ÍNDICE:

1.1 Objeto

El objeto de esta política es la de establecer un marco de actuación en materia de protección de datos para la Mancomunidad de Servicios Sociales de Lazagurría, Lodosa, Mendavia, Sartaguda y Sesma, acorde con la legislación de aplicación.

En particular, la política garantiza el derecho a la protección de los datos de todas las personas físicas que se enmarcan en el servicio, garantizando el derecho al honor y a la intimidad en el tratamiento de las diferentes tipologías de datos personales, especialmente aquellos de características especiales.

1.2 Alcance

Todas las personas que forman parte de la organización tienen la obligación de conocer y cumplir esta política siendo responsabilidad de la organización disponer los medios necesarios para que la información llegue a las personas o servicios afectados.

Esta política es de aplicación a la Mancomunidad de Servicios Sociales de Lazagurría, Lodosa, Mendavia, Sartaguda y Sesma, así como a todos los agentes que intervengan en el mismo, desde la ciudadanía hasta destinatarios de los datos.

1.3 Principios básicos relativos al tratamiento de datos personales

Los principios relativos al tratamiento de los datos personales sobre los que se fundamenta esta política son los que se detallan a continuación:

a. Principios de licitud, lealtad y transparencia (art. 5.1.a RGPD)

Los datos personales deben ser tratados de manera lícita, leal y transparente en relación con la persona interesada. El principio de licitud y lealtad exige que:

- A la persona interesa le debe quedar claro que se están recogiendo, utilizando, consultando o tratando de otra manera sus datos personales, así como en qué medida dichos datos son tratados o serán tratados posteriormente.
- Se debe contar con:
    - Una base jurídica que legitime el tratamiento de esos datos personales (art. 6, 7 y 8 y 11 RGPD).
    - Alguna de las excepciones permitidas cuando los datos tratados son de categoría especial o de naturaleza penal (art. 9 y 10 RGPD).
    - Alguno de los instrumentos habilitantes para llevar a cabo transferencias internacionales cuando se van a transferir fuera del EEE (art. 44-49 RGPD).

El principio de transparencia exige que toda información y comunicación relativa al tratamiento de datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro (art. 12 RGPD). Dicho principio se refiere en particular:

- A informar a las personas interesadas sobre la identidad de la organización responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas interesadas (art. 13 y 14 RGPD).
- Y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan, que sean objeto de tratamiento. Las personas interesadas deben tener conocimiento de los riesgos, las normas, las

salvaguardias y los derechos relativos al tratamiento de datos personales, así como del modo de hacer valer sus derechos en relación con el tratamiento (art. 15-23 RGPD).

b. Principio de limitación de la finalidad (art.5.1.b RGPD)

Los datos personales deben ser recogidos con fines determinados, explícitos y legítimos; deben determinarse en el momento de su recogida y no serán tratados ulteriormente de manera incompatible con dichos fines, el tratamiento ulterior con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales.

c. Principio de minimización de los datos (art. 5.1.c RGPD)

Los datos personales recabados deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

Los datos personales no se deben tratar si lo que se pretende pudiera lograrse razonablemente por otros medios.

d. Principio de exactitud (art. 5.1.d RGPD)

Los datos personales tratados deben ser exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

e. Principio de limitación del plazo de conservación (art. 5.1.e RGPD)

Los datos personales se deben conservar de forma que se permita la identificación de las personas interesadas durante no más tiempo del necesario para los fines del tratamiento para los que fueron recabados; podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el RGPD a fin de proteger los derechos y libertades de la persona interesada.

Se debe garantizar que se limite a un mínimo estricto su plazo de conservación. Para garantizar no se conservan más tiempo del necesario, la organización responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica.

Habrá que tener especialmente en cuenta los criterios, aprobados por la Comisión de Evaluación Documental, para la Administración Foral.

f. Principio de integridad y confidencialidad (art. 5.1.f RGPD)

Los datos personales deben ser tratados de tal manera que se garantice una seguridad adecuada de los mismos, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas. Incluso impidiendo el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento.

Para la adopción de esas medidas apropiadas, que además se deben revisar y actualizar cuando sea necesario, será preciso analizar y evaluar los riesgos que el tratamiento de esos datos personales suponga para la persona interesada (art. 24, 25 y 32 RGPD). La adhesión a códigos de conducta (art. 40-41 RGPD) o a un mecanismo de certificación (art. 42-43 RGPD) podrán ser utilizados como elementos para demostrar el cumplimiento de estas obligaciones.

- Cuando el tratamiento suponga un alto riesgo para la persona interesada, se deberá llevar a cabo de manera previa al inicio del mismo una evaluación de impacto (EIPD) (art. 35); si tras la EIPD el riesgo continúa siendo

alto y no se dispone de medidas para reducirlo, se deberá consultar a la autoridad de control (AC) antes de iniciar el tratamiento (art. 36 RGPD).

- Cuando se produzca una brecha de seguridad a pesar de las medidas implantadas, además de notificarla a la Agencia Española de Protección de Datos si supone un riesgo para las personas interesadas afectados y comunicarla a las propias personas afectadas si este riesgo es alto, se deben adoptar nuevas medidas para poner remedio a la brecha y para mitigar los posibles efectos negativos que suponga la misma (art. 33 y 34 RGPD).

Se deben adoptar no solo medidas técnicas, sino también organizativas, y dentro de estas, son obligatorias:

- Cuando dos o más organizaciones responsables determinen conjuntamente los fines y los medios del tratamiento determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el RGPD (art. 26 RGPD).
- Cuando la organización esté establecida fuera de la UE pero le sea de aplicación el RGPD, designará por escrito un representante en la UE (art. 27 RGPD).
- Se deben elegir solo organizaciones encargadas del tratamiento que ofrezcan suficientes garantías para aplicar medidas de manera que el tratamiento sea conforme al RGPD, encargo que debe regularse a través de un contrato (art. 28 RGPD).
- Se darán indicaciones a través de políticas y/o protocolos a cualquier persona que actúe bajo la autoridad de la organización y tenga acceso a datos personales, para que solo traten dichos datos siguiendo instrucciones de la organización (art. 29 RGPD).
- Cada organización debe llevar un registro de las actividades de tratamiento efectuadas bajo su responsabilidad (organización responsable del tratamiento) y otro de las efectuadas por cuenta de otra entidad (organización encargada del tratamiento) (art. 30).
- Cooperar con la Agencia Española de Protección de Datos cuando lo solicite en el desempeño de sus funciones (art. 31 RGPD).
- Designar una persona Delegada de Protección de Datos siempre que se den las circunstancias en las que la normativa obligue a ello (art. 37, 38 y 39 RGPD).

g. <u>Principio de responsabilidad proactiva (art. 5.2 RGPD)</u>

Este principio implica que se debe no solo cumplir con los principios anteriormente mencionados, sino también demostrar dicho cumplimiento.

El RGPD proporciona un conjunto de herramientas a las organizaciones para que puedan demostrar este cumplimiento, algunas de las cuales deben aplicarse obligatoriamente, por ejemplo, y entre otras:

- Elaborar un registro de todas las actividades de tratamiento (RAT) que se lleven a cabo.
- Llevar a cabo una adecuada gestión de riesgos de todos los tratamientos.
    - Identificación, análisis y evaluación de estos riesgos.
    - Adopción de medidas de seguridad adecuadas a estos riesgos.
- Llevar a cabo una evaluación de impacto relativa a la protección de datos cuando sea probable que un tipo de tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas.

- Designar una persona Delegada de Protección de Datos, si fuese obligatorio.
- Notificar las brechas de seguridad, en caso de que se produzcan.

El RGPD dispone de otros mecanismos para garantizar que se han implementado medidas adecuadas de protección de datos y con ello acreditar su cumplimiento. Estos mecanismos pretenden incrementar la confianza y la transparencia de las actuaciones llevadas a cabo con datos personales por las organizaciones responsables y encargadas del tratamiento. Estos instrumentos, conforme al Reglamento son:

- Auditorías.
- Códigos de conducta: para asociaciones u organismos que representen categorías de responsables o encargadas del tratamiento. (art.40 RGPD).
- Mecanismos de certificación: para organizaciones responsables o encargadas del tratamiento a título individual (Certificados, Sellos y Marcas de protección de datos). (art.42 RGPD).

1.4 Recogida de datos personales

La recogida de datos personales debe estar fundamentada en una base legítima del artículo 6 RGPD:

a) Consentimiento de la persona interesada.

b) El tratamiento es necesario para la ejecución de un contrato en el que la persona interesada es parte o para la aplicación a petición de este de medidas precontractuales.

c) El tratamiento es necesario para el cumplimiento de una obligación legal aplicable a la organización responsable del tratamiento.

d) El tratamiento es necesario para proteger intereses vitales de la persona interesada o de otra persona física.

e) El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos a la organización responsable del tratamiento.

f) El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por la organización responsable del tratamiento o por una tercera persona, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales de la persona interesada que requieran la protección de datos personales, en particular cuando la persona interesada sea menor de edad.

Además, cuando los datos tratados sean de carácter especialmente protegido, habrá que estar a las bases del art. 9 RGPD que levantan la prohibición del tratamiento de dichas categorías de datos:

a) Consentimiento explícito de la persona interesada.

b) El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos de la organización responsable del tratamiento o de la persona interesada en el ámbito del derecho laboral y de la seguridad y protección social.

c) El tratamiento es necesario para proteger intereses vitales de la persona interesada o de otra persona física, en el supuesto de que la persona interesada no esté capacitada, física o jurídicamente, para dar su consentimiento.

d) El tratamiento sea efectuado por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a las personas miembro actuales o antiguos de tales organismos o a personas que mantengan contactos

regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de las personas interesadas.

e) El tratamiento se refiere a datos personales que la persona interesada ha hecho manifiestamente públicos.

f) El tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial.

g) El tratamiento es necesario por razones de interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales de la persona interesada.

h) El tratamiento sea necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria.

i) El tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios.

j) El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

Condiciones para que el consentimiento sea válido

El RGPD define el consentimiento (art. 4.11) como toda manifestación de voluntad libre, específica, informada e inequívoca por la que la persona interesada acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de sus datos personales.

- Cuando el tratamiento se base en el consentimiento de la persona interesada, la organización responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales (art. 7.1 RGPD).
- La solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo (art. 7.2 RGPD).
- La persona interesada tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada (sin efectos retroactivos).

Antes de dar su consentimiento, la persona interesada deberá ser informado de ello. Será tan fácil retirar el consentimiento como prestarlo. (art. 7.3 RGPD). Antes de obtener el consentimiento se debe facilitar a la persona interesada la información del tratamiento establecida en el art. 13 RGPD o, al menos, la información básica establecida en el art. 11 LOPDGDD con una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

Tratamiento de datos de menores de edad

- El consentimiento para la utilización de datos personales de menores de 14 años se otorgará por sus padres, madres o tutores legales. Las personas menores entre 14 y 18 años podrán otorgar el consentimiento para la utilización de sus datos personales por sí mismos, salvo que una norma específica exija la asistencia de los padres o tutores (art. 7.1 LOPDGDD).

- La organización responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por la persona titular de la patria potestad o tutela, teniendo en cuenta la tecnología disponible (art. 8.2 RGPD).

1.5 Derechos de las personas interesadas

Los derechos establecidos en el Capítulo III del RGPD (art. 12 a 23) son aplicables a cualquier persona física:

- Derecho de acceso: La persona interesada tendrá derecho a acceder a sus datos que están siendo tratados por la organización responsable del tratamiento, así como toda la información detallada en el art. 15 RGPD.
- Derecho de supresión. La persona interesada tendrá derecho a obtener sin dilación indebida de la organización responsable del tratamiento la supresión de los datos personales que le conciernan, cuando se den alguna de las siguientes circunstancias:
    - Retire su consentimiento cuando el tratamiento se base en el mismo.
    - Se oponga al tratamiento y no prevalezcan intereses legítimos.
    - Sus datos personales hayan sido tratados ilícitamente.
    - Sus datos deban suprimirse para el cumplimiento de una obligación legal.
    - Sus datos se hayan obtenido en relación con la oferta de servicios de la sociedad de la información.
- Derecho de rectificación: La persona interesada podrá solicitar la rectificación de aquellos datos que sean inexactos.
- Derecho de limitación del tratamiento: La persona interesada tendrá derecho a obtener de la organización responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las siguientes condiciones:
    - La persona interesada impugne la exactitud de los datos personales, durante un plazo que permita a la organización responsable verificar la exactitud de los mismos.
    - El tratamiento sea ilícito y la persona interesada se oponga a la supresión de los datos personales, solicitando en su lugar la limitación.
    - La organización responsable ya no necesite los datos personales para los fines del tratamiento, pero la persona interesada los necesite para la formulación, el ejercicio o la defensa de reclamaciones.
    - La persona interesada se haya opuesto al tratamiento en virtud del art. 21.1 RGPD, mientras se verifica si los motivos legítimos de la organización responsable prevalecen sobre los de la persona interesada.
- Derecho de oposición: La persona interesada tendrá derecho a oponerse en cualquier momento a que sus datos personales sean objeto de un tratamiento basado en una misión de interés público o en el interés legítimo, incluido la elaboración de perfiles.
- Derecho de oposición a las decisiones automatizadas: La persona interesada tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración perfiles, que produzca efectos jurídicos en ella o le afecte significativamente.

Es necesario establecer un procedimiento para gestionar su ejercicio por parte de las personas interesadas.

1.6 Deber de información

En el momento de la recogida de datos de las personas interesadas se debe proceder a informarle de:

- Identidad y datos de contacto de la organización responsable.
- Datos de contacto de la persona Delegada de Protección de Datos, cuando lo hubiese.
- Fines del tratamiento a que se destinan los datos y base jurídica del mismo
- Organización destinataria de los datos.
- Intención de transferir los datos personales a un destinatario de un tercer país u organización internacional.
- Plazo de conservación de los datos personales.
- Existencia del derecho de ejercicio de los derechos de acceso, rectificación, supresión, oposición y limitación.
- Derecho a presentar una reclamación ante la autoridad de control.

En caso de hacerlo en dos capas será necesario que la primera capa incluya al menos la siguiente información:

- Identidad de la organización responsable.
- Finalidad del tratamiento.
- Posibilidad de ejercer los derechos de acceso, rectificación, supresión, oposición y limitación.

En los diferentes impresos o formularios/documentos diversos, se proporcionará a las personas interesadas:

- Información concisa, transparente, inteligible y de fácil acceso.
- Lenguaje claro y sencillo.

1.7 Análisis de riesgos y evaluación de impacto

Es necesario que la organización responsable del tratamiento, así como en su caso las organizaciones encargadas del tratamiento lleven a cabo una valoración del riesgo de los tratamientos que realicen, para poder determinar las medidas que son necesarias aplicar.

Cuando el tratamiento implique un alto riesgo para los derechos y libertades de las personas físicas, será necesario realizar una Evaluación de Impacto, antes de llevar a cabo dicho tratamiento. A través de dicha Evaluación de Impacto, se persigue ponderar los riesgos que entraña el tratamiento para los derechos y libertades de las personas interesadas frente a la consecución de la finalidad perseguida. Ello se llevará a cabo a través de los juicios de idoneidad, necesidad y proporcionalidad.

1.8 Brechas de seguridad

La organización responsable debe contar con un procedimiento para actuar en caso de que se produzca una brecha de seguridad que afecte a datos de carácter personal, ya sea de origen accidental o intencionado. Deberá contar con los medios necesarios para evitar que se produzcan y hacer frente a las mismas en caso de que se hayan materializado.

Si la brecha de seguridad supone un riesgo para los derechos y libertades de las personas se debe notificar a la Agencia Española de Protección de Datos en un plazo máximo de 72 horas desde que se tenga constancia.

1.9 Contrato de encargo de tratamiento

La organización responsable del tratamiento puede encargar el desarrollo de un servicio dentro del tratamiento a una tercera organización, que tendrá la consideración de organización encargada del tratamiento. La organización encargada podrá adoptar todas las decisiones organizativas y operacionales necesarias para la prestación del servicio encomendado, pero no podrá varias las finalidades y usos de los datos ni utilizarlos para sus propias finalidades. Las actuaciones de esta organización estarán circunscritas a las instrucciones recibidas de la organización responsable.

El encargo de tratamiento deberá formalizarse en un contrato. El contenido de este contrato constará de:

- Las instrucciones del responsable del tratamiento.
- El deber de confidencialidad.
- Las medidas de seguridad.
- El régimen de la subcontratación.
- La forma en que el encargado asistirá al responsable en el cumplimiento de responder el ejercicio de los derechos de los afectados.
- La colaboración en el cumplimiento de las obligaciones del responsable.
- El destino de los datos al finalizar la prestación.

Además, la organización encargada del tratamiento debe ofrecer garantías suficientes en lo referente a conocimientos especializados, fiabilidad y recursos, con vistas a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del Reglamento, incluida la seguridad del tratamiento, así como del cumplimiento de la normativa de protección de datos.