Data Processing Agreement (DPA)

Article 28 of Regulation (EU) 2016/679 (GDPR)

Service: Plate & Punch — SaaS management platform for the food and beverage sector

> **NOTICE:** This is a template compliant with Article 28 of the GDPR. Before use in production, review by a qualified legal professional is recommended, in particular of the liability, term and jurisdiction clauses. Fields in square brackets [ ] must be completed with each customer's details.

Parties

DATA CONTROLLER ("the Customer")

Name / Legal entity	[CUSTOMER NAME OR LEGAL ENTITY]
Tax ID (NIF/CIF/VAT)	[TAX ID]
Address	[ADDRESS]
Email	[EMAIL]

DATA PROCESSOR ("the Provider")

Name	PCL
Tax ID (NIF)	46688225L
Address	BARCELONA, -Catalonia- Spain
Data protection email	legal@plateandpunch.rest

Recitals

The Provider supplies the Customer with the Plate & Punch SaaS service (the "Service"). In providing the Service, the Provider processes personal data on behalf of the Customer. This DPA governs such processing in accordance with Article 28 of the GDPR and is incorporated into the Terms of Service. By accepting the Terms of Service or using the Service, the Customer agrees to this DPA.

SPECIMEN

1. Subject matter and duration

1.1. The Provider shall process personal data solely to provide the Service, in accordance with the Customer's documented instructions.

1.2. The duration of the processing coincides with the term of the Service relationship. Upon its end, clause 10 applies.

1.3. The nature, purpose, types of personal data and categories of data subjects are set out in **Annex I**.

2. Customer instructions

2.1. The Provider shall process personal data only on the Customer's documented instructions, including those contained in this DPA, the Terms of Service and the configuration features of the Service itself.

2.2. The Provider shall inform the Customer without delay if, in its opinion, an instruction infringes the GDPR or other applicable data protection law.

2.3. If the Provider is required by law to process data beyond the instructions, it shall inform the Customer before processing, unless the law prohibits this on important grounds of public interest.

3. Confidentiality

3.1. The Provider ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4. Security measures (Article 32)

4.1. The Provider implements appropriate technical and organisational measures proportionate to the risk, including:

- Encryption of communications (TLS/HTTPS).
- Passwords protected with Argon2.
- Role-based access control with granular per-module permissions.
- Multi-tenant isolation of each customer's data.
- Daily encrypted backups (GPG), hosted with a provider bound by a data processing agreement.
- Production environment on a dedicated server in the EU, with a firewall.

4.2. The Provider undertakes to maintain and, where appropriate, update these measures to ensure a level of security appropriate to the risk.

SPECIMEN
SPECIMEN
SPECIMEN

5. Sub-processors

5.1. The Customer grants the Provider a general authorisation to engage the sub-processors listed in **Annex II** to provide the Service.

5.2. The Provider shall inform the Customer of any intended addition or replacement of sub-processors with reasonable prior notice, and the Customer may object on reasonable data-protection grounds.

5.3. The Provider enters into a written agreement with each sub-processor imposing data protection obligations equivalent to those in this DPA, and remains liable to the Customer for the performance of those obligations.

6. International data transfers

6.1. The bulk of the processing takes place in the European Union / EEA. Where a sub-processor is located outside the EEA (e.g. in the USA), the transfer is governed by **Standard Contractual Clauses (SCCs)** approved by the European Commission and, where applicable, additional safeguards, as indicated in Annex II.

7. Assistance to the Customer

7.1. Taking into account the nature of the processing, the Provider assists the Customer, through appropriate technical and organisational measures, to respond to requests by data subjects exercising their rights (access, rectification, erasure, restriction, portability and objection).

7.2. If the Provider receives a request directly from a data subject, it shall advise the data subject to contact the Customer and shall inform the Customer without delay.

8. Assistance with security, breaches and assessments

8.1. The Provider assists the Customer in complying with its obligations under Articles 32 to 36 of the GDPR, taking into account the information available: security, breach notification, data protection impact assessments (DPIA) and prior consultation with the supervisory authority.

9. Personal data breach notification

9.1. The Provider notifies the Customer without undue delay after becoming aware of any personal data breach, providing the information necessary for the Customer to comply with its notification obligations to the supervisory authority and, where applicable, to the data subjects.

10. Deletion or return of data

10.1. Upon termination of the Service, at the Customer’s choice, the Provider deletes or returns the personal data and existing copies, unless retention is required by law.

SPECIMEN
SPECIMEN
SPECIMEN

10.2. The Service implements deletion of the account and its content with a 30-day grace period, retaining only the legally required minimum (e.g. invoicing).

11. Audits and demonstration of compliance

11.1. The Provider makes available to the Customer the information necessary to demonstrate compliance with the obligations under this DPA, and allows for and contributes to audits, including inspections, conducted by the Customer or an auditor appointed by it, with reasonable prior notice and without disproportionately disrupting the Provider's activity.

12. Liability

12.1. Each party is liable for the damage it causes by breaching its obligations under the GDPR and this DPA, in accordance with Article 82 of the GDPR and the Terms of Service.

13. Governing law and jurisdiction

13.1. This DPA is governed by Spanish law and the GDPR. Any dispute shall be submitted to the courts having jurisdiction under applicable law. *(Clause to be validated by legal counsel.)*

Annex I — Details of the processing

Field	Content
Subject matter	Provision of the Plate & Punch SaaS management service.
Nature and purpose	Hosting and processing of the Customer's internal operational data within the application (management of staff and suppliers).
Types of data	Customer's staff: name, email, role within the application (administrator / staff). Suppliers: company details and name of the contact person.
Special categories (Art. 9)	None.
Categories of data subjects	Staff authorised by the Customer; supplier contact persons.

SPECIMEN
SPECIMEN
SPECIMEN

Field	Content
Duration	The term of the Service relationship.

Annex II — List of sub-processors

Sub-processor	Purpose	Location	Transfer safeguard
Hetzner Online GmbH	Hosting (server and database)	Germany (EU)	Processing within the EU
Google Ireland Ltd. (Workspace)	Encrypted backups	EU / EEA	Processing within the EU/EEA
Resend (Plus Five Five, Inc.)	Transactional email delivery	USA	EU SCCs + EU-U.S. Data Privacy Framework
OpenAI Ireland Ltd.	AI features using Customer data *(only if enabled)*	Ireland (EU) / USA	EU SCCs
Stripe	Payment gateway *(when enabled)*	USA	EU SCCs

This list may be updated. Changes will be communicated in accordance with clause 5.2.

Acceptance

This DPA is deemed accepted by the Customer upon acceptance of the Terms of Service or use of the Service. Effective date: the date of acceptance.

The Customer (Controller)	The Provider (Processor)
[Name and signature]	PCL
Date: [DATE]	Date: [DATE]

SPECIMEN
SPECIMEN
SPECIMEN