Política de privacidad

Anexo VI Manual de SGSI

Ed. 0 – Fecha: 26/06/2018

Política de privacidad

Anexo VI Manual de SGSI

Realizado por	Revisado y aprobado por
Responsable del sistema **Consultor externo**	Dirección

Control de versiones

Ed.	Fecha revisión	Observaciones	Aprobado
0	26/06/2018	Versión inicial	26/06/2018

Contenido

1. Introducción....4
2. Ámbito de aplicación....5
3. Marco legal de referencia....6
4. Definiciones....7
   4.1. Datos de carácter personal....7
   4.2. Fichero....7
   4.3. Tratamiento de datos....7
   4.4. Responsable del fichero o tratamiento....7
   4.5. Afectado o interesado....7
   4.6. Procedimiento de disociación....7
   4.7. Encargado del tratamiento....8
   4.8. Consentimiento del interesado....8
   4.9. Cesión o comunicación de datos....8
   4.10. Fuentes accesibles al público....8
5. Contenido....9
6. Recogida de datos....10
7. Principios de la protección de datos....11
   7.1. Calidad....11
   7.2. Información....12
   7.3. Deber de secreto....13
   7.4. Consentimiento....14
   7.5. Datos especialmente protegidos....14
   7.6. CESIONES O COMUNICACIONES DE DATOS....15
   7.7. Prestaciones de servicios....16
   7.8. Ejercicio de derechos....16
   7.9. Medidas de seguridad....19
8. Difusión de la política de privacidad....21

1. Introducción

De acuerdo con lo que establece la RGPD en lo que respecta a los datos de carácter personal, y en defensa de los intereses de los titulares de dichos datos de carácter personal el uso y tratamiento que se realice de sus datos estará sujeto a esta política de privacidad.

2. Ámbito de aplicación

La normativa de protección de datos será aplicable a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores públicos y privados.

3. Marco legal de referencia

- Constitución Española
- RGPD de 25 de Mayo Reglamento europeo de Protección de datos.
- Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación, cancelación y oposición.
- Directiva 94/46/CE del Parlamento Europeo y el Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas, respecto al tratamiento de datos personales y a la libre circulación de las mismas.

4. Definiciones

4.1. Datos de carácter personal

Cualquier información referente a personas físicas identificadas o identificables (voz, imagen, teléfono...). Toda información que se pueda vincular directamente con una persona o indirectamente mediante la conexión de la información con datos identificativos de dicha persona.

4.2. Fichero

Cualquier conjunto organizado de datos de carácter personal, sea cual sea la forma o la modalidad de creación, almacenamiento, organización y acceso (base de datos informatizada, documentos ofimáticos, archivos manuales, etc.)

4.3. Tratamiento de datos

Operaciones y procedimientos técnicos de carácter automatizado o no, que permiten recoger, grabar, conservar, elaborar, modificar, bloquear y cancelar, así como las cesiones de datos que deriven de comunicaciones, consultas, interconexiones y transferencias. Cualquier acción que se lleve a cabo con datos personales entra dentro del concepto de tratamiento.

4.4. Responsable del fichero o tratamiento

Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, el contenido y el uso del tratamiento.

4.5. Afectado o interesado

Persona física titular de los datos personales que son objeto del tratamiento.

4.6. Procedimiento de disociación

Cualquier tratamiento de datos personales de manera que la información que se obtenga no se pueda asociar a una persona identificada o identificable.

4.7. Encargado del tratamiento

Persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trata datos personales por cuenta del responsable del tratamiento. Así, por ejemplo, es encargado del tratamiento una gestoría que lleva a cabo las nóminas por cuenta de **REARMACHINE** o de cualquiera o una empresa informática que gestiona el un software de **REARMACHINE**

4.8. Consentimiento del interesado

Cualquier manifestación de la voluntad, libre, inequívoca, específica e informada, mediante la cual el interesado consiente el tratamiento de datos personales que le conciernen. Por ejemplo cuando un candidato entrega un curriculum en las dependencias de recursos humanos de **REARMACHINE**

4.9. Cesión o comunicación de datos

Revelación de datos efectuada a una persona diferente del interesado.

4.10. Fuentes accesibles al público

Ficheros que podrán ser consultados por cualquier persona, sin que lo impida una norma limitativa o sin otra exigencia que, si es necesario, el abono de una contraprestación. Sólo se consideran fuentes de acceso al público el censo promocional, los repertorios telefónicos en los términos que prevé la normativa específica y las listas de personas que pertenecen a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Así mismo, tienen el carácter de fuentes de acceso público los periódicos y los boletines oficiales y los medios de comunicación.

5. Contenido

La implementación de la normativa de protección de datos exige la definición de un plan de adecuación que ha de comenzar con la identificación de todos los ficheros y tratamientos de datos personales, tanto automatizados como manuales, que se lleven a cabo dentro de **REARMACHINE** y el análisis de cómo están interconectados. Se debe definir el flujo o recorrido de los datos a lo largo de su tratamiento a fin de identificar:

- Qué datos personales se recogen y para que finalidad
- Cómo se recogen (formularios, electrónicamente, telefónicamente....).
- Quién los trata (áreas, departamentos...).
- Cómo circulan dentro de la entidad (en soporte papel, telemáticamente...).
- A quién se ceden o que transferencias internacionales se llevan a cabo.
- Cómo se conservan o como se destruyen.

El resultado de este análisis ha de ser un inventario de los ficheros y tratamientos de datos personales respecto a los cuales se deberán de implementar todos los requerimientos de la normativa de protección de datos.

6. Recogida de datos

Las fuentes de recogida de datos según la legislación vigente en materia de protección de datos de carácter personal son:

- Consentimiento del interesado.
- Fuentes accesibles al público.

7. Principios de la protección de datos

- Calidad
- Información
- Deber de secreto
- Datos especialmente protegidos
- Consentimiento
- Cesiones
- Prestación de servicios
- Ejercicio de derechos
- Medidas de seguridad

7.1. Calidad

En primer término, cualquier entidad que trata datos personales debe analizar si el tratamiento de conformidad con el principio de calidad de los datos personales es legítimo, principio esencial del derecho fundamental a la protección de datos.

El principio de calidad de los datos exige que:

- Los datos personales que se recogen y se tratan sean únicamente los adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades a las cuales se destinen (principio de proporcionalidad).
- Las finalidades para las cuales estos datos personales se recogen y se someten a tratamiento han de ser determinadas, explícitas y legítimas.

Son también requerimientos del principio de calidad de los datos que:

- Los datos personales no se utilicen para finalidades incompatibles con el objetivo para el cual los datos van a ser recogidos
- Los datos personales sean exactos y puestos al día con la finalidad de que respondan a la veracidad de las situaciones de los afectados. La actualización se debe llevar a cabo no solo a petición del interesado en ejercicio de derecho de rectificación, sino también de oficio en el mismo momento en que la entidad tenga conocimiento de la inexactitud.

- Se cancelan los datos personales cuando pasen a ser inexactos o incompletos o cuando ya no sean necesarios o pertinentes de acuerdo con la finalidad para la cual fueron recogidos o registrados.
- Sean anónimos los datos personales o se desasocie la información cuando la identificación del interesado ya no sea necesaria para las finalidades de acuerdo con las cuales los datos hayan sido recogidos o registrados. Así, por ejemplo, se pueden hacer anónimas para realizar estadísticas realizadas por el departamento de calidad de **REARMACHINE**
- Se almacenen los datos personales de manera que se permita el ejercicio eficaz del derecho de acceso del interesado, excepto en los supuestos de cancelación.
- No se recojan datos personales para medios fraudulentos, desleales o ilícitos.

7.2. Información

Tal y como establece el RGPD antes de proceder a la recogida de datos personales se ha de informar a los titulares de manera expresa, precisa e inequívoca:

- de la existencia de un fichero o un tratamiento de datos de carácter personal,
- de la finalidad de la recogida de los datos y de los destinatarios de la información;
- del carácter obligatorio o facultativo de la respuesta a las preguntas que se planteen;
- de las consecuencias de la obtención de los datos o de la negativa a subministrarlos;
- de la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición;
- de la identidad y la dirección del responsable del tratamiento o, si es necesario, de su representante.

En los casos que para la recogida de los datos se utilice cuestionarios o impresos se ha de hacer constar la información anterior de manera claramente legible. Esta información se debe facilitar, en todo caso, con independencia del sistema de recogida de los datos que se utilice. Así, en el caso de recogida telefónica de datos se pueden, por ejemplo, diseñar argumentos para que los operadores que recogen los datos faciliten el derecho de información.

Si los datos no se recogen directamente de su titular se le tiene que informar, dentro de los tres meses siguientes al momento de registrar los datos, de manera expresa, precisa e inequívoca:

a) Del contenido del tratamiento
b) De la procedencia de los datos
c) De la existencia de un fichero o un tratamiento de datos de carácter personal, de la finalidad de la recogida de los datos y de los destinatarios de la información
d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición
e) De la identidad y la dirección del responsable del tratamiento o, si es necesario, de su representante

La información de los apartados c), d) y e) solo se deberá facilitar si no se ha informado al titular anteriormente.

El deber de informar al titular de los datos es una de las principales obligaciones del responsable del fichero, dado que permite garantizar el pleno ejercicio del derecho a la protección de los datos personales, ya que tiene como misión fundamental dar la información necesaria a su titular para controlar, de manera efectiva, los tratamientos que se llevan a cabo con sus datos.

El derecho de información no se ha de confundir con la necesidad de obtener el consentimiento para determinados tratamientos.

Así, en el momento de iniciar un nuevo tratamiento se debe hacer un análisis previo que permita la definición exacta del tratamiento que se quiere llevar a cabo para informar al titular de los datos de la manera más precisa posible.

7.3. Deber de secreto

Los responsables del fichero y todos los participantes en el proceso de gestión de los datos personales están obligados al secreto profesional. Este deber se mantiene una vez extinguida la relación que daba lugar al tratamiento de los datos.

Así, es recomendable incorporar y definir esta obligación en los contratos laborales y en los procedimientos internos y en las regulaciones específicas que recogen los derechos y las obligaciones de los usuarios, de los encargados del tratamiento y de los responsables de los ficheros, con el fin de dar a conocer el contenido y concienciar sobre su aplicación y su cumplimiento.

7.4. Consentimiento

El consentimiento es el eje central en la regulación del derecho a la protección de datos personales, ya que, como regla general, para el tratamiento de los datos de carácter personal es necesario el consentimiento inequívoco de su titular.

Así mismo, no será necesario el consentimiento cuando los datos personales:

- Cuando se refiera a las partes de un contrato o precontrato de una relación laboral, de negocios o administrativa y sean necesarios para su mantenimiento o cumplimiento.
- Cuando el tratamiento de los datos tenga como finalidad proteger un interés vital del interesado.
- Cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero.
- Cuando el tratamiento se ampare a una Ley o norma con rango de Ley.

7.5. Datos especialmente protegidos

Son datos especialmente protegidos estableciéndose unas garantías especiales en la su recogida (consentimiento expreso y en algunos casos también por escrito) los datos de carácter personal que revelen:

- Ideología
- Afiliación sindical
- Religión
- Creencias
- Origen racial
- Salud
- Vida sexual

7.6. CESIONES O COMUNICACIONES DE DATOS

La cesión o comunicación de datos personales se define como cualquier revelación de datos a una persona diferente de su titular.

Se diferencian las cesiones o comunicaciones de las transferencias internacionales, ya que tienen una regulación específica. Son transferencias internacionales las comunicaciones de datos que tienen como destinatario un responsable de fichero situado fuera del territorio español.

En términos generales, la comunicación de datos de carácter personal requiere o bien la obtención del consentimiento del interesado o titular de los datos o bien la existencia de una habilitación expresa prevista en una norma con rango de ley.

Es necesario diferenciar la cesión de datos del acceso a los datos por parte de terceros como consecuencia de la prestación de un servicio. En este último caso, la ley prevé específicamente la figura del encargado de tratamiento que es un tercero, persona o entidad, que trata datos de carácter personal por cuenta del responsable del fichero.

Este acceso por parte de un encargado de tratamiento no es calificado por la normativa como cesión o comunicación de los datos y no le es aplicable el régimen de autorización o habilitación legal, pero sí que requiere la formalización de un contrato o convenio entre el responsable y el encargado que ha de prever las obligaciones de las partes, las medidas de seguridad aplicables con indicación expresa que los datos deberán ser devueltos al responsable o ser destruidos una vez finalizado el servicio.

Los tratamientos de datos personales por parte de entidades están sujetas al régimen general previsto en el RGPD que prevé excepciones a la regla general del consentimiento del interesado en diversos supuestos, entre otros, cuando la comunicación tiene como destinatario el Defensor del Pueblo, el Ministerio Fiscal, los Jueces o tribunales, o cuando la cesión de datos relativos a la salud es necesaria por razón de una urgencia.

Finalmente, respecto a las transferencias internacionales que tengan como destinatario países que no proporcionan un nivel de protección equiparable al previsto en el RGPD, es necesario obtener la autorización previa del director de la Agencia Española de Protección de Datos.

7.7. Prestaciones de servicios

Las comunicaciones o accesos de datos realizados por un tercero para la prestación de un servicio al responsable del tratamiento no se considerarán cesiones propiamente dichas.

La comunicación de datos realizada en una prestación de servicios que no esté regulada por escrito se podrá considerar cesión ilícita de datos.

En consecuencia la empresa o entidad cesionaria de los datos será considerada también responsable del fichero, y responderá ante de los incumplimientos de la normativa en los que haya incurrido.

7.8. Ejercicio de derechos

El derecho a la protección de datos de carácter personal atribuye a su titular un conjunto de potestades o derechos para garantizar y controlar los tratamientos de sus datos personales por parte de terceros.. Estos derechos son:

- Derecho de **acceso**: derecho a solicitar y obtener información de sus datos personales sometidos a tratamiento, sobre su origen y las comunicaciones efectuadas o las que se prevén hacer.
- Derecho de **rectificación**: derecho a rectificar y corregir los errores o las incorrecciones que en todo o en parte presenten los datos personales. Este derecho responde a las exigencias del principio de calidad de los datos personales, que exige que los datos sean exactos y se pongan al día de manera que respondan con la veracidad a la situación actual del afectado.
- Derecho de **cancelación**: derecho a cancelar los datos cuando dejen de ser necesarios o pertinentes para la finalidad que legitimó la obtención.

- Derecho de **oposición**: derecho a oponerse al tratamiento de los datos personales atendiendo a motivos fundamentales y legítimos relativos a una situación personal concreta, en aquellos casos en que el consentimiento para el tratamiento no sea exigido y siempre que una ley no establezca lo contrario.

Los titulares de los datos ejercerán sus derechos ante los responsables de los ficheros o de las unidades designadas a este efecto, y se habrá de definir un procedimiento interno para garantizar el ejercicio. Así, por ejemplo, se pueden designar las áreas relacionadas con el responsable de seguridad de **REARMACHINE** como puntos de recepción de las solicitudes del ejercicio de derechos y que éstas gestionen la respuesta ante estas situaciones.

En cualquier caso, todo el personal de **REARMACHINE** que en un momento concreto puedan atender este tipo de situaciones, ha de estar en disposición de informar a los interesados de dónde y cómo pueden ejercer sus derechos.

Este procedimiento debe ser conforme a los requerimientos siguientes:

- Los derechos de acceso, rectificación, cancelación y oposición, dada su naturaleza de derechos personalísimos, los puede ejercer únicamente su titular o la persona que ostenta la representación; en todo caso, la identidad de la persona que ejerce el derecho deberá de ser debidamente acreditada mediante la correspondiente documentación.

- Toda petición de ejercicio de derechos, presentada ante del responsable o del área designada al efecto, ha de ser contestada formalmente, con independencia que los datos de la persona afectada figuren o no en los correspondientes ficheros de datos personales. La respuesta se debe facilitar a través de un medio que permita acreditar la recepción.

- El derecho de acceso se puede garantizar mediante la mera consulta de los datos, ya sea a través de la visualización o de la indicación de los datos que son objeto de tratamiento, por medio de escrito, copia, o fotocopia, certificada o no, en formato legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos. Este derecho solo se puede ejercer a intervalos no inferiores

a 12 meses, salvo que se acredite un interés legítimo a este efecto. El responsable del fichero o tratamiento debe resolver la petición de acceso en el plazo de un mes. Si la resolución fuera estimatoria será necesario hacer efectivo el acceso en el plazo de 10 días e informar de cuáles son los datos objeto de tratamiento, de su procedencia y finalidades y usos a que son destinados y de las comunicaciones a terceros. Si los datos provienen de diferentes fuentes, será necesario indicarlas.

- La solicitud de ejercicio del **derecho de rectificación** debe indicar el dato que es erróneo y la corrección que ha de realizarse, que se deberá acreditar por medio de la documentación que corresponda, salvo que la rectificación dependa exclusivamente del consentimiento del interesado. El responsable del fichero debe rectificar los datos en los 10 días siguientes al día de la recepción de la petición. Si los datos rectificados se han cedido previamente, el responsable del fichero ha de notificar al destinatario de los datos la rectificación efectuada en el mismo plazo.

- La solicitud de **cancelación de datos personales** ha de indicar que el titular revoca el consentimiento prestado para el tratamiento de sus datos, o si se trata de un supuesto de datos erróneos o inexactos también ha de aportar la documentación acreditativa de este hecho. Si es procedente, la cancelación dará lugar al bloqueo de los datos; únicamente se conservaran a disposición de las administraciones públicas, jueces y tribunales para atender posibles responsabilidades nacidas del tratamiento, durante el plazo de su prescripción. Una vez transcurrido este plazo los datos personales se han de suprimir.

- El responsable del fichero o tratamiento tiene la obligación de hacer efectivo la cancelación del mismo. Esta resolución se debe notificar al interesado y a los terceros que dispongan de estos datos; y estos terceros destinatarios de los datos personales que han de ser objeto de cancelación también han de bloquear o suprimir, según corresponda.

- El ejercicio de los derechos de **acceso, rectificación, cancelación y oposición** al tratamiento de datos de carácter personal es gratuito.

7.9. Medidas de seguridad

El responsable del fichero, y si es el caso, el encargado del tratamiento han de adoptar las medidas de seguridad técnicas y organizativas necesarias para garantizar la seguridad de los datos de carácter personal que tratan, para evitar la alteración, la pérdida o el acceso por parte de terceros no autorizados.

Las medidas mínimas que se han de aplicar a los tratamientos de datos de carácter personal se regulan en el Reglamento Europeo de Protección de Datos de Carácter Personal. Estas medidas se han de aplicar teniendo en cuenta el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos los datos personales.

El Reglamento Europeo de Protección de Datos de Carácter Personal. Establece un conjunto de medidas tanto técnicas como organizativas que serán aplicables en función del tipo de datos tratados y del soporte en el cual se encuentren almacenados. Estas medidas se clasifican en tres niveles de seguridad diferentes según la naturaleza de los datos personales: **básico, medio y alto**.

Las medidas que corresponden al nivel de seguridad básico son aplicables a todos los tratamientos de datos personales.

Las medidas de nivel de seguridad medio se aplican a los ficheros que contienen datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros y los ficheros relativos a los servicios de información sobre solvencia patrimonial y crédito. Así mismo, en los ficheros que contienen un conjunto de datos personales suficientes que permitan obtener una evaluación de la personalidad del individuo serán aplicables determinadas medidas de seguridad de nivel medio.

Las medidas de seguridad que correspondan al nivel de seguridad alto se aplican a los ficheros o tratamientos que contienen datos relativos a la ideología, religión, creencias, origen racial, salud o vida sexual. Además, se aplican también a los ficheros que contienen

datos solicitados para finalidades policiales recogidas sin el consentimiento de los titulares afectados.

Es necesario destacar que el Documento de Seguridad es aquel documento o manual que recoge el conjunto de medidas de seguridad, tanto técnicas como organizativas, que el responsable del fichero y/o el encargado del tratamiento, si es necesario, han de implementar sobre los ficheros que contienen datos personales de **REARMACHINE.** Existe un Documento de Seguridad específico para cada entidad perteneciente al Grupo.

8. Difusión de la política de privacidad

Con fecha 26 de junio 2018 se ha difundido la versión actualizada de la política de privacidad de **REARMACHINE** entre los trabajadores y usuarios de los sistemas, con la intención de concienciar sobre las implicaciones de la misma en el desarrollo de su actividad diaria.