Política de Privacidad - TuM²

Versión 1.0 | Vigencia: 19 de mayo de 2026 | Última revisión: 19 de mayo de 2026

Versión: 1.0

Fecha de vigencia: 19 de mayo de 2026

Última revisión: 19 de mayo de 2026

Aplicable a: aplicación mobile, web pública, panel de comercios, panel administrativo y servicios asociados de TuM².

TuM², también identificado como Tu metro cuadrado, es una plataforma hiperlocal orientada a ayudar a vecinos, vecinas y usuarios a descubrir comercios, servicios y datos operativos de cercanía. Su propuesta es: **Lo que necesitás, en tu zona.**

Esta Política de Privacidad explica qué datos podemos tratar, para qué fines, qué información puede mostrarse públicamente, cómo protegemos la información, con qué proveedores podemos operar y cuáles son los derechos de las personas titulares de datos.

El tratamiento de datos se realiza conforme a esta Política, a los Términos y Condiciones aplicables y a las bases legales correspondientes según el tipo de interacción con TuM².

1. Identificación del responsable del tratamiento

Campo	Dato
Responsable del tratamiento	Ziegler Pablo
CUIT	20-37059179-3
Domicilio legal	Constancio C. Vigil 150, Carlos Spegazzini, Ezeiza, B1812, Provincia de Buenos Aires, Argentina
Email de privacidad	privacidad@tum2.com.ar

Campo	Dato
Email legal	legal@tum2.com.ar
Email de seguridad	seguridad@tum2.com.ar
Email de soporte	soporte@tum2.com.ar

A los efectos de esta Política, TuM² actúa como responsable del tratamiento respecto de los datos personales que recopila y utiliza para operar la plataforma, salvo en aquellos casos en que actúe en otra calidad conforme a una relación contractual o técnica específica.

2. Alcance

Esta Política aplica a:

• la aplicación mobile de TuM²;
• la web pública;
• el panel de comercios;
• el panel administrativo;
• formularios, reportes y canales de soporte;
• comunicaciones operativas;
• servicios técnicos, funciones cloud, hosting, autenticación, almacenamiento, analítica, notificaciones y monitoreo asociados a TuM².

Esta Política alcanza, según corresponda, a:

• visitantes de la web;
• usuarios registrados;
• usuarios invitados o anónimos que consultan información pública;
• titulares, responsables, empleados o representantes de comercios;
• personas que reclaman titularidad de comercios;
• farmacias y responsables operativos de guardias;
• personas que reportan errores, reclamos o sugerencias;
• administradores, moderadores y personal autorizado de TuM².

3. Principios de privacidad aplicados por TuM²

TuM² procura aplicar criterios de privacidad desde el diseño y por defecto. En particular:

• minimización de datos: pedimos y conservamos solo lo necesario para cada finalidad;
• separación entre información pública e información privada;
• escritura controlada de datos públicos mediante procesos backend autorizados;
• uso de roles y permisos para limitar accesos;
• auditoría de acciones relevantes;
• reducción de exposición de datos sensibles o documentación respaldatoria;
• uso de mecanismos de seguridad, rate limiting, App Check y validaciones server-side cuando corresponda;
• separación de ambientes de desarrollo, staging y producción.

La información pública de comercios se gestiona de forma separada de la información privada o administrativa. Los datos públicos del comercio no deben escribirse directamente desde el cliente cuando correspondan a proyecciones calculadas, estados derivados o campos controlados por backend.

4. Datos que podemos tratar

TuM² puede tratar distintas categorías de datos según el uso que cada persona haga del servicio.

4.1. Datos de cuenta y autenticación

Podemos tratar:

• identificador interno de usuario;
• email;
• nombre, si se informa;
• foto de perfil, si se informa;
• proveedor de autenticación;
• rol o segmento de usuario;
• estado de sesión;
• fecha de alta, última actividad y eventos de seguridad asociados.

4.2. Datos de contacto y soporte

Podemos tratar:

• email de contacto;
• teléfono, si el usuario lo informa;
• mensajes enviados a soporte;
• reportes, reclamos, sugerencias o comunicaciones operativas;

• historial de atención y resolución.

4.3. Datos de titulares o responsables de comercios

Cuando una persona reclama, administra o representa un comercio, podemos tratar:

• email autenticado;
• nombre y apellido;
• teléfono opcional;
• relación declarada con el comercio;
• datos de contacto operativo;
• documentación respaldatoria;
• CUIT, CUIL u otra identificación cuando sea necesaria para validar titularidad o prevenir fraude;
• historial de reclamos de titularidad;
• estado de revisión;
• notas internas de soporte, moderación y auditoría.

El CUIT, CUIL, la documentación respaldatoria y las evidencias de titularidad no se publican en fichas públicas de comercios.

4.4. Datos públicos de comercios

Pueden mostrarse públicamente, cuando corresponda:

• nombre comercial;
• rubro o categoría;
• dirección o zona;
• ubicación aproximada o georreferenciada del comercio;
• horarios informados;
• estado operativo, como abierto ahora, cerrado o en revisión;
• estado de farmacia de turno o guardia cuando corresponda;
• teléfono comercial público;
• enlaces públicos informados;
• imágenes comerciales cargadas;
• medios de pago, productos, servicios o atributos visibles;
• fuente pública o método de carga cuando sea relevante.

4.5. Datos de ubicación

TuM² puede tratar:

• zona seleccionada manualmente por el usuario;
• ubicación aproximada;
• ubicación precisa solo cuando el usuario otorgue permiso desde el dispositivo;
• distancia estimada a comercios o servicios cercanos.

4.6. Datos técnicos, analíticos y de rendimiento

Podemos tratar:

• tipo de dispositivo;
• sistema operativo;
• versión de app;
• identificadores técnicos de instalación o sesión cuando resulten necesarios para seguridad, estabilidad o diagnóstico;
• eventos de uso;
• pantallas visitadas;
• búsquedas dentro de la app;
• errores, crashes y diagnósticos;
• rendimiento, latencia y estabilidad;
• información necesaria para detectar abuso, fraude o uso indebido.

4.7. Datos de seguridad, antifraude y abuso

Podemos tratar información técnica destinada a:

• autenticar usuarios;
• prevenir abuso;
• evitar automatizaciones maliciosas;
• limitar escrituras excesivas;
• detectar intentos de fraude;
• proteger comercios, usuarios y datos internos;
• auditar acciones sensibles.

Esto puede incluir logs, marcas temporales, hashes, fingerprints técnicos, pseudónimos internos, identificadores de dispositivo o navegador y otros mecanismos técnicos razonables. Cuando utilizamos hashes, fingerprints o mecanismos pseudonimizados, estos se emplean para reducir riesgos y limitar identificación directa. Sin embargo, ciertos datos pseudonimizados podrían seguir considerándose datos personales conforme la normativa aplicable.

5. Finalidades del tratamiento

Podemos utilizar los datos para:

• operar y mantener TuM²;
• autenticar usuarios;
• administrar cuentas y roles;
• mostrar comercios cercanos y datos relevantes por zona;
• permitir búsquedas, favoritos, reportes y otras funcionalidades;
• validar reclamos de titularidad de comercios;
• moderar información pública;
• publicar información operativa de comercios cuando corresponda;
• administrar farmacias de turno y datos de disponibilidad;
• responder consultas de soporte;
• enviar comunicaciones operativas;
• enviar notificaciones técnicas o de seguridad;
• medir rendimiento, estabilidad y uso general del servicio;
• detectar errores, diagnosticar fallas y mejorar la app;
• prevenir fraude, abuso o accesos no autorizados;
• cumplir obligaciones legales o requerimientos de autoridad competente;
• proteger derechos, seguridad e integridad de usuarios, comercios y TuM².

TuM² no utiliza datos personales para vender información a terceros.

5.1. Contenido contextual, campañas y comercios destacados

TuM² puede mostrar contenido contextual o estacional relacionado con fechas, eventos públicos o momentos de interés para la comunidad, como tarjetas informativas, accesos destacados o superficies promocionales dentro de la aplicación o la web.

En algunos casos, estas superficies pueden incluir comercios locales destacados o espacios patrocinados. Para medir su funcionamiento y mejorar la experiencia, TuM² puede registrar métricas agregadas o técnicas, como visualizaciones de tarjeta, clicks en CTA, clicks en comercio destacado, zona aproximada o `zoneId`, estado de la tarjeta como `lead`, `starts_soon`, `live` o `finalized`, e identificadores internos de campaña. Estas métricas se utilizan para análisis operativo, mejora del producto y medición de campañas.

Para este tipo de medición, TuM² procura evitar incluir en analytics de campaña datos personales directos como nombre, email, teléfono, ubicación precisa o identificadores individuales de usuario compartidos con fines publicitarios. La interacción con un comercio destacado puede dirigir al usuario a una ficha pública dentro de TuM². La disponibilidad de

productos, servicios, horarios o atención del comercio puede variar y depende del propio comercio.

Los datos públicos de comercios destacados o patrocinantes pueden incluir nombre comercial, categoría, zona, imagen pública e indicadores agregados de impresiones o clicks. TuM² no comparte con los comercios patrocinantes datos personales directos de los usuarios, salvo consentimiento expreso, requerimiento legal aplicable o necesidad operativa debidamente justificada.

Las métricas de campaña, rendimiento y diagnóstico se conservan durante el plazo definido por la configuración del proveedor, criterios internos de minimización, necesidades operativas y eventuales procesos de agregación, anonimización o auditoría.

6. Bases legales y criterios de legitimación

El tratamiento de datos puede basarse, según el caso, en:

• consentimiento del usuario;
• ejecución de una relación contractual o precontractual;
• cumplimiento de obligaciones legales;
• interés legítimo relacionado con seguridad, prevención de fraude, estabilidad técnica, soporte, auditoría, mejora del servicio y protección de la plataforma;
• información suministrada voluntariamente por el usuario o por responsables de comercios.

Cuando una funcionalidad requiera consentimiento específico, TuM² procurará solicitarlo de forma clara y permitir su revocación cuando corresponda.

El uso de métricas técnicas, analítica y diagnósticos se realiza procurando minimizar identificación directa, limitar la información recolectada y mantener consistencia con las declaraciones de privacidad de tiendas de aplicaciones y plataformas de distribución.

7. Geolocalización

TuM² puede utilizar ubicación para mostrar comercios cercanos, farmacias de turno, resultados por zona y contenido hiperlocal.

La ubicación puede obtenerse de tres formas:

• selección manual de zona por parte del usuario;
• ubicación aproximada derivada del uso del servicio;
• ubicación precisa del dispositivo, solo si el usuario otorga el permiso correspondiente.

El usuario puede revocar permisos de ubicación desde la configuración del dispositivo. Algunas funcionalidades podrían verse limitadas si no se otorgan permisos de ubicación, aunque TuM² procurará permitir selección manual de zona cuando sea posible.

8. Información pública y privada de comercios

TuM² distingue entre información pública de comercios e información privada o administrativa.

La información pública puede ser consultada por usuarios, visitantes o clientes finales. Incluye datos necesarios para descubrir, contactar o visitar comercios.

La información privada o administrativa puede incluir evidencia de titularidad, documentos, notas internas, historial de moderación, datos de seguridad, reportes, identificadores internos y otros datos no destinados a publicación.

Las transiciones de estado, roles, visibilidad, verificación y titularidad deben realizarse mediante procesos autorizados, auditables y controlados por backend cuando corresponda.

9. Cookies y tecnologías similares

La web de TuM² puede utilizar cookies, almacenamiento local, identificadores técnicos o tecnologías similares.

Estas tecnologías pueden cumplir finalidades como:

• funcionamiento esencial del sitio;
• seguridad;
• mantenimiento de sesión;
• preferencias del usuario;
• analítica y rendimiento;
• diagnóstico de errores;
• medición agregada de uso.

Cuando la web utilice cookies o tecnologías no estrictamente necesarias, TuM² procurará informar al usuario y, cuando corresponda, ofrecer mecanismos de configuración o rechazo conforme la normativa aplicable.

TuM² no utiliza cookies publicitarias ni identificadores publicitarios para publicidad personalizada en esta versión de la Política. Si en el futuro se incorporan publicidad, remarketing, medición publicitaria o personalización avanzada, esta Política deberá

actualizarse y se deberán implementar los consentimientos y controles aplicables.

10. Notificaciones push y comunicaciones

TuM² puede enviar notificaciones push, emails u otras comunicaciones para finalidades operativas, técnicas o de seguridad.

Estas comunicaciones pueden incluir:

• alertas de cuenta o seguridad;
• novedades relevantes del servicio;
• confirmaciones operativas;
• cambios de estado de reclamos de titularidad;
• avisos relacionados con comercios administrados;
• alertas de farmacias de turno o disponibilidad cuando el usuario haya activado esa funcionalidad;
• avisos de incidentes, errores o cambios importantes.

Las comunicaciones no esenciales o promocionales podrán ser desactivadas cuando corresponda. Las comunicaciones estrictamente necesarias para seguridad, funcionamiento de cuenta o cumplimiento legal podrían seguir enviándose aunque el usuario desactive comunicaciones promocionales.

El usuario también puede gestionar permisos de notificaciones desde la configuración de su dispositivo.

11. Proveedores tecnológicos y terceros

TuM² puede utilizar proveedores tecnológicos para operar la plataforma. Estos proveedores pueden prestar servicios de:

• autenticación;
• base de datos;
• almacenamiento;
• hosting;
• funciones serverless;
• analítica;
• crash reporting;
• mapas, geocodificación o búsqueda de lugares;
• notificaciones push;

• seguridad y prevención de abuso;
• soporte técnico y monitoreo.

Entre los proveedores utilizados o previstos pueden incluirse servicios de Google Firebase, Google Cloud, Google Maps Platform, Google Places API y otros proveedores equivalentes o complementarios.

Los proveedores actúan, según corresponda, como encargados de tratamiento, subencargados o prestadores de infraestructura técnica, y solo deberían acceder a los datos necesarios para prestar sus servicios.

TuM² no vende datos personales a terceros. Tampoco comparte datos personales directos con anunciantes o comercios patrocinantes por la mera visualización o interacción con tarjetas contextuales o espacios destacados.

12. Transferencias internacionales

Algunos proveedores tecnológicos utilizados por TuM² pueden almacenar, procesar o respaldar información en servidores ubicados fuera de la República Argentina.

Cuando ello ocurra, TuM² procurará adoptar medidas razonables de protección, incluyendo acuerdos contractuales, controles técnicos, minimización de datos y selección de proveedores con estándares de seguridad adecuados.

El uso de TuM² puede implicar que determinados datos sean tratados en jurisdicciones distintas a la Argentina, siempre para las finalidades descriptas en esta Política y en el marco de los servicios tecnológicos necesarios para operar la plataforma.

13. Conservación de datos

TuM² conserva los datos personales durante el tiempo necesario para cumplir las finalidades descriptas en esta Política, operar el servicio, cumplir obligaciones legales, resolver disputas, prevenir fraude, auditar acciones sensibles y proteger la seguridad de la plataforma.

Criterios orientativos de conservación:

• datos de cuenta: mientras la cuenta permanezca activa y durante un período razonable posterior para seguridad, auditoría o cumplimiento legal;
• datos de autenticación y roles: mientras resulten necesarios para administrar permisos y seguridad;

• evidencias de reclamos de titularidad: mientras el reclamo esté activo y durante el plazo necesario para auditoría, defensa ante reclamos o prevención de fraude;
• reportes, reclamos y soporte: durante el plazo necesario para resolver el caso y mantener historial operativo razonable;
• logs técnicos y de seguridad: durante el plazo necesario para prevenir abuso, investigar incidentes y mantener integridad de la plataforma;
• analytics y diagnósticos: durante el plazo definido por la configuración del proveedor y criterios internos de minimización;
• backups: durante los ciclos técnicos de respaldo y recuperación definidos por TuM² o sus proveedores.

Cuando los datos dejen de ser necesarios, podrán eliminarse, anonimizarse, agregarse, bloquearse o conservarse de forma restringida cuando exista una justificación legal, técnica o de seguridad.

14. Derechos de los titulares de datos

Las personas titulares de datos personales pueden ejercer los derechos previstos por la Ley 25.326 y normativa complementaria, incluyendo, según corresponda:

• acceso;
• rectificación;
• actualización;
• supresión;
• confidencialidad;
• retiro del consentimiento cuando el tratamiento se base en consentimiento.

Las solicitudes pueden enviarse a: privacidad@tum2.com.ar

Para ejercer un derecho, TuM² podrá solicitar información razonable para verificar la identidad del solicitante y evitar accesos o modificaciones no autorizadas.

Como referencia operativa inicial, TuM² procurará responder solicitudes de acceso, rectificación, actualización o supresión dentro de los plazos que resulten aplicables según la normativa vigente.

La Agencia de Acceso a la Información Pública, órgano de control de la Ley 25.326, tiene la atribución de atender denuncias y reclamos vinculados con incumplimientos en materia de protección de datos personales.

15. Seguridad de la información

TuM² adopta medidas técnicas y organizativas razonables destinadas a proteger la información contra accesos no autorizados, pérdida, uso indebido, alteración o divulgación no autorizada.

Las medidas pueden incluir:

• autenticación segura;
• control de acceso por roles;
• reglas de seguridad en base de datos;
• validaciones server-side;
• App Check u otros mecanismos anti-abuso;
• registros de auditoría;
• segregación entre datos públicos y privados;
• cifrado en tránsito cuando corresponda;
• controles de acceso administrativo;
• monitoreo de errores e incidentes.

Ningún sistema es absolutamente seguro. TuM² procura mejorar continuamente sus medidas de seguridad conforme evoluciona el producto.

16. Incidentes de seguridad

Ante incidentes de seguridad que puedan afectar datos personales, TuM² podrá adoptar medidas razonables de:

• detección;
• contención;
• investigación;
• mitigación;
• recuperación;
• comunicación a usuarios o autoridades cuando corresponda;
• documentación interna y aprendizaje preventivo.

La comunicación de un incidente dependerá de su naturaleza, alcance, riesgo potencial, datos afectados y obligaciones legales aplicables.

17. Menores de edad

TuM² no está dirigido específicamente a menores de edad.

Cuando la normativa aplicable lo requiera, el uso por menores deberá contar con autorización de sus representantes legales.

Si TuM² detecta tratamiento indebido de datos de menores o recibe una solicitud fundada de un representante legal, podrá adoptar medidas razonables para restringir, eliminar o bloquear información conforme corresponda.

18. Farmacias, guardias y disponibilidad operativa

TuM² puede mostrar información sobre farmacias, guardias, horarios, turnos, disponibilidad y estado operativo de comercios.

Esa información puede provenir de fuentes públicas, cargas manuales, responsables de comercios, administradores, procesos de importación o validaciones internas. Aun aplicando controles razonables, la información puede variar sin previo aviso, quedar desactualizada o contener errores, demoras u omisiones.

La información sobre farmacias de turno, horarios o disponibilidad no constituye consejo médico, indicación sanitaria, servicio de emergencia ni reemplazo de fuentes oficiales.

Antes de tomar decisiones médicas, sanitarias, urgentes o sensibles, se recomienda verificar directamente con el establecimiento o con fuentes oficiales competentes.

Ante emergencias médicas o sanitarias, el usuario debe comunicarse con los servicios oficiales correspondientes.

19. Contenido aportado por usuarios y reportes

Los usuarios pueden enviar reportes, correcciones, reclamos, sugerencias, imágenes o información sobre comercios.

TuM² puede revisar, moderar, aceptar, rechazar, editar o eliminar aportes cuando sea necesario para proteger la calidad del dato, evitar abuso, cumplir obligaciones legales o mantener la integridad del servicio.

El usuario debe evitar enviar datos sensibles, información de terceros sin autorización, documentación innecesaria o contenido que no sea relevante para la finalidad del reporte o reclamo.

20. Enlaces, fuentes externas y datos de terceros

TuM² puede incluir enlaces, referencias o información proveniente de fuentes externas, comercios, usuarios, bases públicas o proveedores de datos.

TuM² no controla las prácticas de privacidad de sitios o servicios de terceros. Cuando el usuario acceda a servicios externos, deberá revisar las políticas correspondientes de dichos terceros.

21. Cambios en esta Política

TuM² puede actualizar esta Política para reflejar cambios legales, técnicos, operativos, comerciales o de producto.

Cuando los cambios sean relevantes, TuM² procurará informarlos mediante la app, web, email u otros canales razonables.

La fecha de última revisión indicará la versión vigente del documento.

22. Contacto

Para consultas relacionadas con privacidad y protección de datos personales:

• privacidad@tum2.com.ar

Para consultas legales sobre esta Política:

• legal@tum2.com.ar

Para reportes de seguridad o incidentes:

• seguridad@tum2.com.ar

Para soporte operativo general:

• soporte@tum2.com.ar

Domicilio legal:

• Constancio C. Vigil 150, Carlos Spegazzini, Ezeiza, B1812, Provincia de Buenos Aires, Argentina