

## **GDPR**

### **de la sociedad mercantil SupraMedEx s.r.o.**

con domicilio social en: Štěpánská 1742/27, 110 00 Praga  
número de identificación: 176 87 110

inscrita el 27 de octubre de 2022 en el Registro Mercantil  
llevado por el Tribunal Municipal de Praga, sección C,  
inserción 375001  
(en adelante, «SUPRAMEDEX»)  
representada por el administrador  
Daniel Fiala

### **¿Qué significa el GDPR?**

El GDPR, o Reglamento General de Protección de Datos (*General Data Protection Regulation*), también conocido como el Reglamento general sobre la protección de los datos personales, es una legislación de la Unión Europea que refuerza significativamente la protección de los datos personales en los Estados miembros de la UE.

El GDPR fue adoptado por todos los Estados miembros de la UE en abril de 2016, pero no entró en vigor hasta el 25 de mayo de 2018.

El GDPR constituye el marco jurídico básico para la protección de los datos personales en el espacio europeo, con el objetivo de proteger al máximo los derechos de los individuos contra el uso indebido de su información personal. Por lo tanto, se aplica a todas las empresas, instituciones y entidades que manejan y utilizan estos datos. El incumplimiento de las normas del GDPR conlleva sanciones severas, incluso de carácter astronómico.

### **¿Qué datos personales deben protegerse en el marco del GDPR?**

El GDPR regula la protección de todos los datos personales de las personas físicas. Estos datos se dividen en varias categorías. Los datos personales solo pueden ser procesados en el alcance establecido en los Términos y Condiciones del sistema FKP.

### **CATEGORÍAS DE DATOS PERSONALES**

- 1) **Datos personales generales** – nombre, apellido, dirección, residencia permanente, dirección de entrega, sexo, edad, fecha de nacimiento, lugar de nacimiento, número de identificación personal, estado civil, discapacidad, registro fotográfico, grabación de video, grabación de audio, dirección de correo electrónico, número de teléfono, dirección IP, diversos datos de

identificación emitidos por el estado (NIF, CIF, número de documento de identidad, número de permiso de conducir, número de pasaporte, etc.), nivel educativo alcanzado, ingresos laborales, ingresos de pensión, perfil cultural, datos personales del cónyuge, hijos, pareja, etc.

- 2) **Categorías especiales de datos personales** – por ejemplo: origen racial o étnico, opiniones políticas, creencias religiosas, creencias filosóficas, afiliación sindical, estado de salud – datos sobre la salud física o mental, sobre la atención médica recibida, orientación sexual, delitos penales, condenas firmes.

**Datos personales genéticos** – por ejemplo: ADN, ARN, grupo sanguíneo, factor Rh.

**Datos personales biométricos** – imagen facial, huella dactilar, imagen del iris ocular, imagen de la retina, firma, tono de voz. La empresa SupraMedEx s.r.o. no procesa ningún dato personal perteneciente a la categoría especial de datos personales.

### **Principios fundamentales del GDPR:**

- 1) El cliente debe ser informado sobre el alcance y la forma de tratamiento de sus datos personales (DP).
- 2) El cliente tiene derecho a oponerse al tratamiento de sus datos personales – en base a esta objeción, el responsable del tratamiento no podrá continuar procesando dichos datos personales.
- 3) El responsable del tratamiento de datos tiene derecho a la portabilidad de los datos personales a otro responsable, si los datos se procesan de forma automatizada.
- 4) El cliente debe tener acceso en línea a los datos que se recopilan sobre él.
- 5) El cliente tiene derecho a la supresión de sus datos personales y el derecho al olvido – lo que significa que el cliente puede solicitar la eliminación inmediata de sus datos personales, si no existe una razón legal para continuar con su procesamiento.
- 6) El cliente tiene derecho a presentar una queja sobre el alcance y la forma de tratamiento de sus datos personales ante la autoridad supervisora, es decir, ante la Oficina para la Protección de Datos Personales.

### **Inicio de actividades**

La sociedad SupraMedEx s.r.o. – en adelante denominada SupraMedEx – exige de todos sus clientes y asesores, sin excepción, el estricto cumplimiento de todos los principios de protección de datos personales. Al mismo tiempo, SupraMedEx tiene la obligación de garantizar que todos los datos personales de sus clientes y asesores estén protegidos bajo el más alto nivel de seguridad. Asimismo, cada asesor o cliente de SupraMedEx debe ajustar su trabajo conforme al Reglamento GDPR y proteger todos los datos personales de los clientes de SupraMedEx que le sean confiados contra cualquier tipo de fuga, además de tratar a sus clientes con absoluta discreción en el manejo de sus datos personales.

### **¿Cómo asegurar correctamente sus dispositivos contra fugas de datos?**

Recomendamos proteger al máximo su computadora portátil, PC, teléfono móvil y cualquier otro dispositivo que utilice para comunicarse con los clientes, con el fin de evitar cualquier fuga de datos. En este aspecto, la palabra más importante es CONTRASEÑA. La forma más sencilla de protección primaria de datos es establecer en su dispositivo una contraseña "a prueba de todo", es decir, una contraseña de al menos ocho (8) caracteres, que contenga letras mayúsculas, minúsculas, símbolos y números, y que además cambie regularmente. Por supuesto, recuerde cerrar su sesión al abandonar el dispositivo. Sin embargo, una contraseña por sí sola no es suficiente para eliminar todos los posibles riesgos. Los ataques de hackers (o diversos fallos) son muy comunes hoy en día, por lo que es necesario proteger sus dispositivos también mediante otras herramientas para reducir el riesgo de fuga de datos al mínimo.

### **Decálogo para garantizar la máxima seguridad en la protección de datos personales**

1. Aproveche la amplia oferta de programas antivirus.
2. Actualice regularmente las bases de datos de virus.
3. Mantenga siempre instalado un programa antivirus, tanto en el ordenador como en otros dispositivos móviles inteligentes.
4. No olvide mantener actualizado su sistema operativo (y en general todo su software): esto reduce significativamente el riesgo de que sus datos sean atacados (por ejemplo, en el sistema Microsoft Windows mediante Windows Update). En teléfonos móviles, tabletas y otros dispositivos "inteligentes" con sistemas operativos Android o iOS, es necesario descargar regularmente las actualizaciones (ya sea directamente desde Google Play/App Store o desde la Configuración del dispositivo).
5. Utilice siempre conexiones a Internet seguras y de confianza, y evite las redes Wi-Fi públicas.
6. Instale únicamente software conocido y confiable en sus dispositivos; evite instalar programas o utilidades dudosas.
7. No abra ni descargue correos electrónicos ni archivos adjuntos de remitentes desconocidos o con contenido sospechoso.
8. No comparta sus datos de acceso con otras personas. Al hacerlo, estaría proporcionando acceso no solo a sus datos personales, sino también a los datos de sus subordinados o clientes.
9. Actúe con precaución y no descargue todo lo que le ofrezcan los anuncios publicitarios en Internet.
10. La confiabilidad de la seguridad de una página web se incrementa con el cifrado https, que puede identificarse en la barra de direcciones (<https://www.supramedex.cz/>). A veces, aparece un icono de candado con el texto "sitio seguro".

### **¿Cómo funciona en la práctica el GDPR en la red FKP SUPRAMEDEX?**

Todo asesor de larga trayectoria o nuevo asesor entusiasta seguramente se preguntará: ¿qué impacto tiene el Reglamento GDPR en el funcionamiento de la red de asesores y clientes de SupraMedEx?

A modo de resumen, describiremos lo que el GDPR implica para el funcionamiento de la red FKP y qué es necesario explicar a los clientes antes de completar su registro. El principio fundamental del comercio en el marco del GDPR es la posibilidad de revocar en cualquier momento el consentimiento del cliente para el tratamiento de sus datos personales para un fin determinado. Para que todos los consentimientos requeridos en la red sean claros y correctamente comprendidos tanto por el cliente como por el asesor, hemos decidido dividir estos consentimientos en varias categorías.

Categorías de consentimientos para cumplir con las obligaciones del GDPR y otras normativas legales:

**1) Consentimiento con los Términos y Condiciones Comerciales del sistema FKP SUPRAMEDEX**

**2) Consentimiento para el envío de materiales de marketing y comerciales en formato electrónico – incluido en los Términos y Condiciones de SUPRAMEDEX**

**Consentimiento con los Términos y Condiciones Comerciales de FKP SUPRAMEDEX**

El cliente, al registrarse en el sistema FKP, confirma que ha sido informado sobre el funcionamiento de la red FKP SUPRAMEDEX y que consiente plenamente el tratamiento de sus datos personales dentro de toda la red – sus datos personales son utilizados por asesores, clientes y la empresa SupraMedEx para la comunicación comercial y de marketing. Al mismo tiempo, el cliente acepta los principios de manejo seguro de los datos personales de los asesores y clientes con los que colabora.

La concesión de este consentimiento es obligatoria para todo cliente que desee registrarse en el sistema FKP, realizar una compra de productos SUPRAMEDEX a través del formulario de compra de FKP, o beneficiarse de otras bonificaciones y ventajas ofrecidas por la red SUPRAMEDEX, conforme al apartado 4.4.8 de los Términos y Condiciones.

El consentimiento puede ser revocado en cualquier momento; la revocación del consentimiento provocará la cancelación completa del registro del cliente, y no será posible realizar nuevos pedidos ni reactivar dicho registro. La eliminación de los datos personales (DP) se llevará a cabo inmediatamente tras recibir la revocación de este consentimiento, a más tardar dentro de los siete (7) días laborables siguientes. SupraMedEx informará también al asesor superior directo sobre la tramitación de dicha solicitud por parte de su cliente.

**Datos personales (DP) que el cliente debe proporcionar al otorgar su consentimiento:** nombre, apellidos, dirección de facturación, dirección de entrega, país, número de teléfono móvil y correo electrónico.

**En caso de iniciar una colaboración con una persona física que ejerce actividades empresariales (autónomo), también es necesario añadir los siguientes datos personales:** número de identificación fiscal (NIF), número de registro fiscal (IVA) y cuenta bancaria.

**Consentimiento para el envío de materiales comerciales y de marketing en formato electrónico.** Al otorgar su consentimiento, el cliente confirma que SupraMedEx puede enviarle materiales de marketing y comerciales en formato electrónico mediante canales modernos de comunicación online y offline – tienda electrónica, mailing directo, e-mailing, perfil de empresa en Facebook, campañas publicitarias online. Este consentimiento puede ser revocado en cualquier momento; al hacerlo, el registro del cliente sigue siendo válido y el cliente puede seguir realizando pedidos de productos.

**Datos personales que el cliente debe proporcionar al otorgar este consentimiento:** correo electrónico y contraseña. No es necesario volver a introducir estos datos manualmente, ya que se generan automáticamente a partir de los datos obtenidos del consentimiento con los Términos y Condiciones de SupraMedEx.

Todos los datos personales mencionados en las respectivas categorías de consentimiento se procesan en bases de datos seguras ubicadas en servidores cifrados propiedad de SupraMedEx. Por lo tanto, no hay motivo para preocuparse por un uso indebido interno. En caso de que un asesor o cliente de SupraMedEx no garantice la seguridad en el tratamiento y manejo de los datos personales, SupraMedEx podrá imponerle sanciones y, en caso de infracciones graves o repetidas, podrá rescindir la colaboración de forma inmediata (es decir, sin período de preaviso).

## **Recomendaciones para los asesores de SupraMedEx en el manejo de datos personales**

### **¿Cómo trabajar con registros “especiales” propios sobre clientes?**

Si un asesor de SupraMedEx lleva registros detallados sobre sus clientes que le ayudan a optimizar las recomendaciones de productos, debe tener en cuenta varios puntos importantes:

1. Esta base de datos, registro o recopilación no es propiedad de SupraMedEx – el propietario (responsable del tratamiento) es el propio asesor, quien asume la responsabilidad total por dicha base de datos.
2. La base de datos puede contener no solo datos personales, sino también datos muy sensibles sujetos a un régimen especial, que deben protegerse con extrema precaución.
3. El asesor debe garantizar un alto nivel de seguridad y trabajar con estos datos con la máxima cautela y conforme a la legislación vigente.
4. El cliente al que se refieren estos registros debe ser previamente informado de que sus datos serán almacenados, y debe otorgar un consentimiento por escrito.
5. En caso de que el cliente rechace el tratamiento de sus datos personales, el asesor debe respetar esta solicitud inmediatamente y eliminar dichos datos de su base de datos.

## **Uso de herramientas personales de comunicación y marketing**

¿Utilizas una página web personal como asesor, un grupo de Facebook, una página o perfil, o envías correos electrónicos promocionales o mensajes SMS a tus clientes?

También estos canales y herramientas de comunicación deben estar configurados de acuerdo con el GDPR y demás normativas legales aplicables.

**Facebook** – se trata de una red social pública en la que, a pesar de la configuración de privacidad de tu cuenta, es necesario actuar con mucha precaución para evitar cualquier uso indebido o fuga de datos personales. Por tanto, no se recomienda incluir datos personales sensibles tuyos ni de otras personas en publicaciones o mensajes.

**Sitios web personales** – es necesario verificar si el proveedor del dominio tiene el sitio y los servidores debidamente protegidos. Otra regla clave es no exigir que los clientes introduzcan datos en la página web que luego se almacenen en el servidor. Esto se puede evitar ofreciendo, por ejemplo, un formulario de contacto en el que el cliente indique su interés en tus servicios y tú puedas redirigirlo directamente a la tienda en línea segura de SupraMedEx. Además, cada sitio web personal de un asesor de SupraMedEx debe ser aprobado por la dirección de SupraMedEx antes de su publicación.

**Mensajes SMS con publicidad o recordatorios de promociones** – si decides enviar mensajes SMS de forma independiente, tu cliente debe haber dado su consentimiento previo (preferiblemente por escrito), para evitar posibles acusaciones de envío no autorizado o acoso. Si utilizas un programa especial para el envío masivo de mensajes, debes comprobar con el proveedor del software que los números de teléfono introducidos estén protegidos y tomar medidas adicionales para garantizar la seguridad de todos los números almacenados. También debes responder activamente a los comentarios de los clientes que rechacen seguir recibiendo mensajes – elimina inmediatamente dicho número de tu base de datos de envío. Esto te ayudará a evitar sanciones por parte de la Oficina de Protección de Datos Personales.

**Correos electrónicos promocionales masivos** – este tipo de comunicación se gestiona a través de portales especiales, y es importante tener en cuenta que tú eres el solicitante del servicio proporcionado por una tercera parte externa. Por lo tanto, estás confiando los datos personales (DP) de tus clientes a este tercero, y debes asegurarte de que dicho proveedor cuente con medidas de protección de datos adecuadas. En caso de fuga de datos personales, podrías ser también sancionado tú mismo, ya que no garantizaste que el proveedor del servicio estuviera suficientemente protegido.

## **¿Grabas vídeos, tomas fotografías con tus clientes y los publicas en canales accesibles al público?**

Si, como parte de tu trabajo como asesor, realizas grabaciones de vídeo o fotografías con tus clientes que luego utilizas con fines promocionales o simplemente las publicas en canales informativos de acceso público (redes sociales, páginas web personales, etc.), es obligatorio obtener el consentimiento del cliente para tomar dichas imágenes o vídeos. Debes

informar de forma explícita al cliente sobre los fines para los cuales se toman las fotos y vídeos, cómo se van a utilizar, y advertirle de su derecho a revocar su consentimiento en cualquier momento, incluyendo cómo puede hacerlo. Ejemplo: grabas un vídeo de una capacitación sobre novedades de SupraMedEx que luego deseas subir a tu página web personal. Recomendación: al comienzo de la capacitación, proporciona a todos los participantes un formulario para firmar su consentimiento al tratamiento de datos personales, concretamente para la toma de fotos y/o vídeos. El documento debe indicar claramente que se grabará vídeo o se tomarán fotos durante el evento, y cómo se tratarán los datos personales. Si todos los participantes firman este consentimiento, puedes grabar o tomar fotografías y utilizarlas según lo acordado en el consentimiento. Si algún participante no da su consentimiento, debes excluirlo de la grabación y asegurarte de que no aparezca visible en ninguna imagen o vídeo. Asimismo, todos los participantes deben tener la posibilidad de revocar su consentimiento en cualquier momento. En ese caso, deberás eliminar su imagen del material grabado o ocultarla (por ejemplo, desenfocándola).

## **Conclusión**

Es fundamental respetar las normas y principios establecidos por el Reglamento (UE) 2016/679 (GDPR) y otras leyes aplicables cuando se trabaja dentro del sistema FKP de SupraMedEx. Cualquier infracción de estas normas puede suponer un riesgo de seguridad que podría dar lugar a la finalización de la colaboración comercial o a la imposición de sanciones.

Este documento es válido según la versión publicada en el sitio web [www.supramedex.cz](http://www.supramedex.cz), operado por SupraMedEx s.r.o., Štěpánská 1742/27, Praga 1, 110 00, CIF: 17687110.

Este documento entra en vigor el 1 de enero de 2024.

Se reservan los derechos a realizar cambios en el documento.