AUDITORÍA

Asociación Tinerfeña de Esclerosis Múltiple (ATEM)

AUDITORÍA INTERNA DE REVISIÓN EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES DE Asociación Tinerfeña de Esclerosis Múltiple (ATEM)

Antecedentes

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los mismo y por el que se deroga la Directiva 95/46/CE (RGPD) así como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD-GDD) requieren mecanismos de revisión y supervisión de la eficacia del cumplimiento de las obligaciones legales de los responsables que tratan datos personales

El art. 5 del RGPD indica que será el responsable quién deba demostrar dicho cumplimiento legal.

El art. 28 de la LOPDGDD indica que son obligaciones de responsables y encargados tener en cuenta los riesgos que podrían producirse durante el tratamiento de los datos personales. Esta obligación se materializa en el "Análisis de Riesgos". Con el análisis de riesgos se han podido identificar y detectar probables amenazas en los tratamientos de datos personales llevados a cabo por Asociación Tinerfeña de Esclerosis Múltiple (ATEM) Las actividades de tratamiento se resumen en el correspondiente registro de actividades de tratamiento. El resultado del análisis de riesgos determina y muestra los niveles de riesgo relacionados con cada actividad de tratamiento.

En virtud del considerando 74 del RGPD que establece que "...el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el Reglamento General de Protección de Datos, incluida la eficacia de las medidas…" además del análisis de riesgos se precisa disponer de un mecanismo de supervisión de las actuaciones que esta organización realiza en materia de protección de datos.

Objeto y alcance

Este procedimiento de supervisión y valoración se configura como un valioso recurso, sencillo y práctico que permite a la organización garantizar la debida PROACTIVIDAD y DILIGENCIA en ateria de protección de datos.

Se trata de un cuestionario que permite revisar y valorar aspectos de protección de datos que deben ser tenidos en cuenta con el fin de comprobar la eficacia de las medidas adoptadas, detectar posibles mejoras, identificar nuevas necesidades y verificar nuestro nivel de cumplimiento del RGPD.

Metodología y resultados

El cuestionario que se reproduce en la primera parte del presente informe contiene los elementos evaluados

Los resultados de la evaluación muestran sugerencias de actuación que deben tenerse en cuenta al objeto de corregir incumplimientos, desviaciones o realizar mejoras.

El informe consta de dos partes, la primera parte contiene el cuestionario con los elementos evaluados y la segunda parte contiene un resumen de los resultados obtenidos.

1. Primera parte. Cuestionario de evaluación.

2. Segunda parte. Resumen de resultados.

RESPONSABILIDADES DEL RESPONSABLE DE LOS TRATAMIENTOS
ASPECTOS GENERALES DE LOS TRATAMIENTOS
¿ASEGURA QUE LOS DATOS PERSONALES TRATADOS SE MANTIENEN EXACTOS Y ACTUALIZADOS?
SI
¿SE TRATAN ÚNICAMENTE LOS DATOS PERSONALES QUE SON NECESARIOS PARA EL FIN PERSEGUIDO POR LA ORGANIZACIÓN?
SI
¿HA DISPUESTO LA INFORMACIÓN OBLIGATORIA A LOS INTERESADOS DE FORMA QUE ÉSTA SEA LEGIBLE E INTELIGIBLE PARA LOS INTERESADOS?
SI
¿SE HA DETERMINADO EL PLAZO DE CONSERVACIÓN DE LOS DATOS PERSONALES TRATADOS EN FUNCIÓN A CRITERIOS RAZONADOS, OBJETIVOS Y LEGALES?
SI
SI ENCARGA EL TRATAMIENTO DE DATOS PERSONALES A ALGUNA PERSONA FÍSICA O JURÍDICA ¿MANTIENE CON TODOS SUS ENCARGADOS DEL TRATAMIENTO UN CONTRATO DE CONFIDENCIALIDAD?
SI
DERECHOS
¿HA RECIBIDO ALGUNA PETICIÓN DE ACCESO, SUPRESIÓN, RECTIFICACIÓN O EL EJERCICIO DE CUALQUIER OTRO DERECHO Y HA RESPONDIDO DENTRO DEL PLAZO DE 30 DÍAS?
NO
LICITUDES
¿CONSERVA LOS REGISTROS DE LOS CONSENTIMIENTOS QUE LOS INTERESADOS (MAYORES DE 14 AÑOS) LE HAYAN FACILITADO?
SI

SI ALGÚN INTERESADO (MAYOR DE 14 AÑOS) HA RETIRADO EL CONSENTIMIENTO A ALGÚN TRATAMIENTO DE DATOS PERSONALES ¿HA REALIZADO LAS ACTUACIONES OPORTUNAS PARA EVITAR QUE SUS DATOS SIGAN SIENDO TRATADOS?
NO APLICA
SI TRATA DATOS DE MENORES DE 14 AÑOS Y DICHO TRATAMIENTO SE BASA EN EL CONSENTIMIENTO ¿FIGURA EN EL REGISTRO DEL CONSENTIMIENTO LA FIRMA O ACEPTACIÓN DEL TITULAR/ES DE LA PATRIA POTESTAD O TUTELA DEL MENOR?
SI
CUANDO TRATA DATOS PERSONALES QUE SON NECESARIOS PARA LA PRESTACIÓN DE UN SERVICIO/SUMINISTRO DE UN PRODUCTO, ¿CONSERVA EL CONTRATO/PRECONTRATO O LA EVIDENCIA QUE LE PERMITE DEMOSTRAR QUE DICHOS DATOS GUARDAN RELACIÓN CON EL ALCANCE Y LA FINALIDAD DEL SERVICIO/SUMINISTRO?
SI
SI TRATA DATOS PERSONALES POR OBLIGACIÓN LEGAL ¿TIENE DEFINIDA LA NORMATIVA QUE LE OBLIGA A TRATAR DICHOS DATOS?
SI
DATOS DE CATEGORÍAS ESPECIALES
SI TRATA DATOS DE CATEGORÍAS ESPECIALES (DATOS DE SALUD, DATOS BIOMÉTRICOS, GENÉTICOS, DATOS DE ORIGEN ÉTNICO O RACIAL, OPINIONES POLÍTICAS, CONVICCIONES RELIGIOSAS, AFILIACIÓN SINDICAL, ORIENTACIÓN O VIDA SEXUAL) ¿SE HA ASEGURADO QUE CONCURREN LAS CIRCUNSTANCIAS QUE LE PERMITEN TRATAR DICHOS DATOS?
SI
SI TRATA DATOS RELATIVOS A CONDENAS E INFRACCIONES PENALES ¿SE HA ASEGURADO QUE EXISTE SUPERVISIÓN DE LAS AUTORIDADES PÚBLICAS PARA DICHO TRATAMIENTO O QUE EXISTEN NORMAS DE DERECHO QUE LO AUTORICEN?
NO APLICA
DELEGADO DE PROTECCIÓN DE DATOS (DPD)
¿HA SIDO DESIGNADO ATENDIENDO A SUS CUALIDADES DE PROFESIONALIDAD, CONOCIMIENTOS, COMPETENCIAS EN LA MATERIA E IMPARCIALIDAD NECESARIAS?
NO APLICA

¿HA COMUNICADO A LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS LA DESIGNACIÓN DE SU DPD O EL CESE O UN NUEVO NOMBRAMIENTO DE DPD?
NO APLICA
¿GARANTIZA QUE EL DPD NO RECIBE NINGUNA INSTRUCCIÓN POR PARTE DEL RESPONSABLE?
NO APLICA
DELEGADO DE PROTECCIÓN DE DATOS (DPD)
¿HA HABIDO CAMBIOS EN SUS ACTIVIDADES DE TRATAMIENTO?
NO
¿HA REVISADO SUS ACTIVIDADES DE TRATAMIENTO DE DATOS PERSONALES ASÍ COMO LAS MEDIDAS DE PROTECCIÓN, DE SEGURIDAD, ETC.. DE FORMA PERIÓDICA DENTRO DEL ÚLTIMO AÑO?
SI
¿HA REVISADO EL RESULTADO DEL ANÁLISIS DE LOS RIESGOS QUE LOS TRATAMIENTOS PUEDEN OCASIONAR SOBRE LAS LIBERTADES Y DERECHOS DE LOS INTERESADOS?
SI
¿HA SUFRIDO ALGÚN INCIDENTE RELACIONADO CON EL ROBO DE DATOS O CON LA VULNERACIÓN DE LA DEBIDA CONFIDENCIALIDAD?
NO
¿HA SUFRIDO ALGÚN INCIDENTE RELACIONADO CON LA PÉRDIDA DE DATOS DE CARÁCTER PERSONAL?
NO
¿HA DOCUMENTADO CUALQUIER INCIDENTE O BRECHA DE SEGURIDAD QUE HAYA DETECTADO?
NO
¿MODIFICA LAS CLAVES DE ACCESO A LOS SOPORTES ELECTRÓNICOS QUE CONTIENEN DATOS CON REGULARIDAD?
SI

¿HA CONTRATADO ALGÚN NUEVO EMPLEADO/A QUE DENTRO DE SUS FUNCIONES TENGA ACCESO A DATOS PERSONALES DE LA ORGANIZACIÓN?
SI
¿SU ORGANIZACIÓN TIENE DEFINIDA Y DOCUMENTADA SU POLÍTICA DE PROTECCIÓN DE DATOS?
SI
EN EL CASO QUE TENGA OTROS CORRESPONSABLES (RESPONSABLES QUE TAMBIÉN DETERMINAN CONJUNTAMENTE CON USTED QUÉ DATOS TRATAR, QUÉ SE HACE CON LOS DATOS, ETC.) ¿HAN FIRMADO ACUERDO DE CORRESPONSABILIDAD POR ESCRITO?
NO APLICA
EVALUACIÓN DE IMPACTO (EIDP)
¿ESTÁ LA EIPD DOCUMENTADA?
NO APLICA
¿HA REVISADO/ACTUALIZADO LA EIPD ANTE CAMBIOS EN LAS ACTIVIDADES DE TRATAMIENTO?
NO APLICA

ASPECTOS GENERALES DE LOS TRATAMIENTOS

¿ASEGURA QUE LOS DATOS PERSONALES TRATADOS SE MANTIENEN EXACTOS Y ACTUALIZADOS?

Es correcto disponer de procedimientos que aseguren que los datos tratados son correctos y que están actualizados. Mecanismos de sobre los derechos de rectificación de datos entre otros así como medidas que garantizan que los datos inexactos se rectifican o se suprimen sin dilación permiten cumplir con los principios elementales del tratamiento.

¿SE TRATAN ÚNICAMENTE LOS DATOS PERSONALES QUE SON NECESARIOS PARA EL FIN PERSEGUIDO POR LA ORGANIZACIÓN?

Es correcto reducir al mínimo los datos personales tratados con el fin de asegurar que el tratamiento realizado es el adecuado y limitado a lo necesario.

¿HA DISPUESTO LA INFORMACIÓN OBLIGATORIA A LOS INTERESADOS DE FORMA QUE ÉSTA SEA LEGIBLE E INTELIGIBLE PARA LOS INTERESADOS?

Es correcto que la información obligatoria a los interesados contenga los datos del responsable, finalidades del tratamiento, cómo ejercer los derechos, etc… y que ésta sea legible y entendible. La información se facilita desde el momento de recabar los datos de los interesados, bien a través de medios escritos (formularios, etc..) bien a través de medios electrónicos (a través de una web por ejemplo) o a través de una grabación de voz en la que verbalmente se informa a los interesados.

¿SE HA DETERMINADO EL PLAZO DE CONSERVACIÓN DE LOS DATOS PERSONALES TRATADOS EN FUNCIÓN A CRITERIOS RAZONADOS, OBJETIVOS Y LEGALES?

Es correcto recoger en el registro de las actividades de tratamiento los plazos de conservación de datos personales previstos. Transcurrido el plazo, los datos personales se bloquean (únicamente con la finalidad de atender posibles reclamaciones) o se suprimen.

SI ENCARGA EL TRATAMIENTO DE DATOS PERSONALES A ALGUNA PERSONA FÍSICA O JURÍDICA ¿MANTIENE CON TODOS SUS ENCARGADOS DEL TRATAMIENTO UN CONTRATO DE CONFIDENCIALIDAD?

Se han revisado todos los encargados del tratamiento y constatado que están controlados conforme a las indicaciones del RGPD.

DERECHOS

¿HA RECIBIDO ALGUNA PETICIÓN DE ACCESO, SUPRESIÓN, RECTIFICACIÓN O EL EJERCICIO DE CUALQUIER OTRO DERECHO Y HA RESPONDIDO DENTRO DEL PLAZO DE 30 DÍAS?

El RGPD establece que los interesados tienen el derecho a obtener sin dilación indebida (y en todo caso en el plazo máximo de 1 mes) respuesta del responsable ante cualquier petición de derechos, por ejemplo ante una petición del Derecho de ACCESO el responsable está obligado a informar al interesado de los datos personales tratados, de sus fines, destinatarios, plazos de conservación previstos, etc… esta información se recoge en la plataforma a través del menú ACTIVIDADES DE TRATAMIENTO.

LICITUDES

¿CONSERVA LOS REGISTROS DE LOS CONSENTIMIENTOS QUE LOS INTERESADOS (MAYORES DE 14 AÑOS) LE HAYAN FACILITADO?

Para poder demostrar que los interesados consintieron al tratamiento de sus datos personales es imprescindible conservar dichos registros

SI TRATA DATOS DE MENORES DE 14 AÑOS Y DICHO TRATAMIENTO SE BASA EN EL CONSENTIMIENTO ¿FIGURA EN EL REGISTRO DEL CONSENTIMIENTO LA FIRMA O ACEPTACIÓN DEL TITULAR/ES DE LA PATRIA POTESTAD O TUTELA DEL MENOR?

Perfecto. Es obligación del responsable actuar en caso que algún interesado revoque su consentimiento.

CUANDO TRATA DATOS PERSONALES QUE SON NECESARIOS PARA LA PRESTACIÓN DE UN SERVICIO/SUMINISTRO DE UN PRODUCTO, ¿CONSERVA EL CONTRATO/PRECONTRATO O LA EVIDENCIA QUE LE PERMITE DEMOSTRAR QUE DICHOS DATOS GUARDAN RELACIÓN CON EL ALCANCE Y LA FINALIDAD DEL SERVICIO/SUMINISTRO?

Es correcto y necesario que se pueda justificar y evidenciar que el tratamiento de los datos personales es necesario para la correcta prestación del servicio, incluso para la aplicación de medidas precontractuales (petición de presupuestos por ejemplo).

SI TRATA DATOS PERSONALES POR OBLIGACIÓN LEGAL ¿TIENE DEFINIDA LA NORMATIVA QUE LE OBLIGA A TRATAR DICHOS DATOS?

Perfecto, el responsable siempre tiene que poder demostrar la licitud en la que basa el tratamiento de los datos personales, incluso cuando es obligación legal.

DATOS DE CATEGORÍAS ESPECIALES

SI TRATA DATOS DE CATEGORÍAS ESPECIALES (DATOS DE SALUD, DATOS BIOMÉTRICOS, GENÉTICOS, DATOS DE ORIGEN ÉTNICO O RACIAL, OPINIONES POLÍTICAS, CONVICCIONES RELIGIOSAS, AFILIACIÓN SINDICAL, ORIENTACIÓN O VIDA SEXUAL) ¿SE HA ASEGURADO QUE CONCURREN LAS CIRCUNSTANCIAS QUE LE PERMITEN TRATAR DICHOS DATOS?

Perfecto. Es preciso justificar que los tratamientos de datos personales de categorías especiales se realizan en virtud de circunstancias excepcionales recogidas en el art. 9 del RGPD.

RESPONSABILIDADES DEL RESPONSABLE DE LOS DATOS

¿HA HABIDO CAMBIOS EN SUS ACTIVIDADES DE TRATAMIENTO?

Si no ha habido cambios en sus actividades de tratamiento, el registro está actualizado

¿HA REVISADO SUS ACTIVIDADES DE TRATAMIENTO DE DATOS PERSONALES ASÍ COMO LAS MEDIDAS DE PROTECCIÓN, DE SEGURIDAD, ETC.. DE FORMA PERIÓDICA DENTRO DEL ÚLTIMO AÑO?

Es correcto mantener registros de sus actividades, de los cambios, de las medidas de seguridad y de protección, de las personas que tienen acceso a los datos, de las entidades destinatarias de datos, etc.. dado que es obligación del responsable poder demostrar que es capaz de cumplir con lo establecido en la normativa vigente y que lo hace de forma continuada (responsabilidad proactiva)

¿HA REVISADO EL RESULTADO DEL ANÁLISIS DE LOS RIESGOS QUE LOS TRATAMIENTOS PUEDEN OCASIONAR SOBRE LAS LIBERTADES Y DERECHOS DE LOS INTERESADOS?

Cualquier amenaza detectada ha sido subsanada y cualquier riesgo se mantiene en límites tolerables

¿HA SUFRIDO ALGÚN INCIDENTE RELACIONADO CON EL ROBO DE DATOS O CON LA VULNERACIÓN DE LA DEBIDA CONFIDENCIALIDAD?

Perfecto. El hecho de que no se presenten incidentes demuestra que las medidas técnicas y organizativas están funcionando. No obstante no debe bajar la guardia.

¿HA SUFRIDO ALGÚN INCIDENTE RELACIONADO CON LA PÉRDIDA DE DATOS DE CARÁCTER PERSONAL?

Perfecto. El hecho de que no se presenten incidentes demuestra que las medidas técnicas y organizativas están funcionando. No obstante no debe bajar la guardia.

¿HA DOCUMENTADO CUALQUIER INCIDENTE O BRECHA DE SEGURIDAD QUE HAYA DETECTADO?

Recuerde que el art. 33 5) del RGPD le obliga a documentar cualquier violación de seguridad incluidos los hechosrelacionados con ella, sus efectos y las medidas correctivas adoptadas. En dicha documentación se indicará de forma razonada la necesidad de comunicar o no dicha violación.

¿MODIFICA LAS CLAVES DE ACCESO A LOS SOPORTES ELECTRÓNICOS QUE CONTIENEN DATOS CON REGULARIDAD?

Perfecto. El art. 33 del RGPD indica que es obligación del responsable documentar dicho incidente (independientemente de si ha sido necesario comunicarlo a la autoridad de control y a los interesados).

¿HA CONTRATADO ALGÚN NUEVO EMPLEADO/A QUE DENTRO DE SUS FUNCIONES TENGA ACCESO A DATOS PERSONALES DE LA ORGANIZACIÓN?

Recuerde que debe registrar a cualquier nuevo empleado/a, indicando los datos a los que tiene acceso, así como las operaciones que le están permitidas realizar, por ejemplo: acceso, edición, borrado, comunicación, etc…

¿SU ORGANIZACIÓN TIENE DEFINIDA Y DOCUMENTADA SU POLÍTICA DE PROTECCIÓN DE DATOS?

Perfecto, es importante demostrar mediante el compromiso escrito de la organización cuál es su política de protección de datos así como los principios inspiradores de la misma.

NOMBRE, FECHA, FIRMA Y DNI de los implicados.

43812892P MARIA ANGELES GONZALEZ (R: G38380556)

Firmado digitalmente por 43812892P MARIA ANGELES GONZALEZ (R: G38380556)
Fecha: 2024.04.02 11:31:45 +01'00'