UNIVERSIDAD MIGUEL HERNANDEZ

Facultad Ciencias Sociales y Jurídicas de Elche

Grado en RRLL Y RRHH

TRABAJO FIN DE GRADO

REGIMEN GENERAL DE LA PROTECCION DE DATOS:

INTRODUCCIÓN A LA NORMATIVA Y GUÍA DE APLICACIÓN EN ASESORÍA LABORAL

Curso académico: 2019/2020

Alumna: Mari Carmen Casas Fernández

Tutor: Julio Naranjo Berenguer

INDICE

- **Resumen** 3
- **Introducción** 4
- **¿Qué es el RGPD y para qué sirve?** 5
    1. **MARCO JURÍDICO** 6
    2. **OBJETIVO Y DISEÑO DEL RGPD** 9
    3. **NOVEDADES DEL RGPD** 10
    4. **PASOS A SEGUIR PARA REALIZAR UN REGISTRO DE ACTIVIDADES DE TRATAMIENTO** 13
- **Supuesto sobre el que vamos a realizar el RGPD** 13
- **Pasos a seguir para obtener el registro de actividades de tratamiento** 14
    - **a) Análisis de riesgo** 14
    - **b) Responsable del tratamiento de datos** 16
    - **c) Ficheros y tratamientos de datos** 18
        - **c.1) Tratamiento de datos de clientes** 18
        - **c.2) Tratamiento de datos con empleados** 21
        - **c.3) Tratamiento de datos con candidatos** 22
        - **c.4) Contratos con empresas de servicios** 23
            - **c.4.a) Información de videovigilancia** 27
        - **c.5) Registro de actividades de tratamiento** 31
    - **d) Información y consentimiento de los interesados** 34
    - **e) Medidas de seguridad mínimas** 40
- **Conclusiones** 44
- **Bibliografía** 45

Resumen:

En este Trabajo Fin de Grado vamos a hacer una introducción a la normativa del Régimen General de la Protección de Datos (en adelante RGPD) y además haremos una simulación de un tratamiento de datos sobre una empresa ficticia. Vamos a identificar los pasos a seguir por una pequeña empresa, identificando cada documento de seguridad necesario, para tener un adecuado cumplimiento de la normativa del RGPD.

Se ha desarrollado este TFG para dar a conocer la normativa sobre protección de datos que deben cumplir las empresas en el día a día y los derechos que tenemos como consumidores de dichas empresas.

Introducción

Actualmente estamos en un mundo en el que nuestros datos personales se ven expuestos muy fácilmente debido a la globalización. Nos encontramos en un entorno totalmente digitalizado debido a la revolución tecnológica y esto ha hecho que los datos de las personas físicas circulen libremente por todo el mundo.

Todos los datos referentes a una persona física se recogen en las webs o en algunos casos, en establecimientos físicos que usan portales digitales o formato papel para la recogida de datos, usamos los terminales móviles o incluso las pulseras digitales para realizar pagos en establecimientos, las cámaras de seguridad nos graban continuamente, y así, cientos de ejemplos en los que nosotros y nuestros datos quedan expuestos al uso de terceras personas.

Y nosotros, ¿sabemos realmente como se usan nuestros datos?, ¿Qué fin tienen?, ¿Hay alguna forma de controlar el uso que se le dan a nuestros datos?, ¿y al tiempo de uso de estos?, de esta forma, también nos surgen muchas preguntas referentes a como están siendo manipulados nuestros datos y que derechos tenemos sobre el uso que los terceros tienen sobre ellos.

Es complicado realizar una regulación global para el control del uso de nuestros datos personales, pero a través de la normativa que entro en vigor en 2016 y aplicable en España en 2018 con el objetivo de adaptar la legislación española a las disposiciones del Reglamento de la UE 2016/679 (RGPD), conseguimos una regulación muy amplia para nuestros datos personales.

¿Qué es el RGPD y para qué sirve?

El Reglamento General de Protección de Datos es una norma de aplicación directa en todos los estados miembros de la UE la cual se va a encargar de que exista un mayor control y seguridad sobre el uso de los datos personales de los ciudadanos. Esta normativa les da más derechos a los ciudadanos para decidir sobre el uso de sus datos y de cómo desean recibir información de las empresas.

Para poder entender con más exactitud cómo funciona esta normativa, vamos a hacer una introducción sobre la historia de la normativa sobre protección de datos, su objetivo, novedades de la ley, pasos a seguir para hacer un tratamiento de datos y, además, incluiremos un supuesto que hemos realizado a través de la web de la AEPD y “ayudaleyprotecciondatos” para ver cómo es un registro de actividades de tratamiento de protección de datos.

1. MARCO JURÍDICO:

España fue pionera en el reconocimiento de los derechos fundamentales a la protección de datos personales, puesto que en la constitución de 1978 dispuso en su artículo 18.4 que: “La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos” y su artículo 18.1 “Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen”.

El tribunal constitucional señalo que el derecho fundamental a la intimidad, art. 18.1 de la constitución, no protege suficientemente con respecto al progreso tecnológico y la informática y por ello, con la introducción del art. 18.4 en la constitución, se dio visibilidad al conocimiento que el constituyente tenia de los riesgos que podía conllevar el uso de la informática y encargó al legislador la garantía de ciertos derechos fundamentales así como, del pleno ejercicio de los derechos de las personas.

En sus inicios hablaron de “libertad informática”. El Tribunal Constitucional interpreto el art.18.4 como una garantía de los derechos a la intimidad y el honor, además de disfrutar plenamente del resto de derechos de que disponen los ciudadanos que constituye un derecho o libertad fundamenta, además, derecho a la libertad delante de las posibles agresiones a la dignidad y libertad de las personas que disfrutan del mal uso del tratamiento mecanizado de datos, lo que la constitución define como <<la informática>>, y que denominó como <<libertad informática>>.

Con posterioridad, se desarrolla normativamente el derecho a la protección de datos como derecho independiente con dos nuevas leyes:

- “Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (conocida como la LORTAD)”.
- “Ley Orgánica 15/1999, de 13 de diciembre de 1999, de Protección de Datos de Carácter Personal (LOPD). La cuál, derogó la LORTAD y es la que precede al actual RGPD de 25 de mayo de 2018”.

Actualmente, en España contamos con un conjunto único de normas que son de aplicación directa en todos los Estados miembros, el Régimen General de Protección de Datos (RGPD), el cuál entro en vigor el 24 de mayo de 2018.

El RGPD tiene como objeto establecer "normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos", tal como describe en su artículo 1º, este, se justifica en la necesidad de implantar un marco uniforme más firme y congruente para la protección de los datos de la Unión Europea, dada la importancia de crear la confianza que permita a la economía digital extenderse en el mercado interior. Es una solución a la veloz evolución tecnológica y globalización, ya que ha supuesto nuevos retos a la protección de los datos personales. La tecnología faculta a las empresas privadas y autoridades públicas para la utilización de datos personales en sus actividades, a su vez, las personas físicas, difunden con mayor intensidad su información personal a nivel mundial y por ello, es necesaria una mayor protección.

Dicha ley, permite la ampliación normativa por parte de los países miembros, es decir, que los países de la UE, pueden completar la nueva ley con la normativa que ellos tenían hasta el momento de aplicación de esta, siempre y cuando, no se contradiga o incumpla el RGPD.

En España, con la entrada del RGPD, entra el Proyecto de Ley Orgánica de Protección de datos (PLOPD) aprobado el 10 de noviembre de 2017, que entró en vigor el 24 de mayo de 2016 y fue aplicable a partir del 25 de mayo de 2018, con el objetivo de adaptar la legislación española a las disposiciones del Reglamento de la UE 2016/679 (RGPD).

Esta ley complementa las disposiciones del RGPD garantizando igualmente los derechos digitales de los ciudadanos con la entrada en vigor el 7 de diciembre de 2018 de la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

El objeto de la LOPDGDD es adaptar el ordenamiento jurídico español al RGPD, completar sus disposiciones e instaurar que el derecho de las personas físicas a la protección de datos que cita el artículo 18.4 de la CE, se ejerza tal como dicta

el Reglamento (UE) 2016/679 y dicha Ley orgánica, además de que esta ley tiene la obligación de garantizar los derechos digitales de los ciudadanos.

Asimismo, las comunidades autónomas también disponen de competencia propia para desarrollar la normativa y ejecutar el derecho fundamental a la protección de datos.

2. OBJETIVO Y DISEÑO DEL RGPD

El principal objetivo del nuevo RGPD es proteger a las personas físicas en relación con el tratamiento de sus datos personales. Se usará con toda la información relativa a una persona física que pueda ser identificada o sea identificable, entre esa identificación, entran todos los datos seudonimizados imputables a una persona física por medio del uso de información adicional, ya que también se considera información de una persona física.

En relación a las personas jurídicas, no regula el tratamiento de datos ni tampoco se aplica al tratamiento de datos personales por una persona física cuando desarrolla una actividad únicamente personal o doméstica, que no tiene conexión con una actividad profesional o comercial.

El RGPD es de obligado uso en todos los tratamientos de datos personales elaborados por una persona jurídica o autónomo afincado en la Unión Europea, independientemente de que su empleo sea o no, en territorio de la Unión, es decir, los encargados y responsables del tratamiento de datos que no estén establecidos en la UE, tienen la obligación de aplicar el RGPD si las ocupaciones del tratamiento aluden a ofertas de bienes o servicios a dichos interesados o si se usa el tratamiento de datos personales de los interesados que se localicen en la UE por un responsable o encargado cuando esté vinculado a la observación del comportamiento de dichos interesados.

Las empresas tendrán la obligación y responsabilidad de garantizar la seguridad de todos los datos personales a los interesados, en caso de incumplimiento de la ley, dichas empresas podrán ser sancionadas.

3. NOVEDADES DEL RGPD

Existen varias novedades a destacar el nuevo RGPD, el ámbito de aplicación, el principio de responsabilidad proactiva, el enfoque de riesgo, siendo estos dos las mayores novedades del RGPD respecto a los responsables, y obtener el consentimiento expreso para poder usar los datos personales de los interesados.

Ahora el consentimiento será por medio de una declaración inequívoca o una afirmación clara, está será la base para tratar los datos personales ya que el RGPD no admite el consentimiento tácito, por omisión o inacción puesto que estos no expresan un consentimiento en sí.

Respecto al consentimiento de los menores de edad, solo será válido si estos tienen 16 años o más, aunque el RGPD permite a los estados miembros rebajar esta edad hasta los 13 años.

También han incluido dos nuevas categorías especiales de datos personales, los datos genéticos y los biométricos.

Una muy importante modificación es la ampliación de los derechos ARCO.

La nueva normativa, también establece una exhaustiva lista de toda la información que se debe facilitar a los interesados porque el nuevo reglamento señala la información como un derecho de los interesados y añade una lista sobre las nuevas cuestiones sobre las que ha de informas, estas son: “la base jurídica del tratamiento, intereses legítimos perseguidos en que se fundamenta el tratamiento, el deseo de hacer transferencias internacionales, el derecho a solicitar portabilidad o la limitación del tratamiento, el derecho a retirar en cualquier momento el consentimiento prestado, datos del Delegado de Protección de Datos y elaboración de perfiles, entre otras”.

También se añade el derecho al olvido, es decir, los interesados tendrán derecho a solicitar y obtener la eliminación de los datos.

En cuanto a la inscripción de los ficheros y su notificación, el RGPD suprime la obligación de crear dichos ficheros y notificarlos en el registro competente, aunque, todos los responsable y encargados de los tratamientos deben conservar un registro de operaciones de tratamiento en el que conste la información que establece el RGPD.

Las transferencias internaciones en el RGPD siguen la misma línea que la establecida en “la Directiva 95/46 y las legislaciones nacionales de transposición” y establece en qué casos se podrán comunicar los datos fuera del Espacio Económico Europeo.

Respecto al ámbito de aplicación, el RGPD lo amplía hacia el encargado y responsable de la protección de datos no establecidos en la UE.

Además, se amplía el contenido de los contratos de los encargados de tratamientos y también las obligaciones de estos.

Los contratos de encargo realizados antes de la aplicación del nuevo RGPD se deben modificar y adaptar para que se adecue al contenido de este, siendo invalidas las referencias genéricas a los artículos del RGPD que las regule, además, la obligación de firmar nuevos contratos de confidencialidad con los encargados de tratamiento de datos.

El nuevo RGPD visualiza la protección de datos desde el diseño y por defecto, esto es, que los responsables deben seguir unas medidas técnicas y organizativas adecuadas para incluir en los tratamientos las garantías necesarias e incorporar de la forma más efectiva todos los principios del RGPD.

Los responsables y encargados deben constituir las medidas técnicas y organizativas adecuadas para garantizar el nivel de seguridad apropiada en función de los riesgos que se detecten en los análisis previos, además, deben ejecutar una evaluación de impacto sobre la protección de datos (EIPD) cuando el tratamiento, por su contenido, conlleve un “alto riesgo para los derechos y libertades de las personas físicas”. Si tras dicha evaluación, se prevé que el tratamiento de datos puede conllevar la vulnerabilidad del RGPD, el responsable deberá realizar una consulta a la autoridad competente para que esta asesore al responsable (y/o encargado) sobre cómo proceder.

Respecto a las medidas de seguridad, la nueva normativa no es igual a la anterior, ya que ahora no existe una lista con las medidas de seguridad que se deben aplicar según sea el tratamiento, sino que, “condiciona la adopción de las medidas de responsabilidad activa al riesgo que los tratamientos puedan suponer para los derechos y libertades de los interesados” y cada responsable

debe efectuar una valoración del riesgo de cada tratamiento que haga, para poder establecer las medidas de seguridad que se deben aplicar en dicho tratamiento y cómo hacerlo.

Si se produjera una “violación de la seguridad de los datos” de los interesados, el responsable deberá notificarla a la autoridad de protección de datos correspondiente, a menos que dicha violación no sea un riesgo para los derechos y libertades de los responsables.

Se incluyen en el RGPD los códigos de conducta y los mecanismos de certificación, que sirven para la autorregulación y demostración del cumplimiento de la normativa.

El RGPD habilita al Delegado de Protección de datos (DPD), este, asume nuevas competencias respecto a la coordinación y control sobre el cumplimiento de la protección de datos y podrá ser, bien personal de la empresa o un empleado externo. No es obligatoria para todos los tratamientos, pero si lo será en algunos casos (los cuales desarrollaremos más adelante).

4. PASOS A SEGUIR PARA REALIZAR UN REGISTRO DE ACTIVIDADES DE TRATAMIENTO.

Para desarrollar este punto, vamos a realizar un supuesto de registro de actividades de tratamiento e iremos indicando los pasos seguidos para obtenerlo.

Supuesto sobre el que vamos a realizar el RGPD.

Para poder realizar un estudio real sobre la implementación del RGPD, vamos a realizar un supuesto que nos ayude a exponer cada paso a seguir.

Usaremos una empresa ficticia denominada, “Asesoría laboral ASLA, SL.”, la cual se encarga de gestionar todo lo relativo a la documentación laboral de sus clientes, además, de los suyos mismos.

La empresa está compuesta por Carla Cafer, la dueña, que se encarga de la dirección de la asesoría, así como de los temas más enfocados a derecho puesto que es graduada social, además, tres empleados que ocupan los puestos de recepción y asesoría laboral.

Está situada en la ciudad de Elche (Alicante) y todos los empleados trabajan allí.

A parte, cuentan con una limpiadora de una empresa externa.

No tienen web, pero si contactan con los clientes a través de la aplicación Whatsapp o vía email.

Utilizan el software Sage laboral para realizar las diferentes funciones, el cual tiene una atención al cliente que en caso de que surja alguna incidencia con el programa, puede conectarse de forma remota a los pc’s de la asesoría, y, además, tiene una agenda online para almacenar todos los contactos (teléfono fijo, móvil y dirección email de cada cliente).

Tienen contratado un informático externo, el cual se encarga de las incidencias que puedan surgir y también tiene acceso de forma remota a los pc’s de la asesoría.

Todos los documentos que se gestionan, ya sea cara a gestiones administrativas (altas/bajas en la SS, contratos, nominas, etc) o cara a entrevistas laboral

(curriculums laborales, algún documento referente al proceso de selección y los candidatos, etc), se digitalizan y se almacena digitalmente en el expediente de cada cliente. Algunos de estos documentos (en papel) se almacenan en el Archivo que hay en las instalaciones de la propia asesoría, y otros, una vez digitalizados, se destruye.

Tiene una alarma contratada y dos cámaras de seguridad, una en la zona de recepción y otra, que enfoca la entrada a los despachos.

Pasos a seguir para obtener el registro de actividades de tratamiento.

a) ANALISIS DE RIESGO:

   Lo primero que debemos realizar es un análisis de riesgo para establecer las medidas de seguridad y control más adecuadas para nuestra empresa.

   En caso de ser una PYME, dicho análisis se podrá realizar con una simple reflexión o se puede usar la herramienta gratuita “Facilita RGPD”.

   Si se responde de forma negativa a dicha reflexión en caso de ser una PYME, o en el análisis realizado en la empresa, se detecta que el nivel de riesgo es escaso para los derechos y libertades de los interesados, no se deberán hacer análisis adicionales.

   Para nuestro supuesto, hemos usado la herramienta “Facilita RGPD”.

   En primer lugar, se deben contestar una serie de preguntas para saber sobre qué empresa se va a realizar el tratamiento de datos y una vez detectado, indica que tipo de riesgo

   conlleva.

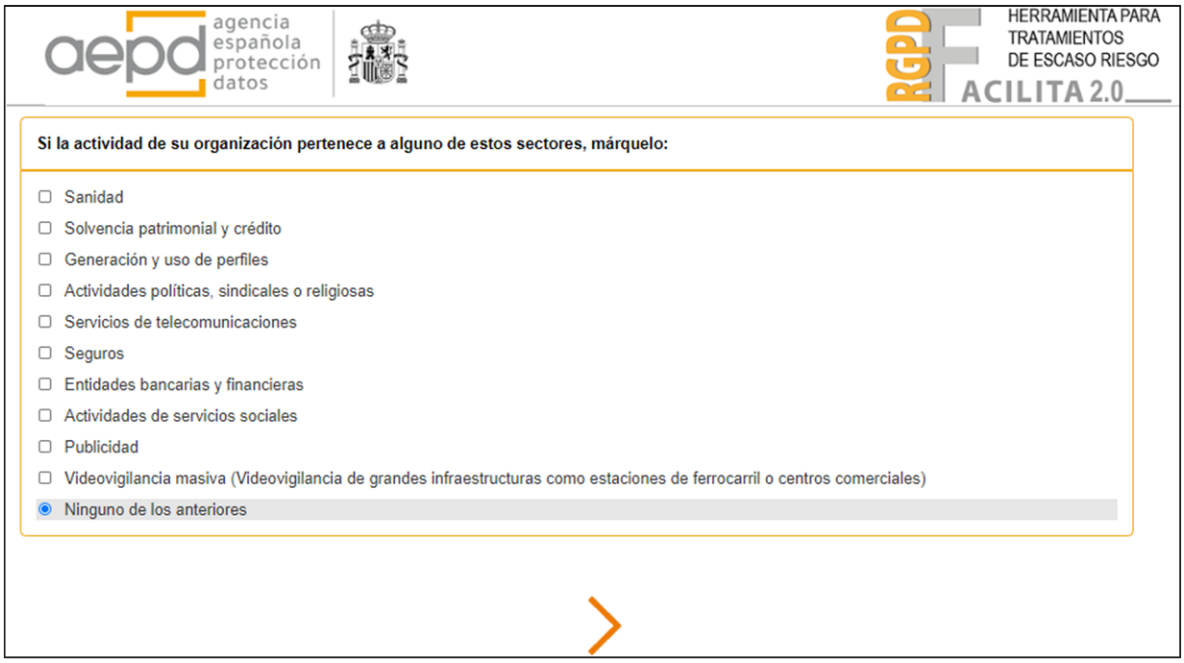

Imagen 1. Obtenida a través de la web https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd.

A continuación, mostramos los pasos seguidos para nuestro supuesto y el resultado obtenido a través de la herramienta “Facilita RGPD”.

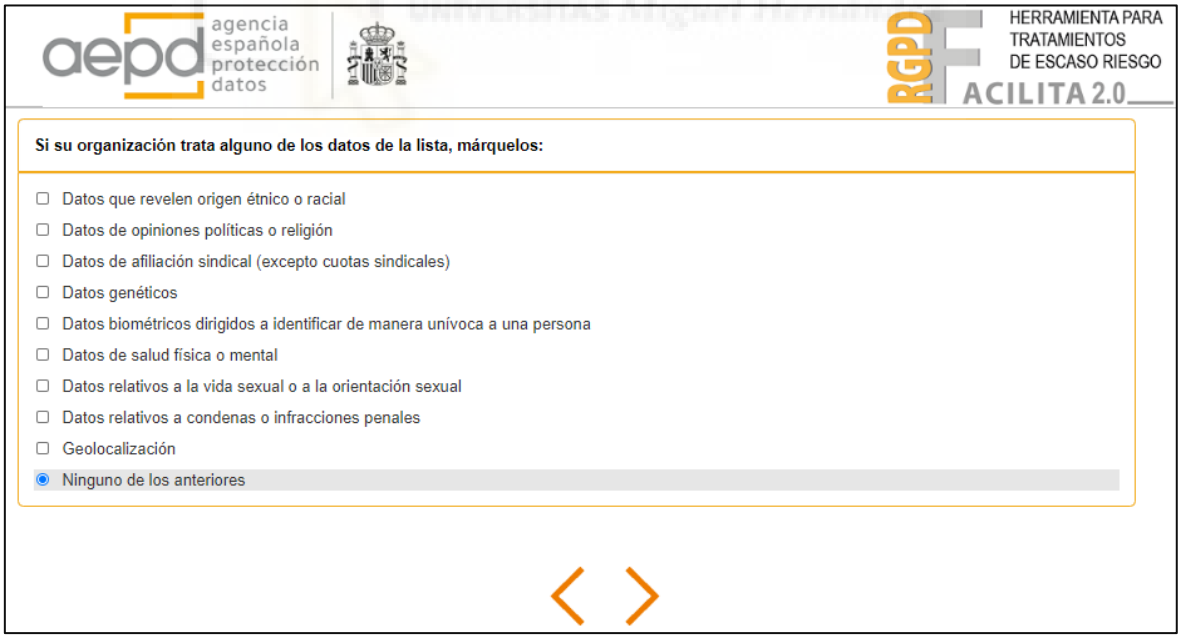

Imagen 2. Obtenida a través de la web https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd.

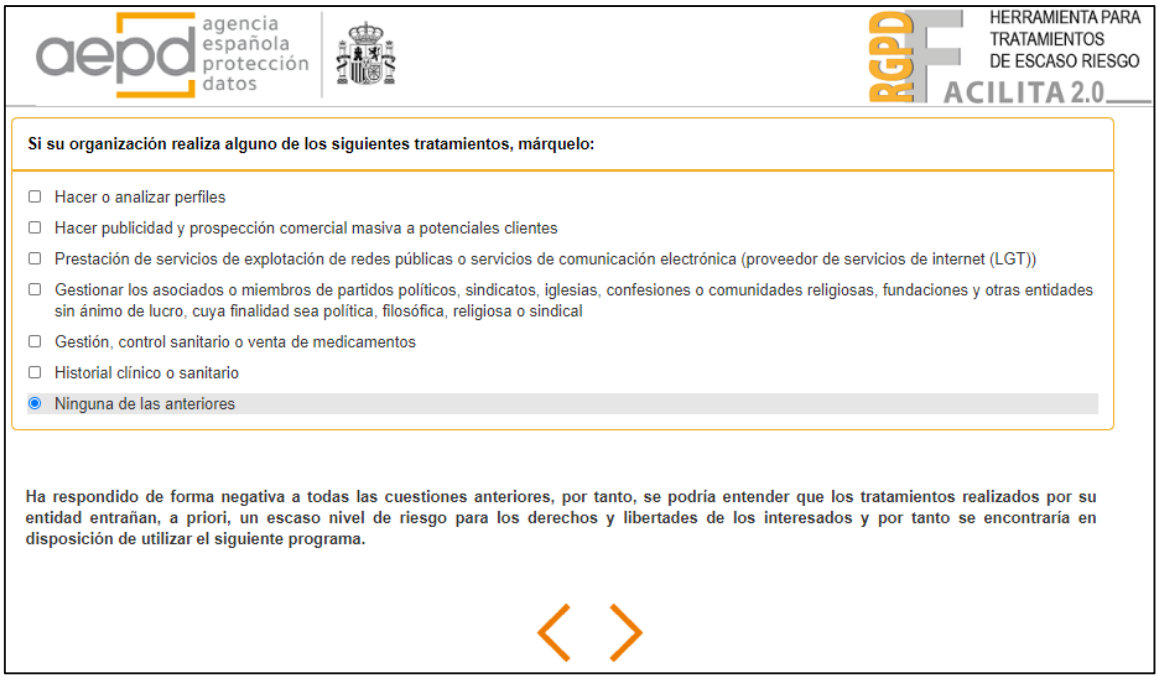

Imagen 3. Obtenida a través de la web https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd.

Al no tratar datos sensibles ni pertenecer a una organización de las indicadas en la primera imagen (“sanidad, solvencia patrimonial y crédito, generación y uso de perfiles, actividades políticas, sindicales o religiosas, servicios de telecomunicaciones, seguros, entidades bancarias y financieras, actividades sociales, publicidad o videovigilancia masiva”), se entiende que la empresa de nuestro supuesto, no entraña un alto riesgo para los derechos y libertades de los interesados, esto quiere decir, que no debemos realizar ningún otro análisis.

b) RESPONSABLE DEL TRATAMIENTO DE DATOS:

Sera necesario un responsable de tratamiento de datos para aquellos tratamientos de datos que conlleven riesgos elevados, tratamientos de administraciones públicas, o de empresas privadas que necesiten de una observación usual y/o repetida de las personas o que traten datos especialmente sensibles o protegidos a gran escala, en nuestro caso, la responsable de dicho tratamiento será “Carla Cafer” que es la dueña y gerente de la Asesoría.

Las funciones de dicho responsable de tratamiento será la de “implementar medidas técnicas y organizativas apropiadas para garantizar y demostrar el cumplimiento del RGPD teniendo en cuenta:

- La naturaleza, ámbito, contexto y fines del tratamiento.
- Los riesgos para los derechos y libertades de los interesados.
- El tipo de organización.
- La aplicación de medidas de protección de datos proporcionadas en relación con las actividades del tratamiento”.

En función del tipo de empresa que tengamos, el RGPD establece unas obligaciones diferentes para los encargados o responsables en el tratamiento de los ficheros.

Las empresas que traten datos cuya responsabilidad es únicamente suya, los ficheros corresponderán al responsable del tratamiento, en caso de que los datos a tratar sean de otras empresas, los ficheros serán responsabilidad del encargado del tratamiento.

Es importante establecer la diferencia entre el encargado y el responsable del tratamiento.

El encargado del tratamiento, sería aquella persona, física o jurídica, que se encarga del tratamiento de datos personales en vez de hacerlo el responsable del tratamiento, esto suele ser un tercero, como por ejemplo asesorías laborales, mutuas…

El Responsable, es la personas, física o jurídica, que decidirá sobre el desarrollo, conservación, cesión, eliminación y demás aspectos decisivos del tratamiento de datos.

En nuestro caso, el supuesto se basa en una asesoría laboral, por lo que seriamos tanto encargados como responsables del tratamiento de datos.

Responsables puesto que seremos nosotros mismos los que procedamos a la inscripción de los ficheros, cumplamos con: el deber de información, confidencialidad de todos los datos y medidas de seguridad adecuadas.

c) FICHEROS Y TRATAMIENTOS DE DATOS:

A continuación, identificaremos los ficheros y tratamientos de datos.

Vamos a proceder a la identificación de todos los datos personales que se hagan en nuestra empresa, esto es, enfocado en nuestro supuesto:

c.1) Tratamiento de datos de clientes:

Existirán diferentes tratamientos de datos. Uno de ellos será con cada cliente, que deberá darnos autorización para el uso de sus datos personales en las gestiones correspondientes, si los clientes son empresas, que es lo habitual ya que es una asesoría, deberá indicarnos por escrito también, que sus trabajadores le han dado el consentimiento (su propio registro de actividades de tratamiento) para que usemos sus datos para las gestiones, por ejemplo, alta y bajas en la SS, gestión de nóminas, contratos, etc.

TRATAMIENTO DE DATOS DE CLIENTES

Clausula informativa:

El texto que se muestra a continuación deberá incluirlo en todos aquellos formularios que utilice para recabar datos personales de sus clientes, tanto si se realiza en soporte papel como si los recoge a través de un formulario web.

Datos del responsable del tratamiento:

Identidad: Asesoría laboral ASLA, SL - NIF: 74360123-A
Dirección postal: Avd. Ausias March, 5
Teléfono: 625054444 - Correo electrónico: AsesoriaAsla@ASLA.com

"En **ASLA** tratamos la información que nos facilita con el fin de prestarles el servicio solicitado y realizar su facturación. Los datos proporcionados se conservarán mientras se mantenga la relación comercial o durante el tiempo necesario para cumplir con las obligaciones legales y atender las posibles responsabilidades que pudieran derivar del cumplimiento de la finalidad para la que los datos fueron recabados. Los datos no se cederán a terceros salvo en los casos en que exista una obligación legal. Usted tiene derecho a obtener información sobre si en ASLA estamos tratando sus datos personales, por lo que puede ejercer sus derechos de acceso, rectificación, supresión y portabilidad de datos y oposición y limitación a su tratamiento ante **Asesoría laboral ASLA, SL. Avd. Ausias March-5**, adjuntando copia de su DNI o documento equivalente. Asimismo, y especialmente si considera que no ha obtenido satisfacción plena en el ejercicio de sus derechos, podrá presentar una reclamación ante la autoridad nacional de control dirigiéndose a estos efectos a la Agencia Española de Protección de Datos, C/ Jorge Juan, 6 – 28001 Madrid.

Asimismo, solicitamos su autorización para ofrecerle productos y servicios relacionados con los contratados y fidelizarle como cliente."

SI ☐

NO ☐

AVISO: Debe tener en cuenta que, si su cliente marca la opción NO, en ningún caso podrá enviarle publicidad.

Texto 1. Obtenido a través de la web https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd.

TRATAMIENTO DE DATOS DE POTENCIALES CLIENTES

Clausula informativa:

El texto que se muestra a continuación deberá incluirlo en todos aquellos formularios que utilice para recabar datos personales de sus potenciales clientes, tanto si se realiza en soporte papel como si los recoge a través de un formulario web.

Datos del responsable del tratamiento:

Identidad: Asesoría laboral ASLA, SL - NIF: 74360123-A
Dirección postal: Avd. Ausias March, 5
Teléfono: 625054444 - Correo electrónico: AsesoriaAsla@ASLA.com

"En ASLA tratamos la información que nos facilita con el fin de prestarles el servicio solicitado o enviare la información requerida. Los datos proporcionados se conservarán mientras no nos solicite el cese de la actividad. Los datos no se cederán a terceros salvo en los casos en que exista una obligación legal. Usted tiene derecho a obtener información sobre si en ASLA estamos tratando sus datos personales, por lo que puede ejercer sus derechos de acceso, rectificación, supresión y portabilidad de datos y oposición y limitación a su tratamiento ante **Asesoría laboral ASLA, SL. Avd. Ausias March-5**, adjuntando copia de su DNI o documento equivalente. Asimismo, y especialmente si considera que no ha obtenido satisfacción plena en el ejercicio de sus derechos, podrá presentar una reclamación ante la autoridad nacional de control dirigiéndose a estos efectos a la Agencia Española de Protección de Datos, C/ Jorge Juan, 6 – 28001 Madrid.

Asimismo, solicitamos su autorización para enviarle publicidad relacionada con nuestros productos y servicios por cualquier medio (postal, email o teléfono) e invitarles a eventos organizados por la empresa."

SI ☐

NO ☐

AVISO: Si compra datos personales a terceros para realizar publicidad de sus productos y servicios, debe tener en cuenta si proceden de fuentes accesibles al público y están contrastados con la lista Robinson.

AVISO: Recuerde que debe borrar los datos cuando haya trascurrido un tiempo sin hacer uso de los mismos.

Texto 2. Obtenido a través de la web https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd.

c.2) Tratamiento de datos con los empleados:

Otro de ellos, será con nuestros empleados, debemos tener documento de consentimiento para el uso de sus datos ya que haremos nosotros mismos cada gestión que proceda de la relación laboral.

TRATAMIENTO DE DATOS DE EMPLEADOS

Clausula informativa:

El texto que se muestra a continuación deberá incluirlo en todos aquellos formularios que utilice para recabar datos personales de sus empleados, tanto si se realiza en soporte papel como si los recoge a través de un formulario web:

Datos del responsable del tratamiento:

Identidad: Asesoría laboral ASLA, SL - NIF: 74360123-A
Dirección postal: Avd. Ausias March, 5
Teléfono: 625054444 - Correo electrónico: AsesoriaAsla@ASLA.com

"En ASLA tratamos la información que nos facilita con el fin del mantenimiento de la relación laboral. Los datos proporcionados se conservarán mientras se mantenga la relación laboral o durante el tiempo necesario para cumplir con las obligaciones legales y atender las posibles responsabilidades que pudieran derivar del cumplimiento de la finalidad para la que los datos fueron recabados. Los datos no se cederán a terceros salvo en los casos en que exista una obligación legal. Usted tiene derecho a obtener información sobre si en ASLA estamos tratando sus datos personales, por lo que puede ejercer sus derechos de acceso, rectificación, supresión y portabilidad de datos y oposición y limitación a su tratamiento **Asesoría laboral ASLA, SL. Avd. Ausias March-5**, adjuntando copia de su DNI o documento equivalente. Asimismo, y especialmente si considera que no ha obtenido satisfacción plena en el ejercicio de sus derechos, podrá presentar una reclamación ante la autoridad nacional de control dirigiéndose a estos efectos a la Agencia Española de Protección de Datos, C/ Jorge Juan, 6 – 28001 Madrid."

AVISO: Recuerde que debe borrar los datos cuando finalice la relación laboral y no haya ninguna obligación legal para mantenerlos.

Texto 3. Obtenido a través de la web https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd.

c.3) Tratamiento de datos con los candidatos:

También tendremos que realizar el tratamiento de datos con cada persona que quiera entregarnos su curriculum vitae (candidatos), ya sea vía email o en mano (en papel).

A continuación, mostramos un ejemplo de documento que deben firmar los candidatos que deseen entregar su curriculum en nuestra empresa:

TRATAMIENTO DE DATOS DE CANDIDATOS

Clausula informativa:

El texto que se muestra a continuación deberá incluirlo en todos aquellos formularios que utilice para recabar datos personales de los candidatos a un puesto de trabajo, tanto si se realiza en soporte papel como si los recoge a través de un formulario web:

Datos del responsable del tratamiento:

Identidad: Asesoría laboral ASLA, SL - NIF: 74360123-A
Dirección postal: Avd. Ausias March, 5
Teléfono: 625054444 - Correo electrónico: AsesoriaAsla@ASLA.com

"En ASLA tratamos la información que nos facilita con el fin de mantenerle informado de las distintas vacantes a un puesto de trabajo que se produzcan en nuestra organización. Los datos proporcionados se conservarán hasta la adjudicación de un puesto de trabajo o hasta que Ud. ejerza su derecho de supresión. Los datos no se cederán a terceros. Usted tiene derecho a obtener información sobre si en ASLA estamos tratando sus datos personales, por lo que puede ejercer sus derechos de acceso, rectificación, supresión y portabilidad de datos y oposición y limitación a su tratamiento ante **Asesoría laboral ASLA, SL. Avd. Ausias March-5,** adjuntando copia de su DNI o documento equivalente. Asimismo, y especialmente si considera que no ha obtenido satisfacción plena en el ejercicio de sus derechos, podrá presentar una reclamación ante la autoridad nacional de control dirigiéndose a estos efectos a la Agencia Española de Protección de Datos, C/ Jorge Juan, 6 – 28001 Madrid."

AVISO: Si los candidatos aportan su CV en formato papel se les pedirá que firmen un formulario fechado en que figure la información antes citada.

Texto 4. Obtenido a través de la web https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd.

c.4) Contratos con empresas de servicios:

Con las empresas de servicios, estas son, servicio de limpieza, videovigilancia, e informáticos externos, debemos tener un contrato especificando las cláusulas que sean más adecuadas a la relación laboral existente entre la asesoría y las empresas externas, por ejemplo, “cláusulas para prestadores de servicio con acceso a los sistemas informáticos” o “cláusulas de confidencialidad para prestadores de servicios con acceso accidental a los datos”. A continuación, mostramos el ejemplo de uno de los contratos con la empresa de videovigilancia, debemos tener un contrato así con cada empresa externa que trabajemos.

EMPRESAS DE SERVICIOS

Contratos:

AVISO: En su contrato con la empresa que le presta el servicio deberá incluir uno de los siguientes tipos de cláusulas contractuales, en función de si la empresa tiene acceso a los sistemas de información en los que el responsable realiza el tratamiento de datos (proveedores de hosting, prestadores de servicio de correo, mantenimiento informático,…) o si sólo tiene acceso accidental a los datos en virtud del servicio que presta y debe de mantener la confidencialidad de aquella información que pudiera llegar a conocer (empresas de servicio de limpieza, empresas de mantenimiento, …).

A) Cláusulas para prestadores de servicio con acceso a los sistemas de información.

1. Objeto del encargo del tratamiento
Mediante las presentes cláusulas se habilita a **TodoInformatica**, como encargado del tratamiento, para tratar por cuenta de **ASLA**, en calidad de responsable del tratamiento, los datos de carácter personal necesarios para prestar el servicio que en adelante se especifican.

El tratamiento consistirá en Servicios Informáticos.

2. Identificación de la información afectada
Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, la entidad **ASLA** como responsable del tratamiento, pone a disposición de la entidad **TodoInformatica** la información disponible en los equipos informáticos que dan soporte a los tratamientos de datos realizados por el responsable.

3. Duración
El presente acuerdo tiene una duración de **un año**, siendo renovado automáticamente salvo decisión en contra por alguna de las partes.

Una vez finalice el presente contrato, el encargado del tratamiento debe devolver al responsable los datos personales tratados y suprimir cualquier copia que mantenga en su poder. No obstante, podrá mantener bloqueados los datos por el tiempo mínimo necesario para atender posibles responsabilidades que pudieran derivarse de su relación con **ASLA**, destruyéndose de forma segura y definitiva al finalizar dicho plazo.

4. Obligaciones del encargado del tratamiento
El encargado del tratamiento y todo su personal se obliga a:

- ✓ Utilizar los datos personales a los que tenga acceso como consecuencia de la prestación del servicio sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.
- ✓ Tratar los datos de acuerdo con las instrucciones documentadas del responsable del tratamiento. Si el encargado del tratamiento considera que alguna de las instrucciones facilitadas infringe el Reglamento General de Protección de Datos o cualquier otra disposición en materia de protección de datos, el encargado informará inmediatamente al responsable.
- ✓ No comunicar ni difundir los datos a terceros, salvo que cuente con la autorización expresa del responsable del tratamiento o en los supuestos legalmente admisibles. Si el encargado quiere subcontratar, total o parcialmente, los servicios objeto de este contrato, tiene que informar al responsable y solicitar su autorización previa.
- ✓ Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice el contrato.
- ✓ Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que el encargado deberá informarles convenientemente.
- ✓ Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.
- ✓ Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.
- ✓ Notificación de violaciones de la seguridad de los datos:

  El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida y a través de la dirección de correo electrónico que le indique el responsable, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

Asimismo, notificará cualquier fallo que haya sufrido en sus sistemas de tratamiento y gestión de la información y que pueda poner en peligro la seguridad de los datos personales tratados, su integridad o disponibilidad, así como cualquier posible vulneración de la confidencialidad como consecuencia de la puesta en conocimiento de terceros de los datos e informaciones accedidos durante la ejecución del contrato.

Se facilitará, como mínimo, la información siguiente:

a) Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

b) Datos de la persona de contacto para obtener más información.

c) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

d) Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

- ✓ Poner disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para permitir y contribuir a la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.
- ✓ Auxiliar al responsable de tratamiento a implantar las medidas de seguridad necesarias para:

a) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

b) Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

c) Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.

- ✓ Destino de los datos:

El encargado del tratamiento no conservará datos de carácter personal relativos a los tratamientos realizados salvo que sea estrictamente necesario para la prestación del servicio objeto del contrato y solo por el tiempo mínimo imprescindible.

Una vez finalizada la prestación del servicio objeto de contrato, el encargado del tratamiento suprimirá, devolverá al responsable o entregará, en su caso, a un nuevo encargado, según determine ASLA, todos los datos de carácter personal.

No procede la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deben devolverse al responsable que garantizará su conservación, debidamente bloqueados, mientras tal obligación persista.

La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado. No obstante, el encargado puede conservar una copia de los datos, debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de los servicios prestados al responsable del tratamiento.

5. Obligaciones del responsable del tratamiento
Corresponde al responsable del tratamiento:

a) Facilitar al encargado el acceso a los equipos a fin de que pueda prestar el servicio contratado.
b) Velar, de forma previa y durante todo el tratamiento, por el cumplimiento de las disposiciones vigentes en material de protección de datos por parte del encargado del tratamiento.
c) Supervisar el tratamiento, incluida la posibilidad de solicitar información para verificar el cumplimiento de las obligaciones establecidas en el presente contrato.

B) Cláusulas de confidencialidad para prestadores de servicio con acceso accidental a los datos.

AVISO: Deberá incluir está cláusula de confidencialidad como una más dentro del contrato que suscriba con el prestador de servicios.

1. Deber de confidencialidad
La prestación de servicio objeto de este contrato no incluye el tratamiento de datos de carácter personal.

No obstante, en el caso de que el personal de **TodoInformatica,** de forma accidental o accesoria, fuera conocedor de información de datos de carácter personal relativa a las actividades de tratamiento de **ASLA**, vendrán obligados a observar estrictamente el deber de secreto y confidencialidad, tanto durante el transcurso de la relación contractual como una vez extinguida esta,

a) siguiendo en todo momento las indicaciones del personal de **ASLA**
b) no pudiendo utilizar la información a la que hubieran podido tener acceso para ninguna finalidad distinta a la derivada de la prestación de servicio y
c) no pudiendo divulgar, dar a conocer ni utilizar en beneficio propio o de terceros la información que hubieran podido conocer durante la prestación del servicio objeto de este contrato.

AVISO: En su contrato con la empresa que le presta el servicio deberá incluir uno de los siguientes tipos de cláusulas contractuales, en función de si la empresa tiene acceso a los sistemas de información en los que el responsable realiza el tratamiento de datos (proveedores de hosting, prestadores de servicio de correo, mantenimiento informático,…) o si sólo tiene acceso accidental a los datos en virtud del servicio que presta y debe de mantener la confidencialidad de aquella información que pudiera llegar a conocer (empresas de servicio de limpieza, empresas de mantenimiento, …).

Texto 5. Obtenido a través de la web https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd

c.4.a) Información de videovigilancia:

En el anexo de nuestro tratamiento de datos, se especifican los datos que debemos saber sobre todo lo relativo a las cámaras de videovigilancia, los derechos que tienen tanto trabajadores como el resto de personas que son grabadas así como los derecho de acceso a las imágenes.

CAPTACIÓN DE IMÁGENES CON CÁMARAS Y FINALIDAD DE SEGURIDAD (VIDEOVIGILANCIA)

La imagen de una persona, en la medida que la identifique o la pueda identificar, constituye un dato de carácter personal que puede ser objeto de tratamiento para diversas finalidades. Si bien la más común consiste en utilizar las cámaras para garantizar la seguridad de personas, bienes e instalaciones, también pueden usarse con otros fines como el control de la prestación laboral de los trabajadores. A continuación, se incluyen las directrices básicas a respetar para que el tratamiento de las imágenes obtenidas a partir de cámaras de videovigilancia sea conforme a la normativa de protección de datos. No obstante, se recomienda la consulta de la Guía sobre el uso de videocámaras para seguridad y otras finalidades para un conocimiento más exhaustivo de las obligaciones que conlleva este tipo de tratamiento.

- **UBICACIÓN DE LAS CÁMARAS**: Se evitará la captación de imágenes en zonas destinadas al descanso de los trabajadores, así como la captación de la vía pública si se utilizan cámaras exteriores, estando únicamente permitido la captación de la extensión mínima imprescindible para preservar la seguridad de las personas, bienes e instalaciones.

- **UBICACIÓN DE MONITORES**: Los monitores donde se visualicen las imágenes de las cámaras se ubicarán en un espacio de acceso restringido de forma que no sean accesibles a terceros. A las imágenes grabadas sólo accederá el personal autorizado.

- **CONSERVACIÓN DE IMÁGENES**: Las imágenes se almacenarán durante el plazo máximo de un mes, con excepción de las imágenes que acrediten la comisión de actos que atenten contra la integridad de personas, bienes e instalaciones. En ese caso las imágenes deben ser puestas a disposición de la autoridad competente en un plazo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación.

- **DEBER DE INFORMACIÓN**: Se informará acerca de la existencia de las cámaras y grabación de imágenes mediante un distintivo informativo colocado en un lugar suficientemente visible donde se identifique, al menos, la identidad del responsable y la posibilidad de los interesados de ejercer sus derechos en materia de protección de datos. En el propio pictograma se podrá incluir también un código de conexión o dirección de internet en la que se muestre esta información. Dispone de modelos, tanto del pictograma como del texto, en la página web de la Agencia.
    - Modelo de cartel de aviso de zona videovigilada.
- **CONTROL LABORAL**: Cuando las cámaras vayan a ser utilizadas con la finalidad de control laboral según lo previsto en el artículo 20.3 del Estatuto de los Trabajadores, se informará al trabajador y a sus representantes sindicales por cualquier medio que garantice la recepción de la información acerca de las medidas de control establecidas por el empresario con indicación expresa de la finalidad de control laboral de las imágenes captadas por las cámaras.

- **DERECHO DE ACCESO A LAS IMÁGENES**: Para dar cumplimiento al derecho de acceso de los interesados a las grabaciones del sistema de videovigilancia se solicitará una fotografía reciente y el Documento Nacional de Identidad del interesado para comprobar su identidad, así como el detalle de la fecha y hora a la que se refiere el derecho de acceso. No se facilitará al interesado acceso directo a las imágenes de las cámaras en las que se muestren imágenes de terceros. En caso de no ser posible la visualización de las imágenes por el interesado sin mostrar imágenes de terceros, se le facilitará un documento en el que se confirme o niegue la existencia de imágenes del interesado.

Para más información puede consultar las guía y las fichas de videovigilancia y los informes jurídicos publicados por la Agencia Española de Protección de Datos en la sección de Videovigilancia.

Texto 6. Obtenido a través de la web https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd

Junto con las plantillas que nos incluyen en el tratamiento de datos para realizar todos los contratos, tratamientos de datos, etc, nos adjuntan el cartel de videovigilancia. Debemos poner uno junto a cada cámara de seguridad que tengamos en nuestras instalaciones, ya que es obligatorio informar a los clientes de que existen dichas cámaras de seguridad.

ZONA VIDEOVIGILADA

RESPONSABLE:

Asesoría laboral ASLA, SL. – 74360123-A

PUEDE EJERCITAR SUS DERECHOS DE PROTECCIÓN DE DATOS ANTE:

Asesoría laboral ASLA, SL.
Avd. Ausias March, 5

MÁS INFORMACIÓN SOBRE EL TRATAMIENTO DE SUS DATOS PERSONALES:

Finalidad del tratamiento: seguridad de las personas, bienes e instalaciones.
Interesados: Personas que acceden o intentan acceder a las instalaciones.
Destinatarios: Fuerzas y Cuerpos de Seguridad.
Plazo de conservación: 1 mes desde la captación

Imagen 4. Obtenida a través de la web https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd.

c.5) Registro de actividades de tratamiento:

También contaremos con un registro de actividades de tratamiento, que es más específico. En el tratamiento de datos tan solo nos dan consentimiento, y en el registro se especifica cada aspecto de la relación entre la asesoría y los clientes, empleados, candidatos y videovigilancia.

En dicho registro se indica:

- Quien es el responsable del tratamiento y su identificación.
- La finalidad del tratamiento.
- Que categoría cumple el interesado.
- Que categoría tienen los datos.
- las categorías de destinatarios.
- Si existen transferencias internacionales.
- Plazo de supresión.
- Medidas de seguridad.

A continuación, mostramos dos ejemplos de registro de actividad que deberá tener nuestra empresa, uno de clientes y otro de empleados

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

El responsable del tratamiento debe revisar los datos consignados en los apartados de los Registros de Actividades de Tratamiento generados y verificar que se corresponden con las circunstancias exactas de los datos recogidos, las comunicaciones realizadas y demás condiciones de cada uno de los tratamientos.

Tratamiento: **Clientes**

a) Responsable del tratamiento	Identidad: Asesoría laboral ASLA, SL - NIF: 74360123-A Dirección postal: Avd. Ausias March, 5 Teléfono: 625054444 Correo electrónico: AsesoriaAsla@ASLA.com
b) Finalidad del tratamiento	Gestión de la relación con los clientes
c) Categorías de interesados	Clientes: Personas con las que se mantiene una relación comercial como clientes
d) Categorías de datos	Los necesarios para el mantenimiento de la relación comercial. Facturar De identificación: nombre y apellidos, NIF, dirección postal, teléfonos, e-mail Características personales: estado civil, fecha y lugar de nacimiento, edad, sexo, nacionalidad Datos académicos Datos bancarios: para la domiciliación de pagos
e) Categorías de destinatarios	Agencia Estatal de Administración Tributaria Instituto Nacional de la Seguridad Social Bancos y entidades financieras
f) Transferencias internacionales	No está previsto realizar transferencias internacionales
g) Plazo de supresión	Los previstos por la legislación fiscal respecto a la prescripción de responsabilidades
h) Medidas de seguridad	Las reflejadas en el ANEXO MEDIDAS DE SEGURIDAD

Texto 7. Obtenido a través de la web https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

El responsable del tratamiento debe revisar los datos consignados en los apartados de los Registros de Actividades de Tratamiento generados y verificar que se corresponden con las circunstancias exactas de los datos recogidos, las comunicaciones realizadas y demás condiciones de cada uno de los tratamientos.

Tratamiento: **Empleados**

a) Responsable del tratamiento	Identidad: Asesoría laboral ASLA, SL - NIF: 74360123-A Dirección postal: Avd. Ausias March, 5 Teléfono: 625054444 Correo electrónico: AsesoriaAsla@ASLA.com
b) Finalidad del tratamiento	Gestión de la relación laboral con los empleados
c) Categorías de interesados	Empleados: Personas que trabajan para el responsable del tratamiento
d) Categorías de datos	Los necesarios para el mantenimiento de la relación comercial. Gestionar la nómina, formación De identificación: nombre, apellidos, número de Seguridad Social, dirección postal, teléfonos, e-mail Características personales: estado civil, fecha y lugar de nacimiento, edad, sexo, nacionalidad y porcentaje de minusvalía Datos académicos Datos profesionales Datos bancarios, para la domiciliación del pago de las nóminas
e) Categorías de destinatarios	Agencia Estatal de Administración Tributaria Instituto Nacional de la Seguridad Social Bancos y entidades financieras Servicio Público de Empleo Estatal [Otros posibles destinatarios]
f) Transferencias internacionales	No está previsto realizar transferencias internacionales
g) Plazo de supresión	Los previstos por la legislación fiscal y laboral respecto a la prescripción de responsabilidades
h) Medidas de seguridad	Las reflejadas en el ANEXO MEDIDAS DE SEGURIDAD

Texto 8. Obtenido a través de la web https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd

d) INFORMACIÓN Y CONSENTIMIENTO DE LOS INTERESADOS:

La información y consentimiento de los interesados, estos son: clientes, empleados y candidatos, se hará en el momento en que recopilamos los datos personales y se informará de todos los datos existentes en los registros de actividad de tratamiento.

Es muy importante que los interesados sean conscientes de todos sus derechos, los denominados “Derechos ARCO” (que desarrollaremos a continuación) y que el consentimiento sea libre, especifico, informado, inequívoco y afirmativo, no sirve el consentimiento por omisión, es decir, no es válido el consentimiento que surge de la no contestación o si el cliente no ha manifestado su negatividad hacia el uso de sus datos, es obligatorio que consienta dicho uso.

DERECHOS ARCO: Los denominados Derechos ARCO, son los que recogía anteriormente la normativa española y son los derechos de Acceso, Rectificación, Cancelación y Oposición. Actualmente, el RGPD recoge los mismos derechos, denominando el de cancelación como de supresión y ampliando con tres derechos más, el derecho al Olvido (que va unido al de supresión), derecho a la Portabilidad y el derecho a la Limitación en el Tratamiento.

En la siguiente imagen se ve más claramente los derechos que vienen de la antigua normativa, LOPD, y los que se incluyen en la última normativa, RGPD:

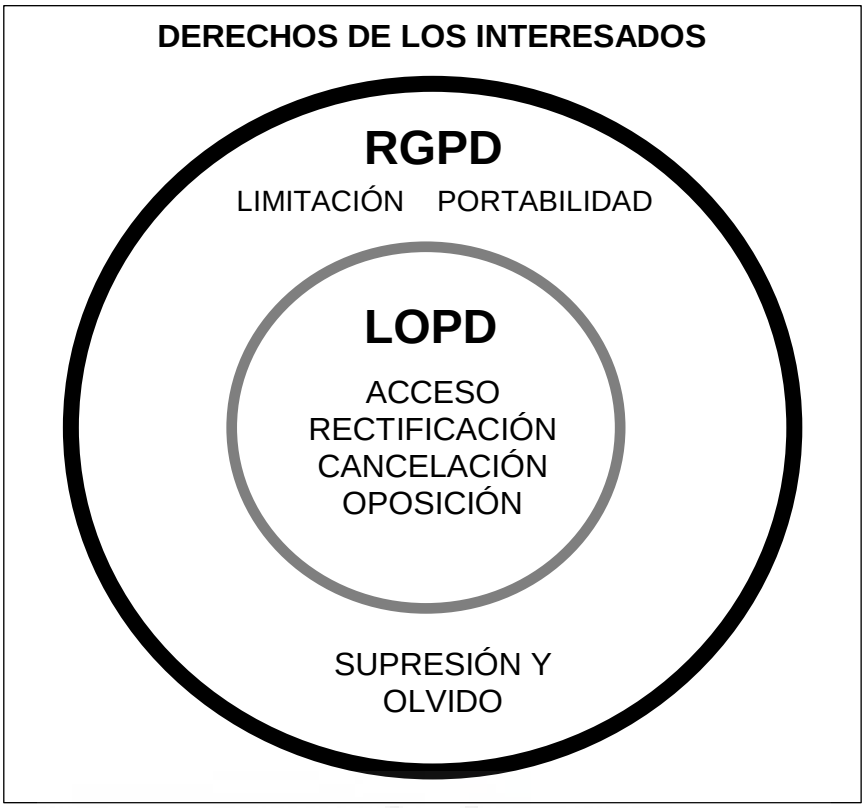

IMAGEN DEL LIBRO: “Protección de datos. Aplicación del RGPD”
Autor: Francis Lefebvre -- Página: 65

Derecho de acceso: esto quiere decir, que el interesado tendrá derecho a ser informado de si sus datos personales están siendo usados, en caso de que su uso se confirme, el encargado del tratamiento tendrá la obligación de darle acceso a sus datos, informarle de la finalidad con la que se están usando, cual es el origen de la obtención de los datos y si se han realizado comunicaciones de los mismos.

Esta información se debe proporcionar en un plazo máximo de 30 días desde que se recibió la solicitud y tras la resolución, el interesado dispondrá de 10 días hábiles para realizar el acceso.

Una vez obtenido el acceso, el encargado del tratamiento deberá proporcionarle toda aquella información que precise y/o desee saber el interesado sin poder oponerse.

- Derecho de rectificación: El interesado tendrá derecho a solicitarle al responsable del tratamiento que sus datos sean modificados en caso de que exista algún tipo de error, ya sea porque son inexactos o incompletos, deberá hacerse por medio de una “declaración rectificativa adicional” y

una vez recibida la solicitud, el responsable dispondrá de 10 días hábiles para dar una resolución.

En caso de que haya habido alguna “comunicación previa de datos de destinatarios”, también habrá que informar a estos para que lleven a cabo la modificación de los datos.

- Derecho de supresión y olvido: Este derecho es una versión mejorada del derecho de cancelación. Este derecho tiene el objetivo de que el interesado pueda pedir a las empresas/compañías que supriman sus datos personales.

  El interesado podrá solicitar la supresión de sus datos cuando el “tratamiento sea ilícito, el interesado haya retirado su consentimiento”, cuando los datos recogidos “ya no sean necesarios en relación con los fines que fueron recogidos o trataos”, cuando “los datos se hayan obtenido en relación con la oferta de servicios de la sociedad de la información, y el interesado haya ejercido el derecho de oposición al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento.

  El responsable tendrá un máximo de 10 días hábiles para dar resolución a la solicitud de supresión y olvido.

  En caso de que existiera “comunicación previa de datos a destinatarios”, a estos también se les comunicara la obligación de supresión de los datos en caso de que proceda.

  Hay situaciones en las que el interesado no tendrá derecho a que sus datos se supriman, estos son: “para ejercer el derecho a la libertad de expresión e información”, cuando sean necesarios “para cumplir una obligación jurídica del responsable del tratamiento”, “para la formulación, ejercicio o defensa de reclamaciones”, y en los casos de que sea “por interés público fundamentado en la legislación vigente, esto es: por razones de salud pública y para fines de investigación histórica, estadística o científica”.

- Derecho a la portabilidad: Derecho a la portabilidad de los datos personales de los interesados.

  Los interesados tienen derecho a solicitar a los responsables de tratamiento que trasmitan sus datos a otros responsables de tratamientos, dicha transmisión deberá hacerse por medio de un formato claro y

estructurado, de “uso habitual y lectura mecánica”, “cuando el tratamiento se efectúe por medios automatizados y base a:

- el consentimiento del interesado para fines específicos; o
- la ejecución de un contrato o precontrato con el interesado”

No se aplicará el derecho a portabilidad cuando:

- “sea técnicamente imposible la transmisión;
- Pueda afectar negativamente a los derechos y libertades de terceros; o
- El tratamiento tenga una misión de interés público, fundamentado en la legislación vigente”.

- Derecho de Limitación: Derecho a la limitación del tratamiento por parte del responsable del tratamiento.

  El interesado tendrá derecho a solicitar la limitación del tratamiento de datos cuando: “impugne la exactitud de sus datos”, “el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos y solicite en su lugar la limitación de su uso”, “el interesado se ha opuesto al tratamiento, mientras se verifica si los motivos legítimos del responsable del tratamiento prevalecen sobre los del interesado”, “el responsable ya no necesite los datos para los fines del tratamiento pero el interesado los necesite para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial”.

  Una vez que el tratamiento se ha limitado, no se podrá levantar dicha limitación, así como así, para poder hacerlo, se deberá comunicar previamente al interesado, y siempre que se de algunos de los siguientes casos: “el consentimiento del interesado”, “la posibilidad de que el tratamiento afecte a la protección de los derechos de otra persona física o jurídica”, “un procedimiento judicial que lo justifique”, “un motivo importante de interés público fundamentado en la legislación vigente”.

  Si se ha dado el caso de que los datos se han comunicado a terceros, el responsable deberá informar a esos terceros para que lambien apliquen la limitación del tratamiento.

- Derecho de oposición: Derecho de oposición al tratamiento de datos personales o incluso a su cese en algunos casos.

El interesado podrá oponerse al tratamiento de datos del responsable del tratamiento cuando los motivos sean por su situación particular o cuando el tratamiento esté basado en:

- “mercadotecnia directa;
- Interés legítimo del responsable del tratamiento o terceros, siempre que no se prevalezcan los intereses o los derechos y libertades del interesado, especialmente si es un menos; o
- Investigación histórica, estadística o científica, salvo que el tratamiento sea necesario por motivos de interés público”.

Hay casos en los que el responsable puede seguir tratando los datos, aunque el interesado quiera ejercer el derecho a oposición, esto será cuando “el interés legítimo del responsable del tratamiento impere sobre los intereses o los derechos y libertades del interesado en un procedimiento judicial que lo justifique”.

En estos casos el responsable tiene la obligación de dar aviso al interesado de los datos personales, debe hacerlo de forma clara, explícita y separada de otra información, mínimo, en la primera comunicación.

Se dará el caso de cese de los datos en los casos:

- “Que no sea necesario su consentimiento,
- En los que los ficheros se usen con finalidades publicitarias,
- O que el tratamiento tenga por finalidad la adopción de una decisión referida al afectado”.

Deben constar “los motivos fundados y legítimos”, referentes a una situación personal concreta del interesado y que pueda justificar el uso de este derecho.

Una vez puesta la reclamación con la solicitud del ejercicio del derecho, el responsable del tratamiento dispondrá de 10 días hábiles para dar una resolución.

El contenido de los derechos de los interesados se especificará en el anexo de nuestro registro de actividad de tratamiento.

Incluyendo un formulario para el ejercicio de cada derecho. A continuación, mostramos el formulario:

EJERCICIO DEL DERECHO DE ACCESO

DATOS DEL RESPONSABLE DEL TRATAMIENTO.

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de acceso: C/Plaza ..... nº ..... C.Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma .....

DATOS DEL AFECTADO O REPRESENTANTE LEGAL.

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., con correo electrónico……..por medio del presente escrito ejerce el derecho de acceso, de conformidad con lo previsto en el artículo 15 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).

SOLICITA

Que se le facilite gratuitamente el derecho de acceso por ese responsable en el plazo de un mes a contar desde la recepción de esta solicitud, y que se remita, a la dirección arriba indicada, la siguiente información: -Copia de mis datos personales que son objeto de tratamiento por ese responsable. -Los fines del tratamiento así como las categorías de datos personales que se traten. -Los destinatarios o categorías de destinarios a los que se han comunicado mis datos personales, o serán comunicados, incluyendo, en su caso, destinatarios en terceros u organizaciones internacionales. -Información sobre las garantías adecuadas relativas a la transferencia de mis datos a un tercer país o a una organización internacional, en su caso. -El plazo previsto de conservación, o de no ser posible, los criterios para determinar este plazo. -Si existen decisiones automatizadas, incluyendo la elaboración de perfiles, información significativa sobre la lógica aplicada, así como la importancia y consecuencias previstas de dicho tratamiento. -Si mis datos personales no se han obtenido directamente de mí, la información disponible sobre su origen. -La existencia del derecho a solicitar la rectificación, supresión o limitación del tratamiento de mis datos personales, o a oponerme a dicho tratamiento. -El derecho a presentar una reclamación ante una autoridad de control.

En .....a.....de.....de 20.....

Firmado

Texto 9. Obtenido a través de la web https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd

e) MEDIDAS DE SEGURIDAD MÍNIMAS:

En el anexo de nuestro registro de actividad del tratamiento, también se especifican las medidas de seguridad mínimas a tener en cuenta, en ellas están incluidas las organizativas y las técnicas, ambas desarrollas en los textos descritos a continuación en el apartado del anexo del tratamiento de datos:

MEDIDAS DE SEGURIDAD

A tenor del tipo de tratamiento que ha puesto de manifiesto cuando ha cumplimentado este formulario, las medidas de seguridad mínimas que debería tener en cuenta son las siguientes:

MEDIDAS ORGANIZATIVAS

INFORMACIÓN QUE DEBERÁ SER CONOCIDA POR TODO EL PERSONAL CON ACCESO A DATOS PERSONALES

Todo el personal con acceso a los datos personales deberá tener conocimiento de sus obligaciones con relación a los tratamientos de datos personales y serán informados acerca de dichas obligaciones. La información mínima que será conocida por todo el personal será la siguiente:

- DEBER DE CONFIDENCIALIDAD Y SECRETO
    - Se deberá evitar el acceso de personas no autorizadas a los datos personales. A tal fin se evitará dejar los datos personales expuestos a terceros (pantallas electrónicas desatendidas, documentos en papel en zonas de acceso público, soportes con datos personales, etc.). Esta consideración incluye las pantallas que se utilicen para la visualización de imágenes del sistema de videovigilancia. Cuando se ausente del puesto de trabajo, se procederá al bloqueo de la pantalla o al cierre de la sesión.
    - Los documentos en papel y soportes electrónicos se almacenarán en lugar seguro (armarios o estancias de acceso restringido) durante las 24 horas del día.
    - No se desecharán documentos o soportes electrónicos (cd, pen drives, discos duros, etc.) con datos personales sin garantizar su destrucción efectiva
    - No se comunicarán datos personales o cualquier otra información de carácter personal a terceros, prestando especial atención a no divulgar datos personales protegidos durante las consultas telefónicas, correos electrónicos, etc.
    - El deber de secreto y confidencialidad persiste incluso cuando finalice la relación laboral del trabajador con la empresa.

- VIOLACIONES DE SEGURIDAD DE DATOS DE CARÁCTER PERSONAL
    - Cuando se produzcan violaciones de seguridad de datos de carácter personal como, por ejemplo, el robo o acceso indebido a los datos personales se notificará a la Agencia Española de Protección de Datos en término de 72 horas acerca de dichas violaciones de seguridad, incluyendo toda la información necesaria para el esclarecimiento de los hechos que hubieran dado lugar al acceso indebido a los datos personales. La notificación 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/sede-electronica-web/.

MEDIDAS TÉCNICAS

IDENTIFICACIÓN

- Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal se recomienda disponer de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesional y personal del ordenador.
- Se recomienda disponer de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.
- Se garantizará la existencia de contraseñas para el acceso a los datos personales almacenados en sistemas electrónicos. La contraseña tendrá al menos 8 caracteres, mezcla de números y letras.
- Cuando a los datos personales accedan distintas personas, para cada persona con acceso a los datos personales, se dispondrá de un usuario y contraseña específicos (identificación inequívoca).
- Se debe garantizar la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. Para la gestión de las contraseñas puede consultar la guía de privacidad y seguridad en internet de la Agencia Española de Protección de Datos y el Instituto Nacional de Ciberseguridad. En ningún caso se compartirán las contraseñas ni se dejarán anotadas en lugar común y el acceso de personas distintas del usuario.

DEBER DE SALVAGUARDA

A continuación, se exponen las medidas técnicas mínimas para garantizar la salvaguarda de los datos personales:

- **ACTUALIZACIÓN DE ORDENADORES Y DISPOSITIVOS**: Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la media posible.
- **MALWARE**: En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema de antivirus que garantice en la medida posible el robo y destrucción de la información y datos personales. El sistema de antivirus deberá ser actualizado de forma periódica.
- **CORTAFUEGOS O FIREWALL**: Para evitar accesos remotos indebidos a los datos personales se velará por garantizar la existencia de un firewall activado y correctamente configurado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales.
- **CIFRADO DE DATOS**: Cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos, se deberá valorar la posibilidad de utilizar un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.
- **COPIA DE SEGURIDAD**: Periódicamente se realizará una copia de seguridad en un segundo soporte distinto del que se utiliza para el trabajo diario. La copia se almacenará en lugar seguro, distinto de aquél en que esté ubicado el ordenador con los ficheros originales, con el fin de permitir la recuperación de los datos personales en caso de pérdida de la información.

Las medidas de seguridad serán revisadas de forma periódica, la revisión podrá realizarse por mecanismos automáticos (software o programas informáticos) o de forma manual. Considere que cualquier incidente de seguridad informática que le haya ocurrido a cualquier conocido le puede ocurrir a usted, y prevéngase contra el mismo.

Si desea más información u orientaciones técnicas para garantizar la seguridad de los datos personales y la información que trata su empresa, el Instituto Nacional de Ciberseguridad (INCIBE) en su página web www.incibe.es, pone a su disposición herramientas con enfoque empresarial en su sección «Protege tu empresa» donde, entre otros servicios, dispone de:

- un apartado de formación con un videojuego, retos para respuesta a incidentes y videos interactivos de formación sectorial,
- un Kit de concienciación para empleados,
- diversas herramientas para ayudar a la empresa a mejorar su ciberseguridad, entre ellas políticas para el empresario, el personal técnico y el empleado, un catálogo de empresas y soluciones de seguridad y una herramienta de análisis de riesgos.
- dosieres temáticos complementados con videos e infografías y otros recursos,
- guías para el empresario,

Además INCIBE, a través de la Oficina de Seguridad del Internauta, pone también a su disposición herramientas informáticas gratuitas e información adicional pueden ser de utilidad para su empresa o su actividad profesional.

Texto 10. Obtenido a través de la web https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd

Conclusión:

Con la realización de este trabajo fin de grado, he tenido la oportunidad de estudiar la normativa actual que existe sobre la protección de los datos personales que hay actualmente en España.

Hasta hace unos años, existía una normativa escueta sobre el tema, la cual no podía cubrir las necesidades que se han creado en la actualidad debido al gran crecimiento tecnológico y la globalización. Con la actual ley de RGPD, nuestro país entra a formar parte de la normativa más actualizada que hay actualmente para la protección de nuestros datos.

En la actualidad, aún hay empresas que no cumplen con la normativa del RGPD, algunas están aún acogidas a la antigua ley que existía en España, la LOPD la cual debía ser modificada y adaptada con la entrada en vigor del RGPD, aunque la gran mayoría, ya están sujetas al RGPD.

Actualmente, existe un gran control sobre el cumplimiento de la normativa y el no cumplimiento de esta, supone multas de altos importes lo que hace que las empresas se motiven a su cumplimiento, dicho sea, también, que para las pequeñas empresas, a veces, es algo complicado el seguir esta normativa bien por el gasto económico, bien por el desarrollo que en ocasiones es algo engorroso de cumplir.

En mi opinión, considero que esta normativa cubre muy ampliamente todo lo relativo a regulación y protección del tratamiento de datos personales de los usuarios, pero claro está, siempre podrá ser mejorado si la ley va actualizándose a la par que se va desarrollando cada vez más el uso de datos personales por las empresas.

Bibliografía:

- Webs:

Autor: Ayuda Ley Protección Datos.
Título del articulo/apartado: Protección de datos para Asesorías
Consultado: 8 y 11 de junio de 2020
https://ayudaleyprotecciondatos.es/2018/07/25/rgpd-asesoria/#Modelos

Autor: Agencia española protección datos
Título del articulo/apartado: Elabora el registro de actividades de tratamiento
Consultado: 14, 16, 25 y 26 de mayo de 2020
https://www.aepd.es/es/prensa-y-comunicacion/blog/elaborar-el-registro-de-actividades-de-tratamiento

Autor: binapsys. Garantía de continuidad
Título del articulo/apartado: Evolución de la protección de datos en España
Consultado: 28 junio de 2020
https://blog.binapsys.com/evolucion-de-la-proteccion-de-datos-en-espana/

Autor: Iberley
Título del articulo/apartado: Objeto y ámbito de aplicación del Reglamento General de protección de Datos (RGPD) y de la LO 3/2018 de 5 de diciembre de protección de datos (LOPDGDD)
Consultado: 26 de mayo y 16 de junio de 2020
https://www.iberley.es/temas/objeto-ambito-aplicacion-rgpd-lopdgdd-62715

Autor: Escuela de Negocios y Dirección. Business Review
Título del articulo/apartado: Conoce las 9 novedades en el RGPD a partir del 25 de mayo
Fecha de publicación: 12 de abril de 2018
Consultado: 15, 16 y 20 de junio de 2020
https://br.escueladenegociosydireccion.com/business/marketing-digital/conoce-las-9-novedades-en-el-rgpd-a-partir-del-25-de-mayo/

Autor: Autoridad Catalana de Protección de Datos
Título del articulo/apartado: Principales novedades del RGPD
Consultado: 15 y 16 de mayo de 2020 y 7, 8 y 9 de junio de 2020
https://apdcat.gencat.cat/es/documentacio/RGPD/novetats/

Autor: Web oficial de la UE
Título del articulo/apartado: ¿Qué significa la protección de datos “desde el diseño” y “por defecto”?
Consultado: 16 y 27 de mayo de 2020 y 8,9, 11 y 16 de junio de 2020
https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_es

Autor: Agencia española de protección de datos. Facilita 2.0
Título del articulo/apartado: Herramienta para ejecución de tratamiento de datos
Consultado: 4, 7, 8, 9, 16, 20 y 25 de junio de 2020
https://servicios.aepd.es/AEPD/view/form/MDAwMDAwMDAwMDAwMDI3NjU1MzYxNTk1OTI3NTE1NTY0?updated=true

Autor: Grupo Ático 34
Título del articulo/apartado: Derechos ARCO, ¿qué son?
Fecha publicación: 21 de enero de 2018
Consultado: 26 de mayo de 2020 y 21 de junio de 2020
https://protecciondatos-lopd.com/empresas/derechos-arco-que-son/

- Libro:

Libro: “Protección de datos. Aplicación del RGPD”

Año de publicación: 2018

Autor: Francis Lefebvre

- TFG:

TRABAJO FIN DE GRADO; Grado en Ingeniería Informática
Aplicación y Guía de la L.O.P.D. en Clínica Dental
Autor: D. David Martín Hernández
Tutor: D. Pablo de la Fuente Redondo