

Política de Privacidad y Protección de Datos Personales

Versión 1.3 · Última actualización: 23 de julio de 2026

Documento legal oficial para usuarios administradores y clínicas registradas en Valdenta.

1. Alcance

Esta Política de Privacidad explica cómo Valdenta trata datos personales y datos relacionados con la operación odontológica de clínicas y consultorios del Ecuador. Aplica a administradores de clínicas, usuarios vinculados y visitantes que utilicen los formularios de registro, inicio de sesión, recuperación de contraseña o contacto de la plataforma.

2. Marco normativo de referencia

Valdenta se diseña tomando como referencia la Ley Orgánica de Protección de Datos Personales del Ecuador, su normativa reglamentaria y los principios reconocidos para el tratamiento de datos personales, incluyendo juridicidad, lealtad, transparencia, finalidad, pertinencia, minimización, confidencialidad, calidad, conservación, seguridad y responsabilidad proactiva. Esta política no reemplaza la asesoría legal específica que cada clínica pueda necesitar.

3. Roles en el tratamiento

Respecto de los datos de pacientes y de la operación clínica ingresados por la clínica, la clínica actúa generalmente como responsable del tratamiento, pues decide qué datos recopila, con qué finalidad y bajo qué base de legitimación. La plataforma actúa como proveedor tecnológico o encargado del tratamiento en la medida en que procesa los datos siguiendo las instrucciones de la clínica y para prestar el servicio contratado. Respecto de datos propios de registro, facturación, seguridad y relación comercial, Valdenta podrá actuar como responsable.

4. Datos tratados

La plataforma puede tratar datos de identificación, contacto, credenciales, información de clínica, roles, actividad de cuenta, direcciones IP, agente de usuario, registros de auditoría, datos de agenda, pacientes, documentos clínicos, antecedentes médicos, alergias, medicación actual, signos vitales, odontogramas, evoluciones, recetas, consentimientos, presupuestos, archivos, inventario, caja y registros administrativos ingresados por la clínica.

5. Datos sensibles y de salud

La información clínica odontológica y de salud de pacientes puede constituir dato sensible. La clínica debe tratar estos datos con especial diligencia, informar a sus pacientes, documentar autorizaciones o bases legales aplicables, limitar accesos internos, asignar roles adecuados y evitar ingresar información innecesaria. El sistema incorpora herramientas técnicas para segregación por clínica, autenticación, roles y registros, pero la pertinencia y legitimidad del dato ingresado corresponde a la clínica.

6. Finalidades

Los datos se tratan para crear y administrar cuentas, prestar el servicio contratado, mantener separación por clínica, gestionar seguridad, generar documentos, facilitar operación clínica, registrar evidencias legales, enviar comunicaciones operativas y atender soporte.

7. Integración opcional con Google Calendar

La integración con Google Calendar es opcional y solo se activa cuando un usuario autorizado decide conectar su cuenta de Google desde la agenda de Valdenta. En ese caso, Valdenta solicita el alcance <https://www.googleapis.com/auth/calendar.events.owned> para crear, consultar, actualizar y eliminar eventos de citas en calendarios de Google propios del usuario, principalmente en su calendario principal. Los datos que pueden enviarse a Google Calendar se limitan a la información necesaria para representar la cita: nombre del paciente, tratamiento o servicio, fecha, hora, duración, profesional asignado y notas de la cita si el usuario las registró. El token OAuth de Google y el mapa entre la cita de Valdenta y el evento de Google se guardan en el navegador del usuario mediante almacenamiento local; Valdenta no almacena tokens de Google Calendar en su backend. El usuario puede desconectar la integración desde Valdenta o revocar el acceso desde su cuenta de Google.

8. Bases de legitimación

El tratamiento puede sustentarse, según el caso, en la ejecución de una relación contractual o precontractual, el consentimiento del titular, el cumplimiento de obligaciones legales, el interés legítimo cuando corresponda, la protección de intereses vitales o la prestación de servicios de salud bajo responsabilidad de profesionales autorizados. La clínica es responsable de determinar y documentar la base aplicable para los datos de sus pacientes.

9. Seguridad

Se aplican controles técnicos y organizativos razonables para proteger la información, incluyendo autenticación, roles, filtros por clínica y controles de acceso. Ningún sistema es completamente inmune a riesgos, por lo que el usuario debe proteger sus credenciales y dispositivos.

10. Medidas técnicas y organizativas de seguridad

Las medidas de seguridad están orientadas a proteger la confidencialidad, integridad, disponibilidad y trazabilidad de la información tratada dentro de la plataforma. Pueden incluir control de acceso basado en roles, separación lógica de información por clínica, registros de auditoría, evidencia de aceptación de documentos legales, protección de archivos clínicos privados, uso de conexiones seguras, copias de seguridad periódicas, gestión de credenciales y restricciones de acceso a información sensible. Estas medidas podrán evolucionar conforme cambien los riesgos tecnológicos, la infraestructura o la normativa aplicable.

11. Controles de acceso y confidencialidad

Cada usuario debe utilizar credenciales propias, mantenerlas en reserva y cerrar sesión en dispositivos compartidos. Los administradores de clínica deben activar, desactivar y asignar roles según necesidad real de acceso. El acceso de un usuario a una clínica puede ser suspendido por el administrador de esa clínica sin afectar necesariamente sus accesos a otras clínicas.

12. Conservación

Los datos se conservarán mientras la cuenta o relación contractual se mantenga activa y durante los plazos necesarios para fines legales, administrativos, de auditoría, soporte, seguridad o continuidad del servicio.

13. Conservación posterior a la terminación del servicio

Cuando una clínica cancele o termine el servicio, la información asociada podrá conservarse durante un período máximo de ciento ochenta (180) días con fines de exportación, migración, continuidad operativa, auditoría, soporte técnico, seguridad o cumplimiento legal. Transcurrido dicho período, la información podrá ser eliminada o anonimizada conforme a las obligaciones legales aplicables y a las políticas internas de conservación.

14. Encargados, proveedores y transferencias

El servicio puede apoyarse en proveedores tecnológicos para infraestructura, almacenamiento, comunicaciones o soporte. Cuando el usuario conecta Google Calendar, Valdenta transfiere a Google únicamente los datos de la cita necesarios para crear, actualizar, consultar o eliminar eventos conforme a la acción solicitada por el usuario. Fuera de esa integración opcional, Valdenta no vende datos personales ni datos de Google, no los utiliza para publicidad y no los transfiere a terceros salvo cuando sea necesario para prestar el servicio, proteger la seguridad, cumplir obligaciones legales o atender instrucciones válidas de la clínica responsable.

15. Transferencias internacionales

Algunos proveedores tecnológicos pueden encontrarse o almacenar información fuera del Ecuador. Cuando exista una transferencia internacional o acceso remoto a datos, se procurará aplicar mecanismos razonables de protección contractual, técnica u organizativa, de acuerdo con la naturaleza del servicio y la normativa aplicable.

16. Derechos de titulares

Los titulares de datos personales podrán solicitar acceso, rectificación y actualización, eliminación, oposición, portabilidad, suspensión del tratamiento, limitación del tratamiento y a no ser objeto de decisiones basadas única o parcialmente en valoraciones automatizadas, cuando corresponda conforme a la normativa aplicable. Las solicitudes relacionadas con pacientes deberán coordinarse principalmente con la clínica responsable del tratamiento.

17. Portabilidad y exportación de datos

La clínica podrá solicitar la exportación de la información asociada a su cuenta mediante los mecanismos disponibles dentro de la plataforma o mediante solicitud formal dirigida a Valdenta. Las exportaciones podrán quedar registradas en los sistemas de auditoría con fines de trazabilidad y seguridad.

18. Procedimiento para ejercer derechos

Las solicitudes deberán identificar al titular, describir claramente el derecho que desea ejercer y acompañar la información necesaria para verificar identidad y legitimación. Cuando Valdenta actúe como encargado de tratamiento, podrá remitir o coordinar la solicitud con la clínica responsable. La atención de solicitudes estará sujeta a los plazos y condiciones previstos por la normativa aplicable.

19. Comunicaciones

Valdenta podrá enviar comunicaciones operativas, legales, de seguridad, activación de cuenta, renovación o soporte al correo o WhatsApp registrado. Estas comunicaciones son necesarias para la prestación y administración del servicio.

20. Registros técnicos, cookies y analítica

La plataforma puede registrar información técnica como dirección IP, dispositivo, navegador, fecha, hora, eventos de autenticación, errores, actividad de seguridad y uso general de módulos para prevenir abuso, diagnosticar fallos, mejorar estabilidad, mantener auditoría y proteger la plataforma. Si se utilizan cookies o tecnologías similares, estas se orientarán a sesión, seguridad, preferencias o medición operativa.

21. Incidentes de seguridad

En caso de identificar un incidente de seguridad que pueda comprometer datos personales, Valdenta evaluará su alcance y adoptará medidas de contención, investigación y comunicación según corresponda. La clínica deberá colaborar cuando el incidente se relacione con sus usuarios, dispositivos, credenciales, datos ingresados o instrucciones de tratamiento.

22. Auditoría y trazabilidad

Podrán mantenerse registros técnicos de auditoría relacionados con accesos, consultas, modificaciones, descargas, exportaciones y otras operaciones relevantes realizadas dentro de la plataforma. Estos registros podrán incluir información como usuario, clínica, fecha, hora, dirección IP, agente de usuario y tipo de acción ejecutada. Su finalidad es apoyar la seguridad, el soporte, la investigación de incidentes, el cumplimiento y la continuidad operativa.

23. Menores de edad y pacientes vulnerables

Cuando la clínica registre información de menores de edad o pacientes en situación de especial protección, deberá contar con las autorizaciones, representación o bases legales exigibles y aplicar medidas reforzadas de confidencialidad, minimización y pertinencia del dato clínico.

24. Evidencia de aceptación

Al aceptar esta política durante el registro, Valdenta almacena evidencia de aceptación vinculada al usuario administrador y a la clínica creada, incluyendo versiones aceptadas, fecha, hora, IP y agente de usuario.

25. Uso limitado de datos de Google

Los datos obtenidos o enviados mediante las APIs de Google se utilizan exclusivamente para ofrecer o mejorar la función visible de sincronización de citas con Google Calendar. Valdenta no vende datos de Google, no los usa para publicidad, retargeting, perfiles publicitarios, modelos de crédito o fines ajenos a la agenda clínica, y no permite lectura humana de dichos datos salvo que sea necesaria para soporte solicitado por el usuario, seguridad, cumplimiento legal o información agregada usada para operación interna conforme a la normativa aplicable.

26. Actualizaciones

Esta política puede actualizarse para reflejar cambios legales, operativos o técnicos. Las nuevas versiones podrán requerir aceptación posterior y se mantendrá historial de aceptaciones anteriores.

27. Contacto para privacidad

Para consultas sobre privacidad, protección de datos, ejercicio de derechos o gestión de información dentro de Valdenta, la clínica o el titular podrá usar los canales oficiales de contacto informados por Valdenta en la plataforma o durante el proceso comercial. Las solicitudes de pacientes podrán requerir coordinación con la clínica responsable.