

POLÍTICA DE PRIVACIDAD:

POLÍTICA DE PRIVACIDAD	
<p>Como seguramente conoce, la entrada en vigor del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de datos personales (en adelante RGPD) y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales (en adelante LOPDGDD), pone de manifiesto la necesidad de reforzar los niveles de seguridad y protección de datos de carácter personal. Queremos informarle que cumplimos todos los requisitos que dicha legislación exige y que todos los datos, bajo nuestra responsabilidad vienen siendo tratados de acuerdo con las exigencias legales y guardándose las debidas medidas de seguridad que garantizan la confidencialidad de los mismos. No obstante, dadas las novedades legislativas habidas, creemos oportuno poner en su conocimiento la siguiente política de privacidad:</p>	
<p>¿Quién es el responsable de tratamiento de sus datos?</p>	
Identidad:	SOTRAFA, S.A.
Dirección Postal:	PARAJE DE CARTABONA 12 - 04710 SANTA MARIA DEL AGUILA (ALMERIA)
Teléfono:	950 40 56 00
Correo electrónico:	gdpr@sotrafa.com
<p>¿Cuáles son sus derechos?</p>	
<ul style="list-style-type: none"> • Cualquier persona tiene derecho a obtener confirmación sobre si estamos tratando datos personales que les conciernan, o no. • Las personas interesadas tienen derecho a acceder a sus datos personales, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines que fueron recogidos" • No resulta posible el ejercicio del derecho de rectificación en el caso del tratamiento de videovigilancia ya que por la naturaleza de los datos -imágenes tomadas de la realidad que reflejan un hecho objetivo-, se trataría del ejercicio de un derecho de contenido imposible. • En determinadas circunstancias, los interesados podrán solicitar la limitación del tratamiento de sus datos, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones. • En determinadas circunstancias y por motivos relacionados con su situación particular, los interesados podrán oponerse al tratamiento de sus datos, en cuyo caso el Responsable de Tratamiento dejará de tratar los datos, salvo por motivos legítimos imperiosos, o el ejercicio o la defensa de posibles reclamaciones. En este sentido, y en relación con las imágenes de videovigilancia, el ejercicio del derecho de oposición plantea enormes dificultades. Si este se interpreta como la imposibilidad de tomar imágenes de un sujeto concreto en el marco de instalaciones de videovigilancia vinculadas a fines de seguridad privada no resultaría posible su satisfacción en la medida en la que prevalece la protección de la seguridad. • En virtud del derecho a la portabilidad, los interesados tienen derecho a obtener los datos personales que les incumben en un formato estructurado de uso común y lectura mecánica y a transmitirlos a otro responsable" • En el caso de que haya otorgado el consentimiento para alguna finalidad específica, tiene derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada. 	
<p>¿Cómo se pueden ejercer los derechos?</p>	
Dónde dirigirse para ejercitar sus derechos:	<p>"Si desea ejercitar sus derechos, por favor, dirijase al canal establecido para el ejercicio de derechos por parte del responsable de tratamiento: gdpr@sotrafa.com a fin de que podamos dar respuesta a su solicitud de forma gestionada"</p>
Información requerida para ejercitar sus derechos:	<ul style="list-style-type: none"> • Para ejercitar sus derechos, necesitamos acreditar su identidad y la petición concreta que nos formula, por cuanto le solicitamos la siguiente información: <ul style="list-style-type: none"> - Información documentada (escrito/correo electrónico) de la petición en la que se concreta la solicitud. - Acreditación de identidad como titular de datos objeto de ejercicio (Nombre, apellidos del interesado y fotocopia del DNI del interesado y/o de la persona que lo represente, así como el documento acreditativo de tal representación (representante legal, en su caso). - En el caso de ejercicio de derechos relacionados con datos de personas fallecidas: Copia de: <ul style="list-style-type: none"> o Libro de Familia o Registro Civil en el que se haga constar la relación de parentesco o de hecho con el fallecido y/o, o Testamento en que se le declara al solicitante como heredero y/o, o Designación expresa a la persona o institución solicitante, por parte del fallecido y/o o Documentación que acredita la representación legal del fallecido. o En el caso de ejercicio de derechos de rectificación y/o supresión: Declaración Responsable del solicitante en el que acredita contar con el consenso del resto de personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos para llevar a cabo dicha solicitud. - Cuando el responsable de tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado. - Dirección a efectos de notificaciones, fecha y firma del solicitante (en caso de escrito), o nombre completo y apellidos (en caso de correo electrónico), o bien validación de la solicitud en zona privada del canal de comunicación con clave personal de autenticación de su identidad) <ul style="list-style-type: none"> • Al ejercer el derecho de rectificación reconocido en el artículo 16 del RGPD, el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento. • Así mismo, cuando tratemos una gran cantidad de datos relativos al afectado y ejercitase su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud.
Procedimiento General de Ejercicio de sus derechos:	<ul style="list-style-type: none"> • Una vez recibida la información requerida procederemos a dar respuesta a su solicitud conforme al procedimiento general de ejercicio de derechos de la organización: • El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22 (Derechos del interesado), y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. • Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. • El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. • Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo. • Sólo en los casos en los que los sistemas de tratamiento del responsable así lo permitan, el derecho de acceso se podrá facilitar a través de un sistema de acceso remoto, directo y seguro a los datos personales que garantice, de modo permanente, el acceso a su totalidad. A tales efectos, la comunicación por el responsable al afectado del modo en que éste podrá acceder a dicho sistema bastará para tener por atendida la solicitud de ejercicio del derecho. No obstante, el interesado podrá solicitar del Responsable de Tratamiento la información referida a los extremos

- previstos en el artículo 15.1 del RGPD que no se incluyese en el sistema de acceso remoto.
- Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.
 - La información facilitada será de carácter gratuito, salvo canon razonable por costes administrativos. Cuando el afectado elija un medio distinto al que se le ofrece que suponga un coste desproporcionado, la solicitud será considerada excesiva, por lo que dicho afectado asumirá el exceso de costes que su elección comporte. En este caso, solo será exigible al Responsable del Tratamiento la satisfacción del derecho de acceso sin dilaciones indebidas.
 - El responsable de tratamiento podrá negarse a actuar respecto de la solicitud, si bien soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud. A los efectos establecidos en el artículo 12.5 del RGPD se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello.
 - En los casos en los que proceda al ejercicio de rectificación o supresión, se procederá al bloqueo de sus datos: El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y sólo por el plazo de prescripción de las mismas. Transcurrido ese plazo se procederá a la destrucción de los datos. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en anteriormente. (art. 16 RGPD y art.32 LOPDGDD).
 - Cuando la supresión derive del ejercicio del derecho de oposición con arreglo al artículo 21.2 del RGPD, el Responsable de Tratamiento podrá conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa. En los casos en los que no desee que sus datos sean tratados para la remisión de comunicaciones comerciales, le remitimos a los sistemas de exclusión publicitaria existentes, conforme a la información publicada por la autoridad de control competente (AEPD) en su sede electrónica www.aepd.es
 - En los casos en los que el tratamiento de los datos personales esté limitado constará claramente en los sistemas de información del Responsable de Tratamiento.
 - Ante la existencia de una deuda cierta, vencida y exigible, se remite una comunicación al deudor a en el momento de requerir el pago acerca de la posibilidad de inclusión en dichos sistemas (tratamientos de morosidad de la organización), con indicación de aquéllos en los que participe (entidades de gestión de cobro para la gestión de la reclamación pertinente ...) en el caso de no ser resuelta la deuda en un plazo máximo de 15 días desde la notificación de la insolvencia, se informa sobre la posibilidad de ejercitar los derechos establecidos en los artículos 15 a 22 del RGPD dentro de los treinta días siguientes a la notificación de la deuda al sistema, permaneciendo bloqueados los datos durante ese plazo.
 - Las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión. Como excepción, las personas a las que se refiere el párrafo anterior no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante.
 - A fin de cumplir con la normativa vigente en materia de videovigilancia Inst 1/2006 de la AEPD, le informamos que el plazo de conservación de las grabaciones es de 1 mes desde su captación, por cuanto no podremos atender solicitudes formalizadas en plazos posteriores. Así mismo para evitar la afección a derechos de terceros, en el caso de solicitud de acceso, procederemos a emitir un certificado en el que, con la mayor precisión posible y sin afectar a derechos de terceros, se especifiquen los datos que han sido objeto de tratamiento. Ej. "Su imagen fue registrada en nuestros sistemas el día ___ del mes del año entre las _ horas y las _ horas. En concreto el sistema registra su acceso y salida de la instalación."

¿Qué vías de reclamación existen?

Si considera que sus derechos no se han atendido debidamente, tiene derecho a presentar una reclamación ante la autoridad de protección de datos competente (www.agpd.es)

INFORMACIÓN ADICIONAL TRATAMIENTO DE DATOS DE CONTACTOS:

¿Con qué finalidad tratamos los datos personales que nos facilita? (*) La relación de actividades de SOTRAFA, S.A. está a su disposición en www.sotrafa.com

- Atención a sus consultas y solicitudes: Gestión de Respuesta a Consultas, Reclamaciones o Incidencias, Solicitudes de Información técnica o corporativa, Recursos y/o de Actividades, y en caso de que haya consentido, para las finalidades descritas en los consentimientos adicionales
- Contacto con el interesado a través de los medios de comunicación facilitados (mail, dirección postal y/o teléfono) a fin de gestionar las consultas que nos haga llegar a través de los canales habilitados a tal efecto, gestionar avisos y coordinar actuaciones derivadas de los servicios que nos solicite por parte de personas relacionadas con SOTRAFA, S.A. y/o por encargados de tratamiento relacionados con la misma para las finalidades legitimadas y/o consentidas.
- Gestión de inscripción en jornadas y eventos de SOTRAFA, S.A.
- Gestión de la suscripción al boletín de SOTRAFA, S.A.
- El contacto y/o envío de encuestas de satisfacción, boletines de noticias e información corporativa y ofertas y promociones de productos y servicios de la organización
- La captación y posterior publicación de material audiovisual y/o gráfico en las que pueda verse involucrado en medios de comunicación corporativos (por ejemplo y no limitativo, web, redes sociales, boletines informativos, memoria de actividad, reportajes, presencia en medios de comunicación) y/u otros medios de comunicación pública (publicaciones sectoriales y/o reportajes en prensa escrita, TV,), como difusión de los resultados de la actividad, promoción y difusión, gestión de campañas, actividades y eventos, si así lo ha consentido
- Gestión asociada, incluida su comunicación con carácter previo, que pudiera derivarse del desarrollo de cualquier operación de modificación estructural de sociedades o la aportación o transmisión de negocio o de rama de actividad empresarial, siempre que los tratamientos fueran necesarios para el buen fin de la operación y garanticen, cuando proceda, la continuidad en la prestación de servicios.
- Inclusión en los sistemas de canal de denuncias de los datos asociados a la puesta en conocimiento (incluso de forma anónima) de la comisión en el seno de la organización o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable.

¿Cuánto tiempo conservamos los datos facilitados?

- Los datos proporcionados se conservarán mientras se mantenga la relación de licitud de tratamiento y expirada la vigencia de la misma no se solicite su supresión por el interesado, con excepción de su conservación para la formulación, el ejercicio o la defensa de reclamaciones del responsable de tratamiento o con miras a la protección de los derechos de otra persona física o jurídica y/o por razones de obligación legal.
- Los datos tratados para la remisión de comunicaciones comerciales serán conservados hasta que revoque el consentimiento otorgado.
- Los datos de quien formule la comunicación de una denuncia y de los empleados y terceros se conservan en el sistema de denuncias para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados, así como posteriormente como evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica, conforme a lo establecido en el artículo 24 de la LOPDGDD.

¿Cuál es la legitimación para el tratamiento de sus datos?

- La base legal para el tratamiento de sus datos es el cumplimiento de la solicitud que nos formula. Los datos solicitados son necesarios para la correcta prestación del mismo.
- Satisfacer un interés legítimo del Responsable: Supuestos de interés legítimo en los que el Responsable pudiera ser parte perjudicada y fuera necesario el tratamiento y la comunicación de los datos del incumplidor a terceros a fin de gestionar el cumplimiento normativo y la defensa de los intereses del responsable de tratamiento, así como supuestos de interés legítimo de tratamientos específicos contemplados en la LOPDGD: Artículo 19. Tratamiento de datos de contacto y de empresarios individuales; Artículo 20. Sistemas de información crediticia; Artículo 21. Tratamientos relacionados con la realización de determinadas operaciones mercantiles (reestructuración societaria o transmisiones de negocio) Artículo 22. Tratamientos con fines de videovigilancia; Artículo 23 Sistemas de exclusión publicitaria; Artículo 24 Sistemas de información de denuncias internas).
- El consentimiento del interesado que nos haya facilitado de forma inequívoca a través de medios formales y/o marcando las casillas habilitadas a tal efecto en las cláusulas de protección de datos habilitadas en el documento base que haya regulado la relación comercial en función del canal de contacto.

¿A qué destinatarios se pueden comunicar sus datos?

- Organizaciones o personas directamente contratadas por el Responsable de Tratamiento para la prestación de servicios vinculados con las finalidades de tratamiento: Colaboradores, Entidades Subcontratadas para la ejecución de proyectos/servicios objeto de solicitud o consulta.
- Canal de Denuncias (Las denuncias sobre vulneración de normativa y código de conducta son transmitidas a la Unidad de Cumplimiento Normativo): El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a quienes, incardinados o no en el seno de la entidad, desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan.
- Fuerzas y Cuerpos de Seguridad: En la medida en que fuera requerido un derecho de acceso justificado en la investigación de un incumplimiento normativo.
- Otros (especificar): Medios de Comunicación y revistas especializadas para la Promoción de las Actividades de la Organización.

¿Bajo qué garantías se comunican sus datos?

La comunicación de datos a terceros se realiza a entidades que acrediten la disposición de un Sistema de Protección de Datos de Carácter Personal acorde a la legalidad vigente.

¿Cómo hemos obtenido sus datos?

- El propio interesado, a través de la comunicación remitida y/o a través de redes sociales profesionales.

¿Qué categoría de datos tratamos?

Datos identificativos y de contacto, los relacionados y/o aportados con la Consulta, Solicitud de Información técnica o corporativa, Recursos y/o de Actividades, Reclamaciones o Incidencias que nos formula, así como los datos personales de terceros que nos pudiera facilitar.

¿Cómo se guardan sus datos personales de forma segura?

SOTRAFA, S.A. ha formalizado acuerdos para garantizar que tratamos sus datos personales correctamente y de acuerdo con la normativa vigente de protección de datos. Estos acuerdos reflejan las respectivas funciones y responsabilidades en relación con usted, y contemplan qué entidad se encuentra en la mejor posición para cumplir con sus necesidades. Estos acuerdos no afectan a sus derechos en virtud de la ley de protección de datos. Para obtener más información sobre estos acuerdos, no dude en ponerse en contacto con nosotros.

El responsable de Tratamiento toma todas las medidas necesarias para guardar sus datos personales de forma privada y segura. Sólo personas autorizadas de SOTRAFA, S.A., personal autorizado de terceros directamente contratados por el Responsable de Tratamiento para la prestación de servicios vinculados con las finalidades de tratamiento o personal autorizado de empresas que giran bajo el nombre comercial de SOTRAFA, S.A.* (que tienen la obligación legal y contractual de guardar toda la información de forma segura) tienen acceso a sus datos personales. Se exige a todo el personal de SOTRAFA, S.A. que tiene acceso a sus datos personales que se comprometa a respetar la Política de Privacidad del responsable de Tratamiento y la normativa de protección de datos y a todos los empleados de Terceros que tienen acceso a tus datos personales que firmen los compromisos de confidencialidad en los términos establecidos en la legislación vigente. Además, se asegura contractualmente que las empresas de terceros que tienen acceso a sus datos personales los mantengan de forma segura. Para asegurarnos de que sus datos personales están protegidos, SOTRAFA, S.A. dispone de un entorno de seguridad IT y adopta las medidas necesarias para evitar accesos no autorizados.

El responsable de Tratamiento ha formalizado acuerdos para garantizar que tratamos sus datos personales correctamente y de acuerdo con la normativa vigente de protección de datos. Estos acuerdos reflejan las respectivas funciones y responsabilidades en relación con usted, y contemplan qué entidad se encuentra en la mejor posición para cumplir con sus necesidades. Estos acuerdos no afectan a sus derechos en virtud de la ley de protección de datos. Para obtener más información sobre estos acuerdos, no dude en ponerse en contacto con nosotros.

INFORMACIÓN ADICIONAL TRATAMIENTO DE DATOS DE CLIENTES:

¿Con qué finalidad tratamos sus datos personales? (*) La relación de actividades de SOTRAFA, S.A. está a su disposición en www.sotrafa.com

- Uso interno, Gestión comercial y relacional, Realización de operaciones y Gestión administrativa, económica y contable derivada de la relación con el cliente y/o deudor
- Uso interno, realización de operaciones y gestión administrativa, económica y contable derivada de la relación con el cedente (relación comercial y/o contractual)
- Oferta y Gestión Comercial de la organización y de sus servicios "Con el fin de facilitar a los interesados ofertas de servicios de su interés"
- Oferta y Gestión Comercial de SOTRAFA, S.A. y de sus servicios "Con el fin de facilitar a los interesados ofertas de servicios de su interés"
- Gestión de la Contratación y prestación de servicios de la organización, así como del cumplimiento de requisitos contractuales
- Gestión de Respuesta a Consultas, Reclamaciones o Incidencias, Solicitudes de Información, Recursos y/o de Actividades
- Promoción y Difusión de la Organización: La Elaboración, Publicación y Comunicación de Estadísticas, Memorias de Actividad, Casos de Éxito e Información asociada a la comunicación y transparencia de su Actividad, así como la Grabación y Publicación de Material Divulgativo, Comunicación y Gestión de Campañas, Actividades, Eventos, Concursos y/o Grabación y Publicación, en los medios de comunicación de la organización (incluida web y redes sociales) y/u otros medios de comunicación pública, de videos, grabaciones y fotos asociadas a las actividades desarrolladas por la organización "Con el fin de facilitar a los grupos de interés información sobre la organización"
- Envío de Boletines de Noticias, Memorias de Actividad e Información asociada a la Actividad de la Organización
- Gestión de la Calidad de procesos y actividades, así como la evaluación de los resultados de satisfacción/percepción y rendimiento de los grupos de interés de la organización.
- Aportación de evidencias de solvencia técnica en presentación ofertas y/o solicitud, gestión y justificación de campañas, actividades, eventos, concursos, proyectos y subvenciones en los que participe la organización
- Gestión del Cumplimiento Normativo (normativa aplicable así como normativa interna de obligado cumplimiento): Investigación, monitorización y auditoría de controles establecidos para la prevención de delitos pudiendo establecerse los controles de acceso a las instalaciones, sistemas de información e impresión de documentación para todos los datos de carácter personal bajo responsabilidad de la organización y por lo tanto

para todos los sistemas de información de dicha entidad, así como los controles relativos al uso de las imágenes captadas por los sistemas de videovigilancia para la investigación de los accidentes y/o incidentes que pudieran producirse, así como incumplimientos de normas laborales, delitos o comportamientos ilícitos.

- Análisis de Perfiles "Con el fin de poder ofrecerle productos y servicios de acuerdo con sus intereses, así como mejorar su experiencia de usuario, elaboraremos un "perfil", en base a la información facilitada. No se tomarán decisiones automatizadas en base a dicho perfil".
- Evaluación de Solvencia Patrimonial y Crédito
- Gestión de Contactos / Agenda
- Fines estadísticos, históricos o científicos
- Gestión de Visitas y Videovigilancia de las Instalaciones, así como de la seguridad y el cumplimiento normativo en las mismas, la investigación de posibles incidentes o accidentes, gestión de seguros asociados y gestión de apercibimientos o sanciones por incumplimientos de normas de seguridad.
- La gestión y auditoría de la calidad, gestión ambiental y/o gestión de seguridad laboral de procesos e instalaciones de la organización
- Consultar los sistemas de exclusión publicitaria que pudieran afectar a su actuación, excluyendo del tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa al mismo a través de la consulta de los sistemas de exclusión publicitaria publicados por la autoridad de control competente.
- Gestión asociada, incluida su comunicación con carácter previo, que pudiera derivarse del desarrollo de cualquier operación de modificación estructural de sociedades o la aportación o transmisión de negocio o de rama de actividad empresarial, siempre que los tratamientos fueran necesarios para el buen fin de la operación y garanticen, cuando proceda, la continuidad en la prestación de servicios.
- Inclusión en los sistemas de canal de denuncias de los datos asociados a la puesta en conocimiento (incluso de forma anónima) de la comisión en el seno de la organización o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable.
- Otros (especificar): En el caso de contratos de depósito, SOTRAFA, S.A. se reserva el derecho de realizar auditorías periódicas en las instalaciones de clientes y otros deudores.

¿Cuánto tiempo conservamos sus datos?

- Los datos proporcionados se conservarán mientras se mantenga la relación de licitud de tratamiento, no se solicite su supresión por el interesado tras finalización formalizada por escrito de la relación con el interesado, con excepción de su conservación para la formulación, el ejercicio o la defensa de reclamaciones del responsable de tratamiento o con miras a la protección de los derechos de otra persona física o jurídica y/o por razones de obligación legal.
- En cualquier caso, al término de la relación los Datos del interesado serán debidamente bloqueados, según lo previsto en la normativa vigente de protección de datos.
- Documentación Contable y Fiscal - A efectos Fiscales: Los libros de contabilidad y otros libros registros obligatorios según la normativa tributaria que proceda (IRPF, IVA, IS, etc), así como los soportes documentales que justifiquen las anotaciones registradas en los libros (incluidos los programas y archivos informáticos y cualquier otro justificante que tengan trascendencia fiscal), deben conservarse, al menos, durante el periodo en que la Administración tiene derecho a comprobar e investigar y, en consecuencia, a liquidar deuda tributaria (Arts. 66 a70 Ley General Tributaria). Plazo prescripción de Delitos Fiscales asociados a la comprobación de las bases o cuotas compensadas o pendientes de compensación o de deducciones aplicadas o pendientes de aplicación y a Delitos contra la Hacienda Pública y la Seguridad Social - Art. 66 bis Ley General Tributaria y Código Penal, respectivamente. - 4 años. Prescripción infracciones 10 años.
- Documentación Contable y Fiscal - A efectos Mercantiles: Libros, correspondencia, documentación y justificaciones concernientes a su negocio, debidamente ordenados a partir del último asiento realizado en los libros, salvo lo que se establezca por disposiciones generales o especiales. Esta obligación mercantil se extiende tanto a los libros obligatorios (ingresos, gastos, bienes de inversión y provisiones además de la documentación y justificantes en que se soporten las anotaciones registradas en los libros (facturas emitidas y recibidas, tickets, facturas rectificativas, documentos bancarios, etc) (Art.30 Código de Comercio) - 6 años.
- Ficheros de Solvencia: Datos referidos a deudas ciertas, vencidas y exigibles y no reclamadas (Art. 20 de LOPDGDD) - mientras persista el incumplimiento, con el límite máximo de cinco años desde la fecha de vencimiento de la obligación dineraria, financiera o de crédito - 5 años
- Las imágenes/sonidos captados por los sistemas de videovigilancia serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones (en cuyo caso, las imágenes serán puestas a disposición de la autoridad competente en un plazo máximo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación), o estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto (Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras y Art.22 LOPDGDD) - 30 días.
- Los datos incluidos en los tratamientos automatizados creados para controlar el acceso a edificios (Instrucción 1/1996, de 1 de Marzo, de la AEPD, sobre Ficheros automatizados establecidos con la finalidad de controlar el acceso a edificios) - 30 días
- Los datos tratados en relación con la garantía legal serán conservados durante la vigencia de la garantía legal y expirada la vigencia de la misma, durante el plazo que pudiera haber una reclamación judicial o administrativa en relación con la garantía legal.
- Los datos tratados para la remisión de comunicaciones comerciales serán conservados hasta que revoque el consentimiento otorgado.
- Los datos de quien formule la comunicación de una denuncia y de los empleados y terceros se conservan en el sistema de denuncias para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados, así como posteriormente como evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica, conforme a lo establecido en el artículo 24 de la LOPDGDD.
- Por lo tanto, los datos serán conservados mientras se mantenga vigente la relación comercial, en base a los plazos de conservación establecidos por la normativa vigente apuntada anteriormente, así como los plazos legal o contractualmente previstos para el ejercicio o prescripción de cualquier acción de responsabilidad por incumplimiento contractual por parte del interesado o de la Organización (reforma del Código Civil establece un plazo de 5 años para poder llevar a cabo una acción por responsabilidad civil, plazo que computa desde la fecha en que pueda exigirse el cumplimiento de la obligación).

¿Cuál es la legitimación para el tratamiento de sus datos?

- La base legal para el tratamiento de sus datos es la ejecución de un contrato: cumplimiento de su solicitud, oferta, pedido y/o contrato comercial, para lo cual los datos facilitados se comunicarán al responsable de la Marca para atender adecuadamente, en su caso, a las garantías y responsabilidades de los productos y servicios que suministra. Los datos solicitados son necesarios para la correcta prestación del mismo.
- El cumplimiento de obligaciones jurídicas: Normativa con rango de ley administrativa, mercantil, tributaria, fiscal, contable y financiera y legislación de defensa de consumidores y usuarios.
- Satisfacer un interés legítimo del Responsable: Tratamiento de datos como partes de una relación comercial y/o contrato, que sean necesarios para su mantenimiento o cumplimiento, transmisiones de datos dentro de grupos empresariales para fines administrativos internos, marketing directo, prevención del fraude, supuestos de interés legítimo en los que el responsable pudiera ser parte perjudicada y fuera necesario el tratamiento y la comunicación de los datos del incumplidor a terceros a fin de gestionar el cumplimiento normativo y la defensa de los intereses del responsable de tratamiento, fines de videovigilancia como interés legítimo de la organización en la protección de sus activos, el interés legítimo de marketing directo habilitado por la LSSICE (envío de comunicaciones comerciales sobre productos o servicios similares a los contratados por el cliente con el que exista una relación contractual previa), así como supuestos de interés legítimo de tratamientos específicos contemplados en la LOPDGDD: Artículo 19. Tratamiento de datos de contacto y de empresarios individuales; Artículo 20. Sistemas de información crediticia; Artículo 21. Tratamientos relacionados con la realización de determinadas operaciones mercantiles (reestructuración societaria o transmisiones de negocio) Artículo 22. Tratamientos con fines de videovigilancia; Artículo 23 Sistemas de exclusión publicitaria; Artículo 24 Sistemas de información de denuncias internas).

• El consentimiento del interesado que nos haya facilitado de forma inequívoca a través de medios formales y/o marcando las casillas habilitadas a tal efecto en las cláusulas de protección de datos habilitadas en el documento base que haya regulado la relación comercial en función del canal comercial de contacto.

¿A qué destinatarios se pueden comunicar sus datos?

- Organizaciones o personas directamente contratadas por el Responsable de Tratamiento para la prestación de servicios vinculados con las finalidades de tratamiento (especificar): Empresas del Grupo (ver relación en www.armandoalvarez.com), Agentes y/o Agencias Comerciales, Empresas relacionadas con la gestión del transporte, Agencias de Publicidad/Marketing, Asesoría Jurídica, Entidades Subcontratadas para la ejecución de trabajos/servicios objeto del contrato con el cliente, Entidades de Cobro y Seguro de Crédito, Auditores de Gestión y/o de Cumplimiento Normativo.
- Organismos u órganos de la Administración Pública con competencias en las materias objeto de las finalidades del tratamiento (especificar): AEAT
- Entidades Financieras (especificar): Domiciliación recibos y/o gestión de cobro efectos y otros medios de pago.
- Fuerzas y Cuerpos de Seguridad (especificar): En la medida en que fuera requerido en la investigación de un incumplimiento normativo.
- Canal de Denuncias Compliance (Las denuncias sobre vulneración de normativa y código de conducta son transmitidas a la Unidad de Cumplimiento Normativo): El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a quienes, incardinados o no en el seno de la entidad, desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan.
- Otros (especificar): Medios de Comunicación y revistas especializadas para la Promoción de las Actividades de la Organización.

¿Bajo qué garantías se comunican sus datos?

La comunicación de datos a terceros se realiza a entidades que acrediten la disposición de un Sistema de Protección de Datos de Carácter Personal acorde a la legalidad vigente.

¿Cómo hemos obtenido sus datos?

- El propio interesado o su representante legal
- Entidad privada (especificar): Otras Empresas del Grupo, Agentes comerciales, así como de la Entidad con la que el responsable de tratamiento mantiene una relación contractual o de prestación de servicios y para lo cual ha de disponer de datos personales de contacto para la gestión administrativa y operacional a fin de gestionar su acceso, incorporación al proyecto/servicio objeto y/o verificación del cumplimiento normativo bajo responsabilidad de la organización.

¿Qué categoría de datos tratamos?

Datos identificativos de Clientes Potenciales y Efectivos, personas de contacto para la gestión administrativa y operacional asociada a la ejecución del contrato/proyecto, así como otros deudores por operaciones de tráfico mercantil; Datos relativos al puesto de personas de contacto para la gestión administrativa y operacional asociada a la ejecución del contrato/proyecto; Información Comercial; Datos económico, financieros y/o de condiciones de pago; Otro tipo de datos (especificar): Nombre, apellidos y NIF de representante legal, datos de contacto de personas de la organización involucradas o relacionadas con el proyecto objeto del contrato/pedido.

¿Cómo se guardan sus datos personales de forma segura?

En relación con el tratamiento de sus datos personales, le informamos:

SOTRAFA, S.A. toma todas las medidas necesarias para guardar sus datos personales de forma privada y segura. Sólo personas autorizadas de SOTRAFA, S.A., personal autorizado de terceros directamente contratados por el Responsable de Tratamiento para la prestación de servicios vinculados con las finalidades de tratamiento o personal autorizado de empresas que giran bajo el nombre comercial de SOTRAFA, S.A. (que tienen la obligación legal y contractual de guardar toda la información de forma segura) tienen acceso a sus datos personales. Se exige a todo el personal de SOTRAFA, S.A. que tiene acceso a sus datos personales que se comprometa a respetar la Política de Privacidad del responsable de Tratamiento y la normativa de protección de datos y a todos los empleados de Terceros que tienen acceso a tus datos personales que firmen los compromisos de confidencialidad en los términos establecidos en la legislación vigente. Además, se asegura contractualmente que las empresas de terceros que tienen acceso a sus datos personales los mantengan de forma segura. Para asegurarnos de que sus datos personales están protegidos, SOTRAFA, S.A. dispone de un entorno de seguridad IT y adopta las medidas necesarias para evitar accesos no autorizados.

El responsable de Tratamiento ha formalizado acuerdos para garantizar que tratamos sus datos personales correctamente y de acuerdo con la normativa vigente de protección de datos. Estos acuerdos reflejan las respectivas funciones y responsabilidades en relación con usted, y contemplan qué entidad se encuentra en la mejor posición para cumplir con sus necesidades. Estos acuerdos no afectan a sus derechos en virtud de la ley de protección de datos. Para obtener más información sobre estos acuerdos, no dude en ponerse en contacto con nosotros.

En relación con datos personales a los que SOTRAFA, S.A. pudiera acceder como consecuencia de los servicios contratados, le informamos:

La prestación de servicios objeto del contrato puede implicar un acceso físico por parte del personal de SOTRAFA, S.A. a locales o instalaciones susceptibles de almacenar datos personales de los que el cliente es responsable de tratamiento. En este sentido, SOTRAFA, S.A. tiene firmados con su personal cláusulas que prohíben el acceso a todo tipo de información confidencial y, en concreto, a datos de carácter personal pertenecientes al cliente, salvo que el servicio contemplara en su alcance el tratamiento de traslado, reparación, destrucción y/o gestión de soportes informáticos que pudieran contener datos personales, en cuyo caso, SOTRAFA, S.A. actuaría como encargado de tratamiento de los mismos, estableciéndose en dicho caso el pertinente contrato conforme a la normativa vigente de protección de datos que contemplaría entre otros aspectos el objeto, duración, naturaleza, finalidad, categoría de los datos objeto de tratamiento, medidas de seguridad, obligaciones y derechos del encargado, medidas de seguridad organizativas y técnicas para garantizar la confidencialidad durante el proceso, así como los acuerdos adoptados entre cliente y encargado en relación con la transmisión de violaciones de seguridad y/o ejercicio de derechos. La no formalización del servicio de tratamiento de datos personales en un contrato por parte del cliente, presupone que SOTRAFA, S.A. no tiene responsabilidad asociada como encargado de tratamiento de los mismos.

No obstante, lo anterior en el supuesto de que llegara a conocer cualquier tipo de información confidencial con objeto de la prestación del servicio, se compromete a guardar secreto respecto de la misma, no divulgarla ni publicarla, bien directamente, bien a través de terceras personas o empresas, o a ponerla a disposición de terceros. Esta obligación de confidencialidad tiene carácter indefinido, subsistiendo a la finalización del contrato por cualquier causa. SOTRAFA, S.A. se compromete a comunicar y a hacer cumplir al personal a su cargo y contratado por su cuenta, las obligaciones establecidas en materia de confidencialidad.

INFORMACIÓN ADICIONAL TRATAMIENTO DE DATOS DE PROVEEDORES:

¿Con qué finalidad tratamos sus datos personales? (*) La relación de actividades de SOTRAFA, S.A. está a su disposición en www.sotrafa.com

• Uso interno, Gestión comercial y relacional, Realización de operaciones y Gestión administrativa, económica y contable derivada de la relación con el proveedor/colaborador

• Uso interno, realización de operaciones y gestión administrativa, económica y contable derivada de la relación con el cedente (relación comercial y/o contractual)

• Gestión de la Contratación y prestación de servicios de la organización, así como del cumplimiento de requisitos contractuales

• Gestión de Respuesta a Consultas, Reclamaciones o Incidencias, Solicitudes de Información, Recursos y/o de Actividades

• Promoción y Difusión de la Organización: La Elaboración, Publicación y Comunicación de Estadísticas, Memorias de Actividad e Información asociada a la comunicación y transparencia de su Actividad, así como la

Grabación y Publicación de Material Divulgativo, Comunicación y Gestión de Campañas, Actividades, Eventos, Concursos y/o Grabación y Publicación, en los medios de comunicación de la organización (incluida web y redes sociales) y/u otros medios de comunicación pública, de videos, grabaciones y fotos asociadas a las actividades desarrolladas por la organización que pueden incorporar a personas en el desarrollo de sus funciones "Con el fin de facilitar a los grupos de interés información sobre la organización"

- Envío de Boletines de Noticias, Memorias de Actividad e Información asociada a la Actividad de la Organización
- Gestión de la Calidad de procesos y actividades, así como la evaluación de los resultados de satisfacción/percepción y rendimiento de los grupos de interés de la organización.
- Gestión de la Selección, Homologación y Contratación de Proveedores/Colaboradores y verificación de cumplimiento normativo
- Gestión de la seguridad y salud (prevención de riesgos laborales y vigilancia de la seguridad) y evaluación de cumplimiento
- Gestión de presentación de solvencia técnica en presentación ofertas y/o solicitud, gestión y justificación de campañas, actividades, eventos, concursos, proyectos y subvenciones en los que participe la organización
- Control horario y/o presencial o de asistencia y monitorización del desempeño funcional
- Gestión del Cumplimiento Normativo (normativa aplicable así como normativa interna de obligado cumplimiento): Investigación, monitorización y auditoría de controles establecidos para la prevención de delitos pudiendo establecerse los controles de acceso a las instalaciones, sistemas de información e impresión de documentación para todos los datos de carácter personal bajo responsabilidad de la organización y por lo tanto para todos los sistemas de información de dicha entidad, así como los controles relativos al uso de las imágenes captadas por los sistemas de videovigilancia para la investigación de los accidentes y/o incidentes que pudieran producirse, así como incumplimientos de normas laborales, delitos o comportamientos ilícitos.
- Gestión de Contactos / Agenda
- Fines estadísticos, históricos o científicos
- Control de accesos y Videovigilancia de las Instalaciones, así como de la seguridad y el cumplimiento normativo en las mismas, preservar la seguridad de las personas y bienes e instalaciones, así como para el ejercicio de las funciones de control de los trabajadores previstas en el artículo 20.3 del Estatuto de los Trabajadores, la investigación de posibles incidentes o accidentes, gestión de seguros asociados y gestión de apercibimientos o sanciones por incumplimientos de normas de seguridad.
- La gestión y auditoría de la calidad, gestión ambiental y/o gestión de seguridad laboral de procesos e instalaciones de la organización
- Gestión asociada, incluida su comunicación con carácter previo, que pudiera derivarse del desarrollo de cualquier operación de modificación estructural de sociedades o la aportación o transmisión de negocio o de rama de actividad empresarial, siempre que los tratamientos fueran necesarios para el buen fin de la operación y garanticen, cuando proceda, la continuidad en la prestación de servicios.
- Inclusión en los sistemas de canal de denuncias de los datos asociados a la puesta en conocimiento (incluso de forma anónima) de la comisión en el seno de la organización o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable.
- Otros: SOTRAFA, S.A. se reserva el derecho de realizar auditorías periódicas en las instalaciones de proveedores y acreedores

¿Cuánto tiempo conservamos sus datos?

- Los datos proporcionados se conservarán mientras se mantenga la relación de licitud de tratamiento, no se solicite su supresión por el interesado tras finalización formalizada por escrito de la relación con el interesado, con excepción de su conservación para la formulación, el ejercicio o la defensa de reclamaciones del responsable de tratamiento o con miras a la protección de los derechos de otra persona física o jurídica y/o por razones de obligación legal.
- En cualquier caso, al término de la relación los Datos del interesado serán debidamente bloqueados, según lo previsto en la normativa vigente de protección de datos.
- Documentación Contable y Fiscal - A efectos Fiscales: Los libros de contabilidad y otros libros registros obligatorios según la normativa tributaria que proceda (IRPF, IVA, IS, etc), así como los soportes documentales que justifiquen las anotaciones registradas en los libros (incluidos los programas y archivos informáticos y cualquier otro justificante que tengan trascendencia fiscal), deben conservarse, al menos, durante el periodo en que la Administración tiene derecho a comprobar e investigar y, en consecuencia, a liquidar deuda tributaria (Arts. 66 a 70 Ley General Tributaria). Plazo prescripción de Delitos Fiscales asociados a la comprobación de las bases o cuotas compensadas o pendientes de compensación o de deducciones aplicadas o pendientes de aplicación y a Delitos contra la Hacienda Pública y la Seguridad Social - Art. 66 bis Ley General Tributaria y Código Penal, respectivamente. - 4 años. Prescripción infracciones 10 años.
- Documentación Contable y Fiscal - A efectos Mercantiles: Libros, correspondencia, documentación y justificaciones concernientes a su negocio, debidamente ordenados a partir del último asiento realizado en los libros, salvo lo que se establezca por disposiciones generales o especiales. Esta obligación mercantil se extiende tanto a los libros obligatorios (ingresos, gastos, bienes de inversión y provisiones además de la documentación y justificantes en que se soporten las anotaciones registradas en los libros (facturas emitidas y recibidas, tickets, facturas rectificativas, documentos bancarios, etc) (Art.30 Código de Comercio) - 6 años.
- Documentación de Prevención de Riesgos Laborales - Documentación sobre información y formación a los trabajadores. Expedientes de accidentes laborales o enfermedades profesionales (RD Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social) - 5 años.
- Las imágenes/sonidos captados por los sistemas de videovigilancia serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones (en cuyo caso, las imágenes serán puestas a disposición de la autoridad competente en un plazo máximo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación), o estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto (Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras y Art.22 LOPDGD) - 30 días.
- Los datos incluidos en los tratamientos automatizados creados para controlar el acceso a edificios (Instrucción 1/1996, de 1 de Marzo, de la AEPD, sobre Ficheros automatizados establecidos con la finalidad de controlar el acceso a edificios) - 30 días
- Los datos tratados en relación con la garantía legal serán conservados durante la vigencia de la garantía legal y expirada la vigencia de la misma, durante el plazo que pudiera haber una reclamación judicial o administrativa en relación con la garantía legal.
- Ficheros de Solvencia: Datos referidos a deudas ciertas, vencidas y exigibles y no reclamadas (Art. 20 de LOPDGD) - mientras persista el incumplimiento, con el límite máximo de cinco años desde la fecha de vencimiento de la obligación dineraria, financiera o de crédito - 5 años
- Los datos tratados para la remisión de comunicaciones comerciales serán conservados hasta que revoque el consentimiento otorgado.
- Los datos de quien formule la comunicación de una denuncia y de los empleados y terceros se conservan en el sistema de denuncias para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados, así como posteriormente como evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica, conforme a lo establecido en el artículo 24 de la LOPDGD.
- Por lo tanto, los datos serán conservados mientras se mantenga vigente la relación comercial, en base a los plazos de conservación establecidos por la normativa vigente apuntada anteriormente, así como los plazos legal o contractualmente previstos para el ejercicio o prescripción de cualquier acción de responsabilidad por incumplimiento contractual por parte del interesado o de la Organización (reforma del Código Civil establece un plazo de 5 años para poder llevar a cabo una acción por responsabilidad civil, plazo que computa desde la fecha en que pueda exigirse el cumplimiento de la obligación).

¿Cuál es la legitimación para el tratamiento de sus datos?

- La ejecución de un contrato: Cumplimiento de la oferta, pedido y/o contrato comercial.

- Cumplir con una obligación jurídica: Normativa con rango de ley administrativa, mercantil, tributaria, fiscal, contable y financiera, de prevención de riesgos laborales, seguridad social y normativa aplicable del sector.
- Satisfacer un interés legítimo del Responsable: Tratamiento de datos como partes de una relación comercial y/o contrato, que sean necesarios para su mantenimiento o cumplimiento, transmisiones de datos dentro de grupos empresariales para fines administrativos internos, prevención del fraude, así como supuestos de interés legítimo en los que el responsable pudiera ser parte perjudicada y fuera necesario el tratamiento y la comunicación de los datos del incumplidor a terceros a fin de gestionar el cumplimiento normativo y la defensa de los intereses del responsable de tratamiento, fines de videovigilancia como interés legítimo de la organización en la protección de sus activos, así como supuestos de interés legítimo de tratamientos específicos contemplados en la LOPDGDD: Artículo 19. Tratamiento de datos de contacto y de empresarios individuales; Artículo 20. Sistemas de información crediticia; Artículo 21. Tratamientos relacionados con la realización de determinadas operaciones mercantiles (reestructuración societaria o transmisiones de negocio) Artículo 22. Tratamientos con fines de videovigilancia; Artículo 24 Sistemas de información de denuncias internas).
- El consentimiento del interesado que nos haya facilitado de forma inequívoca a través de medios formales y/o marcando las casillas habilitadas a tal efecto en las cláusulas de protección de datos habilitadas en el documento base que haya regulado la relación comercial en función del canal de contacto.

¿A qué destinatarios se pueden comunicar sus datos?

- Organizaciones o personas directamente contratadas por el Responsable de Tratamiento para la prestación de servicios vinculados con las finalidades de tratamiento: Empresas del Grupo (ver relación en www.armandoalvarez.com), Asesoría Jurídica, Auditores de Gestión y/o de Cumplimiento Normativo, Servicios de Prevención, terceros a los que se les facilita datos de trabajadores de subcontratas para el acceso a sus instalaciones.
- Organismos u órganos de la Administración Pública con competencias en las materias objeto de las finalidades del tratamiento: AEAT
- Entidades Financieras: Transferencia y/o gestión de efectos de pago.
- Sindicatos, Juntas de Personal/Comité de Empresa: Representantes de los Trabajadores: Contratas o subcontratas que se establezcan (incluidos autónomos) (art.35.2 CC y art.42 ET); CIF/NIF, razón social, domicilio social, objeto de la contrata, número de patronal de inscripción de la Seguridad Social, lugar de ejecución de la contrata, coordinación de actividades desde el punto de vista de riesgos laborales, duración estimada de la contrata (fecha de inicio y término). Número de trabajadores que serán ocupados por la contrata o subcontrata en el centro de trabajo de la empresa principal.
- Canal de Denuncias Compliance (Las denuncias sobre vulneración de normativa y código de conducta son transmitidas a la Unidad de Cumplimiento Normativo): El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a quienes, incardinados o no en el seno de la entidad, desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan.
- Delegados de Prevención de Riesgos se les faculta para acceder a la información y documentación relativa a las condiciones de trabajo que sean necesarias para el ejercicio de sus funciones y, en particular, a la prevista en los artículos 18, 23 Y 36 LPRL. los Delegados de Prevención les será de aplicación lo dispuesto en el apartado 2 del artículo 65 del Estatuto de los Trabajadores en cuanto al sigilo profesional debido respecto de las informaciones a que tuviesen acceso como consecuencia de su actuación en la empresa. (Artículo 37.3 LPRL).
- Servicios de Prevención de Riesgos Laborales: el tratamiento por parte de los servicios de prevención de riesgos laborales del historial médico, consecuencia de los reconocimientos médicos realizados a los trabajadores, deberá limitarse a las previsiones del artículo 22.4 de la LPRL. En este sentido, se prohíbe el acceso a la información médica obtenida al amparo de lo dispuesto en la LPRL por parte del empresario o de cualquier tercero, incluidas las personas u órganos con responsabilidades en materia de prevención, distintos del "personal médico y a las autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores", con la única excepción de las conclusiones derivadas de dicho seguimiento en cuanto a la aptitud de los trabajadores para el desempeño del puesto de trabajo.

¿Bajo qué garantías se comunican sus datos?

La comunicación de datos a terceros se realiza a entidades que acrediten la disposición de un Sistema de Protección de Datos de Carácter Personal acorde a la legalidad vigente.

¿Cómo hemos obtenido sus datos?

- El propio interesado o su representante legal
- Otras Empresas del Grupo, así como la entidad con la que el responsable de tratamiento mantiene una relación contractual o de prestación de servicios y para lo cual ha de disponer de datos personales de personas de contacto para la gestión administrativa y operacional a fin de gestionar su acceso, incorporación al proyecto/servicio objeto y/o verificación del cumplimiento normativo bajo responsabilidad de la organización (pej, datos relativos a trabajadores que vayan a efectuar los trabajos contratados en términos de coordinación de actividades empresariales asociados a la prevención de riesgos laborales).

¿Qué categoría de datos tratamos?

Datos mercantiles, de personas de contacto para la gestión administrativa y operacional asociada a la ejecución del contrato/proyecto y de trabajadores que vayan a efectuar los trabajos contratados en términos de coordinación de actividades empresariales asociados a la prevención de riesgos laborales; Como consecuencia de la aportación de currículum de personal del proveedor involucrado en la prestación del servicio/trabajo, a fin de acreditar solvencia técnica en ofertas; En el caso de trabajadores que vayan a efectuar los trabajos contratados en términos de coordinación de actividades empresariales asociados a la prevención de riesgos laborales (Los datos que pudieran derivarse de posibles incidentes o accidentes laborales de trabajadores de subcontratas estarían incorporados en el tratamiento "Prevención de Riesgos Laborales"); Licencias u homologaciones, en el caso de trabajadores que vayan a efectuar los trabajos contratados en términos de coordinación de actividades empresariales asociados a la prevención de riesgos laborales; Detalles profesionales y de detalle de empleo como consecuencia de la aportación de currículum de personal del proveedor involucrado en la prestación del servicio/trabajo, a fin de acreditar solvencia técnica en ofertas; Datos de información comercial y homologación; Datos económico, financieros y/o de condiciones de cobro; Bienes y servicios suministrados por el afectado, Transacciones financieras; Otro tipo de datos: Nombre, apellidos y NIF de representante legal, datos de contacto de personas de la organización involucradas o relacionadas con el proyecto objeto del contrato/pedido.

La estructura de datos que tratamos no contiene datos relativos a condenas e infracciones penales, ni datos sensibles, salvo en los casos en los que el titular disponga de condiciones especiales y haya de facilitar documentación que incorpore dicha información a fin de que pueda ser acreditado o justificado el cumplimiento de dicha condición.

¿Cómo se guardan sus datos personales de forma segura?

SOTRAFA, S.A. toma todas las medidas necesarias para guardar sus datos personales de forma privada y segura. Sólo personas autorizadas de SOTRAFA, S.A., personal autorizado de Terceros o personal autorizado de nuestras empresas (que tienen la obligación legal y contractual de guardar toda la información de forma segura) tienen acceso a sus datos personales. Se exige a todo el personal de SOTRAFA, S.A. que tiene acceso a sus datos personales que se comprometa a respetar la Política de Privacidad de SOTRAFA, S.A. y la normativa de protección de datos y a todos los empleados de Terceros que tienen acceso a tus datos personales que firmen los compromisos de confidencialidad en los términos establecidos en la legislación vigente. Además, se asegura contractualmente que las empresas de terceros que tienen acceso a sus datos personales los mantengan de forma segura. Para asegurarnos de que sus datos personales están protegidos, SOTRAFA, S.A. dispone de un entorno de seguridad IT y adopta las medidas necesarias para evitar accesos no autorizados. SOTRAFA, S.A. ha formalizado acuerdos para garantizar que tratamos sus datos personales correctamente y de acuerdo con la ley de protección de datos. Estos acuerdos reflejan las respectivas funciones y responsabilidades en relación con usted, y contemplan qué entidad se encuentra en la mejor posición para cumplir con sus necesidades. Estos acuerdos entre empresas del grupo no afectan a sus derechos en virtud de la ley de protección de datos. Para obtener más información sobre estos acuerdos, no dude en ponerse en contacto con nosotros.

CONFIDENCIALIDAD E INFORMACIÓN A TERCEROS DE LOS QUE NOS FACILITE DATOS

En cumplimiento de lo que dispone la normativa de protección de datos de carácter personal tratamos la información que nos facilita (así como los datos personales de personas de contacto para la gestión administrativa y operacional a fin de gestionar su acceso, incorporación al proyecto/servicio objeto del servicio contratado y/o verificación del cumplimiento normativo bajo responsabilidad de la organización, datos personales de los

representantes legales de la entidad y/o de las personas involucradas en el proyecto (currículum vitae) y/o referencias personales de trabajos previos a fin de acreditar solvencia técnica y, en su caso, datos personales relativos a trabajadores que vayan a efectuar los trabajos contratados en términos de coordinación de actividades empresariales asociados a la prevención de riesgos laborales) conforme a lo establecido en la cláusula e información adicional sobre protección de datos.

Con la aceptación y/o validación del proceso que sirve de base para la formalización de su relación con SOTRAFA, S.A., consiente expresamente el tratamiento de datos conforme a lo establecido en la cláusula e información adicional sobre protección de datos, así como informar y disponer del consentimiento de terceros de los que nos facilite datos personales para dicho tratamiento. Asimismo, y en la medida en que como consecuencia de su relación con SOTRAFA, S.A. pueda acceder a datos personales y/o información confidencial, se obliga a mantener absoluta confidencialidad y discreción sobre la información obtenida acerca de las actividades, partes interesadas y entidades relacionadas con SOTRAFA, S.A., especialmente en lo que se refiere a Datos de Carácter Personal, incluso tras la finalización de su relación con la organización.

Conforme a lo señalado anteriormente, se compromete a informar en nombre y por cuenta de SOTRAFA, S.A. de forma expresa, precisa e inequívoca a los titulares de los datos de quienes ceda información a SOTRAFA, S.A. -dentro del mes siguiente al momento de la comunicación de los datos a SOTRAFA, S.A., de los siguientes aspectos "Sus datos personales serán comunicados al Responsable de Tratamiento SOTRAFA, S.A. - gdp@sotrafa.com. Dicha comunicación de datos y el tratamiento de éstos por SOTRAFA, S.A., se realiza en cumplimiento de la legislación vigente en materia contractual, laboral, de prevención de riesgos laborales y de seguridad social, con la finalidad de informar, verificar y controlar el cumplimiento de la legislación aplicable en relación con el personal designado por el proveedor/colaborador para la ejecución de la prestación contratada por SOTRAFA, S.A. y el mantenimiento de históricos de relaciones comerciales. Dicho tratamiento tiene carácter obligatorio de acuerdo con la Legislación vigente. La negativa a suministrar los datos a SOTRAFA, S.A. podrá suponer la resolución del contrato. Asimismo, se informa al interesado que, de conformidad con la legislación vigente, SOTRAFA, S.A. deberá comunicar la información y datos obrantes en el proceso de contratación a organismos y terceros a quienes, en virtud de la normativa vigente, SOTRAFA, S.A. tuviese la obligación de comunicar los datos. **Derechos:** El interesado podrá acceder, rectificar y suprimir los datos, así como limitar, retirar u oponerse al tratamiento conforme a los procedimientos establecidos en nuestra política de privacidad. Si considera que el ejercicio de sus derechos no ha sido plenamente satisfactorio, podrá presentar una reclamación ante la autoridad nacional de control dirigiéndose a estos efectos a la Agencia Española de Protección de Datos, C/ Jorge Juan, 6 - 28001 Madrid. **Origen:** Los datos que tratamos proceden de la entidad con la que el responsable de tratamiento mantiene una relación contractual o de prestación de servicios y para lo cual ha de disponer de datos personales de personas de contacto para la gestión administrativa y operacional a fin de gestionar su acceso, incorporación al proyecto/servicio objeto y/o verificación del cumplimiento normativo bajo responsabilidad de la organización (pej, datos relativos a trabajadores que vayan a efectuar los trabajos contratados en términos de coordinación de actividades empresariales y prevención de riesgos laborales). **La Estructura de datos que tratamos no contiene datos sensibles, salvo en los casos en los que el titular sea beneficiario de condiciones especiales y haya de facilitar registros que permitan acreditar o justificar el cumplimiento de dicha condición. Puede consultar nuestra Política de Privacidad en la web corporativa"**

INFORMACIÓN ADICIONAL TRATAMIENTO DE DATOS DE VIDEOVIGILANCIA Y REGISTRO DE ACCESOS:

¿Con qué finalidad tratamos los datos personales que nos facilita? (*) La relación de actividades de SOTRAFA, S.A. está a su disposición en www.sotrafa.com

- Control de Accesos/Visitas y Videovigilancia de las Instalaciones, así como de la seguridad y el cumplimiento normativo en las mismas, preservar la seguridad de las personas y bienes e instalaciones, así como para el ejercicio de las funciones de control de los trabajadores previstas en el artículo 20.3 del Estatuto de los Trabajadores, la investigación de posibles incidentes o accidentes, gestión de seguros asociados y gestión de apercibimientos o sanciones por incumplimientos de normas de seguridad, a través del sistema de videovigilancia.

- Verificar el cumplimiento por parte de trabajadores de sus obligaciones y deberes laborales conforme al artículo 20.3 del Estatuto de los Trabajadores que faculta al empresario a adoptar medidas de vigilancia y control al efecto (controles relativos al uso de las imágenes captadas por los sistemas de videovigilancia para la investigación de los accidentes y/o incidentes que pudieran producirse, así como incumplimientos de normas laborales, delitos o comportamientos ilícitos).

- Gestión de la seguridad y salud (prevención de riesgos laborales y vigilancia de la seguridad) y evaluación de cumplimiento

- Control horario y/o presencial o de asistencia y monitorización del desempeño funcional

- Gestión del Cumplimiento Normativo (normativa aplicable así como normativa interna de obligado cumplimiento): Investigación, monitorización y auditoría de controles establecidos para la prevención de delitos pudiendo establecerse los controles de acceso a las instalaciones, sistemas de información e impresión de documentación para todos los datos de carácter personal bajo responsabilidad de la organización y por lo tanto para todos los sistemas de información de dicha entidad, así como los controles relativos al uso de las imágenes captadas por los sistemas de videovigilancia para la investigación de los accidentes y/o incidentes que pudieran producirse, así como incumplimientos de normas laborales, delitos o comportamientos ilícitos.

- Registro de Accesos/Visitas y Videovigilancia de las Instalaciones, así como de la seguridad y el cumplimiento normativo en las mismas, la investigación de posibles incidentes o accidentes, gestión de seguros asociados y gestión de apercibimientos o sanciones por incumplimientos de normas de seguridad.

- Otros (especificar): la investigación de posibles incidentes o accidentes laborales, gestión de seguros asociados, así como para la investigación ante incidentes y confirmación del cumplimiento de las normas de seguridad y protección de datos de carácter personal establecidas en los sistemas de protección de datos y sistemas de gestión implantados para todos los datos de carácter personal bajo responsabilidad de la organización y por lo tanto para todos los sistemas de información de dicha entidad, así como los controles relativos al uso de las imágenes captadas por los sistemas de videovigilancia para la investigación de los accidentes y/o incidentes que pudieran producirse, así como incumplimientos de normas laborales, delitos o comportamientos ilícitos.

- Control temporal de la temperatura corporal para poder acceder a la entidad con las siguientes finalidades (detectar posibles personas contagiadas y evitar su acceso a un determinado lugar y su contacto dentro de él con otras personas):

- Proteger la salud y vida de las personas que se encuentran en este centro de trabajo.
- Contribuir a la contención de la pandemia.
- Cumplir con la normativa de prevención de riesgos laborales.
- Verificar el cumplimiento, por parte de los trabajadores, de la obligación de acudir al centro de trabajo sin fiebre.

- Inclusión en los sistemas de canal de denuncias de los datos asociados a la puesta en conocimiento (incluso de forma anónima) de la comisión en el seno de la organización o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable.

¿Cuánto tiempo conservamos los datos facilitados?

- Las imágenes/sonidos captados por los sistemas de videovigilancia serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones (en cuyo caso, las imágenes serán puestas a disposición de la autoridad competente en un plazo máximo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación), o estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto (Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras y Art.22 LOPDGGD) - 30 días.

- Los datos incluidos en los ficheros automatizados creados para controlar el acceso a edificios (Instrucción 1/1996, de 1 de Marzo, de la AEPD, sobre Ficheros automatizados establecidos con la finalidad de controlar el

acceso a edificios) - 30 días

- Los datos de quien formule la comunicación de una denuncia y de los empleados y terceros se conservan en el sistema de denuncias para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados, así como posteriormente como evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica, conforme a lo establecido en el artículo 24 de la LOPDGDD.
- La entidad tiene establecido como periodo de conservación de los datos de control de temperaturas como el necesario para hacer frente a eventuales acciones legales derivadas de la decisión de denegación de accesos

¿Cuál es la legitimación para el tratamiento de sus datos?

- La base legal para el tratamiento de sus datos es satisfacer un interés legítimo del Responsable:
- Seguridad y supuestos de interés legítimo en los que el responsable pudiera ser parte perjudicada y fuera necesario el tratamiento y la comunicación de los datos del incumplidor a terceros a fin de gestionar el cumplimiento normativo y la defensa de los intereses del responsable de tratamiento, así como supuestos de interés legítimo de tratamientos específicos contemplados en la LOPDGDD: Artículo 19. Tratamiento de datos de contacto y de empresarios individuales; Artículo 22. Tratamientos con fines de videovigilancia; Artículo 24 Sistemas de información de denuncias internas).
- Art. 20.3 y 4 Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (ET): El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso.
- El empresario podrá verificar el estado de enfermedad o accidente del trabajador que sea alegado por éste para justificar sus faltas de asistencia al trabajo, mediante reconocimiento a cargo de personal médico. La negativa del trabajador a dichos reconocimientos podrá determinar la suspensión de los derechos económicos que pudieran existir a cargo del empresario por dichas situaciones
- (*) Sentencia del Tribunal Constitucional 39/2016, de 3 de marzo (LA LEY. 218/2016), al argumentar que esta facultad de control viene legitimada por el art. 20.3 del ET, que expresamente faculta al empresario a adoptar medidas de vigilancia y control para verificar el cumplimiento por los trabajadores de sus obligaciones laborales. Esta facultad general de control prevista en la ley, legitima el control empresarial del cumplimiento por parte de los trabajadores de sus tareas profesionales y el consentimiento de los trabajadores a tales efectos viene implícito en la celebración del contrato de trabajo. La legitimación de esta finalidad se cumple con la existencia de varios distintivos desplegados por la organización en las instalaciones que anuncian la presencia de instalación de cámaras y captación de imágenes y con una información explícita, a poder ser por escrito, consistente en que se les va a grabar, con el único objetivo de controlar el cumplimiento de las obligaciones laborales y que se les podrá sancionar con arreglo a las imágenes grabadas en caso de incumplimiento constatado. En el mismo sentido, STS 77/2017 de 31 de enero 2017.
- Guía AEPD Videovigilancia: El artículo 20.3 del Estatuto de los Trabajadores faculta al empresario para adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso. Entre estas medidas puede estar la captación y/o tratamiento de imágenes sin consentimiento. No obstante, tales prácticas se encuentran plenamente sometidos a la LOPD y la Instrucción 1/2006 y deben cumplir con requisitos específicos.
- Como base jurídica del tratamiento asociado al control de temperaturas, se especifica el cumplimiento de la obligación legal de garantizar la seguridad y la salud de los trabajadores. Esta base jurídica se concreta en este caso en las siguientes normas:
 - [Estatuto de los Trabajadores.](#)
 - [Ley 21/1995 de Prevención de Riesgos Laborales.](#)
 - [Real Decreto 664/1997 sobre la protección de los trabajadores contra los riesgos relacionados con la exposición a agentes biológicos durante el trabajo*](#)
 - [Procedimiento de actuación para los servicios de prevención de riesgos laborales frente a la exposición al SARS-CoV-2](#)
 - [Directrices de buenas prácticas en el sector industrial en relación al Covid-19 \(Instituto Nacional de Seguridad y Salud en el Trabajo\).](#)
 - [Directrices adoptadas por el servicio de PRL de la entidad por habilitación legal y delegación de funciones preventivas.](#)

¿A qué destinatarios se pueden comunicar sus datos?

- Organizaciones o personas directamente contratadas por el Responsable de Tratamiento para la prestación de servicios vinculados con las finalidades de tratamiento (especificar): Empresa de seguridad contratada
- Entidades Aseguradoras (especificar): En caso de siniestro, incidente o accidente se facilita a entidades aseguradoras para la investigación del suceso a fin de delimitar alcance y cobertura de la prima de seguro contratada por el responsable de tratamiento.
- Fuerzas y Cuerpos de Seguridad (especificar): En la medida en que fuera requerido un derecho de acceso justificado en la investigación de un incumplimiento normativo.
- El dueño del establecimiento, por interés legítimo en la protección de los activos bajo su propiedad
- Jueces y Tribunales, así como Fuerzas y Cuerpos de Seguridad: En la medida en que fuera requerido un derecho de acceso justificado en la investigación de un incumplimiento normativo.
- En el caso de temperaturas por encima del umbral sanitario, no se permitirá el acceso a la persona y se le encomendará a los servicios de atención primaria (en caso de externos) o al servicio de vigilancia de la salud (en el caso de internos) para, conforme al protocolo, se le realicen las pruebas diagnósticas y demás comunicaciones establecidas conforme al protocolo de control de la pandemia.
- Canal de Denuncias Compliance (Las denuncias sobre vulneración de las normas de protección de datos son transmitidas al “Chief Privacy Officer” que se encuentra en la matriz del Grupo): El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a quienes, incardinados o no en el seno de la entidad, desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan.

¿Bajo qué garantías se comunican sus datos?

La comunicación de datos a terceros se realiza a entidades que acrediten la disposición de un Sistema de Protección de Datos de Carácter Personal acorde a la legalidad vigente.

¿Qué vías de reclamación existen?

Si considera que el ejercicio de sus derechos no ha sido plenamente satisfactorio, podrá presentar una reclamación ante la autoridad nacional de control dirigiéndose a estos efectos a la Agencia Española de Protección de Datos, C/ Jorge Juan, 6 - 28001 Madrid.

¿Qué categoría de datos tratamos?

Imagen y datos identificativos y profesionales, así como motivos de su visita y/o persona a visitar, hora de acceso y salida de la instalación
Así mismo, se pueden disponer de datos de control de temperatura en la medida en que se lleven a cabo controles temporales de temperatura para el acceso a las instalaciones a efectos de control de evitación de pandemias, según Protocolo de Tratamiento de Datos COVID que pudiera establecerse en términos de garantizar la seguridad laboral de las personas de la organización.

¿Cómo se guardan sus datos personales de forma segura?

SOTRAFA, S.A. toma todas las medidas necesarias para guardar sus datos personales de forma privada y segura y atenderá en cualquier caso a lo previsto en la Ley 5/2014, de 4 de abril, de Seguridad Privada y sus

disposiciones de desarrollo. En este sentido, establece y le informa de las siguientes medidas de seguridad:

- **DEBER DE INFORMACIÓN:** Se informa acerca de la existencia de las cámaras y grabación de imágenes, a fin de cumplir con el deber de información previsto en el artículo 12 del RGPD a través de un dispositivo informativo en lugar suficientemente visible identificando la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del RGPD. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información. En todo caso, SOTRAFA, S.A. mantiene a disposición de los afectados la información a la que se refiere el citado reglamento en la presente Política de Privacidad referenciada en el citado dispositivo. En el supuesto de que se haya captado la comisión flagrante de un acto ilícito se entenderá cumplido el deber de informar cuando exista al menos el dispositivo informativo de videovigilancia.
- **UBICACIÓN DE LAS CÁMARAS:** SOTRAFA, S.A. sólo captará imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad de preservación de seguridad. En ningún caso SOTRAFA, S.A. instala sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos.
- **CAPTACIÓN DE SONIDOS:** SOTRAFA, S.A. sólo llevará a cabo la grabación de sonidos cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías.
- **UBICACIÓN DE MONITORES:** Los monitores donde se visualizan las imágenes de las cámaras se ubican en un espacio de acceso restringido de forma que no sean accesibles a terceros no autorizados.
- **CONSERVACIÓN:** Las imágenes/sonidos captados por los sistemas de videovigilancia serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones (en cuyo caso, las imágenes serán puestas a disposición de la autoridad competente en un plazo máximo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación), o estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto (Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras y Art.22 LOPDGDD) - 30 días.
- **CONTROL LABORAL:** El tratamiento se realiza para el ejercicio de las funciones de control de los trabajadores previstas en el artículo 20.3 del Estatuto de los Trabajadores, dentro de su marco legal y con los límites inherentes al mismo. En la medida en que las cámaras pueden ser utilizadas con la finalidad de control laboral según lo previsto en el artículo 20.3 del Estatuto de los Trabajadores, se informa a los trabajadores y a sus representantes acerca de las presentes medidas de control establecidas por el empresario con indicación expresa de la finalidad de control laboral de las imágenes captadas por las cámaras, conforme a lo indicado en la cláusula de notificación de inclusión y en la presente política de privacidad.
- **DERECHO DE ACCESO A LAS IMÁGENES:** Para dar cumplimiento al derecho de acceso de los interesados se solicitará una fotografía reciente y el Documento Nacional de Identidad del interesado, así como el detalle de la fecha y hora a la que se refiere el derecho de acceso. No se facilitará al interesado acceso directo a las imágenes de las cámaras en las que se muestren imágenes de terceros. Para evitar la afeción a derechos de terceros, en el caso de solicitud de acceso, procederemos a emitir un certificado en el que, con la mayor precisión posible y sin afectar a derechos de terceros, se especifiquen los datos que han sido objeto de tratamiento. Ej. "Su imagen fue registrada en nuestros sistemas el día ___ del mes del año entre las _ horas y las _ horas. En concreto el sistema registra su acceso y salida de la instalación."

SOTRAFA, S.A. ha formalizado acuerdos para garantizar que tratamos sus datos personales correctamente y de acuerdo con la normativa vigente de protección de datos. Estos acuerdos reflejan las respectivas funciones y responsabilidades en relación con usted, y contemplan qué entidad se encuentra en la mejor posición para cumplir con sus necesidades. Estos acuerdos no afectan a sus derechos en virtud de la ley de protección de datos. Para obtener más información sobre estos acuerdos, no dude en ponerse en contacto con nosotros.

El responsable de Tratamiento toma todas las medidas necesarias para guardar sus datos personales de forma privada y segura. Sólo personas autorizadas de SOTRAFA, S.A., personal autorizado de terceros directamente contratados por el Responsable de Tratamiento para la prestación de servicios vinculados con las finalidades de tratamiento o personal autorizado de empresas que giran bajo el nombre comercial de SOTRAFA, S.A. (que tienen la obligación legal y contractual de guardar toda la información de forma segura) tienen acceso a sus datos personales. Se exige a todo el personal de SOTRAFA, S.A. que tiene acceso a sus datos personales que se comprometa a respetar la Política de Privacidad del responsable de Tratamiento y la normativa de protección de datos y a todos los empleados de Terceros que tienen acceso a sus datos personales que firmen los compromisos de confidencialidad en los términos establecidos en la legislación vigente. Además, se asegura contractualmente que las empresas de terceros que tienen acceso a sus datos personales los mantengan de forma segura. Para asegurarnos de que sus datos personales están protegidos, SOTRAFA, S.A. dispone de un entorno de seguridad IT y adopta las medidas necesarias para evitar accesos no autorizados.

CAMBIOS EN POLÍTICA DE PRIVACIDAD

SOTRAFA, S.A. se reserva el derecho a efectuar, en cualquier momento, cuantas modificaciones, variaciones, supresiones o cancelaciones en los contenidos y en la forma de presentación de los mismos que considere oportunas, por cuanto le recomendamos que consulte nuestra política de privacidad siempre que lo considere pertinente. Si no está de acuerdo con cualquiera de los cambios, puede ejercer sus derechos conforme al procedimiento descrito enviando un correo a gdpr@sotrafa.com

En cumplimiento de lo que dispone la normativa de protección de datos de carácter personal, tratamos la información que nos facilita (así como los datos personales de otras personas que nos pudiera facilitar) con las finalidades especificadas en la presente política de privacidad. En este sentido, declara haber sido informado, consentir, así como informar y disponer del consentimiento de terceros de los que nos facilite datos personales para dicho tratamiento.

Con el acceso a las instalaciones sometidas a videovigilancia consiente expresamente el tratamiento de datos conforme a lo establecido en la cláusula e información adicional sobre protección de datos, así como informar y disponer del consentimiento de terceros de los que nos facilite datos personales para el tratamiento de registro de accesos.

Así mismo, con la aceptación y/o validación del proceso, declara ser mayor de 14 años y disponer de capacidad jurídica*** y consiente expresamente el tratamiento de datos conforme a lo establecido en la cláusula e información adicional sobre protección de datos. Si ha marcado la casilla correspondiente de consentimiento, la base legal para dichos fines es su consentimiento, que puede retirar en cualquier momento.

(***) En los casos en los que represente a un menor de 14 años o a una persona con incapacidad jurídica, declara responsablemente disponer de la patria potestad o tutela del menor o de la representación legal jurídica correspondiente, cuya justificación podrá ser requerida por parte del Responsable de Tratamiento a fin de legitimar el consentimiento aceptado.