SCLOG SOFTWARE

RETENCIÓN Y TRATAMIENTO DE DATOS DE LEADS

Política bilingüe vigente para WordPress, Kommo CRM, Bookings, correo y WhatsApp

English version notice: The English version of this document appears immediately after the complete Spanish text.

1. Objetivo

Esta política se aplica a SCLOG Software, LLC y, cuando corresponda al servicio o mercado, a SCLOG Software CALA. El sitio está orientado principalmente a relaciones empresariales B2B en Estados Unidos y Latinoamérica.

Esta política establece reglas de minimización, conservación, revisión, anonimización y eliminación de leads capturados mediante el sitio web, correo, Microsoft Bookings, WhatsApp, Kommo CRM, eventos o referencias.

2. Roles y responsabilidades

SCLOG actúa como responsable o controlador de los datos de sus leads. Brandlex y los proveedores autorizados actuarán únicamente conforme a instrucciones documentadas, obligaciones contractuales y permisos mínimos necesarios.

3. Calendario de retención

- Lead sin respuesta o no calificado: 12 meses desde la última interacción.
- Oportunidad descartada: 24 meses, salvo solicitud válida de eliminación u obligación diferente.
- Prospecto con consentimiento de marketing: hasta la revocación o 24 meses de inactividad, lo que ocurra primero, sujeto a revisión periódica.
- Cliente, contrato, propuesta aceptada y facturación: durante la relación y 7 años después, de acuerdo con obligaciones fiscales, contractuales y de defensa de reclamaciones.
- Registros de consentimiento y solicitudes de privacidad: 5 años o el plazo de prescripción aplicable.
- Logs de seguridad y respaldos: entre 90 y 365 días, según riesgo, finalidad y ciclo técnico aprobado.

4. Reglas operativas

Kommo CRM debe conservar origen, finalidad, consentimiento, última interacción, responsable, estado y fecha de revisión. No deben almacenarse contraseñas, datos de pago ni datos sensibles en notas de leads. Las exportaciones locales deben limitarse, protegerse y eliminarse al finalizar su uso autorizado.

5. Eliminación y anonimización

Al vencer el plazo, los datos se eliminarán de los sistemas activos o se anonimizarán de manera irreversible. Los respaldos se depurarán conforme a su ciclo. Podrá conservarse un registro mínimo de supresión para evitar recontacto y demostrar el cumplimiento de la solicitud.

6. Solicitudes y excepciones

Las solicitudes deben dirigirse a sclog@sclogsoftware.com. La retención podrá extenderse por litigio, fraude, auditoría, seguridad, obligación legal o contrato, documentando el motivo, alcance, acceso permitido y fecha de revisión.

7. Supervisión y revisión

SCLOG realizará una revisión trimestral de leads inactivos y una revisión anual de esta política. Cada nueva integración, plugin o proveedor deberá evaluarse en materia de datos, permisos, seguridad y retención antes de habilitarse.

8. Referencias regulatorias consideradas

La política considera los principios de limitación de finalidad, minimización, exactitud, limitación del plazo de conservación, seguridad y responsabilidad demostrada previstos, según su aplicabilidad, en el Reglamento General de Protección de Datos; CCPA y CPRA; Ley 1581 de 2012 de Colombia y sus normas relacionadas; Ley Orgánica de Protección de Datos Personales de Ecuador; reglas de conservación contractual, fiscal y probatoria; y prácticas de seguridad y eliminación responsable promovidas por la FTC.

SCLOG SOFTWARE

LEAD DATA PROCESSING AND RETENTION

Current document for website publication

1. Purpose

This policy applies to SCLOG Software, LLC and, where relevant, SCLOG Software CALA. It establishes minimization, retention, review, anonymization, and deletion rules for leads collected through the website, email, Microsoft Bookings, WhatsApp, Kommo CRM, events, or referrals.

2. Roles and responsibilities

SCLOG acts as controller of lead data. Brandlex and authorized providers will process data only under documented instructions, contractual obligations, and minimum necessary permissions.

3. Retention schedule

- Unresponsive or unqualified lead: 12 months from the last interaction.
- Closed or rejected opportunity: 24 months, unless a valid deletion request or different obligation applies.
- Prospect with marketing consent: until withdrawal or 24 months of inactivity, whichever occurs first, subject to periodic review.
- Customer, contract, accepted proposal, and billing records: during the relationship and for 7 years afterward, according to tax, contractual, and claims-defense obligations.
- Consent records and privacy requests: 5 years or the applicable limitation period.
- Security logs and backups: 90 to 365 days, based on risk, purpose, and the approved technical cycle.

4. Operational rules

Kommo CRM must retain source, purpose, consent, last interaction, owner, status, and review date. Passwords, payment data, and sensitive data must not be stored in lead notes. Local exports must be limited, protected, and deleted after authorized use ends.

5. Deletion and anonymization

At the end of the retention period, data will be deleted from active systems or irreversibly anonymized. Backups will be purged according to their cycle. A minimal suppression record may be retained to prevent recontact and demonstrate compliance with a request.

6. Requests and exceptions

Requests must be sent to sclog@sclogsoftware.com. Retention may be extended for litigation, fraud, audit, security, legal obligations, or contract requirements, with the reason, scope, permitted access, and review date documented.

7. Oversight and review

SCLOG will conduct quarterly reviews of inactive leads and an annual review of this policy. Each new integration, plugin, or provider must be assessed for data, permissions, security, and retention before activation.

8. Regulatory references considered

This policy considers the purpose limitation, minimization, accuracy, storage limitation, security, and accountability principles under, where applicable, the General Data Protection Regulation; CCPA and CPRA; Colombia's Law 1581 of 2012 and related rules; Ecuador's Organic Law on Personal Data Protection; contractual, tax, and evidentiary retention rules; and FTC practices concerning security and responsible disposal.