INFORME DE AUDITORIA EN EL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DEDATOS:

FUNDACIÓN CEPAIM

OBJETO DE LA AUDITORIA

El presente documento tiene por objeto comprobar el grado de adecuación de la entidad a la normativa en protección de Datos y a la Ley Orgánica 3/2018 de 5 de diciembre de protección de datos personales y Garantía de los Derechos Digitales y al Reglamento 679/2016 de 27 de Abril.

El objetivo final de la auditoria es verificar el grado de adecuación de la entidad a las medidas y controles de la normativa en Protección de Datos, identificando sus deficiencias y proponiendo las medidas correctoras o complementarias necesarias. A su vez, incluye los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

Los puntos básicos a revisar en este documento:

Aspecto Técnico: se revisa el cumplimiento de las medidas de seguridad que deben reunir los tratamientos de datos.

Aspecto Organizativo: se revisan los procedimientos normativos y reglas de seguridad elaborados e implantados por la entidad.

Aspecto Jurídico: se revisa la tipología de los datos almacenados en los sistemas de información y aplicaciones informáticas, y se realiza un análisis de riesgos y se determina si la entidad debe de contar con Evaluaciones de impacto de algunos de los tratamientos que realiza y con la persona delegada de protección de datos.

FASES EN LA REALIZACIÓN DE LA AUDITORÍA

La auditoría y el listado de cumplimiento normativo se han realizado con visitas presenciales de un agente externo que ha constado de las siguientes fases:

1. Conocimiento genérico de la entidad, su ámbito de negocio, los sistemas de información de que disponen, su estructura administrativa y el organigrama de sus trabajadores, sus relaciones con organismos oficiales, asociaciones, instituciones y empresas.
2. Elaboración de un programa de trabajo en el que se detallan las actividades o tareas a auditar, teniendo para ello en cuenta, por un lado, los requisitos de revisión impuestos por el Reglamento en relación con la auditoría, y por el otro, el ámbito de negocio ysistemas de la entidad.
3. Realización del trabajo de campo, esto es, la revisión práctica de las actividades incluidasen el plan de trabajo.
4. Análisis de los puntos débiles y obtención de conclusiones y recomendaciones.
5. Elaboración del informe.

PLAN DE AUDITORÍA

A partir del hecho de que la auditoría debe verificar el cumplimiento del Reglamento y la normativa de Protección de Datos, el Plan de Trabajo deberá incluir específicamente la comprobación de todos losartículos de aquel que sean de aplicación a tenor del tipo de tratamientos de que disponga FUNDACION CEPAIM

Para la realización organizada de esta auditoría se ha preparado una tabla de control o de "checklist" basada en alguno de los modelos propuestos por la Agencia Española de Protección de Datos y desarrollada de manera independiente.

A continuación, se incluye la tabla "checklist" de los puntos auditados de las áreas anteriormente mencionadas, así como los resultados obtenidos para cada apartado.

1.- PRINCIPIOS RELATIVOS AL TRATAMIENTO
2.- LICITUD DEL TRATAMIENTO
3.- CONDICIONES PARA EL CONSENTIMIENTO
4.- CONSENTIMIENTO DE NIÑOS EN RELACIÓN CON LOS SERVICIOS DE LA SOCIEDADDE LA INFORMACIÓN
5.- TRATAMIENTO DE CATEGORIAS ESPECIALES DE DATOS
6.- TRATAMIENTOS RELATIVOS A CONDENAS E INFRACCIONES PENALES
7.- TRATAMIENTOS QUE NO REQUIEREN IDENTIFICACIÓN
8.- DERECHOS DEL INTERESADO. TRANSPARENCIA DE LA INFORMACIÓN
9.- DERECHOS DEL INTERESADO. INFORMACIÓN A FACILITAR CUANDO LOS DATOS SE OBTIENEN DEL INTERESADO
10.-DERECHOS DEL INTERESADO. INFORMACIÓN A FACILITAR CUANDO LOS DATOS NOSE OBTIENEN DEL INTERESADO
11.-DERECHOS DEL INTERESADO:
    a. DERECHO DE ACCESO
    b. DERECHO DE RECTIFICACIÓN
    c. DERECHO DE SUPRESIÓN («EL DERECHO AL OLVIDO»)
    d. DERECHO A LA LIMITACIÓN DEL TRATAMIENTO
    e. DERECHO A LA PORTABILIDAD DE LOS DATOS
    f. DERECHO DE OPOSICIÓN
12.-DERECHOS DEL INTERESADO. DECISIONES INDIVIDUALES AUTOMATIZADAS,INCLUIDA LA ELABORACIÓN DE PERFILES
13.-RESPONSABILIDAD DEL RESPONSABLE DEL TRATAMIENTO
14.-PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO
15.-CORRESPONSABLES DEL TRATAMIENTO
16.-ENCARGADO DEL TRATAMIENTO
17.-REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO
18.-SEGURIDAD DEL TRATAMIENTO
19.-BRECHAS DE LA SEGURIDAD:
    a. NOTIFICACIÓN DE BRECHAS DE LA SEGURIDAD DE LOS DATOS PERSONALES ALA AUTORIDAD DE CONTROL
    b. COMUNICACIÓN DE UNA BRECHA AL INTERESADO20.-EVALUACIÓN DE IMPACTO
21.-DELEGADO DE PROTECCIÓN DE DATOS
22.-TANSFERENCIAS A PAÍSES TERCEROS U ORGANIZACIONES INTERNACIONALES

1.-PRINCIPIOS RELATIVOS AL TRATAMIENTO

En este apartado comprobaremos el tipo de datos que se tratan en la entidad y su finalidad

PRINCIPIOS RELATIVOS AL TRATAMIENTO	SI/NO
Se recogen los datos personales con fines determinados	SI
Se recogen los datos personales con fines explícitos	SI
Se recogen los datos personales con fines legítimos	SI
Se tratan ulteriormente de manera incompatible con otros fines	NO
Los datos personales se mantienen exactos	SI
Se mantienen actualizados	SI
Se rectifican los datos personales inexactos respecto de la finalidad	SI
Se suprimen los datos personales inexactos respecto de la finalidad	SI
Se mantienen durante más tiempo del necesario respecto de la finalidad	NO
Se tratan con fines de archivo en interés público	NO
Se tratan con fines de investigación científica	NO
Se tratan con fines históricos	NO
Los datos personales se tratan con fines estadísticos	NO
Se han implantado medidas de seguridad para proteger la integridad y confidencialidad de los datos	SI
Se han implantado medidas de seguridad contra el tratamiento no autorizado oilícito de los datos	SI
Se han implantado medidas de seguridad para evitar su pérdida, destrucción odaño accidental	SI
Se mantiene la trazabilidad de los fines del tratamiento	SI

NIVEL DE CUMPLIMIENTO

Satisfactorio. El tipo de datos que se recogen para los diversos fines para los cuales han sido recabados son adecuados, pertinentes y limitados en relación con los fines para los que son tratados y se procede ala eliminación cuando dejan de ser necesarios o inexactos.

RECOMENDACIONES

No se debe de recoger más información de la que resulte necesaria en atención a los fines. Se procederá a Actualización los datos cuando sean necesario.

Reglamento UE 679/2016

Art. 5. Principios Relativos al Tratamiento:

1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) 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 («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo delnecesario para los fines del tratamiento de los datos personales; los datos personales 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, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos ylibertades del interesado («limitación del plazo de conservación»);

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida laprotección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o dañoaccidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

Ley orgánica de protección de datos
Principios de protección de datos
Artículo 4. Exactitud de los datos.

1. Conforme al artículo 5.1.d) del Reglamento (UE) 2016/679 los datos serán exactos y, si fuere necesario, actualizados.

2. A los efectos previstos en el artículo 5.1.d) del Reglamento (UE) 2016/679, no será imputableal responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos:

a) Hubiesen sido obtenidos por el responsable directamente del afectado.
b) Hubiesen sido obtenidos por el responsable de un mediador o intermediario en caso de que las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establecieran la posibilidad de intervención de un intermediario o mediador que recoja en nombre propio los datos de los afectados para su transmisión al responsable. El mediador o intermediario asumirá las responsabilidades que pudieran derivarse en el supuesto de comunicación al responsable de datos que no se correspondan con los facilitados por el afectado.
c) Fuesen sometidos a tratamiento por el responsable por haberlos recibido de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad conforme al artículo 20 del Reglamento (UE) 2016/679 y lo previsto en esta ley orgánica.
d) Fuesen obtenidos de un registro público por el responsable.

2.-LICITUD DEL TRATAMIENTO

LICITUD DEL TRATAMIENTO	SI/NO
Se tiene consentimiento para cada finalidad del tratamiento	SI
El tratamiento es necesario para ejecutar un contrato o precontrato	SI
Existe obligación legal	SI
El tratamiento es necesario para proteger intereses vitales	NO
El tratamiento es necesario para el cumplimiento de interés público	NO
El tratamiento es necesario para satisfacer intereses legítimos	SI

NIVEL DE CUMPLIMIENTO

Satisfactorio. Se cumplen los requisitos para que los tratamientos sean lícitos. Se han determinado los tratamientos que realiza FUNDACION CEPAIM, *su legitimación que está basada en el consentimiento de las personas afectadas, en la ejecución de un contrato o el cumplimiento de una obligación legal para los responsables.*

RECOMENDACIONES

Los tratamientos siempre han de ser legítimos y basados en el consentimiento de la persona interesada, en el establecimiento o desarrollo de un contrato de prestación de servicios o estar amparados en la ley.

Como la mayor parte de los tratamientos tienen como causa de legitimación el consentimiento de laspersonas afectadas o de sus representantes legales, este debe de obtenerse desde el primer contacto.

Los tratamientos relativos a los candidatos y trabajadores se legitiman por el consentimiento de losinteresados, por ser parte los mismos de una relación laboral o el cumplimiento de una obligación legal para el responsable.

LEGISLACION

Reglamento UE 679/2016

Art. 6 Licitud del Tratamiento:

1- El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno ovarios fines específicos;
b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte opara la aplicación a petición de este de medidas precontractuales;
c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsabledel tratamiento;
d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra personafísica;
e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o enel ejercicio de poderes públicos conferidos al responsable del tratamiento;
f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Ley orgánica de protección de datos

Artículo 6. Tratamiento basado en el consentimiento del afectado.

1. De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.
2. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectadopara una pluralidad de finalidades será preciso que conste de manera específica e inequívoca quedicho consentimiento se otorga para todas ellas.
3. No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrolloo control de la relación contractual.

Artículo 8. Tratamiento de datos por obligación legal, interés público o ejercicio depoderes públicos.

1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.
2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley.

3.-CONDICIONES PARA EL CONSENTIMIENTO

Comprobaremos si cumplen las condiciones para recabar el consentimiento:

CONDICIONES PARA EL CONSENTIMIENTO	SI/NO
Se puede demostrar que el afectado dio su consentimiento para el tratamiento	Si
Se puede demostrar que el tratamiento se realiza como resultado del cumplimiento deuna obligación legal	SI
Se solicita el consentimiento de forma clara e independiente de los demás asuntos	SI
Se solicita el consentimiento de forma inteligible y de fácil acceso	SI
Se solicita usando lenguaje claro y sencillo	SI
Se informa con carácter previo a recabar el consentimiento	SI
Se permite retirar el consentimiento con la misma facilidad que se recaba	SI
Se ofrecen medios para retirar el consentimiento en cualquier momento	SI
Se recaba el libre consentimiento	SI
Para prestar un servicio se solicitan sólo los datos necesarios	SI
Para ejecutar un contrato se solicitan sólo los datos necesarios	SI

NIVEL DE CUMPLIMIENTO

Satisfactorio. En los tratamientos cuya legitimación se funda en el consentimiento de las personas afectadas o de sus representantes legales se conservan los documentos que sirven de soporte.

RECOMENDACIONES

Debe de guardarse prueba material del consentimiento de las personas afectadas, en cualquier soporte digital o material.

LEGISLACION

Reglamento UE 679/2016

Art. 7 Condiciones para el Consentimiento:

1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.
2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, 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. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.
3. El interesado 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. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.

1. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

Ley orgánica de protección de datos

Artículo 6. Tratamiento basado en el consentimiento del afectado.

1. De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

2. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectadopara una pluralidad de finalidades será preciso que conste de manera específica e inequívoca quedicho consentimiento se otorga para todas ellas.

3. No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrolloo control de la relación contractual.

4.-CONSENTIMIENTO DE MENORESENRELACIÓN CON LOS SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN

CONSENTIMIENTO DE NIÑOS EN RELACIÓN CON LOS SERVICIOS DE LASOCIEDAD DE LA INFORMACIÓN	SI/NO
Se recaba el consentimiento de menores de 14 años al titular de la patria potestado tutela sobre el niño	SI
Se verifica que el consentimiento fue dado por el titular de la patria potestad otutela sobre el niño	SI

NIVEL DE CUMPLIMIENTO

Satisfactorio.

RECOMENDACIONES

Los tratamientos siempre han de ser legítimos y basados en el consentimiento de la persona interesadao en el cumplimiento de alguna de las condiciones establecidas en la normativa. En el caso de los menores se ha de atender a su edad y siendo menores de 14 años se debe de recabar el consentimiento de sus padres/madres o tutores/as . Cuando superen la edad de 14 años y para determinados tratamientos deberá de recabarse el consentimiento de los representantes legales.

Reglamento UE 679/2016

Art. 8 Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información:
Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de serviciosde la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente seconsiderará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y sólo en la medida en que se dio o autorizó.

Ley orgánica de protección de datos

Artículo 7. Consentimiento de los menores de edad.

1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años. Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

2. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.

5.-TRATAMIENTO DE CATEGORIAS ESPECIALES DE DATOS

TRATAMIENTO DE CATEGORIAS ESPECIALES DE DATOS	SI/NO
Se tratan los datos sólo cuando existen normas que lo exceptúen	SI
Se tratan los datos con consentimiento explícito y no existen normas de derecho queprohíban expresamente su tratamiento	SI
Es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos en el ámbito del derecho laboral y de la seguridad y protección en la medida que está establecido por las normas de derecho	SI
Es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos en el ámbito del derecho laboral y de la seguridad y protección en la medida que existe un convenio colectivo con arreglo a derecho	SI
Es necesario para proteger los intereses vitales de una persona y el interesado noestá capacitado, física o jurídicamente, para dar su consentimiento	NO
Se efectúa en el ámbito de actividades legítimas y con las debidas garantías y se refiere exclusivamente a los miembros actuales o antiguos o a personas que mantienen contactos regulares en relación con la finalidad (política, filosófica, religiosa o sindical)	NO
Se efectúa en el ámbito de actividades legítimas y con las debidas garantías y no secomunican a terceros sin consentimiento de los interesados	SI
Se tratan datos que el interesado ha hecho manifiestamente públicos	SI
Es necesario para la formulación, el ejercicio o la defensa de reclamaciones	SI

Es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento detipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social	SI
Es necesario por razones de interés público en el ámbito de la salud pública sobre la base normas de Derecho que establece medidas adecuadas y específicas paraproteger los derechos y libertades del interesado, en particular el secreto profesional	NO
Es necesario con fines de archivo en interés público, fines de investigación científicao histórica o fines estadísticos en base a normas de derecho	NO
Se realiza cumpliendo las condiciones con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud que establece la normativa nacional	SI

NIVEL DE CUMPLIMIENTO

Satisfactorio. El tratamiento de datos especialmente protegidos solo es justificado en determinados casos establecidos en la normativa. Los datos especialmente protegidos que habitualmente trata FUNDACION CEPAIMy son referidos a salud, siendo su legitimación el consentimiento de las personas afectadas y/o de sus representantes legales y el tratamiento de datos en el desarrollo de un contrato en el que la persona interesada es parte.

RECOMENDACIONES

Solo se pueden tratar datos especialmente protegidos cuando exista una causa legítima para hacerlo

LEGISLACION

Reglamento UE 679/2016

Art. 9 Tratamiento de categorías especiales de datos personales

1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.
2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:
   a. el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales conuno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estadosmiembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantadapor el interesado;
   b. el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechosespecíficos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de losEstados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;
   c. el tratamiento es necesario para proteger intereses vitales del interesado o de otra personafísica, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar suconsentimiento;

d. el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías,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 los miembros 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 los interesados;

e. el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento detipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

f. 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, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional.

3.

a. el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, 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 del interesado.

Ley Orgánica de protección de datos

Artículo 9. Categorías especiales de datos.

1. A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico. Lo dispuesto en el párrafo anterior no impedirá el tratamiento de dichos datos al amparo de los restantes supuestos contemplados en el artículo 9.2 del Reglamento (UE) 2016/679, cuando así proceda.

2. Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en unanorma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad. En particular, dicha norma podrá amparar el tratamiento de datos en el ámbitode la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria ysocial, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte.

6.-TRATAMIENTOS RELATIVOS A CONDENAS E INFRACCIONES PENALES

TRATAMIENTOS RELATIVOS A CONDENAS E INFRACCIONES PENALES	SI/NO
Se tratan los datos bajo la supervisión de las autoridades públicas	SI
Se tratan los datos bajo la autorización de normas de derecho	SI
El registro completo de condenas penales se realiza bajo el control de las autoridades públicas	N.A.

NIVEL DE CUMPLIMIENTO

Satisfactorio. No se tratan datos de condenas o infracciones penales más que de manera circunstancial,respondiendo al requerimiento de autoridades administrativas o judiciales.

RECOMENDACIONES

El tratamiento de datos relativos a condenas y/o infracciones penales solo puede hacerse en los casos permitidos en la legislación.

LEGISLACION

Reglamento UE 679/2016

Art. 10 Tratamiento de datos personales relativos a condenas e infracciones penales

El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas.

Ley Orgánica de protección de datos

Artículo 10. Tratamiento de datos de naturaleza penal.

El tratamiento de datos personales relativos a condenas e infracciones penales, así como procedimientos y medidas cautelares y de seguridad conexas, para fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución desanciones penales, solo podrá llevarse a cabo cuando se encuentre amparado en una norma de Derecho de la Unión, en esta ley orgánica o en otras normas de rango legal.

El registro completo de los datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas a que se refiere el artículo 10 del Reglamento (UE) 2016/679, podrá realizarse conforme con lo establecido en la regulación del Sistema de registros administrativos de apoyo a la Administración de Justicia.

Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones

7.-TRATAMIENTOS QUE NO REQUIEREN IDENTIFICACIÓN:

TRATAMIENTOS QUE NO REQUIEREN IDENTIFICACIÓN	SI/NO
Se mantiene información adicional con vistas a identificar al interesado cuandolos fines no requieren esa identificación	N.A
Se obtiene y/o trata información adicional con vistas a identificar al interesadocuando los fines no requieren esa identificación	N.A
Se puede demostrar que los datos anonimizados no permiten identificar a losinteresados	SI
Se informa al interesado y se recaba su consentimiento cuando se llega a suidentificación	SI
Se cancelan los datos cuando se llega a identificar al interesado	N.A.

NIVEL DE CUMPLIMIENTO

N.A. No se realizan tratamiento para identificar a los interesados en tratamientos que no requieran deella.

RECOMENDACIONES

No procede.

LEGISLACION

Reglamento UE 679/2016

Art. 11 Tratamiento que no requiere identificación:

1. Si los fines para los cuales un responsable trata datos personales no requieren o ya no requieren la identificación de un interesado por el responsable, este no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidadde cumplir el presente Reglamento.

2. Cuando, en los casos a que se refiere el apartado 1 del presente artículo, el responsable sea capaz de demostrar que no está en condiciones de identificar al interesado, le informará en consecuencia, de ser posible. En tales casos no se aplicarán los artículos 15 a 20, excepto cuando el interesado, a efectos del ejercicio de sus derechos en virtud de dichos artículos, facilite información adicional que permita su identificación.

8.-DERECHOS DEL INTERESADO. TRANSPARENCIA

DERECHOS DEL INTERESADO. TRANSPARENCIA DE LA INFORMACIÓN	SI/NO
Se toman medidas para facilitar al interesado toda la información Relativa al tratamiento	SI
La información se facilita de forma concisa, transparente e inteligible	SI
La información se facilita en lenguaje claro y sencillo	SI
Se facilita por escrito o por otros medios, incluidos los electrónicos	SI
Se facilita verbalmente, previa acreditación de su identidad	SI

Se facilita al interesado el ejercicio de sus derechos	SI
Se atienden las peticiones del ejercicio de derechos, aunque el tratamiento norequiera identificación salvo que no se pueda identificar al interesado	SI
Se informa al interesado en el plazo de un mes desde la recepción de su solicitud	SI.
Se informa ante el ejercicio de derechos complejos o ante muchas solicitudes en elplazo máximo de tres meses desde la recepción de la solicitud	SI
Se informa en el plazo de un mes de la prórroga de tres meses indicando el motivo de ladilación	SI
Se permite a los interesados el ejercicio de derechos por medios electrónicos	SI
Se informa por medios electrónicos cuando se recibe la solicitud por esos mediossalvo que solicite que se realice por otro medio	SI
Se informa de las razones de la no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales, en elplazo de un mes desde la recepción de la solicitud cuando no se da curso a la	SI
Se facilita gratuitamente el ejercicio de derechos	SI
Se solicita información para acreditar la identidad de la persona física que ejerce susderechos	SI
Cuando la información que se facilita utiliza iconos normalizados, el formatoelectrónico es legible mecánicamente	SI

NIVEL DE CUMPLIMIENTO

Satisfactorio. Se informa adecuadamente a las personas interesadas de sus derechos y de como ejercitarlos

RECOMENDACIONES

En los documentos informativos sobre los tratamientos, así como en los que sirven para recoger el consentimiento deben de figurar los derechos de las personas interesadas y una descripción de comoejercitarlos. En el ejercicio de los derechos del afectado se deben de respetar los plazos establecidos para la contestación y se debe de facilitar la información de forma concisa, transparente e inteligible.

LEGISLACION

Reglamento UE 679/2016

Art. 12. Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado

1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.

Ley orgánica de protección de datos

Ejercicio de los derechos
Artículo 12. Disposiciones generales sobre ejercicio de los derechos.

7. Los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, podrán ejercerse directamente o por medio de representante legal o voluntario.

1. El responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el afectado. El ejercicio del derecho no podrá ser denegado por el solo motivo de optar el afectado por otro medio.
2. El encargado podrá tramitar, por cuenta del responsable, las solicitudes de ejercicio formuladas por los afectados de sus derechos si así se estableciere en el contrato o acto jurídico que les vincule.
3. La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado recaerá sobre el responsable.
4. Cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en el Capítulo III del Reglamento (UE) 2016/679, se estará a lo dispuesto en aquellas.
5. En cualquier caso, los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de catorce años los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la presente ley orgánica.
6. Serán gratuitas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos, sin perjuicio de lo dispuesto en los artículos 12.5 y 15.3 del Reglamento (UE) 2016/679 y en los apartados 3 y 4 del artículo 13 de esta ley orgánica.

9.-DERECHOS DEL INTERESADO. INFORMACION CUANDO LOSDATOS SE OBTIENEN DEL INTERESADO

DERECHOS DEL INTERESADO. INFORMACIÓN A FACILITAR CUANDO LOSDATOS SE OBTIENEN DEL INTERESADO	SI/NO
Se facilita la identidad y los datos de contacto del responsable y, en su caso, del representante cuando se solicitan datos	SI
Se facilitan los datos de contacto del delegado de protección de datos	SI
Se facilitan los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento	SI
Se facilita información sobre el interés legitimo	SI
Se informa sobre los destinatarios o las categorías de destinatarios	SI
Se informa del plazo de conservación de los datos personales o los criterios utilizados para determinarlo	SI
Se informa sobre la existencia del derecho a solicitar el acceso, rectificación osupresión, la limitación del tratamiento, a oponerse y el derecho a la portabilidad	SI
Si el tratamiento se basa en el consentimiento se informa de la existencia delderecho a retirarlo en cualquier momento	SI
Se informa del derecho a presentar una reclamación ante una autoridad de control	SI
Se informa de las cesiones basadas en requisitos legales o contractuales	SI
Se informa de las cesiones basadas en un requisito necesario para suscribir un contrato	SI
Se informa de la existencia de decisiones automatizas, elaboración de perfiles, sobrela lógica aplicada, la importancia y consecuencias previstas del tratamiento	SI
Antes de realizar tratamientos de datos personales para una finalidad distinta de la que fueron recogidos, se informa al interesado y la información abarca esa otra finalidad y cualquier otra información pertinente	SI

NIVEL DE CUMPLIMIENTO

Satisfactorio. Se cumple con la normativa. Han sido revisadas las cláusulas de información y consentimiento.

RECOMENDACIONES

La información a las personas interesadas se debe de aportar de manera clara y concisa en los términosprevistos.

LEGISLACION

Reglamento UE 679/2016

Art.13. Información que deberá facilitarse cuando los datos personales se obtengan delinteresado.
1- Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento,en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

- **a.** la identidad y los datos de contacto del responsable y, en su caso, de su representante;
- **b.** los datos de contacto del delegado de protección de datos, en su caso;
- **c.** los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
- **d.** cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;
- **e.** los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
- **f.** en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

2- Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

- a. el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
- b. la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
- c. cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado2, letra a), la existencia del 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;
- d. el derecho a presentar una reclamación ante una autoridad de control;
- e. si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos; la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

10.-DERECHOS DEL INTERESADO. INFORMACION CUANDO LOS DATOS NO SE OBTIENEN DEL INTERESADO

DERECHOS DEL INTERESADO. INFORMACIÓN A FACILITAR CUANDO LOSDATOS NO SE OBTIENEN DEL INTERESADO	SI/NO
Se informa de la identidad y los datos de contacto del responsable y, en su caso, de surepresentante	SI
Se informa de los datos de contacto del DPD	SI

Se informa de los fines del tratamiento	SI
Se informa de la base jurídica del tratamiento	SI
Se informa de las categorías de datos personales de que se trate	SI
Se informa de los destinatarios o las categorías de destinatarios de los datos	SI
Se informa del plazo durante el cual se conservarán los datos personales	SI
Se informa de los criterios utilizados para determinar este plazo el plazo deconservación cuando no es posible informar del mismo	SI
Se informa de los intereses legítimos concretos en que se basa el tratamiento	SI
Se informa del derecho a solicitar el acceso a sus propios datos personales	SI
Se informa del derecho a solicitar la rectificación de sus datos	SI
Se informa del derecho a solicitar la supresión	SI
Se informa del derecho a la limitación del tratamiento	SI
Se informa del derecho a oponerse al tratamiento	SI
Se informa del derecho a la portabilidad de los datos	SI
Se informa de la existencia del derecho a retirarlo el consentimiento en cualquiermomento	SI
Se informa del derecho a presentar una reclamación ante una autoridad de control	SI
Se informa de la fuente de la que proceden los datos personales	SI
Si proceden de fuentes de acceso público, se informa de ello	SI
Se proporciona la información antes de un mes	SI
Si los datos personales se utilizan para comunicación con el interesado, se le comunica la información a que tiene derecho en el momento de la primera comunicación	SI
Si está previsto comunicar los datos personales del interesado a otro destinatario,se le comunica la información a más tardar en el momento en que los datos personales son comunicados por primera vez	SI
Se informa al interesado si se realizan tratamientos para finalidades diferentes de laque fueron recogidos	SI
No se informa cuando ya dispone de la información el interesado	NO
No se informa cuando la comunicación de dicha información resulta imposible osupone un esfuerzo desproporcionado	NO
No se informa porque puede imposibilitar u obstaculizar gravemente el logro de los objetivos del tratamiento, pero se adoptan medidas para proteger los derechos, libertades e intereses legítimos del interesado	NO
No se informa porque la obtención o la comunicación está expresamente establecidapor normas de derecho aplicables	SI
No se informa porque los datos personales tienen carácter confidencial sobre labase de una obligación de secreto profesional regulada por normas de Derecho	SI

NIVEL DE CUMPLIMIENTO

Satisfactorio.

RECOMENDACIONES

La información a las personas interesadas se debe de aportar de manera clara y concisa en los términosprevistos.

Reglamento UE 679/2016
Art.14 Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado

1. Cuando los datos personales no se hayan obtenidos del interesado, el responsable del tratamientofacilitará la siguiente información:

d. la identidad y los datos de contacto del responsable y, en su caso, de su representante;
e. los datos de contacto del delegado de protección de datos, en su caso;
f. los fines del tratamiento a que se destinan los datos personales, así como la base jurídica deltratamiento;
g. las categorías de datos personales de que se trate;
h. los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
i. en su caso, la intención del responsable de transferir datos personales a un destinatario en untercer país u organización internacional y la existencia o ausencia de una decisión de adecuaciónde la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los mediospara obtener una copia de ellas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparenterespecto del interesado:

a. el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, loscriterios utilizados para determinar este plazo;
b. cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable del tratamiento o de un tercero;
c. la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
d. cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada;
e. el derecho a presentar una reclamación ante una autoridad de control;
f. la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;
g. la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere elartículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

11.-DERECHOS DE LOS INTERESADOS.TIPOS

11. 1.- DERECHO DE ACCESO

DERECHO DE ACCESO	SI/NO
Se informa respecto a los fines del tratamiento	SI
Se informa de las categorías de datos personales que se tratan	SI
Se informa de los destinatarios o las categorías de destinatarios a los que secomunicaron o serán comunicados los datos personales	SI
Se informa del plazo previsto de conservación de los datos personales	SI
Se informa de los criterios utilizados para determinar el plazo de conservación	SI
Se informa del derecho a solicitar la rectificación o supresión de sus datos	SI
Se informa del derecho a solicitar la limitación del tratamiento de los datos	SI
Se informa del derecho a solicitar la oposición al tratamiento	SI
Se informa del derecho a presentar una reclamación ante una autoridad de control	SI
Se proporciona información sobre el origen de los datos cuando no recogen del propiointeresado	SI
Se facilita copia de los datos personales objeto de tratamiento cuando el interesado lo Solicita	SI
Se facilita la información en formato electrónico de uso común si lo solicita pormedios electrónicos salvo que se facilite otro medio	SI

NIVEL DE CUMPLIMIENTO

Satisfactorio. Están previstos los mecanismos para atender las solicitudes de los interesados correctamente y en tiempo.

RECOMENDACIONES

La información a las personas interesadas se debe de aportar de manera clara y concisa en los plazos yen los términos previstos.

LEGISLACION

Reglamento UE 679/2016

Art. 15 Derecho de Acceso del interesado.

1- El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:

a. los fines del tratamiento;
b. las categorías de datos personales de que se trate;
c. los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;
d. de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible,los criterios utilizados para determinar este plazo;
e. la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;

f. el derecho a presentar una reclamación ante una autoridad de control;
cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;
g. la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado

11. 2.- DERECHO DE RECTIFICACION

DERECHO DE RECTIFICACION	SI/NO
Se rectifican los datos personales inexactos sin dilación indebida	SI
Se completan los datos personales incompletos teniendo en cuenta los fines deltratamiento	SI

NIVEL DE CUMPLIMIENTO
Satisfactorio. Están previstos los mecanismos para atender las solicitudes de los interesadoscorrectamente y en tiempo.

RECOMENDACIONES
Siempre han de contestarse las comunicaciones solicitadas por escrito.

LEGISLACIÓN

Reglamento UE 679/2016

Art. 16 Derecho de Rectificación

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

11. 3.- DERECHO DE SUPRESION

En este punto analizaremos el derecho a la eliminación de los tratamientos o "al derecho al olvido":

DERECHO DE SUPRESIÓN. "DERECHO AL OLVIDO"	SI/NO
Se suprimen los datos cuando no son necesarios en relación con los fines para losque fueron recogidos	SI
Se suprimen los datos cuando se retira el consentimiento en que se basa eltratamiento	SI
Se suprimen los datos cuando el interesado se opone al tratamiento	SI
Se suprimen los datos cuando han sido tratados ilícitamente	N.A.
Se suprimen los datos cuando lo exige una obligación legal	SI
Se suprimen los datos cuando se obtienen en relación con la oferta de serviciosde la sociedad de la información	SI

NIVEL DE CUMPLIMIENTO
Satisfactorio. Están previstos los mecanismos para atender las solicitudes de los interesadoscorrectamente y en tiempo.

RECOMENDACIONES
Los datos personales deben de ser suprimidos a solicitud de la persona interesada si no existe obligaciónlegal de que se conserven y en todo caso cuando dejen de ser necesarios.

LEGISLACIÓN

Reglamento UE 679/2016

Art. 17 Derecho de Supresión (<<el derecho al olvido>>)

1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a. los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;
b. el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;
c. el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan
d. otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;
e. los datos personales hayan sido tratados ilícitamente;
f. los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;
g. los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1

Ley orgánica de protección de datos

Artículo 15. Derecho de supresión.
1. El derecho de supresión se ejercerá de acuerdo con lo establecido en el artículo 17 del Reglamento(UE) 2016/679.
2. Cuando la supresión derive del ejercicio del derecho de oposición con arreglo al artículo 21.2 del Reglamento (UE) 2016/679, el responsable podrá conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa.

11. 4.- DERECHO A LA LIMITACIÓN DEL TRATAMIENTO

DERECHO A LA LIMITACIÓN DEL TRATAMIENTO	SI/NO
Se limita el tratamiento durante un plazo para verificar la exactitud de los datos, cuando el interesado impugna su exactitud	SI
Se limita el tratamiento cuando es ilícito y el interesado se opone a la supresión desus datos personales y solicita en su lugar la limitación de su uso	SI
Se limita el tratamiento cuando no son necesarios para los fines pero el interesadolos necesita para la formulación, el ejercicio o la defensa de reclamaciones	SI
Se limita el tratamiento cuando el interesado se opone al tratamiento mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado	SI
Se informa al interesado cuando se levanta la limitación del tratamiento	SI

NIVEL DE CUMPLIMIENTO

Satisfactorio. Están previstos los mecanismos para atender las solicitudes de los interesadoscorrectamente y en tiempo.

RECOMENDACIONES

Se debe procederá la limitación de tratamiento de los datos en los plazos y ocasiones establecidas en elReglamento

LEGISLACIÓN

Reglamento UE 679/2016

Art. 18 Derecho a la limitación del tratamiento

1.El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a. el interesado impugne la exactitud de los datos personales, durante un plazo que permita alresponsable verificar la exactitud de los mismos;
b. el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;
c. el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;
d. el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

Ley orgánica de protección de datos

Artículo 16. Derecho a la limitación del tratamiento.

1. El derecho a la limitación del tratamiento se ejercerá de acuerdo con lo establecido en el artículo 18del Reglamento (UE) 2016/679.
2. El hecho de que el tratamiento de los datos personales esté limitado debe constar claramente en lossistemas de información del responsable.

11. 5.- DERECHO A LA PORTABILIDAD DE LOS DATOS

DERECHO A LA PORTABILIDAD DE LOS DATOS	SI/NO
Se facilitan los datos cuando el interesado lo solicita en un formato estructurado, deuso común y lectura mecánica	SI
Se transmiten dichos datos a otro responsable si el tratamiento está basado en el consentimiento o en un contrato	SI
Se transmiten dichos datos si el tratamiento se efectúe por medios automatizados	SI
Se transmiten los datos al nuevo responsable que el interesado determina, si es posible técnicamente	SI

NIVEL DE CUMPLIMIENTO

Satisfactorio. Están previstos los mecanismos para atender las solicitudes de los interesadoscorrectamente y en tiempo.

RECOMENDACIONES

Se debe de contar con procedimientos internos que permitan atender el derecho a la portabilidad de losdatos de las personas interesadas.

LEGISLACIÓN

Reglamento UE 679/2016

Art. 20 Derecho a la portabilidad de los datos

1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:
   a. el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), oel artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y
   b. el tratamiento se efectúe por medios automatizados.

2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado
tendrá derecho a que los datos personales se transmitan directamente de responsable a responsablecuando sea técnicamente posible.

Ley orgánica de protección de datos

Artículo 17. Derecho a la portabilidad.

El derecho a la portabilidad se ejercerá de acuerdo con lo establecido en el artículo 20 del Reglamento(UE) 2016/679.

11. 6.- DERECHO DE OPOSICION

DERECHO DE OPOSICION	SI/NO
Están previstos los mecanismos para atender las solicitudes de oposición y se dejande tratar los datos	SI
Están previstos los mecanismos para atender las solicitudes de oposición pero no se dejan de tratar los datos por motivos legítimos imperiosos para el tratamiento que prevalecen sobre los intereses, los derechos y las libertades o para la formulación, el ejercicio o la defensa de reclamaciones	NO
Se ponen los medios necesarios para que pueda ejercer su derecho a oponersepor medios automatizados	SI

NIVEL DE CUMPLIMIENTO

Satisfactorio. Están previstos los mecanismos para atender las solicitudes de los interesadoscorrectamente y en tiempo.

RECOMENDACIONES

Se debe de contar con procedimientos internos que permitan dejar de tratar los datos de aquellosinteresados que se opongan a su tratamiento.

LEGISLACIÓN

Reglamento UE 679/2016

Art. 21 Derecho de Oposición

1. El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con susituación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base dedichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.
2. Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.
3. Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines

Ley orgánica de protección de datos

Artículo 18. Derecho de oposición.

El derecho de oposición, así como los derechos relacionados con las decisiones individuales automatizadas, incluida la realización de perfiles, se ejercerán de acuerdo con lo establecido,respectivamente, en los artículos 21 y 22 del Reglamento (UE) 2016/679.

11. 7 DERECHOS DE LOS INTERESADOS. DECISIONES INDIVIDUALES AUTOMATIZADAS, INCLUIDA LA ELABORACIÓNDE PERFILES

DERECHOS DEL INTERESADO. DECISIONES INDIVIDUALES AUTOMATIZADAS, INCLUIDA LA ELABORACIÓN DE PERFILES	SI/NO
No se realizan tratamientos que supongan la toma una decisión basada únicamenteen el tratamiento automatizado y que produzca efectos jurídicos	NO
Se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos porque es necesario parala celebración o la ejecución de un contrato	NO
Se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos porque están autorizados en Derecho	NO
Se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos porque se cuenta con el consentimiento explícito	NO
Si se realizan tratamientos que suponen la toma una decisión basada únicamente enel tratamiento automatizado y que producen efectos jurídicos se adoptan las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos	NO
Si se realizan tratamientos que suponen la toma una decisión basada únicamente enel tratamiento automatizado y que producen efectos jurídicos se adoptan medidas adecuadas para salvaguardar el derecho a obtener intervención humana por parte del responsable	NO
Si se realizan tratamientos que suponen la toma una decisión basada únicamente enel tratamiento automatizado y que producen efectos jurídicos se adoptan medidas adecuadas para dar al interesado ocasión de expresar su punto de vista e impugnar ladecisión	N.A.
Se toman decisiones individuales automatizadas, incluida la elaboración de perfiles, que se basen en las categorías especiales de datos personales porque se cuenta conel consentimiento del interesado	NO
Se toman decisiones individuales automatizadas, incluida la elaboración de perfiles, que se basen en las categorías especiales de datos personales porque se cuenta con habilitación legal	NO
Se informa a los interesados acerca de estas decisiones individuales automatizadas yde la habilitación legal de las mismas	N.A.
Se toman decisiones individuales automatizadas, incluida la elaboración de perfiles, que se basen en las categorías especiales de datos personales porque se han tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado	N.A.

NIVEL DE CUMPLIMIENTO

Satisfactorio. No se realizan tratamientos que supongan la toma de decisiones individuales automatizas,incluida la elaboración de perfiles.

RECOMENDACIONES

Las personas tenemos derecho a que nuestros datos no se incluyan en tomas de decisiones individualesautomatizadas sin que se nos advierta previamente de ello:

LEGISLACIÓN

Reglamento UE 679/2016

Art.22 Decisiones individuales automatizadas, incluida la elaboración de perfiles

1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.
2. El apartado 1 no se aplicará si la decisión:
   a. es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;
   b. está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o
   c. se basa en el consentimiento explícito del interesado.

11. RESPONSABILIDAD DEL RESPONSABLE DEL TRATAMIENTO

RESPONSABILIDAD DEL RESPONSABLE DEL TRATAMIENTO	SI/NO
Se tiene en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamientopara garantizar y poder demostrar que el tratamiento es conforme con el RGPD	SI
Se tienen en cuenta los riesgos de diversa probabilidad y gravedad para los derechosy libertades de las personas físicas	SI
Se aplican medidas técnicas y organizativas apropiadas	SI
Las medidas se revisan y actualizan cuando es necesario	SI
Se han confeccionado políticas de protección de datos	SI
Se aplican las políticas de protección de datos	SI

NIVEL DE CUMPLIMIENTO

Satisfactorio. Se ha realizado un análisis de riesgo para determinar las amenazas en el tratamiento de datos personales y valorar si fuera necesario establecer más medidas de seguridad de las que actualmente existen en FUNDACION CEPAIM y sus centros especiales de empleo.

RECOMENDACIONES

Las medidas implantadas han de actualizarse siempre que sea necesario. FUNDACION CEPAIM y sus centros especiales de empleo tienen implantado un plan General de Seguridad Informática. Las medidas de seguridad implantadas se revisan y verifican periódicamente.

LEGISLACIÓN

Reglamento UE 679/2016

Art.24 Responsabilidad del Responsable del Tratamiento

1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como losriesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, elresponsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

Ley orgánica de protección de datos

Artículo 28. Obligaciones generales del responsable y encargado del tratamiento.

1. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular
2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en lossiguientes supuestos:
    1. Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.
    2. Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.
    3. Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especialesde datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta leyorgánica o de los datos relacionados con la comisión de infracciones administrativas.
    4. Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin decrear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.
    5. Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.
    6. Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.
    7. Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.
    8. Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.

CUMPLIMIENTO

Satisfactorio. Se tienen establecidos los modelos de contrato a suscribir con los encargados de tratamiento. Se conoce su número, los tratamientos en los que intervienen y los medios que emplean.Se tienen firmados contratos escritos con ellos en esta materia, De la misma manera se tienen preparados modelos de contratos para cuando FUNDACION CEPAIM o sus centros especiales de empleo actúan como encargados de tratamiento.

RECOMENDACIONES

Cada vez que se subcontrate una tarea se debe de verificar si implica acceso a datos personales. En casoafirmativo, y una vez comprobada la solvencia del proveedor se debe de suscribir con él un contratoescrito en materia de protección de datos.

LEGISLACIÓN

Reglamento UE 679/2016

Art.28 Encargado del tratamiento

1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativasapropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.

2. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito,específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.

3. En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamentou otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

1. Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro actojurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otroencargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.

Ley orgánica de protección de datos
Artículo 33. Encargado del tratamiento.

1. El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesariospara la prestación de un servicio al responsable no se considerará comunicación de datos siempre quese cumpla lo establecido en el Reglamento (UE) 2016/679, en la presente ley orgánica y en sus normas de desarrollo.

2. Tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propionombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados auncuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del Reglamento(UE) 2016/679. Esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco dela legislación de contratación del sector público. Tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades.
3. El responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos personales deben ser destruidos, devueltos al responsable o entregados, en sucaso, a un nuevo encargado. No procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al responsable, que garantizará su conservación mientras tal obligación persista.
4. El encargado del tratamiento podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.
5. En el ámbito del sector público podrán atribuirse las competencias propias de un encargado del tratamiento a un determinado órgano de la Administración General del Estado, la Administración de las comunidades autónomas, las Entidades que integran la Administración Local o a los Organismos vinculados o dependientes de las mismas mediante la adopción de una norma reguladora de dichas competencias, que deberá incorporar el contenido exigido por el artículo 28.3 del Reglamento (UE)2016/679.

17.- REGISTRO DE ACTIVIDADES DE TRATAMIENTO

REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO	SI/NO
Se lleva un registro de las actividades de tratamiento	SI
El registro recoge el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos	SI
El registro recoge los fines del tratamiento	SI
Recoge una descripción de las categorías de interesados y de las categorías de datospersonales	SI
Recoge las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales	SI
Recogen las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional	SI
Incluye los plazos previstos para la supresión de las categorías de datos	SI
Incluye una descripción general de las medidas técnicas y organizativas apropiadasal riesgo de los tratamientos	SI

NIVEL DE CUMPLIMIENTO

Satisfactorio. Existe un Registro de actividades de tratamiento elaborado de conformidad con el Reglamento UE 679/2016 y con el contenido establecido en la norma. El registro está elaborado tanto para FUNDACION CEPAIM como para sus centros especiales de empleo.

RECOMENDACIONES

El registro de actividades de tratamiento debe de estar permanentemente actualizado y responder a la realidad de los tratamientos efectuados, describir los procedimientos y medidas de seguridad existentes,y las políticas de privacidad. Al menos ha de ser revisado cada dos años.

LEGISLACIÓN

Reglamento UE 679/2016

Art.30 Registro de las actividades de tratamiento

1. Cada responsable y, en su caso, sus representantes llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

a. el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;
b. los fines del tratamiento;
c. una descripción de las categorías de interesados y de las categorías de datos personales;
d. las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
e. en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en elcaso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
f. cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
g. Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

Ley orgánica de protección de datos

Artículo 31. Registro de las actividades de tratamiento.

1. Los responsables y encargados del tratamiento o, en su caso, sus representantes deberánmantener el registro de actividades de tratamiento al que se refiere el artículo 30 del Reglamento (UE) 2016/679, salvo que sea de aplicación la excepción prevista en su apartado 5. El registro, que podrá organizarse en torno a conjuntos estructurados de datos, deberá especificar, según sus finalidades, las actividades de tratamiento llevadas a cabo y las demás circunstancias establecidas en el citado reglamento. Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos deberán comunicarle cualquier adición, modificación o exclusión en el contenido del registro.

2. Los sujetos enumerados en el artículo 77.1 de esta ley orgánica harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 del Reglamento (UE) 2016/679 y su base legal.

18. SEGURIDAD DEL TRATAMIENTO

SEGURIDAD DEL TRATAMIENTO	SI/NO
Las medidas a aplicar tienen en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, alcance, contexto y fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas	SI
Se aplican las medidas técnicas y organizativas apropiadas para garantizar un nivelde seguridad adecuado al riesgo	SI
Se han incluido medidas para asegurar la confidencialidad, integridad, disponibilidady resiliencia permanentes de los sistemas y servicios de tratamiento	SI
Medidas para asegurar la capacidad de restaurar la disponibilidad y el acceso a losdatos personales de forma rápida en caso de incidente físico o técnico	SI
Existe un proceso de verificación, evaluación y valoración regular de la eficacia de lasmedidas técnicas y organizativas para garantizar la seguridad del tratamiento	SI
Se han tenido en cuenta los riesgos que presenta el tratamiento como consecuencia de su destrucción, pérdida o alteración accidental o ilícita que son transmitidos, conservados o tratados, o la comunicación o acceso no autorizados a dichos datos para evaluar el nivel de seguridad aplicado	SI
Se han tomado medidas para garantizar que las personas autorizadas a acceder adatos sólo los tratan siguiendo instrucciones	SI

NIVEL DE CUMPLIMIENTO

Satisfactorio. Se estima que las medidas de seguridad son adecuadas atendiendo a los resultados del análisis de riesgo, así como por tener implantado un plan integral de Seguridad informática que engloba a Fundación Cepaim, así como a sus centros especiales de empleo.

RECOMENDACIONES

La eficacia de las medidas de seguridad y los procedimientos han de ser evaluados periódicamente.

LEGISLACIÓN

Reglamento UE 679/2016

Art.32 Seguridad del tratamiento

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, queen su caso incluya, entre otros:

a. la seudonimización y el cifrado de datos personales;
b. la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentesde los sistemas y servicios de tratamiento;
c. la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d. un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

19. BRECHAS DE SEGURIDAD

19. 1.- NOTIFICACION DE BRECHA DE SEGURIDAD A LA AEPD

NOTIFICACIÓN DE BRECHAS DE LA SEGURIDAD DE LOS DATOSPERSONALES A LA AUTORIDAD DE CONTROL	SI/NO
Se ha establecido un procedimiento para identificar y gestionar las brechas de seguridad	SI
Existe un procedimiento para que los encargados del tratamiento notifiquen lasbrechas al responsable en el momento en que tengan conocimiento de ellas	SI
Existe un procedimiento para notificar a la autoridad de control en el plazo de 72horas	SI
Existe un procedimiento para documentar los motivos por los que no se puedenotificar en el plazo de 72 horas	SI
Existe un procedimiento para facilitar la información de manera gradual cuando noes posible facilitarla simultáneamente	SI
Se documenta cualquier brecha de seguridad de los datos personales	SI
En la documentación se incluyen los hechos relacionados con ella, sus efectos y lasmedidas correctivas adoptadas	SI
Se ha comprobado que el procedimiento de notificación funciona	SI

NIVEL DE CUMPLIMIENTO

Satisfactorio. Existe un procedimiento adecuado para notificar brechas de seguridad a la AgenciaEspañola de Protección de datos.

RECOMENDACIONES

Los procedimientos han de ser revisados periódicamente.

LEGISLACIÓN

Reglamento UE 679/2016

Art.33 Notificación de una violación de seguridad de los datos personales a la Autoridad deControl

1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades delas personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas,deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

19. 2.- NOTIFICACION DE BRECHA DE SEGURIDAD AL INTERESADO

COMUNICACIÓN DE UNA BRECHA AL INTERESADO	SI/NO
Existe un procedimiento para comunicar la brecha sin dilación indebida cuando seaprobable que entrañe un alto riesgo para los derechos y libertades	SI
La comunicación al interesado, se lleva a cabo en un lenguaje claro y sencillo,describe la naturaleza de la brecha	SI

NIVEL DE CUMPLIMIENTO

Satisfactorio. Existe un procedimiento adecuado para notificar brechas de seguridad a los interesados

RECOMENDACIONES

Los procedimientos han de ser revisados periódicamente.

LEGISLACIÓN

Reglamento UE 679/2016

Art.34 Notificación de una violación de seguridad de los datos personales al interesado

1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33.

20. DELEGADO DE PROTECCION DE DATOS (DPD)

DELEGADO DE PROTECCIÓN DE DATOS	SI/NO
Se ha designado un DPD por requerimiento legal	SI
Se ha designado un DPD atendiendo a sus cualidades de profesionalidad,conocimientos y competencias en la materia	SI.
Se han publicado los datos de contacto del DPD y se ha comunicado a la autoridadde control	SI
Se garantiza que el DPD participa de forma adecuada y en tiempo oportuno en todaslas cuestiones relativas a la protección de datos personales	SI.
Se da respaldo en el desempeño sus funciones	SI.
Se le facilitan los recursos necesarios para el desempeño de sus funciones, el accesoa los datos personales y a las operaciones de tratamiento	SI.
Se le facilitan los recursos necesarios para mantener sus conocimientos	SI
Se garantiza que el DPD no recibe ninguna instrucción en lo que respecta aldesempeño de sus funciones	SI.
No se puede destituir ni sancionar al DPD por desempeñar sus funciones	NO.

El DPD rinde cuentas directamente al más alto nivel jerárquico	SI.
El DPD atiende las solicitudes de los interesados	SI.
El DPD está obligado a mantener la confidencialidad en el desempeño de susfunciones	SI.
Si el DPD desempeña otras funciones, se garantiza que no dan lugar a conflicto deintereses	SI
Las funciones del DPD son informar, asesorar y formar al personal de lasobligaciones que les incumben	SI.
El DPD coopera y actúa como punto de contacto con la autoridad de control	SI

NIVEL DE CUMPLIMIENTO

Satisfactorio. Dentro del Registro de actividades de tratamiento de la entidad se ha determinado que dado que FUNDACION CEPAIM trata a "gran escala" datos de salud debe de contar con un Delegado de protección de datos. Se ha determinado que resulta obligatorio y se ha designado a la entidad IÑIGO SERVICIOSINTEGRALES estando ya tramitada su inscripción . Se procederá también a nombrar a esta misma entidad de manera voluntaria para SAEMA, SOEMCA y DIVERSIA EMPLEO

RECOMENDACIONES

Facilitar la labor del Delegado.

LEGISLACIÓN

Se ha revisado también lo establecido en la ley orgánica 3/2018 de 5 de diciembre de protección

Reglamento UE 679/2016

Art.37 Designación del Delegado de Protección de Datos

1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempreque:
   a. el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales queactúen en ejercicio de su función judicial;
   b. las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o
   c. las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

Art 34. Designación de un delegado de protección de datos

1. Los responsables y encargados del tratamiento deberán designar un delegado de protecciónde datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de las siguientes entidades:

a) Los colegios profesionales y sus consejos generales.

b) Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.

Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.

a) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.

b) Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación,supervisión y solvencia de entidades de crédito.

c) Los establecimientos financieros de crédito.

d) Las entidades aseguradoras y reaseguradoras.

e) Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores. i)Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.

j) Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a losresponsables de los ficheros regulados por la legislación de prevención del blanqueo de capitalesy de la financiación del terrorismo.

k) Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.

l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes. Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.

m) Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.

n) Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego. ñ) Lasempresas de seguridad privada.

o) Las federaciones deportivas cuando traten datos de menores de edad.

1. Los responsables o encargados del tratamiento no incluidos en el párrafo anterior podrán designar de manera voluntaria un delegado de protección de datos, que quedará sometido al régimen establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica. 3. Los responsables y encargados del tratamiento comunicarán en el plazo de diez días a la

2. Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, las designaciones, nombramientos y ceses de los delegados de protección de datos tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria.

3. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán, en el ámbito de sus respectivas competencias, una lista actualizada de delegados de protección de datos que será accesible por medios electrónicos.

4. En el cumplimiento de las obligaciones de este artículo los responsables y encargados del

5. tratamiento podrán establecer la dedicación completa o a tiempo parcial del delegado, entre otros criterios, en función del volumen de los tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos o libertades de los interesados.

21. EVALUACION DE IMPACTO

EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS	SI/NO
Se recaba el asesoramiento del DPD	SI.
Se realiza EIPD antes del tratamiento cuando es probable que entrañe un alto riesgopara los derechos y libertades de las personas	N.A.
Se realiza una EIPD antes en tratamientos a gran escala de categorías especiales dedatos o relativos a condenas e infracciones penales	N.A.
Se realiza una EIPD antes de tratamiento que suponen una observación sistemáticaa gran escala de una zona de acceso público	N.A.
Se realiza una EIPD en operaciones de tratamiento incluidas en la lista publicada porla autoridad de control	N.A.
La EIPD incluye una descripción sistemática de las operaciones de tratamientoprevistas y de los fines del tratamiento, y cuando procede el interés legítimo	N.A.
Incluye una evaluación de la necesidad y la proporcionalidad de las operaciones detratamiento con respecto a su finalidad	N.A.
La EIPD incluye una evaluación de los riesgos para los derechos y libertades	N.A.
Incluye medidas previstas para demostrar la conformidad con el RGPD, teniendo encuenta los derechos e intereses legítimos de los interesados y de otras personas	N.A.
Incluye las medidas previstas para afrontar los riesgos, garantías y mecanismospara garantizar la protección de datos	N.A.
Se reexaminan las EIPD siempre que es necesario y cuando exista un cambio de losriesgos que representen las operaciones de tratamiento	N.A.
Se consulta a la autoridad de control antes de proceder al tratamiento cuando unaEIPD muestre que el mismo entrañaría un alto riesgo si no se toman medidas para	N.A.
Se informa de las responsabilidades respectivas de los implicados en el tratamientoen la consulta a la autoridad de control	N.A.
Se informa de los fines y medios del tratamiento previsto en la consulta	N.A.
Se informa de las medidas y garantías establecidas para proteger los derechos ylibertades en la consulta	N.A.
Se facilitan los datos de contacto del delegado de protección de datos	N.A.
Se incluye la evaluación de impacto	N.A.
Cuando se consulta se facilita cualquier información adicional que solicite laautoridad de control	N.A.

NIVEL DE CUMPLIMIENTO

Satisfactorio. Dentro del Registro de actividades de tratamiento de la entidad se ha realizado un análisisde riesgo, así como otros análisis de necesidad, para determinar que en este momento se dan alguno delos supuestos que obligarían a FUNDACION CEPAIM a realizar evaluaciones de impacto sobre los tratamientos que se realizan, en particular sobre el tratamiento AUSUARIOS. No obstante, este es un tratamiento que serealizaba antes de la entrada en vigor del reglamento UE 679/2016 sin que haya habido cambios quejustifiquen la realización de una evaluación de impacto.

RECOMENDACIONES

En caso de que los tipos de tratamiento cambien, o se apruebe una nueva regulación normativa se deberá de revisar la obligación de realizar alguna evaluación de impacto.

LEGISLACIÓN

Reglamento UE 679/2016

Art.35 Evaluación de Impacto relativa a la protección de datos

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

a. evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b. tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o

c. observación sistemática a gran escala de una zona de acceso público.

La Agencia española de protección de datos publicó una instrucción estableciendo un listado de tratamientos que necesitaban la realización de una evaluación de impacto. Como requisito adicional debían de darse dos o más de los supuestos que así lo determinaban:

1. Tratamientos que impliquen perfilado o valoración de sujetos, incluida la recogida de datos del sujetoen múltiples ámbitos de su vida (desempeño en el trabajo, personalidad y comportamiento), que cubranvarios aspectos de su personalidad o sobre sobre sus hábitos.
2. Tratamientos que impliquen la toma de decisiones automatizadas o que contribuyan en gran medida ala toma de tales decisiones, incluyendo cualquier tipo de decisión que impida a un interesado el ejerciciode un derecho o el acceso a un bien o un servicio o formar parte de un contrato.
3. Tratamientos que impliquen la observación, monitorización, supervisión, geolocalización o control delinteresado de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden serlos servicios web, TV interactiva, aplicaciones móviles, etc.
4. Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPDo datos que permitan determinar la situación financiera o de solvenciapatrimonial o deducir informaciónsobre las personas relacionada con categorías especiales de datos.

5. Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de maneraúnica a una persona física.

6. Tratamientos que impliquen el uso de datos genéticos para cualquier fin.

7. Tratamientos que impliquen el uso de datos a gran escala. Para determinar si un tratamiento se puede considerar a gran escala se considerarán los criterios establecidos en la guía WP243 "Directrices sobre los delegados de protección de datos (DPD)" del Grupo de Trabajo del Artículo 29.

8. Tratamientos que impliquen la asociación, combinación o enlace de registros de bases de datos dedos o más tratamientos con finalidades diferentes o por responsables distintos.

Tratamientos de datos de sujetos vulnerables o en riesgo de exclusión social, incluyendo datos de menores de 14 años, mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género, así como sus descendientes y personas que esténbajo su guardia y custodia

10. Tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas.

11. Tratamientos de datos que impidan a los interesados ejercer sus derechos, utilizar un servicio o ejecutar un contrato, como por ejemplo tratamientos en los que los datos han sido recopilados por un responsable distinto al que los va a tratar y aplica alguna de las excepciones sobre la información que debe proporcionarse a los interesados según el artículo 14.5 (b,c,d) del RGP

22. TRANSFERENCIA A TERCEROS PAISES U ORGANIZACIONESINTERNACIONALES

TRANSFERENCIAS A PAÍSES TERCEROS U ORGANIZACIONES INTERNACIONALES	SI/NO
Se realizan transferencias a países, o sectores de los mismos, u organizacionesinternacionales declarados de nivel de protección adecuado por la Comisión Europea	NO
Se realiza un seguimiento de la validez de las decisiones de adecuación de laComisión europea	N.A.
Se realizan transferencias mediante garantías adecuadas que ofrezcan a losinteresados derechos exigibles y posibilidad de acciones legales.	N.A.
Existe un instrumento jurídico vinculante y exigible entre las autoridades uorganismos públicos	N.A.
Existen normas corporativas vinculantes	N.A.
Existen cláusulas tipo de protección de datos adoptadas por la Comisión	N.A.
Existen cláusulas tipo de protección de datos adoptadas por una autoridad de controly aprobadas por la Comisión	N.A.
Existe un código de conducta junto con compromisos vinculantes y exigibles en eltercer país que permita aplicar garantías adecuadas	N.A.
Existe un mecanismo de certificación junto con compromisos vinculantes y exigiblesen el tercer país que permita aplicar garantías adecuadas	N.A.

Existen cláusulas contractuales que requieren la autorización previa de la autoridadde control	N.A.
Existen acuerdos administrativos entre autoridades y organismos públicos que incorporen disposiciones que incluyan derechos efectivos y exigibles para los interesados	N.A.
Se realizan transferencias internacionales en ausencia de decisión de adecuación dela Comisión europea y de garantías adecuadas	N.A.
Se dispone del consentimiento explícito del interesados y se le ha informado de losposibles riesgos	N.A.
Son necesarias para la ejecución de un contrato con el interesado o para la ejecuciónde medidas precontractuales adoptadas a solicitud del interesado	N.A.
Son necesarias para la formulación, ejercicio o la defensa de reclamaciones	N.A.
Son necesarias para la protección de los intereses vitales del interesado o de otraspersonas, cuando el interesado esté incapacitado para dar su consentimiento	N.A.
Por intereses legítimos imperiosos	N.A.
Afecta a un número limitado de interesados y no es repetitiva	N.A.
Se han evaluado todas las circunstancias concurrentes y se han ofrecido garantíasapropiadas	N.A.
Se ha informado a la autoridad de control	N.A.

NIVEL DE CUMPLIMIENTO

Satisfactorio. No se realizan transferencias internacionales.

RECOMENDACIONES

Antes de realizar una transferencia internacional de datos se ha de verificar el cumplimiento de lo establecido en el Reglamento UE 679/2016.

LEGISLACIÓN

Reglamento UE 679/2016

Capítulo V: Transferencia de Datos personales a terceros países u Organizaciones internacionales

Art.44 Principio general de las transferencias.

Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlotras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores dedatos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel deprotección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado.

Ley orgánica de protección de datos

Transferencias internacionales de datos

Artículo 40. Régimen de las transferencias internacionales de datos.

Las transferencias internacionales de datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica y sus normas de desarrollo aprobadas por el Gobierno, y en las circulares de la Agencia Española de Protección de Datos y de las autoridades autonómicas de protección de datos, en el ámbito de sus respectivas competencias. En todo caso se aplicarán a los tratamientos en que consista la propia transferencia las disposiciones contenidas en dichas normas, en particular las que regulan los principios de protección de datos.

Artículo 41. Supuestos de adopción por la Agencia Española de Protección de Datos.

La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán adoptar, conforme a lo dispuesto en el artículo 46.2.c) del Reglamento (UE) 2016/679, cláusulas contractuales tipo para la realización de transferencias internacionales de datos, que se someterán previamente al dictamen del Comité Europeo de Protección de Datos previsto en el artículo 64 del citado reglamento.

La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán aprobar normas corporativas vinculantes de acuerdo con lo previsto en el artículo 47 del Reglamento (UE) 2016/679. El procedimiento se iniciará a instancia de una entidad situada en España y tendrá una duración máxima de nueve meses. Quedará suspendido como consecuencia de la remisión del expediente al Comité Europeo de Protección de Datospara que emita el dictamen al que se refiere el artículo 64.1.f) del Reglamento (UE) 2016/679, ycontinuará tras su notificación a la Agencia Española de Protección de Datos o a la autoridad autonómica de protección de datos competente

CONCLUSIONES FINALES

Una vez realizada la auditoría en materia de protección de datos de FUNDACION CEPAIM y verificado el cumplimiento de todos los ítems detallados con anterioridad y basándonos en el nivel de cumplimiento en los diversos apartados comprobados:

ACREDITAMOS

QUE SE HA REALIZADO:

- ✓ Identificación de las Actividades de Tratamiento realizadas en calidad de Responsable y Encargado del Tratamiento, así como la elaboración del Registro de Actividades del Tratamiento, conforme indica el art. 30 del RGPD.
- ✓ Revisión de los consentimientos para que sean expresos y en todo caso legítimos en las otrascircunstancias de licitud del art. 6.1del RGPD.
- ✓ Adaptación de las cláusulas de información a los requisitos de los arts. 13 y 14 del RGPD, parainformar en todos los tratamientos de datos de:
  - La identidad del Responsable del Tratamiento.
  - Los datos de contacto del Responsable del Tratamiento.
  - La finalidad del tratamiento.
  - La legitimación para el tratamiento.

- Los destinatarios o las categorías de destinatarios de los datos personales.
- Las transferencias de datos personales a terceros países previstas.
- Los plazos de conservación previstos.
- Los derechos que asisten al interesado y la forma de ejercerlos.
- El derecho a reclamar ante la AEPD.

✓ Revisión de la información solicitada, así como la recibida, para cumplir con el principio de minimización y de privacidad por defecto (art. 25 RGPD)

✓ Determinación de los plazos de conservación, teniendo en consideración los plazos mínimos de conservación marcados por la normativa que resulta de aplicación.

✓ Concienciación y comunicación a los trabajadores sobre la observancia de los principios recogidos en el art. 5 del RGPD, así como de su participación en las solicitudes de ejercicio de derechos, la notificación de las violaciones de seguridad y los requisitos necesarios para la comunicación de datos y las Transferencias Internacionales de Datos.

✓ Adaptación del procedimiento de atención de solicitudes de ejercicio de derechos para que sea ejercido, preferiblemente, por medios electrónicos y que incluya el ejercicio de todos los derechos reconocidos en los arts. 15 a 22 del RGPD:

- Acceso.
- Rectificación.
- Supresión.
- Limitación del tratamiento
- Portabilidad
- Oposición.
- Derecho a no ser objeto de decisiones automatizadas.

✓ Generación e implementación de un procedimiento específico para la revisión de los nuevostratamientos de datos, para garantizar que los mismos cumplen con las obligaciones del RGPD desde el diseño (Privacidad desde el diseño art. 25 RGPD).

✓ Creación de contratos específicos con los Encargados de Tratamiento o de confidencialidad, en función del tipo de servicio que se presten. (Art. 28 del RGPD)

✓ Realización del análisis de riesgos, conforme a la metodología. (art. 32 RGPD)

✓ Identificación y aplicación de las medidas de seguridad idóneas para mitigar los riesgos identificados.

✓ Generación del procedimiento de notificación de violaciones de seguridad a la Autoridad deControl, así como a los interesados, partiendo del Registro de Incidencias, en cumplimiento de los artículos 33 y 34 del RGPD.

Determinación de la necesidad de realizar Evaluación del Impacto relativa a la Protección de Datos en aquellos tratamientos de datos que entrañan un alto riesgo para los derechos y libertad de las personas físicas. (Art. 35 RGPD).