



POLÍTICA DE PRIVACIDAD

ARTÍCULO 1: PREÁMBULO

La protección de los Datos personales es primordial para Dental Monitoring SAS («DM»). DM se compromete a cumplir con la reglamentación francesa y europea en materia de protección de datos personales, en particular con el Reglamento general de protección de datos (UE) del 27 de abril de 2016 («GDPR»), con la Loi Informatique et Libertés de 1978 en su versión enmendada («LIL»), así como con cualquier reglamentación local de protección de datos aplicable al procesamiento de datos.

Para cumplir con el GDPR y otras normativas locales de protección de datos como la HIPAA y para proteger la confidencialidad, integridad y disponibilidad de los Datos Personales, incluidos los Datos relativos a la salud («**Datos relativos a la salud**») como la Información médica protegida («**PHI**»), DM ha desarrollado e implementado estrictos estándares de ciberseguridad, políticas, procedimientos y capacitaciones para sus empleados, así como sólidas medidas de seguridad.

DM cuenta con un equipo dedicado a la protección de Datos Personales, que incluye un responsable de la Protección de datos y del HIPAA, un equipo de seguridad y un equipo jurídico especializado en cuestiones de privacidad.

Además, DM cuenta con las certificaciones ISO 13485 (Sistema de gestión de calidad de los dispositivos médicos), ISO/IEC 27001 (Seguridad de la información) y HDS/HDH (Almacenamiento de datos sanitarios). Asimismo, los Datos Personales de los Profesionales de la salud y sus Pacientes están alojados en servidores AWS locales (certificados ISO27001 y HDS/HDH), bajo la responsabilidad de Dental Monitoring.

ARTÍCULO 2: DEFINICIONES

Los términos en mayúsculas recogidos a continuación, incluidos los del preámbulo de la Política de Privacidad, se interpretarán de la siguiente manera:

«**Ley de protección de datos**» se refiere (i) al Reglamento general de protección de datos de la UE 2016/679 («**RGPD**»), (ii) la Directiva sobre la privacidad y las comunicaciones electrónicas 2002/58/CE («**Directiva sobre la privacidad electrónica**»), y cualquier otra normativa aplicable que sustituya a la Directiva sobre la privacidad electrónica y/o al RGPD; (iii) cualquier ley, estatuto o reglamento de protección de datos de un Estado miembro de la Unión Europea («UE»), que pueda aplicarse a una de las Partes en virtud de sus actividades de Tratamiento de datos o de su establecimiento en la UE; y (iv) cualquier directriz o dictamen adoptado por el Comité europeo de protección de datos («**CEPD**») en cuanto a interpretaciones de la aplicación del RGPD y de la Directiva sobre la Privacidad Electrónica; (v) cualquier fallo de la Autoridad de control o de los tribunales judiciales o administrativos de un Estado miembro de la UE que sea vinculante para una de las Partes en virtud de sus actividades de tratamiento de datos o de su establecimiento en la UE; y (vi) cualquier fallo adoptado por el Tribunal de justicia de la Unión Europea (TJUE) o el Tribunal europeo de derechos humanos (TEDH) en relación con la protección de los datos personales, la privacidad, la libertad de expresión o la libertad de información; y (vii) cualquier otra norma local de protección de datos



aplicable al procesamiento de datos, incluida, por ejemplo, la HIPAA o las leyes federales y estatales o locales, entre las que se incluyen, sin carácter exhaustivo, la Ley de Protección de la Información Personal y los Documentos Electrónicos («**PIPEDA**»), la Ley de Protección de la Información Personal (Alberta) («**PIPA Alberta**»), la Ley de Protección de la Información Personal (Columbia Británica) («**PIPA BC**») y la Ley de Protección de la Información Personal en el Sector Privado («**Ley de Privacidad de Quebec**») para ciudadanos canadienses.

«**Responsable del tratamiento**», «**Tratamiento**» y «**Autoridad de control**» tendrán el significado que se les asigna en el artículo 4 del RGPD.

Panel de control: se refiere a la interfaz web para los Profesionales de la salud autenticados, accesible tras crear una Cuenta Profesional en la Plataforma DM.

Condiciones: Se refiere a estos Términos y Condiciones de uso.

Aplicación móvil de DM: se refiere a la aplicación DM.

Plataforma DM: se refiere a la plataforma DM.

Productos y servicios de software de DM: se refiere a DentalMonitoring, Engage, Smart STL, descritos en los Términos de Uso y facilitados por DM a través de las Plataformas de DM y la aplicación móvil DM;

Sistemas de hardware de DM: se refiere a la ScanBox DM, Retractores de mejillas DM, ScanBox Pro y Adaptador led.

Solución DM: se refiere al software, infraestructuras digitales, protocolos, interfaces, aplicaciones móviles y hardware desarrollados, fabricados y distribuidos por DM para su uso en el sector de la salud dental.

Usuario (s) final (es) o Paciente (s): se refiere al/los paciente(s) que utilizan los Productos y servicios de software de DM;

Datos relativos a la salud: tendrán el significado que se les asigna en el artículo 4 del GDPR, incluida la PHI;

Profesional(es) de la salud (HCP por sus siglas en inglés): se refiere al/los proveedor(es) de servicios de la salud calificado(s) para ejercer la odontología u ortodoncia en su jurisdicción.

Cuenta del Paciente: se refiere a la cuenta del Usuario final creada por el Profesional de la salud en DentalMonitoring o por el mismo Paciente, para acceder a la Aplicación DM, y por tanto, a los Productos y servicios de software DM.

Datos personales: tendrá el significado que se les asigna en el artículo 4 del RGPD, incluidos los Datos relativos a la salud y, por tanto, la PHI.

Política de privacidad: se refiere a la política de privacidad, disponible en la Plataforma y Aplicaciones móviles de DM, que informa a los Usuarios y a los Usuarios finales de los compromisos asumidos por DM para proteger los Datos personales de los Usuarios y de los Usuarios finales cuando estos utilizan los Productos y servicios de software de DM.

Información médica protegida o PHI: se refiere a la información, incluidos los datos demográficos, que (1) hacen referencia a (i) una enfermedad o condición física o mental pasada, presente o futura; (ii) el suministro de atención médica pasada, presente o futuro; o (iii) el pago por una prestación de atención médica pasada, presente o futura; y (2) identifican a la persona titular de la información u ofrecen una base razonable que indica que la información se refiere a dicha persona. La Información médica protegida se limita a la información de la entidad cubierta creada o recibida por DM de parte



o en nombre del Cliente o de la entidad cubierta.

Finalidad: se refiere a las principales finalidades del uso de los Datos personales.

Stripe: se refiere a la plataforma dedicada a los pagos en línea utilizada por DM para gestionar los pagos realizados por los Usuarios en la Plataforma de DM, a través de la Tienda.

Usted/Su/Sus: Le designa a usted.



ARTÍCULO 3. ¿QUÉ SON LOS DATOS PERSONALES?

Un dato personal es cualquier información relativa a una persona física identificada o identificable («**Sujeto de datos**»). El Sujeto de datos es una persona que puede ser identificada, directa o indirectamente, particularmente mediante un identificador como su nombre, número de identificación, datos de localización, un identificador electrónico o uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de esa persona física.

ARTÍCULO 4. ¿CUÁL ES EL OBJETIVO DE ESTA POLÍTICA DE PRIVACIDAD?

Esta Política de Privacidad expone:

- cómo DM recoge, utiliza y comparte Sus Datos personales cuando usted utiliza los Productos y servicios de software de DM y los Sistemas de hardware de DM;
- cómo DM protege y garantiza la seguridad, integridad y confidencialidad de sus Datos

personales. DM sigue estos principios para proteger Sus Datos personales:

- DM no recoge más Datos personales de los necesarios;
- DM solo utiliza sus Datos personales para los fines especificados en esta

Política de privacidad, a menos que usted acepte lo contrario;

- DM no conserva sus Datos personales cuando ya no son necesarios; y
- Fuera de lo especificado en esta Política de privacidad, DM no comparte sus Datos personales con terceros.
- DM no alquila ni vende sus Datos personales a terceros.

Ya sea usted Profesional de la salud o Paciente, por favor tómese el tiempo para leer y entender esta Política de privacidad.

ARTÍCULO 5. ¿QUIÉN RECOGE LOS DATOS PERSONALES?

Datos de los Profesionales de la salud	Datos de los pacientes
DM actúa como único Responsable del tratamiento para los tratamientos n°1 a n°6 descritos en la Sección 7 de la presente Política de privacidad. Como excepción, cuando se trate de contratos con organismos o entidades públicas (como hospitales): DM actúa como único Responsable del tratamiento en el caso del tratamiento n°1 descrito en la Sección 7 de la presente Política de privacidad.	DM actúa como Corresponsable del tratamiento junto con el Profesional de la salud (cuando este trabaja por cuenta propia) o con el empleador del Profesional de la salud (cuando este trabaja para una empresa) para el Tratamiento n° 1 descrito en la Sección 7 de la presente Política de Privacidad. DM actúa como único Responsable del tratamiento para los tratamientos del n°2 a n°6 descritos en la Sección 7 de la presente Política de privacidad. Como excepción, cuando se trate de contratos con organismos o entidades públicas (como



DM actúa como único Responsable del tratamiento para los tratamientos del n°2 a n°6 descritos en la Sección 7 de la presente Política de privacidad.	hospitales): DM actúa como único Responsable del tratamiento en el caso del tratamiento n°1 descrito en la Sección 7 de la presente Política de privacidad. DM actúa como único Responsable del tratamiento para los tratamientos del n°2 a n°6 descritos en la Sección 7 de la presente Política de privacidad.
--	---

DM y Stripe actúan como Corresponsables del tratamiento en el caso del Tratamiento n°3 de la Sección 7 de la presente Política de privacidad, tanto en relación con los Profesionales de la salud como con los Pacientes.

Para cualquier otro dato recopilado o procesado por el Profesional de la salud durante el curso del tratamiento del paciente que no sea compartido con DM Profesionales de la salud serán los únicos responsables del cumplimiento de las leyes y reglamentos aplicables.



ARTÍCULO 6. ¿QUÉ DATOS PERSONALES SE RECOGEN?

DM recoge Datos personales tanto de los Profesionales de la salud como de los Pacientes.

DE LOS PROFESIONALES DE LA SALUD

Los Datos personales de los Profesionales de la salud procesados por DM son recogidos a través de diferentes canales.

DM recopila los datos personales de los Profesionales de la salud cuando se suscriben a uno de los Productos y servicios de software de DM.

DM puede recopilar los siguientes Datos personales cuando un Profesional de la salud se inscribe a uno de los Productos y servicios de software de DM:

Datos de la cuenta	• Credenciales de la cuenta (nombre de usuario, correo electrónico, hash de contraseña); • Datos personales del profesional de la salud (nombre y apellidos, teléfono, correo electrónico); • Configuración del usuario (preferencias del boletín, idioma, protocolos, configuración de las notificaciones, país).
---------------------------	--

DM puede recopilar los siguientes Datos personales cuando un Profesional de la salud utiliza uno de los Productos y servicios de software de DM:

Datos técnicos	• Información sobre el dispositivo (tipo de dispositivo, dirección IP, identificador único, modelo de dispositivo, sistema operativo y versión, navegador utilizado, cookies o tecnologías similares, idioma); • Información sobre el uso de los Productos y servicios de software de DM (dirección IP, fecha y hora de conexión, páginas visitadas); • Datos sobre la conexión a Internet (proveedor de servicios de Internet, tipo de conexión (4G, 3G, DSL).
Datos de uso	• Registros de actividad del usuario; • Mensajes enviados a los Pacientes; • Citas reservadas con los Pacientes; • Configuración de la cuenta (plantillas de correo electrónico, preferencias de anotación dental, catálogos de tratamientos, protocolos)

DM puede recoger los siguientes Datos personales cuando un Profesional de la salud se pone en contacto con el servicio de atención al cliente:

Datos de los tickets de soporte	• Datos relativos a los tickets de soporte técnico (fecha, hora, asunto y contenido de los tickets) • Contenido de los intercambios con los agentes (correos electrónicos, chat) • Cualquier otro dato que pueda ser necesario para resolver los tickets
--	--



DM puede recopilar los siguientes Datos personales cuando un Profesional de la salud se suscribe a uno de los Productos y servicios de software de DM o compra un Sistema de hardware de DM:

Datos de suscripción / datos del pedido	• Facturas, notas de crédito y otros documentos administrativos; • Datos de la transacción (método de pago, fecha y hora de la transacción, moneda, importe pagado); • Información de contacto (nombre, apellido, correo electrónico, número de teléfono); • Dirección de envío (calle, ciudad, código postal, país); • Datos del pedido.
--	---

DE LOS PACIENTES

DM recopila los datos personales de los Pacientes cuando se suscriben a uno de los Productos y servicios de software de DM.

DM recoge los Datos personales de los Pacientes previo consentimiento de estos mediante un formulario de consentimiento del Paciente. Si el paciente es menor de edad en su país de residencia, el consentimiento lo gestionan sus tutores legales, salvo que se trate de menores emancipados. Por favor, lea detenidamente nuestras Condiciones de uso para más información.

Los Datos personales de los Pacientes procesados por DM son recopilados a través de diferentes canales.

Los Datos personales pueden ser recogidos directamente del Paciente o indirectamente a través del Profesional de la salud. En el caso de que un Profesional de la salud introduzca los Datos personales de un Paciente en un Producto o servicio de software de DM a nombre del Paciente, el Profesional de la salud es responsable de asegurarse de estar legalmente autorizado a hacerlo y de haber tomado las medidas necesarias para cumplir con las leyes y reglamentos aplicables.

DM puede recopilar los siguientes Datos personales cuando un Paciente se suscribe a uno de los Productos y servicios de software de DM:

Datos de la cuenta	• Credenciales de la cuenta (nombre de usuario, correo electrónico, hash de contraseña); • Datos personales y de contacto (nombre y apellidos, número de teléfono, dirección de correo electrónico, foto de perfil (foto de la cara), fecha de nacimiento, representante legal cuando proceda, nombre de la clínica en la que el paciente recibe tratamiento, dirección postal); • Configuración del usuario (protocolos, configuración de las notificaciones).
---------------------------	---



DM puede recopilar los siguientes Datos personales cuando un Paciente utiliza uno de los Productos y servicios de software de DM:

Datos técnicos	• Información sobre el dispositivo (tipo de dispositivo, dirección IP, identificador único, modelo de dispositivo, sistema operativo y versión, navegador utilizado, cookies o tecnologías similares, idioma); • Información sobre el uso del software (dirección IP, fecha y hora de conexión, páginas visitadas); • Datos sobre la conexión a Internet (proveedor de servicios de Internet, tipo de conexión (4G, 3G, DSL).
Datos de uso	• Mensajes enviados al Profesional de la salud; • Citas con el Profesional de la salud; • Preferencias del usuario;
Datos personales	• Fotos de la boca del paciente; • Foto de perfil (foto de la cara); • Tratamiento y/o consejo médico prescrito por el Profesional de la salud; • Tipo y fase del tratamiento; • Resultados de las pruebas/análisis/simulación; • Mensajes enviados entre el profesional de la salud y el paciente que contengan datos médicos como síntomas, motivos de consulta e información médica general; • Impresión digital de la boca del paciente.

DM puede recoger los siguientes Datos personales cuando un Paciente se pone en contacto con el servicio de atención al cliente:

Datos de los tickets de soporte	• Datos relativos a los tickets de soporte técnico (fecha, hora, asunto y contenido de los tickets); • Contenido de los intercambios del Paciente con el personal de DM (correos electrónicos, chat); • Cualquier otro dato que pueda ser necesario para resolver los tickets.
--	--

DM puede recoger los siguientes Datos personales cuando un Paciente usuario de DM compra directamente algún Sistema de hardware de DM, siguiendo las recomendaciones del Profesional de la salud:

Datos del pedido	• Información de contacto (nombre, apellido, correo electrónico, número de teléfono); • Dirección de envío (calle, ciudad, código postal, país); • Datos del pedido.
-------------------------	--

ARTÍCULO 7. ¿POR QUÉ Y CÓMO TRATAMOS SUS DATOS PERSONALES?

DM trata los Datos Personales en el marco de múltiples Tratamientos y para fines múltiples. Dependiendo de las finalidades, el Tratamiento puede basarse en (i) intereses legítimos de DM, (ii) obligaciones contractuales, o (iii) porque usted ha otorgado su consentimiento.

Tenga en cuenta que los Tratamientos enumerados a continuación describen el objetivo principal y, a continuación, los objetivos secundarios.



EN RELACIÓN CON LOS PROFESIONALES DE LA SALUD

DM trata los Datos personales del Profesional de la salud con las siguientes finalidades y sobre la base de los siguientes fundamentos jurídicos:

TRATAMIENTO nº1: EL OBJETIVO PRINCIPAL ES SUMINISTRAR LOS PRODUCTOS Y SERVICIOS DE SOFTWARE DM (MONITORING, ENGAGE, SMART STL)	
Subobjetivo	Fundamento jurídico
Para su establecimiento, configurar y gestionar las cuentas de los Profesionales de la salud (para MONITORING y ENGAGE)	El Tratamiento nº1 es necesario para la ejecución de cualquier contrato en el que participe el Profesional de la salud (Sujeto de datos) (artículo 6.1 (b) del RGPD)
Para que el Profesional de la salud pueda monitorizar a distancia el tratamiento de ortodoncia y la salud bucal de sus Pacientes (solo para MONITORING)	
Para proporcionar a los Profesional de la salud evaluaciones de la salud oral y dental de sus Pacientes (Solo para ENGAGE)	
Para que los Profesionales de la salud puedan mostrar a sus Pacientes simulaciones de su apariencia durante y después tratamiento de ortodoncia (solo para ENGAGE).	
Para generar archivos inteligentes STL (archivos de objetos 3D generados a partir de Scans, archivos STL del escaneo intraoral inicial y del plan de tratamiento del Usuario Final) y fabricar alineadores (solo para SMART STL)	
TRATAMIENTO nº2: EL OBJETIVO PRINCIPAL ES GESTIONAR LOS TICKETS DE LOS PROFESIONAL DE LA SALUD (COMENTARIOS/QUEJAS/PREGUNTAS) ENVIADOS A LOS SERVICIOS DE ATENCIÓN AL CLIENTE EN RELACIÓN CON CUALQUIERA DE LOS PRODUCTOS Y SERVICIOS DE SOFTWARE DE DM	
Subobjetivo	Fundamento jurídico
Para gestionar los comentarios, quejas y reclamaciones de los Profesionales de la salud, incluido el envío de mensajes a los mismos Profesionales de la salud (SMS, WhatsApp, correo electrónico, notificaciones)	El Tratamiento nº2 es necesario para la ejecución de cualquier contrato en el que participe el Profesional de la salud (Sujeto de datos) (artículo 6.1 (b) del RGPD) o cumplir sus obligaciones legales (artículo 6.1 (c) del RGPD) como la transferencia de solicitudes de acceso a los datos privados.
Para transferir las solicitudes de datos personales al equipo encargado de la privacidad	
Para mejorar la calidad y la rapidez de la atención al cliente que DM ofrece a los Profesionales de la salud y sus Pacientes	



TRATAMIENTO nº3: EL OBJETIVO PRINCIPAL ES GESTIONAR LOS PAGOS Y ÓRDENES DE ENVÍO DE LOS PROFESIONALES DE LA SALUD RELATIVOS A CUALQUIER PRODUCTO Y SERVICIO DE SOFTWARE Y SISTEMA DE HARDWARE DE DM	
Subobjetivo	Fundamento jurídico
Para procesar los pagos cuando los Profesionales de la salud se suscriben a los Productos y servicios de software o compran Sistemas de hardware de DM	El Tratamiento nº3 es necesario para la ejecución de un contrato en el que participe el Profesional de la salud (Titular de datos) (artículo 6.1 (b) del RGPD) o para el cumplimiento de sus obligaciones legales (artículo 6.1 (c) del RGPD), como la legislación y reglamentos fiscales.
Para proceder al envío de los pedidos	
Para cumplir con las obligaciones contables y legales de DM	
TRATAMIENTO nº4: EL OBJETIVO PRINCIPAL ES MEJORAR LOS PRODUCTOS Y SERVICIOS DE SOFTWARE Y SISTEMAS DE HARDWARE DE DM	
Subobjetivo	Fundamento jurídico
Para mejorar los Productos y servicios de software de DM y desarrollar nuevas funcionalidades	El tratamiento nº4 se basa en el interés legítimo de DM por mejorar la calidad de los servicios sanitarios (artículo 6.1 (f) del RGPD).
Para enviar encuestas a los Profesionales de la salud con el fin de recopilar experiencias y optimizar los Productos y servicios de software de DM	
TRATAMIENTO nº5: EL OBJETIVO PRINCIPAL ES PROTEGER LOS PRODUCTOS Y SERVICIOS DE SOFTWARE Y SISTEMAS DE HARDWARE DE DM	
Subobjetivo	Fundamento jurídico
Para garantizar la seguridad, confidencialidad, integridad y disponibilidad de los Productos y servicios de software de DM	El tratamiento nº5 se basa en el interés legítimo de DM por mejorar la calidad de los servicios sanitarios y cumplir con las leyes de protección de datos (artículo 6.1 (f) del GDPR)
TRATAMIENTO nº6: EL OBJETIVO PRINCIPAL ES MEJORAR LAS RELACIONES CON EL PROFESIONAL DE LA SALUD	
Subobjetivo	Fundamento jurídico
Para mantener una buena relación comercial con el Profesional de la salud a través de concursos, programas de fidelidad, patrocinios y descuentos	El tratamiento nº6 se basa en el interés legítimo de DM por mejorar la calidad de los servicios sanitarios y cumplir con las leyes de protección de datos (artículo 6.1 (f) del GDPR)

DATOS DE LOS PACIENTES

DM trata los Datos personales de los Pacientes con las siguientes finalidades y sobre la base de los siguientes fundamentos jurídicos:

TRATAMIENTO n°1: EL OBJETIVO PRINCIPAL ES SUMINISTRAR LOS PRODUCTOS Y SERVICIOS DE SOFTWARE DM (MONITORING, ENGAGE, SMART STL)	
Subobjetivo	Fundamento jurídico
Para configurar y gestionar las cuentas de los Pacientes (solo para MONITORING y ENGAGE)	El Tratamiento n°1 es necesario para la ejecución de cualquier contrato en el que participe el Profesional de la salud (Sujeto de datos) (artículo 6.1 (b) del RGPD) y depende del consentimiento explícito del Paciente obtenido mediante la lectura y aceptación del formulario de consentimiento del Paciente (artículo 9.2.2 (a) del RGPD) <i>Tenga en cuenta que, al contratar con organizaciones o entidades públicas (como hospitales), DM se basa en el consentimiento del Paciente para el tratamiento de sus datos personales; es posible que las organizaciones públicas que supervisan los tratamientos de los Pacientes no se basen en el consentimiento, sino en la «función pública», de conformidad con las normativas específicas y locales en materia de privacidad.</i>
Para contactar por teléfono o enviar mensajes (por SMS, WhatsApp, correo electrónico o notificaciones) a los Pacientes en nombre de su Profesional de la salud para recordarles que envíen sus escaneos (tratamiento basado en IA para el envío de notificaciones si los Profesional de la salud deciden utilizar herramientas de comunicación basadas en IA para comunicar con sus pacientes) (solo para MONITORING).	
Para que los profesionales de la salud puedan supervisar de forma remota los tratamientos de ortodoncia y la salud bucodental de sus pacientes y ayudarles a tomar decisiones sobre los tratamientos de sus pacientes, proporcionar apoyo analítico y optimizar los resultados de los tratamientos (tratamiento basado en IA) (solo para MONITORING).	
Para proporcionar al Profesional de la salud y a sus Pacientes una evaluación de: ○ la salud de los dientes ○ la salud de las encías ○ la alineación de los dientes (Tratamiento basado en IA) (solo para ENGAGE)	
TRATAMIENTO n°2: EL OBJETIVO PRINCIPAL ES GESTIONAR LOS TICKETS DE LOS PACIENTES (COMENTARIOS/QUEJAS/PREGUNTAS) ENVIADOS A LOS SERVICIOS DE ATENCIÓN AL CLIENTE EN RELACIÓN CON CUALQUIERA DE LOS PRODUCTOS Y SERVICIOS DE SOFTWARE DE DM	
Subobjetivo	Fundamento jurídico
Para gestionar los comentarios, quejas y reclamaciones de Pacientes	El Tratamiento n°2 es necesario para la ejecución de cualquier contrato en el que

Para transferir las solicitudes de datos personales al equipo encargado de la privacidad	participe el Profesional de la salud (Sujeto de datos) (artículo 6.1 (b) del RGPD) o cumplir sus obligaciones legales (artículo 6.1 (c) del RGPD) como la transferencia de solicitudes de acceso a los datos privados.
Para mejorar la calidad y la rapidez de la atención al cliente que DM ofrece a los pacientes	
TRATAMIENTO nº3: EL OBJETIVO PRINCIPAL ES MEJORAR LOS PRODUCTOS Y SERVICIOS DE SOFTWARE Y SISTEMAS DE HARDWARE DE DM	
Subobjetivo	Fundamento jurídico
Para mejorar los Productos y servicios de software de DM y desarrollar nuevas funcionalidades, para entrenar los sistemas de IA a fin de mejorar el funcionamiento interno (tratamiento basado en IA)	El Tratamiento nº3 se basa en el interés legítimo de DM por mejorar la calidad de los servicios sanitarios (artículo 6.1 (f) del RGPD) y/o en el consentimiento explícito del Paciente obtenido mediante la lectura y aceptación del formulario de consentimiento del Paciente (artículo 9.2.2 (a) del RGPD)
Para enviar encuestas a los Pacientes con el fin de recopilar experiencias y optimizar los Productos y servicios de DM	
Hacer algunos estudios o estadísticas sobre el desempeño de los Productos y Servicios de DM (excluyendo estudios clínicos) con el fin de optimizar los Productos y Servicios de DM (dichas estadísticas se basan en datos de Pacientes, pero generan resultados agregados y datos relacionados con el uso de los Productos y Servicios de DM por parte de los Profesionales de la salud; excluyen datos personales).	
TRATAMIENTO nº4: EL OBJETIVO PRINCIPAL ES ILUSTRAR CASOS DE PACIENTES EN PRESENTACIONES O EN CUENTAS DEMO	
Subobjetivo	Fundamento jurídico
Para ilustrar seminarios web, presentaciones de los Productos y servicios de software de DM (solo en casos concretos y cuando sea apropiado para ilustrar casos específicos, nunca para todos los Pacientes en general)	El tratamiento nº4 se basa en el interés legítimo de DM por mejorar la calidad de los servicios sanitarios (artículo 6.1 (f) del RGPD).
TRATAMIENTO nº5: EL OBJETIVO PRINCIPAL ES PROTEGER LOS PRODUCTOS Y SERVICIOS DE SOFTWARE Y SISTEMAS DE HARDWARE DE DM	
Subobjetivo	Fundamento jurídico
Para garantizar la seguridad, confidencialidad, integridad y disponibilidad de los Productos y servicios de software de DM	El tratamiento nº5 se basa en el interés legítimo de DM por mejorar la calidad de los servicios sanitarios y cumplir con las leyes de protección de datos (artículo 6.1 (f) del GDPR)

Procesamiento basado en IA

Algunos datos personales (incluidos datos de salud) pueden procesarse utilizando sistemas de inteligencia artificial («IA») para facilitar la monitorización del tratamiento, mejorar la precisión del servicio y ayudar a los Profesionales de la salud, tal y como se describe en la lista de tratamientos anterior (véanse los tratamientos nº 1 y nº 3 para Pacientes). Estos sistemas de IA están diseñados para ayudar a los Profesionales de la salud proporcionándoles información o recomendaciones automatizadas basadas en los datos recopilados en relación con los tratamientos dentales a distancia, los tratamientos de ortodoncia y los controles bucodentales de los Pacientes.

Los resultados generados por los productos y servicios de software de DM están pensados para ser utilizados como soporte durante el diagnóstico, con el fin de respaldar el criterio clínico de profesionales dentales cualificados, y no como única base para la toma de decisiones clínicas.

ARTÍCULO 8: ¿CÓMO COMPARTIMOS LOS DATOS PERSONALES?

Uso interno: Los Datos personales de los Profesionales de la salud y de los Pacientes podrán ser tratados por los empleados de DM (dentro de los límites de sus respectivas facultades y solo cuando sea necesario) y de sus filiales y empresas del grupo, exclusivamente para alcanzar las finalidades de esta Política de privacidad.

Uso externo: DM podrá compartir los Datos personales (solo cuando sea apropiado y en la medida en que lo permita la legislación aplicable) con los siguientes tipos de terceros:

DATOS DE LOS PROFESIONALES DE LA SALUD

Proveedores técnicos	● Proveedores de servicios en la nube y de almacenamiento (AWS) ● Proveedores de redes y telecomunicaciones ● Proveedores de mantenimiento ● Proveedores de servicios de seguridad ● Proveedores de sistemas de gestión de la propiedad (cuando proceda)
Procesadores de pago	● Procesador de pagos con tarjeta de crédito (Stripe) ● Procesador de pagos por domiciliación bancaria (GoCardless) ● Bancos de DM
Proveedores externos utilizados por los Profesionales de la salud	● Fabricantes de alineadores y proveedores de servicios PMS utilizados por los Profesionales de la salud.
Proveedores de servicios de marketing	● Software de gestión de la relación con el cliente ● Software de automatización del marketing
Autoridades	● Autoridades legales y administrativas

DATOS DE LOS PACIENTES

Proveedores técnicos	● Proveedores de servicios en la nube y de almacenamiento (AWS) ● Proveedores de redes y telecomunicaciones ● Proveedores de mantenimiento ● Proveedores de servicios de seguridad
Procesadores de pago	● Procesador de pagos con tarjeta de crédito (Stripe)
Proveedores externos utilizados por los Profesionales de la salud	● Fabricantes de alineadores y proveedores de servicios PMS utilizados por los Profesionales de la salud
Autoridades	● Autoridades legales y administrativas

DM garantiza que las transferencias a estos terceros son seguras y siguen un estricto proceso de conformidad con la norma ISO 27001 para verificar que cuentan con las medidas organizativas y técnicas necesarias para cumplir con los requisitos legales de protección de datos, las normas de seguridad y los estándares de calidad pertinentes.

Algunos de estos terceros pueden estar en el extranjero o pueden alojar los datos del paciente en el extranjero. Para este tipo de transferencias de datos transfronterizas, DM ha establecido cláusulas contractuales específicas de privacidad de datos con el fin de garantizar que estos terceros apliquen medidas de protección a los Datos personales del Paciente que respeten los requisitos legales del país del Paciente.

ARTÍCULO 9. ¿DÓNDE ALMACENAMOS SUS DATOS PERSONALES?

Los Productos y servicios de software están alojados en los servicios en la nube Amazon Web Service Inc (AWS), con servidores en diferentes lugares alrededor del mundo, con el fin de almacenar los Datos Personales a nivel local, en Europa, EE.UU., Japón y la región APAC, en función del lugar de residencia del Paciente.

Los servidores de AWS cumplen con las normas ISO 27001 y HDS/HDH y las sedes de almacenamiento de Datos personales cumplen con la normativa de cada país donde opera DM.

ARTÍCULO 10. ¿CUÁNTO TIEMPO ALMACENAMOS SUS DATOS PERSONALES?

Conservamos los Datos personales de los Profesionales de la salud y Pacientes durante el tiempo que requieren los fines para los que fueron recogidos, cumpliendo con las leyes y reglamentos aplicables.

ARTÍCULO 11. ¿CUÁLES SON SUS DERECHOS EN MATERIA DE PROTECCIÓN DE DATOS?

¿CÓMO PUEDE EJERCER SUS DERECHOS?

Las leyes de Protección de datos otorgan derechos a los ciudadanos europeos en lo referente a sus Datos personales. Puesto que el RGPD es considerado mundialmente como la norma de referencia en materia de protección de datos personales, DM permite a sus usuarios de todo el mundo beneficiarse de estos derechos (algunos de estos derechos pueden estar limitados por leyes y reglamentos locales aplicables en determinadas circunstancias). Los derechos son:

- **Derecho de acceso** es el derecho a saber si sus datos personales están siendo tratados y, en tal caso, a poder acceder a los Datos personales y a la siguiente información: los fines del tratamiento, las categorías de Datos personales en cuestión, los destinatarios o categorías de destinatarios a los que se han comunicado o se comunicarán los Datos personales,

especialmente destinatarios de países terceros u organizaciones internacionales, etc.

- **Derecho de rectificación**, sin demoras injustificadas, de cualquier Dato personal inexacto, incompleto, obsoleto que le concierna, o cuya recopilación esté prohibida;
- **Derecho de oposición** es el derecho a oponerse antes de un Tratamiento de Datos personales realizado por el Responsable del tratamiento o de una transferencia de Datos personales, salvo que existan razones legítimas e ineludibles que prevalezcan sobre sus intereses;
- **Derecho de supresión** es el derecho a solicitar al Responsable del tratamiento la supresión de sus datos personales sin demora injustificada, lo que obliga al Responsable del tratamiento a suprimir sus Datos personales sin demora injustificada siempre que se aplique alguno de los siguientes fundamentos:
 - Los datos personales ya no son necesarios para cumplir con las Finalidades;
 - Usted revoca el consentimiento sobre el que se basa el Tratamiento de acuerdo con el artículo 6, apartado 1, letra a, o el artículo 9, apartado 2, letra a, y no existe ningún otro fundamento jurídico para el Tratamiento;
 - Usted se opone al Tratamiento de acuerdo con el artículo 21(1) y no existen motivos legítimos prevalentes para el Tratamiento o DM se opone al Tratamiento de acuerdo con el artículo 21(2);
 - Los Datos personales han sido tratados ilegalmente;
 - Los Datos Personales deben ser borrados para cumplir con una obligación legal de la legislación de la Unión Europea o de los Estados miembros, a la que está sujeto el Responsable del tratamiento;
 - Los Datos personales se han recogido como parte de la oferta de servicios de la sociedad de la información contemplados en el artículo 8, apartado 1.
- **Derecho a la portabilidad**, es decir, el derecho a recibir los Datos Personales que usted ha facilitado a un Responsable del tratamiento, en un formato estructurado, de uso común y legible por máquina, y a poder transmitir esos datos a otro Responsable del tratamiento sin que el Responsable del tratamiento al que se han facilitado originalmente los Datos personales ponga trabas, siempre que:
 - (a) El Tratamiento se base en el consentimiento de conformidad con el artículo 6, apartado 1, letra a, o el artículo 9, apartado 2, letra a, o bien con un contrato con arreglo al artículo 6, apartado 1, letra b; y
 - b) El Tratamiento se realice por medios automatizados.
- Derecho a oponerse y solicitar información sobre la toma de decisiones individuales automatizada (IA).

Usted puede solicitar información para saber si los sistemas de IA han procesado sus datos y de qué manera lo han hecho. Usted tiene derecho a obtener información relevante sobre la lógica utilizada y las posibles consecuencias de dicho tratamiento. Puede solicitar la intervención humana o la revisión de cualquier resultado asistido por IA que le concierna.

- Derecho a presentar una reclamación ante la Autoridad de control, si considera que el Tratamiento de los Datos personales que le conciernen infringe las leyes de Protección de datos.

Para cualquier reclamación, puede presentar una queja ante la autoridad nacional de control («**Autoridad de control**») responsable de la protección de Datos personales, a saber, **la Agencia Española de Protección de Datos «AEPD» en España.**

Todos los usuarios de otros países, incluidos los estadounidenses, pueden consultar las leyes de su jurisdicción para obtener más información sobre sus derechos y sobre la Autoridad de control. Por ejemplo:

- HIPAA y cualquier otra ley estatal o territorial relativa a la protección de la Privacidad de los ciudadanos estadounidenses;
- Ley Federal de Privacidad de 1988 (Federal Privacy Act 1988) y cualquier otra ley estatal y territorial, incluidas, sin carácter exhaustivo, las siguientes: Information Privacy Act 2014 (Territorio de la Capital Australiana), Information Act 2002 (Territorio del norte), Privacy and Personal Information Protection Act 1998 (Nueva Gales del Sur) Information Privacy Act 2009 (Queensland), Personal Information Protection Act 2004 (Tasmania) y Privacy and Data Protection Act 2014 (Victoria) para los ciudadanos australianos;
- Leyes federales y estatales o territoriales, como la Ley de Protección de la Información Personal y los Documentos Electrónicos (PIPEDA), la Ley de Protección de la Información Personal (Alberta) (PIPA Alberta), la Ley de Protección de la Información Personal (Columbia Británica) (PIPA BC) y la Ley de Protección de la Información Personal en el Sector Privado (Ley de Privacidad de Quebec) para ciudadanos canadienses.
- el GDPR del Reino Unido y las leyes de protección de datos de los ciudadanos británicos. etc.

Para ejercer cualquiera de sus derechos, puede enviar una solicitud:

- Por correo electrónico a la siguiente dirección: privacy@dental-monitoring.com.
- Por carta a la siguiente dirección: Data Protection Officer - Dental Monitoring SAS, 75 rue de Tocqueville, 75017 París, Francia

En caso de que usted ejerza alguno de sus derechos por vía electrónica, DM le facilitará los Datos personales, cuando proceda, por vía electrónica, en la medida de lo posible, salvo que usted haya solicitado expresamente que se proceda de otro modo.

Los Profesionales de la salud y Pacientes deben especificar la naturaleza de su solicitud en el asunto del correo electrónico e incluir los detalles de la solicitud en el propio correo electrónico. Es posible que DM solicite información adicional al Profesional de la salud o al Paciente, para verificar su identidad, antes de seguir adelante con la solicitud.

ARTÍCULO 12. ¿CÓMO SE PROTEGEN Y ASEGURAN SUS DATOS PERSONALES?

DM ha tomado medidas para que los Profesionales de la salud y sus Pacientes puedan estar seguros de que sus Datos personales están a salvo cuando utilizan los Productos y servicios de software de DM y, de manera general, cuando sus Datos personales son tratados por DM.

Existen medidas de seguridad técnicas, organizativas y estructurales para proteger sus Datos personales contra el acceso, divulgación, alteración, pérdida o destrucción accidental, no autorizada o ilegal y, por lo tanto, para garantizar la seguridad, integridad y confidencialidad de sus Datos personales.

DM desarrolla sus sistemas bajo el principio de "privacidad por diseño".

También cumplimos con los principios de minimización de datos y hemos establecido las siguientes medidas:

- Técnicas de seudonimización y anonimización siempre que sean técnicamente viables; y
- Restricción del acceso a los Datos personales exclusivamente para los empleados que necesitan acceder a los Datos personales para llevar a cabo los servicios previstos en la descripción del servicio, garantizada mediante una revisión periódica de los derechos de acceso por parte del departamento informático.

Hemos implementado medidas de seguridad informática de última generación para proteger sus Datos personales y realizamos periódicamente pruebas de penetración para detectar cualquier

incidente a causa de una vulnerabilidad.

En caso de incidente, DM investigará el incidente y llevará a cabo una evaluación de riesgos para determinar nuestro curso de acción de cara al futuro. DM ha implementado una política específica que hace referencia a un procedimiento específico para el tratamiento de incidentes relacionados con Datos Personales.

Dependiendo de los resultados de esta evaluación, DM tomará todas las medidas y acciones necesarias y necesarias para cumplir con las leyes y reglamentos aplicables, que pueden incluir la notificación a los usuarios afectados en caso de un riesgo más alto contra sus derechos y libertades, la notificación a las Autoridades de Supervisión si es necesario, etc.

ARTÍCULO 13. ¿PUEDE MODIFICARSE LA POLÍTICA DE PRIVACIDAD?

DM puede ocasionalmente actualizar la Política de privacidad y, en tal caso, notificará a los Profesionales de la salud y Pacientes de cualquier cambio significativo en la forma en que tratamos los Datos personales a través de un comunicado. Le recomendamos que revise periódicamente esta página para obtener la información más reciente sobre nuestras políticas de privacidad.