POLÍTICA DE CUMPLIMIENTO EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES Y PRIVACIDAD

CRISTINA PEÑO HERNAN

POLÍTICA DE CUMPLIMIENTO EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES Y PRIVACIDAD DE CRISTINA PEÑO HERNAN

INTRODUCCIÓN

Las disposiciones establecidas en esta Política tienen su fundamento en las definiciones, principios básicos y requisitos legales exigidos por 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 estos datos (en adelante, el 'RGPD'), y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) recogiendo la política de protección de datos de la organización así como las medidas de índole técnica y organizativa necesarias para garantizar la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal.

Definiciones

A los efectos de un entendimiento de los términos de protección de datos personales y privacidad, los siguientes términos tendrán el significado que se da a continuación:

•Datos personales: toda información sobre una persona física identificada o identificable (el 'Interesado'). Se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

•Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

•Responsable del tratamiento: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

•Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

•Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

•Destinatario: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero.

•Tercero: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

•Consentimiento del interesado: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

•Violación de la seguridad de los datos personales: toda violación de la seguridad que ocasione 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.

•Categorías especiales de datos: Son aquellos 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 vida sexual o las orientaciones sexuales de una persona física y datos de naturaleza penal.

PRINCIPIOS DEL TRATAMIENTO DE LOS DATOS PERSONALES

CRISTINA PEÑO HERNAN con CIF/NIF 04187621B , y dirección en C/ MARIA DE PIMENTEL, 4 LOCAL 3, TALAVERA DE LA REINA (45600), es responsable de los tratamientos de datos de carácter personal que realiza.

CRISTINA PEÑO HERNAN aplica el principio de responsabilidad activa en el tratamiento de sus datos de carácter personal, manteniendo una constante puesta al día y una promoción de la mejora continua del sistema de protección de datos. Mantiene toda la documentación y los registros a disposición de la autoridad de control y de los encargados del tratamiento aportando las evidencias que demuestren su firme compromiso con la protección de los datos de carácter personal.

Los principios por los que se rige CRISTINA PEÑO HERNAN y que regulan cómo se deben tratar los datos personales responsabilidad de la misma son:

•Licitud, lealtad y transparencia: los datos personales se tratan de forma lícita, leal y transparente, de manera que el interesado conozca el tratamiento que, en su caso, se va a hacer de sus datos.

•Limitación de la finalidad: los datos personales solo se recogen con fines determinados, explícitos y legítimos y no se usan posteriormente de manera incompatible con dichos fines.

•Minimización de datos: los datos personales son adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

Solo son objeto de tratamiento aquellos datos personales que resulten estrictamente necesarios para la finalidad para la que se recojan o traten y adecuados a tal finalidad.

•Exactitud: los datos personales son exactos y, si fuera necesario, actualizados. Se toman 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.

•Limitación del plazo de conservación: los datos personales se mantienen de forma que se permita la identificación de los interesados durante un período no superior al necesario para los fines para los que se tratan los datos personales

•Integridad y confidencialidad: los datos personales son tratados de tal manera que se garantice una seguridad adecuada de estos, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, utilizando las medidas técnicas u organizativas adecuadas.

Los datos personales recabados y tratados por la empresa son conservados con la máxima confidencialidad y secreto, no pudiendo ser utilizados para otros fines distintos de los que justificaron y permitieron su recogida y sin que puedan ser comunicados o cedidos a terceros fuera de los casos permitidos por la legislación aplicable.

•Protección de datos personales desde el diseño y por defecto: la empresa aplica las medidas técnicas y organizativas apropiadas, en función del riesgo de la acción, desde el diseño de la misma y por defecto.

•Evaluación de riesgo e impacto en materia de protección de datos personales: cuando una actividad conlleve el tratamiento de datos personales que pueda suponer un riesgo elevado para los derechos y libertades del interesado, en la medida y forma en que la normativa lo exija, CRISTINA PEÑO HERNAN llevará a cabo una evaluación de riesgos e impacto en la protección de los datos personales y privacidad antes del inicio del tratamiento.

•Gestión de incidentes de seguridad de los datos personales: en caso de que se produzca un incidente que afecte a la seguridad de los datos personales, se seguirán los procedimientos corporativos de seguridad de la información de la empresa, así como aquellos específicos de protección de datos personales y privacidad que incluyan la gestión de las notificaciones a autoridades y/o interesados.

•Derechos de los interesados: la empresa garantiza que los interesados puedan ejercitar los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición que sean de aplicación en cada jurisdicción, estableciendo a tal efecto la normativa interna que resulte necesaria para cumplir, al menos, los requisitos exigidos por la normativa en cada caso.

•Contratación de encargados del tratamiento. Con carácter previo a la contratación de cualquier encargado del tratamiento que acceda a datos personales que sean responsabilidad de la empresa, así como durante la vigencia de la relación contractual, ésta adopta las medidas necesarias para garantizar y, cuando sea legalmente exigible, demostrar, que el tratamiento de datos por parte del encargado se lleva a cabo conforme a la normativa aplicable.

En los casos en que los encargados del tratamiento puedan tener acceso a los datos personales de los cuales es responsable CRISTINA PEÑO HERNAN:

- •dicho acceso se limita únicamente a los datos personales estrictamente necesarios
- •se elige diligentemente al encargado del tratamiento. En particular, se tiene en cuenta las medidas de seguridad técnicas y organizativas proporcionadas
- •se regula debidamente la relación entre la empresa y el encargado del tratamiento , a través de las cláusulas contractuales adecuadas para el tratamiento de datos personales.

•Transferencias internacionales de datos: la empresa cumple con los requisitos establecidos para las transferencias internacionales de datos personales que sean, en su caso, aplicables en los mercados en los que opera.

•Registro de actividades de tratamiento: la empresa se responsabiliza de llevar un registro en el que se describa, de acuerdo con la normativa aplicable, los tratamientos de datos personales que se lleven a cabo en el marco de las actividades de la empresa.

•Delegado de protección de datos: En los casos previstos en la ley, se designará a un delegado de protección de datos con el fin de garantizar el cumplimiento de la normativa de protección de datos en la empresa, y pondrá a disposición de los interesados y las autoridades sus datos de contacto.

ALCANCE y ÁMBITO DE APLICACIÓN

CRISTINA PEÑO HERNAN está establecida en España y realiza, para el ejercicio de sus actividades, el tratamiento de datos de carácter personal de ciudadanos residentes en la Unión Europea. Es responsable del tratamiento de los datos personales. En representación legal actúa CRISTINA PEÑO HERNAN CRISTINA PEÑO HERNAN con DNI 04187621B.

Las actividades desarrolladas se pueden resumir en las siguientes: OTRAS ACTIVIDADES.

Para el desarrollo de sus actividades la organización cuenta con los siguientes centros:

•CENTRO DE TRABAJO con dirección en CALLE MARIA DE PIMENTEL, 4 LOCAL 3, TALAVERA DE LA REINA (45600), TOLEDO y actividad de PELUQUERIA

Los corresponsables del tratamiento, cuando existan, determinan de modo transparente y de mutuo acuerdo las responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el Reglamento (UE) 2016/679 y por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). El contenido del acuerdo se encuentra en el ACUERDO DE 'CORRESPONSABILIDAD' DEL TRATAMIENTO DE LOS DATOS.

Las actividades de tratamiento realizadas por la organización se recogen en el Registro de Actividades de Tratamiento de la presente política de protección de datos. En el citado registro queda recogido el ámbito territorial de cada una de las actividades. El contenido del Registro de actividades de tratamiento se encuentra recogido en los ANEXOS EXTERNOS: Registro de Actividades de Tratamiento.

Para el cumplimiento de las obligaciones como encargado del tratamiento, cuando se traten datos por cuenta de terceros y en virtud del art. 28 del Reglamento (UE) 2016/679 y del art.33 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) se estará a lo dispuesto por las cláusulas contractuales que se añaden al contrato de prestación de servicios.

En cuanto al sistema de tratamiento y/o almacenamiento de datos, la organización realiza:

•Tratamiento automatizado de datos personales (Digital / Informática). Datos que son tratados de manera automatizada o mecanizada, es decir, en formato electrónico o digital mediante sistemas informáticos.

•Tratamiento no automatizado de datos personales (Manual / Papel). Datos que son tratados de manera manual, sin ningún sistema automatizado, es decir, los datos que se tratan exclusivamente en formato papel

BASES DE LEGITIMACIÓN PARA EL TRATAMIENTO DE DATOS

Identificación de la base legal sobre la que se desarrolla el tratamiento

El Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) conserva el principio establecido en la Directiva 95/46 en virtud del cual todo tratamiento de datos personales debe apoyarse en una base jurídica que lo legitime.

Establece, como regla general, que los datos personales deben ser tratados con el consentimiento del interesado, pero admite cualquier otra base legítima conforme a Derecho: relación contractual, intereses vitales del interesado o de terceros, obligación legal para el responsable, interés público, etc.

Teniendo en cuenta el principio general de 'responsabilidad proactiva', es un requisito apoyar el tratamiento de los datos en una base que lo legitime. Se tiene documentado el interés legítimo en el que se fundamenta cada actividad de tratamiento y así lo establece el Registro de Actividades de Tratamiento.

Asimismo, teniendo en cuenta el principio de transparencia y de información, la organización proporciona la base legal del tratamiento a todos los interesados como se indica en el apartado correspondiente de la presente política.

Licitud basada en el contrato de prestación de servicios

El tratamiento de los datos personales necesarios para la correcta prestación de los servicios acordados contractualmente fija la base jurídica necesaria para efectuar dicho tratamiento. Sólo se recaba el consentimiento de los interesados si las finalidades son distintas a las acordadas contractualmente.

Licitud basada en el consentimiento

El consentimiento del interesado podrá ser escrito, por medios electrónicos o por voz (según prioridad de la organización y modo habitual de comunicación), conservando los registros a disposición de la autoridad de control. Se dispone de los contenidos necesarios para recabar el consentimiento de los interesados.

El consentimiento en el caso de menores de 14 años

El artículo 8 del Reglamento (UE) 2016/679 y el art.7 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) establece nuevas pautas sobre el consentimiento de los menores de edad en el tratamiento de sus datos personales con el fin de aumentar la privacidad de la información.

El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años. 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.

Licitud basada en una obligación legal

El tratamiento de los datos personales necesarios para el cumplimiento de las obligaciones legales fija su base jurídica en las normas establecidas.

La organización trata los datos de carácter personal de sus empleados como consecuencia inevitable y necesaria de la relación laboral, y actuaría de forma engañosa si intentara legitimar este tratamiento a través del consentimiento. Por lo tanto la organización no basa el tratamiento de los datos de carácter personal de sus empleados en el consentimiento, sino que emplea el contrato laboral como base jurídica.

Para el tratamiento de datos con una finalidad distinta al cumplimiento de una obligación legal (como el contrato laboral o la comunicación con la administración tributaria o con la seguridad social) se estará a lo dispuesto en el apartado anterior (consentimiento).

Licitud para el tratamiento de los datos que no han sido recabados directamente de los interesados

En el caso que se traten datos de carácter personal que no han sido recabados directamente de los interesados, se garantiza que los derechos y libertades de los interesados prevalecen sobre los intereses legítimos perseguidos por la organización, por ejemplo para el envío de publicidad. Asimismo se garantiza que la fuente de obtención de los datos es una fuente de acceso público y que los interesados no están inscritos en la Lista Robinson.

TRATAMIENTO DE CATEGORÍAS ESPECIALES DE DATOS

El Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) establecen en el art. 9 las categorías especiales de datos refiriéndose a los datos sensibles que precisan una especial protección, ya sea por su naturaleza o por la relación que puedan tener con los derechos y las libertades fundamentales de las personas y les aplica disposiciones específicas cuando su tratamiento pueda entrañar altos riesgos en la protección de datos.

El Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) establece por defecto la prohibición del tratamiento de estas categorías de datos con excepciones específicas para cuando el interesado haya dado su consentimiento explícito o en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales.

También determina que se podrán tratar datos sensibles cuando exista un interés público fundamentado en la legislación vigente de cada país de la UE, por ejemplo en el ámbito laboral, protección social, pensiones, sanidad u otras amenazas graves para la salud.

Como excepción a la prohibición por defecto expuesta en el apartado anterior, la organización sólo trata categorías especiales de datos cuando:

- El interesado haya dado su consentimiento explícito para fines específicos (excepto si está prohibido por la legislación vigente).
- Es necesario para proteger los intereses vitales del interesado, cuando está incapacitado para dar su consentimiento.
- El tratamiento lo realiza legítimamente una organización sin ánimo de lucro con finalidad política, filosófica, religiosa o sindical con relación a sus fines.
- El interesado ha hecho manifiestamente públicos sus datos.

O cuando el tratamiento está fundamentado en la legislación vigente:

- Bajo la responsabilidad de personas sujetas a la obligación del secreto profesional.
- Para fines de asistencia sanitaria o social, medicina preventiva o laboral o diagnóstico médico incluida la evaluación de la capacidad laboral del trabajador.
- Para procedimientos judiciales.
- Es necesario para cumplir la legislación laboral, o la de seguridad o protección social o la de convenios colectivos.
- Es necesario por razones de interés público en el ámbito de la salud pública o la asistencia sanitaria.
- Es necesario para fines de archivo en interés público en investigaciones científicas, históricas o estadísticas.

La organización realizará tratamiento de datos basado en una elaboración de perfiles que contemple la confección de decisiones individuales basadas en un tratamiento automatizado destinado a evaluar aspectos personales o analizar o predecir datos de salud, cuando el interesado ha dado su consentimiento para fines específicos permitidos por la legislación vigente o el tratamiento se realice para fines de interés público o bajo la supervisión de poderes públicos, fundamentados en la legislación vigente.

Cuando la organización pretenda realizar tratamientos que puedan afectar a los derechos fundamentales de las personas afectadas se determinará a través del análisis de riesgos la existencia o no de riesgos inherentes al tratamiento que se desea realizar. En caso de no poder reducir los riesgos a límites tolerables será necesaria la realización de una evaluación de impacto tal como se determina en el apartado correspondiente.

Determinados tratamientos requieren la designación de un delegado de protección de datos. La organización mantendrá un delegado de protección de datos en su caso, informando sobre el mismo, identificación y contacto, a todos los interesados.

TRANSPARENCIA E INFORMACIÓN A LOS INTERESADOS.

El Reglamento (UE) 2016/679 recoge que la información a los interesados, tanto respecto a las condiciones de los tratamientos que les afecten, como en las respuestas a los ejercicios de los derechos, deberá proporcionarse de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.

Según la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, la información básica que se facilita a los interesados comprende:

a) La identidad del responsable del tratamiento y de su representante, en su caso.

b) La finalidad del tratamiento.

c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

Si existe elaboración de perfiles o se elaboran decisiones automatizadas se facilita igualmente esta información.

Cuando los datos personales no han sido obtenidos del afectado, se facilita a los interesados la información básica anterior junto con un enlace que les permite acceder a toda la información de las actividades de tratamiento de la organización, incluyendo las categorías de datos objeto de tratamiento, así como las fuentes de las que proceden los datos.

Los datos de carácter personal podrán ser cedidos, previa autorización del interesado previo análisis de la cesión (las cesiones pueden estar basadas en requisitos legales o contractuales o en un requisito necesario para suscribir un contrato)

La existencia de decisiones automatizadas y elaboración de perfiles o la decisión de adoptarlas estarán sujetas al correspondiente análisis de riesgos y a una evaluación de impacto en caso de que los riesgos no hayan podido ser reducidos a límites aceptables.

Antes de realizar tratamientos de datos personales para una finalidad distinta de la que fueron recogidos, se procede a realizar un análisis de los riesgos. Si el riesgo es aceptable se tratarán los datos con la nueva finalidad, siempre bajo una base legal y se incluirá en la información que se facilita a los interesados.

La información que se facilita a los interesados se recoge en los documentos INFORMACIÓN Y CONSENTIMIENTO.

Si los datos personales se utilizan para establecer comunicación con el interesado, se le comunica la información a que tiene derecho en el momento de la primera comunicación y si está previsto comunicar los datos a otro destinatario, se le comunica la información a más tardar en el momento en que los datos personales son comunicados por primera vez.

No es necesario informar a los interesados cuando ya disponen de la información, cuando la comunicación de dicha información resulta imposible o supone un esfuerzo desproporcionado, cuando la información imposibilita u obstaculiza el logro de los objetivos del tratamiento, cuando la obtención o la comunicación está expresamente establecida por normas de derecho aplicables, o cuando los datos personales tienen carácter confidencial sobre la base de una obligación de secreto profesional.

Se han evitado fórmulas especialmente farragosas y se emplea un vocabulario que facilita la comprensión por parte de cualquier interesado.

Las cláusulas informativas explican el contenido al que inmediatamente se refieren de forma clara y accesible para los interesados, con independencia de sus conocimientos en la materia.

La información a los interesados se facilita por escrito, incluidos los medios electrónicos, incluso se facilita verbalmente, previa acreditación de la identidad del interesado.

DERECHOS DE LOS INTERESADOS

Procedimiento para el ejercicio y obligaciones para el responsable.

Con carácter general, el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) exigen a los responsables que faciliten a los interesados el ejercicio de sus derechos. Este mandato supone que los procedimientos y formas para ello deben ser visibles, accesibles y sencillos. El Reglamento (UE) 2016/679 no establece un modo concreto para el ejercicio de derechos, pero sí requiere a los responsables que posibiliten la presentación de solicitudes por medios electrónicos, especialmente cuando el tratamiento se realiza por esos medios.

CRISTINA PEÑO HERNAN garantiza que el ejercicio de estos derechos es gratuito para el interesado, siempre que las solicitudes no sean manifiestamente infundadas o excesivas, especialmente por repetitivas, correspondiendo al responsable de la organización demostrar el carácter infundado o excesivo de las solicitudes, pudiendo en estos casos el responsable cobrar un canon que compense los costes administrativos de atender a la petición o negarse a actuar.

Se informará al interesado sobre las actuaciones derivadas de su petición dentro del plazo de un mes, que podrá extenderse dos meses más cuando se trate de solicitudes especialmente complejas. Esa ampliación del plazo se notifica dentro del primer mes. Si el responsable decide no atender la solicitud, debe informar de ello, motivando su negativa, dentro del plazo de un mes desde su presentación.

Se toman todas las medidas razonables para verificar la identidad de quienes ejerzan los derechos reconocidos en el Reglamento (UE) 2016/679, a través del requerimiento del documento nacional de identidad o documento equivalente que acredite la identidad del interesado. Asimismo mantiene un REGISTRO DE EJERCICIOS DE LOS DERECHOS donde se recogen y se mantiene un control de todos los ejercicios de los derechos solicitados por los interesados.

Para el ejercicio de los derechos a través de solicitudes la organización facilita a los interesados que deseen ejercitar sus derechos los modelos correspondientes y concretados en los puntos siguientes:

Derecho de acceso

El derecho de acceso viene regulado en al art. 15 del Reglamento (UE) 2016/679 y en el art.13 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). En los considerandos 63 y 64, se recoge como un derecho del interesado a obtener, del responsable del tratamiento, confirmación de si se están tratando o no datos personales que le conciernen.

Para atender los derechos de acceso de cualquier interesado CRISTINA PEÑO HERNAN le facilita un modelo de solicitud adecuado, modelo recogido en el Anexo Externo SOLICITUD DE ACCESO A DATOS.

El interesado que solicite este derecho y que se identifique convenientemente obtendrá de la organización la debida respuesta mediante un documento informativo (modelo recogido en el Anexo Externo RESPUESTA AL EJERCICIO DEL DERECHO de ACCESO).

Si la empresa trata una gran cantidad de datos relativos al interesado y ejercita el derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, la organización podrá solicitarle, antes de facilitarle la información, que el interesado especifique los datos o actividades del tratamiento a los que se refiere la solicitud.

Si la respuesta al derecho de acceso se remitiera por correo, al solicitante del derecho se le remitirá el documento de respuesta mediante carta con acuse de recibo, burofax o cualquier otro medio que acredite el envío y la recepción.

Si la respuesta es estimatoria, la información incluirá los datos personales del interesado que son objeto de tratamiento, los fines del tratamiento, las categorías de datos personales tratados así como los destinatarios o categorías de destinatarios a los que se comunican o serán comunicados los datos, además de cualquier información disponible sobre el origen de los datos, el plazo previsto de conservación de los mismos o, de no ser posible, los criterios utilizados para determinar este plazo, así como el derecho a presentar una reclamación ante una autoridad de control. Asimismo, se indicará al interesado 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.

Derecho de rectificación

El derecho de rectificación viene recogido en el artículo 16 del Reglamento (UE) 2016/679 y en el art. 14 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, por el que 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.

El interesado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya que realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos personales objetos del tratamiento.

En el caso que los datos del interesado sean incompletos o inexactos, la organización garantiza la actualización de los mismos sin dilación indebida.

El interesado puede solicitar el derecho de rectificación de sus datos mediante el modelo de solicitud que se acompaña en el Anexo Externo SOLICITUD DE RECTIFICACIÓN DE DATOS.

Una vez rectificados los datos la organización informará al interesado sobre la rectificación llevada a cabo (Anexo Externo RESPUESTA AL EJERCICIO DE LOS DERECHOS).

Derecho a la limitación del tratamiento

El derecho a la limitación del tratamiento viene regulado en el art. 18 del Reglamento (UE) 2016/679 y el art. 16 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y establecen el derecho a que los datos sean limitados a petición del interesado

El interesado puede solicitar el derecho a la limitación de sus datos mediante el modelo de solicitud que se acompaña en el Anexo Externo SOLICITUD DE LIMITACIÓN DEL TRATAMIENTO DE DATOS.

La organización en respuesta puede proceder a la limitación del tratamiento de los datos del interesado si concurre alguna de las circunstancias siguientes:

- cuando el interesado impugna su exactitud, se limita el tratamiento durante el plazo necesario para verificar la exactitud de los datos.
- cuando el tratamiento de los datos es ilícito pero el interesado se opone a la supresión de sus datos
- cuando los datos ya no son necesarios para las finalidades de la organización pero si son necesarios para el interesado (reclamaciones, etc...)
- cuando el interesado se opone al tratamiento mientras se verifica si los intereses legítimos de la organización prevalecen sobre los del interesado.

Para la limitación de los datos, la organización seguirá alguno de los siguientes métodos:

- trasladará temporalmente los datos seleccionados a otro sistema de tratamiento.
- impedirá el acceso de usuarios a los datos personales seleccionados.
- retirará temporalmente los datos publicados de un sitio internet.
- indicará claramente en el sistema (fichero automatizado) que los datos que se pretenden tratar encuentra limitado su tratamiento.

En los casos en los que la organización proceda a la limitación del tratamiento, los datos del afectado sólo podrán ser objeto de tratamiento:

- para su conservación.
- con el consentimiento del interesado.
- para la formulación, el ejercicio o defensa de reclamaciones.
- para la protección de los derechos de la persona física o jurídica.
- por razones de interés público de la UE o Estados miembros.

Una vez limitados los datos se informará al interesado justificando su decisión (Anexo Externo RESPUESTA AL EJERCICIO DE LOS DERECHOS) así como la limitación llevada a cabo.

Igualmente se informará cuando se levante la limitación al tratamiento.

Derecho de supresión / derecho al olvido

El art. 17 del Reglamento (UE) 2016/679 y el artículo 15 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales indican que el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan.

El interesado puede solicitar el derecho de supresión/derecho de olvido de sus datos mediante el modelo de solicitud que se acompaña en el AnexoExterno SOLICITUD DE SUPRESIÓN/DERECHO AL OLVIDO.

La organización procede a la supresión del tratamiento de los datos del interesado cuando concurra alguna de las circunstancias siguientes:

- los datos personales ya no son necesarios en relación con los fines para los que fueron recogidos.
- el interesado retira el consentimiento en que se basa el tratamiento y no se base en otro fundamento jurídico
- el interesado se opone al tratamiento (derecho de oposición).
- los datos personales se han tratado de forma ilícita.
- los datos personales se suprimen para el cumplimiento de una obligación legal que se aplique al responsable del tratamiento.
- los datos personales se han obtenido en relación con la oferta directa a niños de servicios de sociedad de la información.

La organización no procede a aceptar las peticiones de supresión del interesado cuando el tratamiento sea necesario en los siguientes supuestos:

- para ejercer el derecho a la libertad de expresión e información.
- para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la UE o de los Estados miembros que se aplique al responsable del tratamiento o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.
- por razones de interés público en el ámbito de la salud pública.
- con fines de archivo en interés público, investigación científica o histórica o fines estadísticos.
- para la formulación, el ejercicio o la defensa de reclamaciones.

La organización informa sin dilación del carácter estimatorio o desestimatorio del derecho solicitado por el interesado, así como la supresión llevada a cabo. Modelo Anexo Externo RESPUESTA AL EJERCICIO DE LOS DERECHOS.

Derecho de oposición

El derecho de oposición viene regulado en el art. 21 del Reglamento (UE) 2016/679 y en el art.18 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Podemos decir que es el derecho del interesado a oponerse, en cualquier momento, por motivos legítimos y fundados relacionados con su situación particular, a que los datos personales que le conciernan sean objeto de un tratamiento.

Para atender el derecho de oposición de cualquier interesado CRISTINA PEÑO HERNAN facilita un modelo de solicitud adecuado, modelo recogido en el Anexo Externo SOLICITUD DE OPOSICIÓN.

Cuando el interesado ejercite el derecho de oposición, CRISTINA PEÑO HERNAN dejará de tratar dichos datos personales, realizando un análisis con el fin de considerar si prevalece o no el derecho del interesado sobre los intereses legítimos de la organización. Para tal fin se analizará pormenorizadamente la situación, los motivos y la documentación aportada por el interesado.

Si existen motivos legítimos que justifiquen el tratamiento (por ejemplo para la formulación, el ejercicio o la defensa de reclamaciones) se seguirán tratando los datos, aunque se atienda la solicitud del interesado, pudiendo desestimarse.

La organización informa sin dilación del carácter estimatorio o desestimatorio del derecho solicitado por el interesado. Modelo Anexo Externo RESPUESTA AL EJERCICIO DE LOS DERECHOS.

Derecho de portabilidad

El art. 20 del Reglamento (UE) 2016/679 y el artículo 17 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, recogen que los usuarios tienen un nuevo derecho, el derecho a la portabilidad. Este derecho complementa al derecho de acceso, ya que permite a los interesados obtener los datos que se han proporcionado en un formato estructurado, de uso común y de lectura mecánica.

El derecho a la portabilidad también implica que los datos personales del interesado podrán transmitirse directamente de una entidad o organización a otra, sin necesidad de ser entregados al propio interesado, siempre que ello sea técnicamente posible.

El Reglamento abre así la posibilidad no sólo de obtener los datos y reutilizarlos, sino también de transmitirlos a otro proveedor de servicios. Por tanto, el interesado tendrá la opción de solicitar sus datos o la transmisión de los mismos directamente de una entidad a otra.

La organización garantiza el ejercicio del derecho a la portabilidad del interesado mediante un modelo de solicitud adecuado, modelo recogido en el Anexo Externo SOLICITUD DE PORTABILIDAD.

Una vez solicitado el derecho, se remiten al interesado todos aquellos datos personales que le incumban y que haya facilitado, siempre y cuando el tratamiento esté basado en el consentimiento o sea necesario para la ejecución de un contrato y el mismo se efectúe por medios automatizados.

Asimismo facilita que los interesados reciban los datos en un formato estructurado de uso común y de lectura mecánica e interoperable, siempre que la tecnología lo permita.

La organización no aplica el derecho a la portabilidad a los datos que el interesado haya facilitado sobre terceras personas ni sobre los datos que le hayan sido proporcionados a través de terceros.

Derecho a la desconexión digital

CRISTINA PEÑO HERNAN reconoce a todas las personas trabajadoras que forman parte de esta organización, independientemente de su contrato, puesto, modalidad: presencial, a distancia, teletrabajo, los derechos digitales recogidos en el artículo 88 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y en la Ley 10/2021, de 9 de julio, de trabajo a distancia.

CRISTINA PEÑO HERNAN fomenta una cultura de desconexión digital encaminada a mitigar los efectos negativos de la hiperconectividad (estar siempre conectados puede derivar en problemas de salud: estrés, fatiga, dependencia.), a conseguir una mejor conciliación entre la vida personal y profesional, a crear hábitos saludables y a facilitar el ejercicio de los derechos de nuestro personal.

CRISTINA PEÑO HERNAN ha elaborado un PROTOCOLO DE DESCONEXIÓN DIGITAL, consensuado con los trabajadores, y se articula a través de las siguientes pautas de actuación:

•Con el fin de garantizar el descanso de todo el personal no se realizarán llamadas ni se enviarán mails o mensajes instantáneos fuera de la jornada laboral ordinaria salvo casos de fuerza mayor o circunstancias excepcionales debidamente justificadas.

•Si alguna persona quiere enviar un correo fuera del horario de trabajo es preferible que configure el envío de correo diferido.

•Las personas trabajadoras de esta organización tienen derecho a no responder a ninguna comunicación una vez finalizada su jornada laboral ordinaria, independientemente del medio utilizado: correo, mensaje, llamada telefónica, etc...

•Para garantizar que las personas que disponen de dispositivos electrónicos para trabajar (ordenadores, tablets, teléfonos móviles, etc..) puedan gestionar mejor las cargas de trabajo se respetarán los descansos entre jornadas de trabajo, descanso semanal, festivos, vacaciones y cualquier ausencia justificada

•Durante los descansos superiores a un día, configurar los correos con mensajes automáticos de respuesta informando al remitente sobre la persona trabajadora a la que se puede dirigir durante su ausencia.

•Las reuniones, tanto presenciales como telemáticas, serán convocadas dentro de la jornada laboral ordinaria. Si por razones justificadas e ineludibles debieran desarrollarse fuera de la jornada laboral ordinaria, serán consideradas excepcionales y, siempre que sea posible, serán convocadas con al menos 24 horas de antelación, indicando hora de inicio y hora máxima de finalización. En este supuesto se procurará que las reuniones sean telemáticas con el fin de evitar desplazamientos y optimizar el tiempo.

RELACIONES RESPONSABLE - ENCARGADO

Elección del encargado del tratamiento

El art. 28 del Reglamento (UE) 2016/679 manifiesta que 'el responsable del tratamiento elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado'.

El artículo 33 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) establece que tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro establezca relaciones con los afectados aun cuando 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 de la 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.

A su vez, en el considerando 81 se añade que, en particular, el responsable atenderá a los conocimientos especializados, fiabilidad y recursos del encargado de tratamiento, de cara a la aplicación de las medidas técnicas y organizativas que cumplan los requisitos del Reglamento.

CRISTINA PEÑO HERNAN garantiza una diligencia debida en la elección del encargado del tratamiento que ofrezca garantías suficientes para que el tratamiento de los datos se realice conforme al Reglamento (UE) 2016/679, y proteja los derechos de las personas afectadas.

CRISTINA PEÑO HERNAN es responsable de los tratamientos de datos realizados por el encargado y no pierde esta consideración en ningún caso.

Con todos y cada uno de los encargados de tratamiento elegidos CRISTINA PEÑO HERNAN suscribe un contrato de confidencialidad vinculante regulando la relación entre ambos y estableciendo un adecuado control de firma.

Es posible que el acuerdo de confidencialidad entre responsable y encargado forme parte del contrato de prestación de servicios. En este caso se añadirá al contrato una cláusula de protección de datos específica que recoja el contenido del anexo citado en el párrafo anterior.

El contrato garantiza entre otros aspectos:

- que el encargado del tratamiento no recurre a otro encargado del tratamiento sin la autorización previa por escrito de la organización responsable de los tratamientos de datos.
- que las personas autorizadas a tratar los datos se han comprometido a respetar la confidencialidad de los datos y que poseen la formación necesaria en la materia.
- que el encargado del tratamiento pondrá a disposición del responsable toda la documentación necesaria para demostrar el cumplimiento de las obligaciones y que contribuirá a la realización de auditorías por parte del responsable.

En el REGISTRO DE ENCARGADOS DE TRATAMIENTO (ver Anexo) se recogen todos los encargados del tratamiento contratados por la organización.

Verificación del cumplimiento de las obligaciones

En función al art. 28 apdo 3.h) del Reglamento (UE) 2016/679, CRISTINA PEÑO HERNAN requiere a cada encargado del tratamiento para que al menos con una periodicidad anual demuestre que mantiene el cumplimiento de las obligaciones contractuales, así como las medidas de seguridad que garantizan la protección de los datos.

Para ello se podrán realizar auditorías de revisión sobre los encargados del tratamiento o en su lugar instar a que el encargado aporte las pruebas documentales necesarias.

Tratamiento de datos por encargo

Cuando un responsable (un cliente habitualmente) solicite el tratamiento de datos por encargo, CRISTINA PEÑO HERNAN actuará como encargado del tratamiento, ateniéndose a todas las obligaciones establecidas por el art. 28 del Reglamento (UE) 2016/679.

En el Anexo Externo CLÁUSULA CONTRACTUAL PARA LA PRESTACIÓN DE SERVICIOS COMO ENCARGADO DEL TRATAMIENTO se recoge el contenido contractual vinculante que debe estar suscrito por ambas partes o en su defecto el acuerdo contractual que el responsable del tratamiento establezca.

MEDIDAS DE RESPONSABILIDAD ACTIVA

Análisis de riesgos. Registro de actividades de tratamiento.

El Reglamento (UE) 2016/679 no ofrece un repertorio de medidas de seguridad predefinidas. Lo que plantea es que las medidas de seguridad se establezcan en función al riesgo detectado y que puedan adaptarse en función a los nuevos riesgos o a las circunstancias cambiantes de la organización.

Básicamente se trata de un enfoque proactivo en lo que respecta a la seguridad que exige no sólo la existencia de esas medidas en un papel sino a su aplicación efectiva.

CRISTINA PEÑO HERNAN cumple con el citado enfoque proactivo en la seguridad del tratamiento de los datos estableciendo garantías de seguridad adecuadas que eviten, fundamentalmente:

- El tratamiento no autorizado o ilícito de datos personales.
- La pérdida de los datos personales, la destrucción o el daño accidental.

Para determinar las medidas técnicas y organizativas se tiene en cuenta el estado de la técnica, los costes de la aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos que éstos pueden generar sobre los derechos y libertades de las personas físicas.

El análisis de los riesgos es el resultado de una reflexión sobre las implicaciones que los tratamientos de datos de carácter personal tienen sobre los interesados.

Para ello, se han definido la naturaleza y los tipos de tratamiento que CRISTINA PEÑO HERNAN realiza, sus características, finalidades, modos de tratamiento, posibles destinatarios y control del personal con acceso a los datos.

Del análisis de riesgos efectuado se determina si para cada actividad de tratamiento llevada a cabo por la organización, así como cualquier cambio o nueva actividad que se vaya a realizar, se presentan riesgos para los derechos y libertades fundamentales de las personas.

Los resultados del análisis de riesgos se recogen en el INFORME DE ANÁLISIS DE RIESGOS correspondiente, documento que evidencia tanto los aspectos analizados como los resultados obtenidos.

Si el resultado del análisis de riesgos determina que el riesgo es reducido no será necesaria ninguna actuación. En caso que el análisis de riesgos determine que existen riesgos elevados, se procede a adoptar las medidas correctivas y preventivas necesarias con el fin de reducir los niveles de riesgo encontrados. Se realizará evaluación de impacto cuando las medidas adoptadas no consigan reducir los riesgos.

Todas actividades de tratamiento llevadas a cabo por la organización se recogen en el Anexo Externo REGISTRO DE ACTIVIDADES DE TRATAMIENTO de la presente política. No sólo se define el alcance de cada actividad: definición de categorías de datos, tipos de datos, operaciones, finalidades, licitudes, orígenes de los datos, destinatarios, ámbito de actuación de cada una, así como la existencia de elaboración o no de perfiles, sino que se analizan los accesos, permisos, trabajadores implicados, tratamientos por encargo y los soportes vinculados a cada actividad.

Cualquier variación de las actividades o de su organización se actualiza en el REGISTRO DE ACTIVIDADES DE TRATAMIENTO que evidencia el firme compromiso de la organización con la protección y el control de los datos personales.

Protección de datos desde el diseño y por defecto

En virtud del art. 25 del Reglamento (UE) 2016/679 y teniendo en cuenta la naturaleza, el ámbito de aplicación, el contexto y la finalidad de los tratamientos indicados en el apartado anterior, la organización tiene implantadas las medidas de seguridad, tanto técnicas como organizativas, que garantizan que los tratamientos son realizados de forma segura.

Asimismo, la organización garantiza que el tratamiento de los datos se analiza con carácter previo y durante la actividad de tratamiento, determinando el alcance del tratamiento, los datos mínimos necesarios para atender la finalidad prevista, la duración del tratamiento, la conservación de los datos y el control de acceso a los mismos.

Para cada actividad de tratamiento y con carácter previo al mismo, cumpliendo con la protección desde el diseño y por defecto, la organización analiza todos los aspectos implicados en la seguridad del tratamiento: los riesgos para las libertades y los derechos de las personas en función a la naturaleza de los datos que se van a solicitar, la finalidad para la que se solicitan, el origen, el tipo de tratamiento, los destinatarios, la posibilidad de realizar transferencias internacionales de los datos, la posibilidad de realizar estudios de perfiles y la cantidad de datos que se esperan tratar.

En base a lo anterior se determinan los medios de tratamiento más adecuados, siendo en cualquier caso, medios técnicos y organizativos que garanticen el cumplimiento del Reglamento (UE) 2016/679.

Durante las actividades de tratamiento la organización adopta las medidas de control, técnicas y organizativas, que se describen en este manual tanto sobre los medios de tratamiento como sobre las personas con acceso a los datos tratados.

La organización garantiza que, por defecto, los datos no son accesibles a un número indeterminado de personas físicas, que sólo son accesibles para las personas autorizadas (tanto encargados del tratamiento como trabajadores de la organización), y a través de medios controlados y supervisados de forma periódica.

En el siguiente apartado se recogen las medidas adoptadas, tanto de índole técnica como organizativa, para la protección de los datos; soportes y modos de almacenamiento, control de accesos, copias de seguridad, compromisos de confidencialidad, etc.

Medidas de seguridad técnicas y organizativas

El Reglamento (UE) 2016/679 indica que las medidas de seguridad deberán ser proporcionales y adecuadas al riesgo detectado en cada actividad de tratamiento.

Las medidas técnicas y organizativas desarrolladas tienen en cuenta:

•Los trabajadores que tienen acceso a datos, estableciendo controles de acceso, determinando y registrando las actividades de tratamiento que realizada cada uno, estableciendo un mecanismo de formación a trabajadores en materia de protección de datos que pueda concienciar y garantizar el conocimiento de las responsabilidades, estableciendo un mecanismo de compromiso de confidencialidad que los trabajadores con acceso a datos se comprometen adoptar con su firma y determinando los trabajadores que asumen ciertas funciones en materia de protección de datos, creando un sistema de nombramientos aceptados.

•Los soportes empleados para el almacenamiento y el tratamiento de los datos, estableciendo un control de soportes, así como las actividades de tratamiento vinculadas a cada uno, las medidas de seguridad de acceso, copiado, borrado, cifrado, etc… y un sistema de control de entradas y salidas.

•La existencia de accesos remotos y servidores externos, ya sean públicos o privados, analizando las características de seguridad ofrecidos por los mismos y asegurando una protección eficaz.

•Así como otras medidas de restricción y de control de accesos a datos que se determinen en función a los resultados de los análisis de riesgos realizados.

Para garantizar la protección permanente de los datos se realiza un proceso de verificación y evaluación periódica de la eficacia de las medidas adoptadas. El proceso de evaluación periódica consiste en una revisión sistemática de las actividades de tratamiento llevadas a cabo o las que se pretendan iniciar, del personal que cuenta con acceso a las mismas, control de los compromisos de confidencialidad, control de los destinatarios y especialmente de los encargados de tratamiento, así como cualesquiera otras indicadas en el informe del análisis de riesgos que se realice.

El procedimiento de control analiza todos los soportes, tanto electrónicos (ordenadores, dispositivos electrónicos inteligentes, servidores, etc..) como manuales (archivadores, carpetas, etc..) y determina los riesgos en función a las actividades de tratamiento que contengan.

Asimismo, se han incluido medidas para asegurar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de cada uno de los soportes o sistemas de tratamiento, así como medidas para asegurar la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

Se atiende el compromiso de formar a todos los trabajadores que tienen acceso y/o tratan datos de carácter personal. Una formación en materia de protección de datos adecuada y revisable (en el registro de control se incluye un apartado específico para la formación de cada trabajador).

Todos los empleados de CRISTINA PEÑO HERNAN son responsables del cumplimiento de esta Política y de la normativa interna que la desarrolle o complemente. En particular, cada empleado deberá:

•cumplir, en el desempeño de su actividad en la empresa, con sus obligaciones de confidencialidad y secreto con respecto a los datos personales a los que tengan acceso.

•utilizar los datos personales únicamente para la finalidad para la que se recabaron y en el marco del cumplimiento de sus responsabilidades laborales.

•asistir a las formaciones relacionadas con la privacidad o la protección de datos.

•cooperar en la implantación de las medidas y facilitar la información y documentación que se les solicite para acreditar el cumplimiento en materia de protección de datos personales y privacidad.

•comunicar cualquier incumplimiento de la presente Política poniéndose en contacto con su responsable directo o funcional, o directamente con el DPD en el caso de que la empresa lo tenga.

Violaciones de seguridad de datos de carácter personal. Brechas de seguridad.

CRISTINA PEÑO HERNAN ha 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.

Cuando se produzcan violaciones de seguridad como por ejemplo, el robo o acceso indebido a los datos personales y en cumplimento de los artículos 33 y 34 del Reglamento (UE) 2016/679 de datos de carácter personal, se seguirá el procedimiento de registro de la violación de seguridad detectada.

Para la gestión de la brecha o violación de la seguridad de los datos, el responsable de seguridad (o el delegado de protección de datos en su caso) actuará llevando a cabo un procedimiento de análisis y registro de la situación.

Para el análisis se tendrá en cuenta si la violación de los datos afectados supone un riesgo para los derechos y libertades de las personas que pueda provocar daños y perjuicios físicos, materiales o inmateriales o que pueda suponer:

- problemas 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 o social significativo.

Asimismo se analiza si la violación de los datos puede privar a los interesados de sus derechos y libertades o les impide ejercer el control sobre datos personales que revelen:

- el origen étnico o racial
- las opiniones políticas.
- la religión o creencias filosóficas
- la militancia en sindicatos
- el tratamiento de datos genéticos
- datos relativos a la salud o datos sobre la vida sexual
- relativos a las condenas e infracciones penales o medidas de seguridad conexas

Se analizan los casos en los que se evalúen aspectos personales:

- en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo
- situación económica
- datos de salud
- preferencias o intereses personales

•fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales.

Igualmente se analizan los casos en los que se traten datos personales de personas vulnerables, en particular niños.

Si en el análisis anterior se llega a la conclusión que la brecha afecta o puede suponer un riesgo para las personas físicas, se notificará dicha violación en el Registro de la Agencia Española de protección de datos y se notificará al afectado.

Notificación de violaciones de seguridad de los datos

En caso de que sea necesario notificar la brecha de seguridad, la notificación se realizará antes de las 72 horas siguientes a que el responsable tenga constancia de ella.

Se realizará por medios electrónicos a través de la sede electrónica de la Agencia Española de Protección de Datos en la dirección: https://sedeagpd.gob.es aportando toda la información necesaria para el esclarecimiento de los hechos que hubieran dado lugar a la incidencia. La notificación incluye:

•La naturaleza de la violación, categorías de datos y de interesados afectados.

•Las medidas impuestas por el responsable para resolver esa quiebra.

•Si procede, las medidas adoptadas para reducir los posibles efectos negativos sobre los interesados. La notificación a los afectados se realizará en el mismo plazo y forma que el descrito.

Evaluación de impacto sobre protección de datos

La evaluación de impacto es un ejercicio posterior al análisis de los riesgos que un determinado tratamiento puede requerir para garantizar el derecho a la protección de datos de los afectados. Consiste en una evaluación pormenorizada de los tratamientos que, como resultado del análisis, requieran la adopción de otras medidas adicionales necesarias que eliminen o atenúen en lo posible aquellos riesgos que se hayan tipificado como intolerables.

La organización recaba el asesoramiento del delegado de protección de datos, en su caso, al realizar la evaluación de impacto.

En tratamientos a gran escala de categorías especiales de datos, tratamientos de datos relativos a condenas e infracciones penales, los que suponen una observación sistemática a gran escala de una zona de público o en los tratamientos cuyo análisis de riesgos resulte intolerable, se realiza evaluación de impacto. La evaluación incluirá una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, así como el interés legítimo. Incluirá la evaluación de los riesgos para los derechos y libertades así como las medidas previstas para afrontar los riesgos, garantías y mecanismos para garantizar la protección de datos.

Todas las evaluaciones de impacto que la organización deba realizar quedarán debidamente documentadas.

Delegado de protección de datos

La organización declara su compromiso con el art. 34 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales designando un delegado de protección de datos en caso de que esté obligada.

Asimismo, si tras el análisis de las actividades de tratamiento se determina que la organización requiere el nombramiento de un Delegado de Protección de Datos, lo hará por requerimiento legal atendiendo a sus cualidades de profesionales, conocimientos y competencias en la materia.

En su caso la organización mantendrá un delegado de protección de datos, identificado para los interesados y notificado a la Autoridad competente en materia de protección de datos garantizando que el delegado de protección de datos:

•participa de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.

•respalda a la organización en el desempeño de sus funciones.

•dispone de los recursos necesarios para el desempeño de sus funciones y para el mantenimiento de sus conocimientos, el acceso a los datos personales y a las operaciones de tratamiento.

•no recibe ninguna instrucción en lo que respecta al desempeño de sus funciones.

•no se destituye ni se sanciona al delegado de protección de datos por desempeñar sus funciones.

•rinde cuentas a la empresa al más alto nivel jerárquico.

•atiende a los interesados y mantiene la confidencialidad en el desempeño de sus funciones.

Si el delegado de protección de datos desempeñase otras funciones dentro de la organización se garantiza que la situación no da lugar a conflicto de intereses.

TRANSFERENCIAS INTERNACIONALES

Para poder realizar transferencias internacionales de datos personales el art. 44 Reglamento (UE) 2016/679 impone sobre el responsable y el encargado del tratamiento la obligación de cumplir con las condiciones del capítulo V. Podrá realizarse la transferencia cuando:

1. existan garantías para la protección de los datos de las personas físicas en el tercer país destinatario de los datos

2. se hayan elaborado y aprobado normas corporativas vinculantes (NCV)

3. a falta de lo anterior, cuando pueda acogerse a una de las excepciones previstas.

Cuando la organización realice transferencias internacionales de datos o utilice servidores de internet para el almacenamiento de datos de carácter personal, realizará un estudio de la situación de dichos servidores, así como de sus proveedores, analizando si existen garantías para las personas cuyos datos se encuentran en dicha situación, concretamente si:

•existe un instrumento jurídico vinculante y exigible entre las autoridades u organismos públicos de los diferentes países.

•existen normas corporativas vinculantes (aprobadas por la autoridad de control/comisión) entre la organización y las organizaciones destinatarias de los datos.

•existen cláusulas tipo (aprobadas por la autoridad de control/comisión) anexadas al contrato de servicios.

•existe un código de conducta (aprobado por la autoridad de control/comisión) junto con compromisos vinculantes exigibles por el tercer país.

•existe un mecanismo de certificación.

•se dispone del consentimiento explícito del interesado y se le ha informado de los posibles riesgos.

Los resultados quedarán debidamente documentados en el registro de actividades de tratamiento.

RESPONSABILIDADES

CRISTINA PEÑO HERNAN es el responsable de velar por el cumplimiento adecuado de esta Política y por integrar las obligaciones de cumplimiento en materia de protección de datos personales y privacidad dentro de sus actividades diarias, lo que compete a toda la organización y, por lo tanto, a sus órganos de gobierno y a todos sus empleados.

VERIFICACIÓN PERIÓDICA DEL SISTEMA DE PROTECCIÓN DE DATOS

Con el fin de mantener un control constante de los sistemas de protección de datos adoptados por la organización, con carácter periódico y cada vez que se realicen cambios en las actividades de tratamiento la organización se compromete a realizar auditorías internas de verificación periódicas, donde se analicen todos los puntos de control relacionados con las actividades de tratamiento llevadas a cabo. Los resultados serán documentados y puestos a disposición de la autoridad de control y los interesados que así lo soliciten como prueba de conformidad

ANEXOS 1

REGISTRO DE TRABAJADORES

TRABAJADOR/A: DOMINGUEZ DIAGO, DANIELA - AYUDANTE PELUQUERIA
Centro de trabajo: CENTRO DE TRABAJO con dirección en CALLE MARIA DE PIMENTEL, 4 LOCAL 3, TALAVERA DE LA REINA (45600), TOLEDO
Nombramiento asignado:
Fecha en la que se inicia el acceso a los datos: 05/07/2024
Formación en proteccion de datos: Sin formación especificada en protección de datos
Soportes vinculados al trabajador: Sin soportes asignados a este trabajador.