All employees, contractors and third parties should receive some form of training to provide appropriate knowledge to ensure compliance with the information security policy in their position.
    e. In the event of termination, there must be a formal procedure, with clearly defined and assigned responsibilities, for employees, contractors and third-party users to return the organization's assets in their possession, and for access rights to both systems and information processing facilities to be withdrawn.

4. Physical and environmental security:
    a. The areas where the information processing equipment is located must be physically separated from other working environments.
    b. These areas must have adequate controls to ensure access to authorized personnel only.
    c. Such areas must have physical protection measures, at least against fire, flood and civil unrest, among other forms of natural or human disaster.
    d. The equipment shall be protected against power supply failures or other electrical anomalies in the support equipment.
    e. Equipment should be properly maintained to ensure its continued availability and integrity.

5. Operational controls
    a. Changes in information processing systems and resources should be controlled, with a prior testing plan and authorization process for the execution of such changes.

b. Procedures must be in place to ensure segregation of duties and areas of responsibility to reduce the likelihood of unintentional or unauthorized modifications.

c. Detection, prevention and recovery controls against malicious software must be implemented.

d. All essential business information must be backed up to guarantee the agreed SLA.

e. Technical measures must be implemented at network level to guarantee an adequate level of protection in systems and applications both at the perimeter level and between segments of the network itself.

f. There will be measures to request access to the network, the consequent approval, registration of activity and subsequent revision of the traces, with a system that guarantees the appropriate security measures to control the network access points.

g. There must be a procedure for the management of removable computer resources.

h. Measures must be in place for the confidential destruction of computer storage media (internal or external) as well as the information they contain when they cease to be part of the service.

i. It will be necessary to apply security policies to those mobile devices that may potentially have access to the information.

j. In the case of providing services managed through a web application, a tool for the prevention of specific attacks on web applications must be available.

k. It will be necessary to have a system that helps prevent and control the exfiltration of information from the systems.

l. Encryption of information with confidentiality requirements must be guaranteed at rest, in transit and in use.

m. The encryption of the information must be guaranteed in all the supports used for the provision of the service (desktop computers, laptops, etc...).

n. A system must be in place to monitor and record all activity carried out by users, as well as all exceptions and security events in the corporate network in order to provide forensic analysis and access control services.

o. Define a procedure for the assignment and use of privileges within information systems.

p. Define a procedure to control the assignment of passwords and ensure that they comply with regulatory requirements of complexity (minimum length of 8 characters, composed of alphanumeric and symbols and with a maximum expiration date of 90 days, with temporary blocking of this in case of repeated attempt of failed access).

q. The synchronization of all the clocks of the information processing systems within the organization or the security domain must be guaranteed, with an agreed source (preferably the clock of the Spanish Navy) and exact in time.

r. Have a procedure for periodically updating systems to eliminate known vulnerabilities of the systems, patching the criticisms in a maximum period of 48 hours.

s. Have a procedure for the management of technical vulnerabilities, or a periodic audit service to detect deficiencies in the configurations of information and protection systems. The results of these audits may be required by the information security team of the CONTROLLER.

6. Information security governance:

   a. The identification and subsequent management of the technological risk to which the company is exposed will be carried out, determining the impact that the materialization of the threats would have, with at least an annual review.

   b. There must be a procedure for responding to updated incidents that includes notification of information leakage to the CONTROLLER in the event of regulatory non-compliance or in situations in which the confidentiality of the information has been compromised.

7. Operational controls

   a. To have a continuity plan at least for those activities that are fundamental for the provision of services to the CONTROLLER.

   b. The business continuity plan must be regularly updated and tested.

   c. Have a disaster recovery plan for the information systems and have it updated and tested annually.

B. In addition, the PROCESSOR shall adopt any other technical and organizational measures necessary to guarantee a level of security adequate to the risk, considering the state of the art, application costs and the nature, scope, context and purposes of the processing, in accordance with the data protection regulations applicable always.

Appendix III: Sub-processors

The current list of authorized Sub-processors, including corporate name, location, activities, and country of processing where applicable, is available through the Provider's privacy page, customer portal, or equivalent legal notices page and is incorporated by reference into this DPA. Changes to Sub-processors are governed by Clause FOURTH m).

Appendix IV: International data transfers

The current transfer information, including relevant countries and safeguards such as adequacy decisions or EU Standard Contractual Clauses where applicable, is available through the Provider's privacy page, customer portal, or equivalent legal notices page and is incorporated by reference into this DPA. If EU Standard Contractual Clauses are used, the relevant module and annex information may be made available through those resources.

Appendix V: Information on the oricessor's data protection officer

Where the PROCESSOR has appointed a Data Protection Officer, the relevant details will be made available through the Provider's Privacy Policy, customer portal, or equivalent legal notices page. If no Data Protection Officer has been appointed, the PROCESSOR's data protection contact point identified in the Information Section shall apply.