Contrato de encargo del tratamiento
de conformidad con el artículo 28 del Reglamento general de protección de datos (RGPD)

en lo sucesivo, "el Contrato"

entre

Comunidad de propietarios

Responsable del tratamiento –en lo sucesivo, el Cliente–

y

Ista Metering Services España S.A.

Encargado del tratamiento –en lo sucesivo, el Contratista–

1. Objeto y duración del Contrato

1. Objeto del Contrato

El objeto del Contrato y los datos de contacto del Cliente se derivan de los respectivos contratos, en base a los cuales el Contratista proporciona determinados servicios al Cliente a los que se hace referencia en el Contrato de prestación de servicios de **Lectura de datos de consumo de agua, emisión de los recibos correspondientes a cada contador individual** (en lo sucesivo, el Contrato de Servicios).

2. Duración

La duración del presente Contrato (plazo) se corresponde con la duración del plazo del Contrato de servicios.

2. Especificación del contenido del Contrato

1. Tipo y objeto del tratamiento de datos previsto

El tipo y objeto del tratamiento de datos personales por parte del Contratista para el Cliente se describen específicamente en el Contrato de Servicios.

La prestación del tratamiento de datos acordado contractualmente se produce exclusivamente en un Estado miembro de la Unión Europea o en otro estado que sea parte en el Acuerdo sobre el Espacio Económico Europeo. Para cualquier transferencia a un tercer país será necesario el consentimiento previo del Cliente y sólo podrá realizarse si se cumplen los requisitos especiales del artículo 44 y siguientes del RGPD.

2. Tipos de datos

El objeto del tratamiento de datos personales implica los siguientes tipos/categorías de datos:

- Datos identificativos
- Datos de contacto (p. ej., teléfono, correo electrónico)
- Datos contractuales (relación contractual, interés contractual o de producto)
- Historial del cliente
- Lecturas diarias
- Recibos de consumos
- Datos de control y planificación
- Datos del arrendatario (p. ej., nombre, dirección, prorrateo, datos de consumo tales como lecturas diarias y de fin del periodo de liquidación, etc.)

3. Categorías de personas afectadas

Las categorías de personas afectadas por el tratamiento incluyen:

- Clientes
- Socios de servicio de Ista (lectores de contadores, instaladores)
- Empleados
- Proveedores
- Contactos
- Arrendatarios

3. Medidas técnicas y organizativas

1. El Contratista aplicará las medidas técnicas y organizativas del **Anexo**. Las medidas documentadas constituyen la base del Contrato. Si de la inspección realizada por la autoridad de control o de la Evaluación de Impacto de Protección de Datos realizada se desprendiese la necesidad de efectuar ajustes en dichas medidas, estos deberán aplicarse de mutuo acuerdo.

2. El Contratista deberá mantener la seguridad de conformidad con los artículos 28, apartado 3, letra c), y 32 del RGPD, en particular en relación con el artículo 5, apartados 1 y 2 del RGPD. En general, las medidas que se deben adoptar son relativas a la seguridad de los datos y a garantizar un nivel de protección adecuado al riesgo respecto a la confidencialidad, integridad, disponibilidad y capacidad de los sistemas. Se deben tener en cuenta el estado de la tecnología, los costes de aplicación y el tipo, alcance y finalidad del tratamiento, así como la diferente probabilidad de que los riesgos se produzcan y la gravedad que dichos riesgos supongan para los derechos y libertades de las personas físicas en el sentido del artículo 32, apartado 1 del RGPD. Encontrará información más detallada en el **Anexo**

3. Las medidas técnicas y organizativas están sujetas al avance técnico y el desarrollo. A este respecto, el Contratista está autorizado a aplicar medidas adecuadas alternativas. El nivel de

seguridad de las medidas definidas no debe reducirse. Los cambios significativos deben documentarse.

4. Corrección, restricción y eliminación de datos

1. El Contratista no puede rectificar, borrar ni restringir el tratamiento de los datos que se procesan en el Contrato por iniciativa propia sino únicamente después de las instrucciones documentadas del Cliente. Si una persona afectada se pone en contacto con el Contratista directamente a este respecto, este deberá remitir inmediatamente dicha solicitud al Cliente.
2. En la medida en que el alcance de los servicios lo incluya, el Contratista deberá atender cualquier solicitud de ejercicio de derechos, relacionada con el acceso a la información, la supresión de datos, su rectificación, oposición a determinados tratamientos, limitación de los mismos, portabilidad de los datos o retirada del consentimiento previamente prestado, de conformidad con las instrucciones documentadas del Cliente.

5. Garantía de calidad y otras obligaciones del Contratistas

Además de cumplir las normas de esta Contrato, el Contratista tiene obligaciones legales de conformidad con los artículos 28 a 33 del RGPD; a este respecto, deberá garantizar el cumplimiento de los siguientes requisitos en particular:

a) Nombramiento por escrito de un delegado de protección de datos que llevará a cabo sus obligaciones de conformidad con los artículos 38 y 39 del RGPD, en caso de que la presencia de dicha figura sea aplicable al caso concreto.
   Los datos de contacto):
   Ista Metering Services España S.A.
   Avenida de la Albufera 319, 4º planta, 28037 Madrid
   Correo electrónico: **RGPD@ista.es**

b) La protección de la confidencialidad de conformidad con los artículos 28, apartado 3, letra b), 29 y 32, apartado 4, del RGPD. A la hora de desempeñar el trabajo, el Contratista debe emplear únicamente a trabajadores que estén sujetos a la obligación de confidencialidad, y que estén familiarizados de antemano con las disposiciones de protección de datos pertinentes. El Contratista y cualquier persona sujeta a él que tenga acceso a datos personales podrá tratarlos exclusivamente de conformidad con las instrucciones del Cliente, incluidas las facultades otorgadas en el presente contrato, a menos que estén legalmente obligados a tratarlos.

c) La aplicación y el cumplimiento de todas las medidas técnicas y organizativas exigidas para la presente Contrato de conformidad con los artículos 28, apartado 3, letra c), y 32 del RGPD (detalles en el **Anexo**).

d) El Cliente y el Contratista deberán, previa solicitud, colaborar con la autoridad de control para ejecutar sus tareas.

e) Información inmediata al Cliente sobre las medidas y las acciones de control adoptadas por la autoridad de control, en la medida en que estén relacionadas con el presente Contrato. Esta obligación será igualmente de aplicación si una autoridad competente lleva a cabo una investigación en el contexto de procedimientos administrativos o penales, respecto al tratamiento de datos personales llevado a cabo en ejecución del presente Contrato.

f) En la medida en que el Cliente por su parte esté sujeto a una inspección por parte de la autoridad de control que investigue la comisión de una infracción administrativa, o cuando se halle inmerso en un procedimiento penal, o de reclamación de responsabilidad de una persona afectada o de un tercero, o deba hacer frente a cualquier otra reclamación en relación con el tratamiento de los datos, el Contratista deberá prestarle su colaboración, al objeto de facilitarle el cumplimiento de las obligaciones que le sean legalmente exigibles.

g) El Contratista supervisará periódicamente los procesos internos y las medidas técnicas y organizativas para asegurarse de que el tratamiento dentro de su área de responsabilidad se realiza de acuerdo con los requisitos puestos por la legislación vigente en materia de protección de datos, y en particular la protección de los derechos del interesado.

h) La verificabilidad de las medidas técnicas y organizativas adoptadas respecto al cliente en el ámbito de sus facultades de control de conformidad con el punto 7 del presente Contrato.

6. Relaciones de subcontratación

1. Se entenderá que las relaciones de subcontratación en el sentido de la presente disposición serán aquellos servicios que estén directamente relacionados con la prestación del servicio principal. Esto no incluirá los servicios auxiliares que utilice el Contratista, como servicios de telecomunicaciones, postales o de transporte, servicios de mantenimiento y de usuario o la disposición de soportes de datos, así como otras medidas destinadas a garantizar la confidencialidad, disponibilidad, integridad y resiliencia del hardware y el software de los sistemas de tratamiento de datos. No obstante, con el fin de garantizar la protección y la seguridad de los datos del Cliente, el Contratista está obligado a adoptar medidas de control y acuerdos contractuales adecuados y conformes legalmente, aun en el supuesto de los servicios auxiliares subcontratados.

2. El Contratista podrá utilizar a otros contratistas basándose en el consentimiento por escrito que se otorga de forma general por la presente. El Contratista deberá informar al Cliente acerca de cualquier cambio previsto en relación con la participación o sustitución de otros contratistas poniendo a disposición la lista actual de contratistas en la dirección de correo electrónico RGPD@ista.es. El Cliente estará informado del estado actual de los encargados consultando en www.ista.com/es/RGPD (p. ej., mediante precauciones técnicas adecuadas).

3. La transferencia de los datos personales del Cliente al subcontratista y su primera acción solo estarán permitidas si se cumplen todos los requisitos para la subcontratación.

4. Si el subcontratista realiza el servicio acordado fuera de la UE o el EEE, el Contratista adoptará las medidas adecuadas para garantizar la admisibilidad con arreglo a la legislación sobre protección de datos. Lo mismo será de aplicación si se van a emplear proveedores de servicios auxiliares, en el sentido del apartado 1.

5. Para llevar a cabo cualquier otra subcontratación que no estuviese sujeta a las reglas anteriores será necesario el consentimiento expreso del Cliente principal (el correo electrónico será suficiente); todas las obligaciones de protección de datos asumidas por el Contratista con arreglo al presente contrato (en la medida pertinente para la relación de subcontratación) también deberán imponerse al otro subcontratista.

7. Derechos de control del Cliente

1. El Cliente tendrá derecho a comprobar el cumplimiento del presente contrato por parte del Contratista en sus operaciones comerciales mediante inspecciones aleatorias, que se anunciarán con un plazo de al menos dos semanas. Las personas empleadas por el Cliente a tal efecto deberán comprometerse a mantener la confidencialidad respecto al Contratista. La obligación de confidencialidad deberá cumplir requisitos de seguridad exigentes. Es posible que las personas empleadas no tengan ninguna relación con un competidor del Contratista.

2. El Contratista deberá asegurarse de que el Cliente pueda comprobar el cumplimiento de las obligaciones por parte del Contratista de conformidad con el artículo 28 del RGPD. El Contratista se compromete a proporcionar al Cliente la información necesaria previa solicitud y, en particular, a proporcionar pruebas de la aplicación de las medidas técnicas y organizativas.

3. La prueba de dichas medidas, que no solo afectan a el Contrato en concreto, podrán realizarse a través de los certificados actuales, informes o extractos de informes de autoridades independientes (p. ej., auditor, auditoría, delegado de protección de datos, departamento de seguridad informática, auditores de protección de datos, auditores de calidad) o un certificado adecuado de la auditoría de protección de datos o de seguridad informática.

8. Remuneración

La remuneración acordada en el Contrato de Servicios abarcará la prestación de servicios estándar, que se prestarán a todos los clientes de igual forma. En función de la presente Contrato, es posible que deban prestarse servicios adicionales relacionados con la protección de datos, cuyo tipo y alcance dependerá en gran medida de cada cliente (p. ej., para la auditoría, apoyo en caso de que tenga lugar una investigación por parte de las autoridades de control). Dichos servicios adicionales serán objeto de una remuneración además de la remuneración por los servicios no relacionados con la protección de datos especificados en el contrato de servicios de acuerdo con el gasto real en el que se incurra en cada caso. Se aplicarán los precios normales a la remuneración basada en los gastos en cada caso.

9. Notificación en caso de incumplimiento por el Contratista

El Contratista ayudará al Cliente a cumplir las obligaciones mencionadas en los artículos 32 a 36 del RGPD relativas a la seguridad de los datos personales, la comunicación de obligaciones en caso de fuga de datos, evaluaciones de impacto de protección de datos y consultas previas. Esto incluirá, entre otros aspectos:

a) garantizar un nivel adecuado de protección mediante medidas técnicas y organizativas que tengan en cuenta las circunstancias y los objetivos del tratamiento, así como la probabilidad prevista y la gravedad de un posible incumplimiento de los derechos debido a defectos de seguridad y permitir determinar inmediatamente los incumplimientos pertinentes;
b) la obligación de notificar infracciones de los datos personales al Cliente sin demora;
c) la obligación de apoyar al Cliente en el contexto de su deber de informar a la persona afectada y de poner a su disposición toda la información pertinente a tal efecto sin demora;
d) ayudar al Cliente respecto a la evaluación del impacto de la protección de datos;
e) ayudar al Cliente en el marco de consultas previas a la autoridad de control.

10. Facultad del Cliente

1. El Cliente confirmará las instrucciones verbales por escrito (el correo electrónico será suficiente) sin demora.

2. El Contratista informará al responsable sin demora si considera que una instrucción infringe la normativa de protección de datos. El Contratista tendrá derecho a suspender la ejecución de la instrucción correspondiente hasta que el Cliente la confirme o modifique.

11. Eliminación y devolución de datos personales

1. No podrán realizarse copias ni duplicados de los datos sin el conocimiento del Cliente. Quedarán excluidas las copias en la medida en que sean necesarias para la ejecución del Contrato y para garantizar un tratamiento de datos ordenado, así como los datos para los que exista la obligación de guardarlos de conformidad con una norma legal.

2. Después de terminar el trabajo acordado contractualmente o antes a petición del Cliente (como máximo cuando se extinga el Contrato de Servicios) el Contratista entregará al Cliente todos los documentos, resultados del uso y tratamiento creados, y datos almacenados respecto a la relación contractual o los destruirá de conformidad con los reglamentos de protección de datos previo consentimiento. Lo mismo será de aplicación al material de prueba y desecho. El registro de eliminaciones deberá enviarse si así se solicita.

3. Los datos estarán excluidos de la obligación de eliminación y devolución si existe la obligación legal de guardarlos (p. ej., el Contratista deberá conservar la documentación que sirva de prueba de un tratamiento de datos ordenado y adecuado de conformidad con los periodos de conservación respectivos después de la extinción del contrato).

Anexo 1. Medidas técnicas y organizativas

1. Confidencialidad [artículo 32, apartado 1, letra b) del RGPD]

- Control de acceso
  - Prohibición de acceso a las personas no autorizadas a los sistemas de tratamiento de datos del centro de datos y los servidores de sucursal.
  - Control de identificación de acceso a las áreas sensibles de los centros de datos.
  - Acceso a las instalaciones empresariales controlado por los empleados durante el horario comercial; los visitantes de la sede de la empresa reciben un ID y están acompañados durante la visita.
  - Determinación de las personas autorizadas en listas para las áreas sensibles del centro de datos.
  - Lista clave de las sedes.
  - Medidas de protección contra robos (videovigilancia, seguridad de puertas, sistema de alarma con servicio de seguridad).
  - Normas para las personas externas (pase de visita, véase más arriba).
  - Registro de las visitas a las sedes de la empresa y las sucursales.

- Control de entrada
  - Prohibición de acceso a las personas no autorizadas a los sistemas de tratamiento de datos del centro de datos y los servidores de sucursal.
  - Control de identificación de acceso a las áreas sensibles de los centros de datos.
  - Acceso a las instalaciones empresariales controlado por los empleados durante el horario comercial; los visitantes de la sede de la empresa reciben un ID y están acompañados.
  - Determinación de las personas autorizadas en listas para las áreas sensibles del centro de datos.
  - Lista clave de la oficina central y las ubicaciones.
  - Medidas de protección contra robos (videovigilancia, seguridad de puertas, sistema de alarma con servicio de seguridad).
  - Normas para las personas externas (pase de visita, véase más arriba).
  - Registro de las visitas a las sedes de la empresa y las sucursales.

- Control de acceso
  - Las personas autorizadas sólo pueden acceder a los datos que se les haya autorizado.
  - Los datos personales guardados sólo se pueden leer, copiar, modificar o eliminar en el marco del concepto de autorización.
  - Concepto de autorización gradual dependiendo de la función de la persona correspondiente para ejecutar el Contrato.
  - Uso de software de protección antivirus continuamente actualizado.
  - Protección del tráfico de correo electrónico contra los virus y el correo no deseado (protección central de virus y sistema de filtrado de correo no deseado).
  - Sistemas de cortafuegos.
  - Protección mediante contraseña (al menos 8 dígitos, combinación de letras, números, caracteres especiales, cambio obligatorio después de 90 días).
  - Separación de los datos maestros del cliente y de facturación a través de diferentes derechos de acceso.
  - Registro de cambios de datos.

- Control de separación
  - Uso de software probado.
  - Separación del entorno de desarrollo, prueba y productivo.
  - Separación lógica en función de los mecanismos de control de acceso.
  - Procedimiento de liberación diferenciado (gestión de cambios).

2. Integridad [artículo 32, apartado 1, letra b) del RGPD]

- Control de entrega
  - Encriptado/uso de túneles de VPN para las transmisiones.
  - Encriptado SSL para el acceso a la Web.
  - Control del tráfico de comunicación de los sistemas (sistemas de cortafuegos centrales, conexiones WAN exclusivas con controles de acceso) y registro (autenticación de usuarios, tiempo).

- Control de introducción
  - Es posible determinar posteriormente si se han introducido, modificado o eliminado datos maestros del cliente y por quién en los sistemas de tratamiento de datos (registro).
  - Concepto de autorización.

3. Disponibilidad y capacidad [artículo 32, apartado 1, letras b) y c) del RGPD]

- Comprobación de la disponibilidad
  - Los datos personales están constantemente disponibles y protegidos frente a destrucciones o pérdidas accidentales mediante copias de seguridad permanentes.
  - Concepto de copia de seguridad de datos (copia de seguridad periódica: diaria, semanal, mensual), modalidades de almacenamiento para las copias de seguridad (compartimentos cortafuegos separados y seguros).
  - Secciones de centros de datos de protección especial (separación estructural, sistemas de control de acceso separados, cortafuegos para todas las áreas de centros de datos, alimentación eléctrica mediante dos conexiones geográficamente separadas, UPS redundante, dos sistemas separados de aviso anticipado de incendios con conexión al centro de control del cuerpo de bomberos).
  - Dispositivos de protección contra incendios en la oficina central y las ubicaciones.
  - Fuente de alimentación ininterrumpida.
  - Fuentes de alimentación redundantes.
  - Sistemas de supervisión y señalización.

4. Procedimientos para la revisión, evaluación y valoración periódicas [artículos 32, apartado 1, letra d) y 25, apartado 1, del RGPD]

- Concepto de protección de datos/seguridad de datos.
- Gestión de respuesta ante incidentes.
- Ajustes previos de protección de datos (artículo 25, apartado 2, del RGPD).
- Control del Contrato
  - Tratamiento únicamente de conformidad con las instrucciones documentadas del Cliente.
  - Las instrucciones se proporcionan entre personas de contacto acordadas expresamente.
  - Especificaciones concretas para el embalaje y envío de documentos/objetos que contengan datos importantes.
  - Se informa a las personas empleadas sobre los requisitos de protección de datos; estarán obligadas a mantener el secreto de los datos por escrito.
  - Los subcontratistas serán objeto de un examen minucioso en relación con su adecuación para el cumplimiento de las precauciones de seguridad pertinentes y estarán obligados por escrito a cumplir los reglamentos vigentes sobre protección de datos.