CONTRATO DE ENCARGO DE TRATAMIENTO

(Data Processing Agreement — DPA)

Conforme al artículo 28 del Reglamento (UE) 2016/679 (RGPD)

Versión 1.0 — Marzo 2026

1. Partes

ENCARGADO DEL TRATAMIENTO: Impulso Inteligente SL, con CIF [COMPLETAR_CIF], domicilio social en [COMPLETAR_DOMICILIO], El Tiemblo, Ávila, España. Correo electrónico: privacidad@verilabo.com. En adelante, "el Encargado" o "Verilabo".

RESPONSABLE DEL TRATAMIENTO: La persona física o jurídica que contrata los servicios de Verilabo y acepta los presentes Términos de Servicio. En adelante, "el Responsable" o "el Cliente".

El presente contrato forma parte integrante de los Términos y Condiciones de Uso de la plataforma Verilabo (verilabo.com) y se perfecciona con la aceptación de los mismos al registrarse en el servicio.

2. Objeto del Tratamiento

El presente contrato tiene por objeto regular las condiciones bajo las cuales Verilabo, como Encargado del Tratamiento, tratará datos personales por cuenta del Responsable del Tratamiento, en el marco de la prestación de los siguientes servicios:

a) Registro horario digital de empleados conforme al RD-ley 8/2019 y la reforma laboral 2025.

b) Canal de denuncias anónimo conforme a la Ley 2/2023, de 20 de febrero.

c) Registro retributivo con cálculo de brecha salarial conforme al RD 902/2020.

d) Inspector View: portal de acceso certificado para la Inspección de Trabajo.

3. Duración

El presente contrato de encargo de tratamiento tendrá la misma duración que la relación contractual de prestación de servicios entre el Encargado y el Responsable. A la finalización de la relación, se aplicará lo dispuesto en la cláusula 10 del presente contrato.

4. Naturaleza y Finalidad del Tratamiento

4.1 Categorías de interesados

Empleados, trabajadores y colaboradores del Responsable del Tratamiento. En el caso del canal de denuncias, también denunciantes (que pueden ser anónimos) y personas denunciadas.

4.2 Categorías de datos personales

Registro horario: nombre, apellidos, identificador de empleado, fecha y hora de entrada/salida, geolocalización (si se activa), dirección IP.

Canal de denuncias: contenido de la denuncia, datos identificativos del denunciante (salvo denuncia anónima), datos del denunciado, documentación adjunta, trazabilidad del expediente.

Registro retributivo: nombre, apellidos, categoría profesional, sexo, retribución salarial y complementos, tipo de jornada.

Datos de acceso a la plataforma: correo electrónico, contraseña (hash), registro de actividad (logs de auditoría).

4.3 Finalidad del tratamiento

Los datos serán tratados únicamente para la prestación de los servicios contratados por el Responsable. Verilabo no utilizará los datos para finalidades propias, analítica comercial, perfilado ni ninguna otra finalidad que no sea estrictamente la ejecución de los servicios descritos en la cláusula 2.

5. Obligaciones del Encargado

Verilabo, como Encargado del Tratamiento, se compromete a:

e) Tratar los datos personales únicamente conforme a las instrucciones documentadas del Responsable, incluyendo las transferencias de datos a terceros países u organizaciones internacionales, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros.

f) Garantizar que las personas autorizadas para tratar datos personales se han comprometido a respetar la confidencialidad o están sujetas a una obligación legal de confidencialidad.

g) Aplicar las medidas técnicas y organizativas apropiadas detalladas en el Anexo I de Medidas de Seguridad.

h) No recurrir a otro encargado del tratamiento (subencargado) sin la autorización previa del Responsable. La lista actualizada de subencargados se encuentra en el Anexo II del presente contrato.

i) Asistir al Responsable en la atención del ejercicio de derechos de los interesados (acceso, rectificación, supresión, portabilidad, limitación, oposición).

j) Asistir al Responsable en el cumplimiento de las obligaciones relativas a la seguridad del tratamiento, notificación de violaciones de seguridad y evaluaciones de impacto.

k) Suprimir o devolver todos los datos personales al Responsable una vez finalizada la prestación de los servicios, y suprimir las copias existentes salvo que el Derecho de la Unión o nacional exija la conservación de los datos.

l) Poner a disposición del Responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el artículo 28 del RGPD, así como para permitir y contribuir a la realización de auditorías e inspecciones.

6. Notificación de Violaciones de Seguridad

Verilabo notificará al Responsable, sin dilación indebida y en un plazo máximo de 24 horas desde su detección, cualquier violación de la seguridad de los datos personales de la que tenga conocimiento, facilitando la siguiente información:

m) Descripción de la naturaleza de la violación, incluyendo las categorías y número aproximado de interesados afectados.

n) Nombre y datos de contacto del punto de contacto para obtener más información.

o) Descripción de las posibles consecuencias y de las medidas adoptadas o propuestas para remediar la violación.

La comunicación se realizará a través del correo electrónico del Responsable registrado en la plataforma, y adicionalmente a través de la propia plataforma Verilabo.

7. Subencargados del Tratamiento

El Responsable autoriza con carácter general la subcontratación por parte de Verilabo de los servicios auxiliares detallados en el Anexo II del presente contrato. Verilabo se compromete a:

p) Informar al Responsable de cualquier cambio previsto en la incorporación o sustitución de subencargados, dándole la oportunidad de oponerse a dichos cambios en un plazo de 15 días naturales.

q) Imponer a los subencargados las mismas obligaciones de protección de datos que las establecidas en el presente contrato (flow-down contractual).

r) Seguir siendo plenamente responsable ante el Responsable del cumplimiento de las obligaciones de los subencargados.

8. Transferencias Internacionales de Datos

Los datos personales se alojan en servidores de Supabase (Supabase Inc.) ubicados en la Unión Europea (Alemania, región eu-central-1). El tratamiento principal de datos se realiza dentro del Espacio Económico Europeo (EEE).

Determinados subencargados (Stripe, Inc. y Resend, Inc.) tienen su sede en Estados Unidos. Las transferencias de datos a estos proveedores se realizan al amparo del EU-US Data Privacy Framework, estando ambas entidades certificadas bajo dicho marco. En caso de invalidación del marco de adecuación, Verilabo implementará cláusulas contractuales tipo (CCT) aprobadas por la Comisión Europea como garantía alternativa.

Verilabo no realizará transferencias de datos a países fuera del EEE que no cuenten con una decisión de adecuación o garantías apropiadas sin la autorización previa y explícita del Responsable.

9. Ejercicio de Derechos de los Interesados

Cuando un interesado ejerza sus derechos de acceso, rectificación, supresión, portabilidad, limitación del tratamiento u oposición directamente ante Verilabo, éste lo comunicará al Responsable en un plazo máximo de 2 días hábiles.

Verilabo pondrá a disposición del Responsable las herramientas técnicas necesarias dentro de la plataforma para facilitar la gestión de estos derechos, incluyendo funcionalidades de exportación y eliminación de datos.

10. Finalización del Tratamiento

Una vez finalizada la relación contractual, Verilabo:

s) Ofrecerá al Responsable la posibilidad de exportar todos sus datos en formato estándar (CSV/JSON) durante un periodo de 30 días naturales tras la finalización.

t) Transcurrido dicho plazo, procederá a la supresión completa e irreversible de todos los datos del Responsable, incluyendo copias de seguridad, en un plazo máximo de 60 días naturales adicionales.

u) Emitirá un certificado de destrucción de datos al Responsable que lo solicite.

Se exceptúan de la supresión aquellos datos cuya conservación venga impuesta por obligación legal (por ejemplo, registros de denuncias según Ley 2/2023 durante los plazos legalmente establecidos).

11. Responsabilidad

Verilabo responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido las obligaciones del RGPD específicamente dirigidas a los encargados del tratamiento, o cuando haya actuado al margen o en contra de las instrucciones legítimas del Responsable.

12. Legislación Aplicable y Jurisdicción

El presente contrato se regirá e interpretará conforme a la legislación española, en particular el Reglamento (UE) 2016/679 (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

Para la resolución de cualquier controversia derivada del presente contrato, las partes se someten a los Juzgados y Tribunales de Ávila, con renuncia expresa a cualquier otro fuero que pudiera corresponderles.

ANEXO I — MEDIDAS DE SEGURIDAD TÉCNICAS Y ORGANIZATIVAS

De conformidad con el artículo 32 del RGPD, Verilabo implementa las siguientes medidas de seguridad para proteger los datos personales tratados en nombre del Responsable:

A.1 Cifrado

Cifrado en tránsito: todas las comunicaciones se realizan mediante TLS 1.2 o superior (HTTPS). No se permite el acceso a la plataforma mediante protocolos no cifrados.

Cifrado en reposo: los datos almacenados en Supabase (PostgreSQL) están cifrados mediante AES-256. Las copias de seguridad también se almacenan cifradas.

Cifrado del canal de denuncias: los contenidos de las denuncias se cifran con cifrado adicional a nivel de aplicación para garantizar la confidencialidad reforzada exigida por la Ley 2/2023.

A.2 Control de Acceso

Autenticación mediante credenciales únicas por usuario con contraseñas hasheadas (bcrypt). Soporte para autenticación multifactor (MFA/2FA) disponible para todos los usuarios.

Sistema de roles y permisos granular: administrador, gestor de RRHH, empleado, auditor externo, inspector. Cada rol tiene acceso únicamente a los datos necesarios para su función (principio de mínimo privilegio).

Separación lógica de datos entre clientes mediante Row Level Security (RLS) de Supabase, garantizando que ningún cliente puede acceder a datos de otro.

A.3 Registros de Actividad y Auditoría

Registro inmutable de todas las acciones realizadas en la plataforma: fichajes, accesos, modificaciones, consultas y exportaciones de datos.

Los logs de auditoría se conservan durante un mínimo de 12 meses y no pueden ser modificados ni eliminados por ningún usuario, incluidos administradores.

Trazabilidad completa de accesos al portal Inspector View, incluyendo timestamp, datos consultados y duración de la sesión.

A.4 Copias de Seguridad

Copias de seguridad automáticas diarias de la base de datos, con retención de 30 días. Las copias se almacenan en ubicaciones geográficas separadas dentro de la UE (Alemania).

Pruebas de restauración periódicas para verificar la integridad y disponibilidad de las copias.

A.5 Gestión de Vulnerabilidades

Actualización regular de dependencias y componentes de software. Monitorización continua de vulnerabilidades conocidas (CVE) en las dependencias utilizadas.

Política de parcheado: las vulnerabilidades críticas se parchean en un plazo máximo de 48 horas desde su identificación.

A.6 Medidas Organizativas

Todo el personal con acceso a datos personales está sujeto a obligaciones de confidencialidad formalizadas por escrito.

Formación periódica en protección de datos y seguridad de la información para todo el personal.

Política de escritorio limpio y dispositivos seguros para el acceso a sistemas de producción.

Procedimiento documentado de gestión de incidentes de seguridad con asignación de responsabilidades y canales de comunicación.

ANEXO II — LISTA DE SUBENCARGADOS DEL TRATAMIENTO

Última actualización: marzo de 2026

La siguiente tabla recoge los subencargados de tratamiento autorizados por el Responsable con carácter general al aceptar el presente contrato:

Subencargado	Servicio	Ubicación	Datos tratados
Supabase Inc.	Base de datos y backend (PostgreSQL)	Alemania (UE) — eu-central-1	Todos los datos de la plataforma
Stripe, Inc.	Procesamiento de pagos y facturación	EE.UU. (EU-US DPF)	Datos de facturación del Cliente (no datos de empleados)
Resend, Inc.	Envío de emails transaccionales	EE.UU. (EU-US DPF)	Dirección de email, nombre del destinatario
Hostinger International Ltd.	Hosting web (frontend)	UE (Lituania)	Datos de navegación, cookies técnicas

Los subencargados con sede en Estados Unidos están certificados bajo el EU-US Data Privacy Framework. En caso de que dicho marco sea invalidado, Verilabo implementará cláusulas contractuales tipo (CCT) de la Comisión Europea como mecanismo de garantía alternativo en un plazo máximo de 30 días.

Cualquier cambio en la lista de subencargados será notificado al Responsable con un mínimo de 15 días naturales de antelación, ofreciendo la posibilidad de oponerse. La lista actualizada estará siempre disponible en verilabo.com/legal/subencargados.

ANEXO III — REGISTRO DE ACTIVIDADES DE TRATAMIENTO (RAT)

Conforme al artículo 30.2 del RGPD, Verilabo como Encargado del Tratamiento mantiene el siguiente registro:

Tratamiento 1: Registro Horario Digital

Responsable(s)	Clientes de Verilabo (empresas/autónomos con empleados)
Finalidad	Prestación del servicio de registro de jornada laboral conforme a RD-ley 8/2019
Categorías de interesados	Empleados y trabajadores del Responsable
Categorías de datos	Nombre, apellidos, ID empleado, fechas/horas de fichaje, geolocalización (opcional), IP
Transferencias internacionales	No (datos en Supabase UE). Emails transaccionales vía Resend (EE.UU., EU-US DPF)
Medidas de seguridad	Cifrado AES-256, TLS 1.2+, RLS, registros inmutables, MFA disponible
Plazo de conservación	Durante la vigencia del contrato + 4 años (prescripción infracciones laborales)

Tratamiento 2: Canal de Denuncias

Responsable(s)	Clientes de Verilabo obligados por Ley 2/2023
Finalidad	Gestión de denuncias internas conforme a Ley 2/2023
Categorías de interesados	Denunciantes (pueden ser anónimos), personas denunciadas
Categorías de datos	Contenido denuncia, datos identificativos (si no anónima), datos denunciado, documentación adjunta
Transferencias internacionales	No (datos en Supabase UE). Cifrado adicional a nivel de aplicación
Medidas de seguridad	Cifrado E2E adicional, acceso restringido por rol, anonimización técnica, logs de acceso
Plazo de conservación	Máximo 3 meses para decisión sobre investigación. Si hay procedimiento: duración del mismo

Tratamiento 3: Registro Retributivo

Responsable(s)	Clientes de Verilabo sujetos a RD 902/2020
Finalidad	Cálculo automático de brecha salarial y generación de registro retributivo
Categorías de interesados	Empleados del Responsable
Categorías de datos	Nombre, categoría profesional, sexo, retribución total y complementos, tipo de jornada
Transferencias internacionales	No (datos en Supabase UE)
Medidas de seguridad	Cifrado AES-256, TLS 1.2+, RLS, acceso limitado a rol RRHH/admin
Plazo de conservación	Durante la vigencia del contrato + 4 años

El presente Registro de Actividades de Tratamiento se mantiene actualizado y a disposición de la Agencia Española de Protección de Datos (AEPD) cuando esta lo requiera.