

BORRADOR — PENDIENTE DE REVISIÓN LEGAL

Documento de trabajo generado desde docs/legal/dpa-art28.md. No es asesoramiento legal ni un acuerdo ejecutado. Los campos [...] deben completarse por un abogado antes de su uso.

Data Processing Agreement (GDPR Article 28)

DRAFT — REQUIRES LEGAL REVIEW

*This document is a working draft prepared for the operator's lawyer to review, adapt, and execute. It is **not** legal advice and is **not** an executed agreement. Every field marked [...] (e.g. [RAZÓN SOCIAL], [NIF], [DOMICILIO], [REGISTRO MERCANTIL]) and every [VERIFY] flag **MUST** be completed/confirmed by qualified counsel before use.*

Canonical company-identity source of truth:

*apps/web/src/app/core/legal/company-legal.ts — fix the [PENDIENTE] placeholders **there** first, then mirror the confirmed values into this DPA.*

Version: 0.1-draft · Drafted: 2026-06-23

How to read this document

This DPA is provided **bilingual**: the authoritative working language should be agreed by the parties. The Spanish version comes first, followed by the English version. In case of discrepancy, the parties must designate one prevailing language clause (see §13 / §13 EN — [VERIFY: prevailing language]).

Role mapping:

- **Encargado del tratamiento / Processor** = Boty ([RAZÓN SOCIAL]), the SaaS provider operating the Boty Agency platform (Leads, Social, Mail and related verticals).
- **Responsable del tratamiento / Controller** = the operator (customer / tenant) that subscribes to the platform and determines the purposes and means of processing their end-users' personal data.

■■ VERSIÓN EN ESPAÑOL

Acuerdo de Encargo del Tratamiento (Art. 28 RGPD)

Entre:

- **El Responsable del Tratamiento** (en adelante, el «Responsable»): la persona física o jurídica titular de la cuenta de operador que contrata la plataforma Boty, cuyos datos identificativos constan en el formulario de contratación o en la cuenta de operador.
- **El Encargado del Tratamiento** (en adelante, el «Encargado»):
- Razón social: [RAZÓN SOCIAL] (actualmente registrado en código como Boty Social SL — [VERIFY] denominación registral exacta)
- NIF/CIF: [NIF]
- Domicilio: [DOMICILIO], Madrid, España
- Datos registrales: [REGISTRO MERCANTIL] (tomo, folio, hoja, sección)
- Correo de contacto en materia de protección de datos:
privacy@boty.agency

Ambas partes reconocen que el presente Acuerdo regula el tratamiento de datos personales que el Encargado realiza por cuenta del Responsable en el marco de la prestación de los servicios de la plataforma Boty (en adelante, los «Servicios»), de conformidad con el artículo 28 del Reglamento (UE) 2016/679 («RGPD») y la Ley Orgánica 3/2018 (LOPDGDD).

1. Objeto y duración

1.1. **Objeto.** El Encargado tratará por cuenta del Responsable los datos personales necesarios para prestar los Servicios contratados (gestión de leads y conversaciones, programación y publicación social, envíos de email marketing, analítica de la cuenta y funcionalidades asociadas).

1.2. **Duración.** El presente Acuerdo estará vigente mientras lo esté el contrato principal de prestación de Servicios. Finalizada la relación, se estará a lo dispuesto en la cláusula 9 (devolución/supresión).

2. Naturaleza y finalidad del tratamiento

2.1. **Naturaleza.** Operaciones de recogida, registro, estructuración, conservación, consulta, comunicación por transmisión, cotejo, supresión y destrucción de datos personales, realizadas de forma total o parcialmente automatizada mediante la plataforma.

2.2. **Finalidad.** Exclusivamente la prestación de los Servicios contratados

por el Responsable. El Encargado no tratará los datos para finalidades propias ni distintas de las instruidas por el Responsable.

3. Categorías de interesados y de datos personales

3.1. Categorías de interesados (según el vertical contratado):

- Contactos y leads del Responsable (potenciales clientes que interactúan por los canales conectados).
- Destinatarios de campañas de email marketing del Responsable.
- Seguidores/audiencia de los perfiles sociales gestionados por el Responsable.
- Usuarios y miembros del equipo del Responsable con acceso a la cuenta.

3.2. Categorías de datos personales:

- Datos identificativos y de contacto (nombre, email, teléfono, identificadores de mensajería/redes sociales).
- Contenido de las comunicaciones (mensajes, conversaciones, notas).
- Datos de consentimiento y preferencias (suscripción, RGPD, bajas).
- Metadatos de uso y actividad asociados a los interesados.
- [VERIFY] El Responsable es responsable de **no** introducir categorías especiales de datos (art. 9 RGPD) salvo pacto expreso y medidas adicionales.

4. Obligaciones del Encargado

El Encargado se obliga a:

- a) Tratar los datos personales **únicamente** conforme a las instrucciones documentadas del Responsable, incluidas las relativas a transferencias internacionales, salvo obligación legal (en cuyo caso lo informará previamente, salvo prohibición legal).
- b) Garantizar que las personas autorizadas para tratar los datos se hayan comprometido a respetar la confidencialidad o estén sujetas a un deber de confidencialidad de naturaleza estatutaria.
- c) Adoptar las medidas técnicas y organizativas apropiadas (cláusula 6).
- d) Respetar las condiciones de subcontratación (cláusula 5).
- e) Asistir al Responsable para responder a las solicitudes de ejercicio de derechos (cláusula 7).
- f) Asistir al Responsable en el cumplimiento de las obligaciones de los

artículos 32 a 36 RGPD (seguridad, notificación de brechas, evaluaciones de impacto y consultas previas).

g) A elección del Responsable, suprimir o devolver los datos al finalizar la prestación (cláusula 9).

h) Poner a disposición del Responsable la información necesaria para demostrar el cumplimiento y permitir auditorías (cláusula 10).

i) Informar inmediatamente al Responsable si, en su opinión, una instrucción infringe el RGPD u otras normas de protección de datos.

5. Subcontratación (subencargados)

5.1. El Responsable **autoriza de forma general** al Encargado a recurrir a los subencargados necesarios para prestar los Servicios. El listado actualizado y versionado de subencargados se mantiene en el registro de subencargados: [docs/legal/subprocessors.md](./subprocessors.md).

5.2. El Encargado informará al Responsable de cualquier **alta o sustitución** de subencargados con una antelación razonable ([VERIFY] plazo recomendado: 30 días), dando al Responsable la posibilidad de oponerse por motivos justificados.

5.3. El Encargado impondrá a cada subencargado, mediante contrato, las mismas obligaciones de protección de datos que las estipuladas en este Acuerdo. El Encargado seguirá siendo plenamente responsable frente al Responsable del cumplimiento por parte del subencargado.

6. Medidas de seguridad (art. 32 RGPD)

El Encargado aplica, como mínimo, las siguientes medidas técnicas y organizativas ([VERIFY] contra la configuración real de producción):

- **Cifrado en tránsito (TLS)** de todas las comunicaciones con la plataforma.
- **Aislamiento multi-tenant mediante Row-Level Security (RLS)** de PostgreSQL, garantizando que cada operador solo accede a sus propios datos.
- **Hashing de contraseñas** con función de derivación de clave robusta (PBKDF2). [VERIFY] La política de privacidad pública menciona bcrypt; unificar la referencia con la implementación real antes de firmar.
- **Firma HMAC** de webhooks y eventos salientes para garantizar integridad y autenticidad.
- **Limitación de tasa (rate limiting)** sobre endpoints sensibles para mitigar abusos y ataques de fuerza bruta.

- **Sesiones mediante cookies técnicas HTTP-only** de corta duración con token de renovación.
- Control de acceso por roles y por vertical; registro de actividad; segregación de entornos. [VERIFY] ampliar según auditoría interna.

7. Asistencia en el ejercicio de derechos

7.1. El Encargado asistirá al Responsable, mediante las funcionalidades de la plataforma (exportación y supresión de datos) y, cuando proceda, mediante soporte, para atender las solicitudes de acceso, rectificación, supresión, oposición, portabilidad y limitación de los interesados.

7.2. Si un interesado dirige una solicitud directamente al Encargado, este la remitirá al Responsable sin dilación indebida.

8. Notificación de violaciones de seguridad (brechas)

8.1. El Encargado notificará al Responsable **sin dilación indebida** y, en la medida de lo posible, **dentro de las 72 horas** desde que tenga conocimiento de una violación de la seguridad de los datos personales, proporcionando al menos: naturaleza de la brecha, categorías y número aproximado de interesados y de registros afectados, consecuencias probables y medidas adoptadas o propuestas.

8.2. El canal de notificación de incidentes es `security@boty.agency`.

9. Devolución o supresión al finalizar

A elección del Responsable, una vez finalizada la prestación de los Servicios el Encargado **devolverá** o **suprimirá** todos los datos personales y eliminará las copias existentes, salvo que la normativa exija su conservación ([VERIFY] plazos de gracia y formato de exportación; alineado con la conservación fiscal de hasta 5 años indicada en la política de privacidad).

10. Auditoría

10.1. El Encargado pondrá a disposición del Responsable la información razonable necesaria para demostrar el cumplimiento del art. 28 RGPD.

10.2. El Responsable podrá realizar auditorías, incluidas inspecciones, directamente o a través de un auditor designado, con preaviso razonable ([VERIFY] plazo y periodicidad), respetando la confidencialidad y la seguridad del resto de clientes de la plataforma multi-tenant.

11. Transferencias internacionales

11.1. Parte de la infraestructura y de los subencargados se encuentran fuera del Espacio Económico Europeo (principalmente EE. UU.). Dichas transferencias se amparan en las **Cláusulas Contractuales Tipo (CCT)** adoptadas por la Comisión Europea y, en su caso, en medidas complementarias y en los acuerdos de tratamiento de datos de cada subencargado.

11.2. El detalle por subencargado (región y base de transferencia) consta en [docs/legal/subprocessors.md](./subprocessors.md).

12. Responsabilidad

La responsabilidad de las partes se regirá por lo dispuesto en el contrato principal y por la normativa aplicable. [VERIFY] límites de responsabilidad e indemnización.

13. Ley aplicable y jurisdicción

El presente Acuerdo se rige por la legislación española y el Derecho de la Unión Europea. [VERIFY: fuero/jurisdicción] y [VERIFY: idioma prevalente en caso de discrepancia].

■■ ENGLISH VERSION

Data Processing Agreement (Art. 28 GDPR)

Between:

- **The Controller** (hereinafter, the "Controller"): the natural or legal person holding the operator account that subscribes to the Boty platform, whose identifying details appear in the subscription form or operator account.
- **The Processor** (hereinafter, the "Processor"):
 - Legal name: [RAZÓN SOCIAL] (currently registered in code as Boty Social SL — [VERIFY] exact registered name)
 - Tax ID (NIF/CIF): [NIF]
 - Registered address: [DOMICILIO], Madrid, Spain
 - Commercial registry details: [REGISTRO MERCANTIL] (volume, folio, sheet, section)
 - Data-protection contact email: privacy@boty.agency

Both parties acknowledge that this Agreement governs the processing of personal

data carried out by the Processor on behalf of the Controller in the context of providing the Boty platform services (hereinafter, the "Services"), pursuant to Article 28 of Regulation (EU) 2016/679 ("GDPR") and Spanish Organic Law 3/2018 (LOPDGDD).

1. Subject-matter and duration

1.1. Subject-matter. The Processor will process, on behalf of the Controller, the personal data necessary to provide the contracted Services (lead and conversation management, social scheduling and publishing, email-marketing sends, account analytics and related functionality).

1.2. Duration. This Agreement remains in force for as long as the main Services contract is in force. Upon termination, clause 9 (return/deletion) applies.

2. Nature and purpose of processing

2.1. Nature. Collection, recording, structuring, storage, consultation, disclosure by transmission, matching, erasure and destruction of personal data, carried out wholly or partly by automated means through the platform.

2.2. Purpose. Solely the provision of the Services contracted by the Controller. The Processor will not process the data for its own purposes or for any purpose other than those instructed by the Controller.

3. Categories of data subjects and personal data

3.1. Categories of data subjects (depending on the contracted vertical):

- The Controller's contacts and leads (prospects who interact via the connected channels).
- Recipients of the Controller's email-marketing campaigns.
- Followers/audience of the social profiles managed by the Controller.
- The Controller's users and team members with account access.

3.2. Categories of personal data:

- Identifying and contact data (name, email, phone, messaging/social media identifiers).
- Communication content (messages, conversations, notes).
- Consent and preference data (subscription, GDPR, opt-outs).
- Usage and activity metadata associated with the data subjects.

- [VERIFY] The Controller is responsible for **not** entering special categories of data (Art. 9 GDPR) unless expressly agreed with additional measures.

4. Processor obligations

The Processor undertakes to:

- a) Process personal data **only** on documented instructions from the Controller, including with regard to international transfers, unless required by law (in which case it will inform the Controller beforehand, unless legally prohibited).
- b) Ensure that persons authorized to process the data have committed to confidentiality or are under a statutory obligation of confidentiality.
- c) Implement appropriate technical and organizational measures (clause 6).
- d) Respect the sub-processing conditions (clause 5).
- e) Assist the Controller in responding to data-subject-rights requests (clause 7).
- f) Assist the Controller in complying with the obligations under Articles 32 to 36 GDPR (security, breach notification, impact assessments and prior consultations).
- g) At the Controller's choice, delete or return the data upon termination of the Services (clause 9).
- h) Make available to the Controller the information necessary to demonstrate compliance and allow audits (clause 10).
- i) Immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other data-protection rules.

5. Sub-processing

5.1. The Controller grants a **general written authorization** for the Processor to engage the sub-processors necessary to provide the Services. The up-to-date, versioned list of sub-processors is maintained in the sub-processor register: [docs/legal/subprocessors.md](./subprocessors.md).

5.2. The Processor will inform the Controller of any **addition or replacement** of sub-processors with reasonable prior notice ([VERIFY] recommended period:

30 days), giving the Controller the opportunity to object on justified grounds.

5.3. The Processor will impose on each sub-processor, by contract, the same data-protection obligations as those set out in this Agreement. The Processor remains fully liable to the Controller for the sub-processor's performance.

6. Security measures (Art. 32 GDPR)

The Processor implements at least the following technical and organizational measures ([VERIFY] against the actual production configuration):

- **Encryption in transit (TLS)** for all communications with the platform.
- **Multi-tenant isolation via PostgreSQL Row-Level Security (RLS)**, ensuring each operator can access only its own data.
- **Password hashing** using a strong key-derivation function (PBKDF2).
[VERIFY] The public privacy policy mentions bcrypt; reconcile the reference with the actual implementation before signing.
- **HMAC signing** of webhooks and outbound events to ensure integrity and authenticity.
- **Rate limiting** on sensitive endpoints to mitigate abuse and brute-force attacks.
- **HTTP-only technical session cookies** of short duration with a renewal token.
- Role-based and per-vertical access control; activity logging; environment segregation. [VERIFY] expand per internal audit.

7. Assistance with data-subject rights

7.1. The Processor will assist the Controller, through the platform's functionality (data export and deletion) and, where appropriate, through support, in handling data-subject requests for access, rectification, erasure, objection, portability and restriction.

7.2. If a data subject addresses a request directly to the Processor, the Processor will forward it to the Controller without undue delay.

8. Personal data breach notification

8.1. The Processor will notify the Controller **without undue delay** and, where feasible, **within 72 hours** of becoming aware of a personal data breach, providing at least: the nature of the breach, the categories and approximate number of data subjects and records affected, the likely consequences, and the

measures taken or proposed.

8.2. The incident-notification channel is `security@boty.agency`.

9. Return or deletion on termination

At the Controller's choice, upon termination of the Services the Processor will **return** or **delete** all personal data and delete existing copies, unless storage is required by law ([VERIFY] grace periods and export format; aligned with the up-to-5-year tax retention stated in the privacy policy).

10. Audit

10.1. The Processor will make available to the Controller the reasonable information necessary to demonstrate compliance with Art. 28 GDPR.

10.2. The Controller may conduct audits, including inspections, directly or through a mandated auditor, with reasonable prior notice ([VERIFY] notice period and frequency), respecting the confidentiality and security of the other customers of the multi-tenant platform.

11. International transfers

11.1. Part of the infrastructure and sub-processors are located outside the European Economic Area (mainly the USA). Such transfers are covered by the **Standard Contractual Clauses (SCCs)** adopted by the European Commission and, where applicable, by supplementary measures and by each sub-processor's data processing agreement.

11.2. The per-sub-processor detail (region and transfer basis) is set out in `[docs/legal/subprocessors.md](./subprocessors.md)`.

12. Liability

The parties' liability is governed by the main contract and by applicable law. [VERIFY] liability caps and indemnification.

13. Governing law and jurisdiction

This Agreement is governed by Spanish law and the law of the European Union. [VERIFY: forum/jurisdiction] and [VERIFY: prevailing language in case of discrepancy].

Operator checklist before execution

- ☐ Fill [RAZÓN SOCIAL] / legal name (confirm vs Boty Social SL).
- ☐ Fill [NIF].
- ☐ Fill [DOMICILIO].
- ☐ Fill [REGISTRO MERCANTIL].
- ☐ Resolve PBKDF2 vs bcrypt discrepancy (code vs privacy policy).
- ☐ Confirm sub-processor change-notice period (§5.2).
- ☐ Confirm audit notice/frequency (§10.2).
- ☐ Confirm prevailing language and jurisdiction (§13).
- ☐ Have qualified counsel review the full document.