UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería Informática

Gestión de la protección de datos para aplicaciones Android / iOS

Trabajo Fin de Grado

Grado en Ingeniería Informática

AUTOR/A: Domingo Parra, José

Tutor/a: Oltra Gutiérrez, Juan Vicente

CURSO ACADÉMICO: 2022/2023

Resumen

En este trabajo de final de grado vamos a trabajar sobre sobre la importancia de los datos personales de cada persona y como ante el creciente uso de aplicaciones móviles, tanto en Android como en iOS, debemos tener unos mecanismos y así pues una gestión acorde a las leyes europeas y españolas para la correcta protección de los datos

Palabras clave: Protección de Datos; Grupo 29; App; LOPD, Datos personales, protección

Abstract

In this final degree project, we are going to work on the importance of the personal data of each person and how, given the growing use of mobile applications, both on Android and iOS we must have mechanisms and management in accordance with European laws and Spanish for the correct protection of data.

Keywords : Data Protecction; Group 29; App; LOPD, personal data, protection

Tabla de contenidos

Contenido

1. Introducción 5
2. Motivación 5
3. Estado del arte y Crítica 7
4. Asignaturas relacionadas 7
5. Metodología 8
6. Tiempos empleados en el desarrollo del TFG 9
7. Ámbito objetivo y subjetivo de la Ley Orgánica 3/2018 9
8. Términos referentes a Protección de datos 11
9. Personas físicas 13
10. Personas Jurídicas 15
11. Responsable del tratamiento de datos y Encargado del tratamiento de datos 15
12. Agencias de protección de Datos 17
13. Derechos específicos de las personas físicas en materia de Protección de Datos y su ejercicio 19

13.2 Derecho de rectificación 20
13.3 Derecho de supresión 20
13.4 Derecho a la limitación del tratamiento 21
13.5 Derecho a la portabilidad de los datos 22
13.6 Derecho de Oposición 22
13.7 Procedimientos reglamentarios para ejercitar los derechos 23

14. Gestión de datos personales en aplicaciones Android/iOS 24
15. Conclusiones 43
16. Bibliografía 44

1. Introducción

En el año 2022 pudimos observar que el 99,2% de la población entre 16 y 74 años han utilizado un dispositivo móvil en 2022[1]. Sabiendo estos datos, es normal que nos surjan dudas sobre si nuestros datos personales están a salvo o no. Para ello se va a realizar un estudio sobre que son los datos personales, que figuras intervienen en la protección de datos y como las aplicaciones de Android e iOS deben estar programadas y configuradas acorde a las distintas leyes existentes. A su vez daremos unas herramientas para asegurarnos de que todo se cumple y un análisis de futuros estudios y como pueden afectar las nuevas tecnologías a la protección de datos.

2. Motivación

Mi motivación al elegir este Trabajo Final de Grado es como he comentado anteriormente que cada día más gente utiliza dispositivos móviles, y los datos personales de cada uno son lo más preciado que tenemos, pues imagínate que, por instalarte una aplicación bancaria, el banco pudiera tener acceso a todo tu historial medico y a las conversaciones que tienes.

Para ello tanto la UE como España han tenido que desarrollar una serie de Leyes y Reglamentos que regulen estas actividades, y en los últimos años han sido mucho los cambios ya que las tecnologías también han crecido a pasos agigantados y esto hace que me parezca un tema muy versátil y con mucho trayecto aun por recorrer.

Por otro lado, mi carrera profesional se está enfocando hacia la calidad de producto y la rama de Tester. Por tanto, para poder asegurar una buena calidad de producto debo saber, estudiar y comprobar que las leyes de protección de datos se cumplen en todo momento, y que, a la hora de dar soporte al usuario, poder referirles correctamente a sus datos o a la persona encargada de tratarlos, haciendo así una aplicación mucho más robusta y de mayor calidad.

Por todo ello, mi intención con este trabajo es hacer una guía actualizada para los desarrolladores y empresas explicando cuales son los derechos actuales de protección de datos y como afectan al desarrollo de las aplicaciones en Android e iOS.

[1] INE, Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación (TIC) en los Hogares Año 2022

Igualmente, la intención es crear un conjunto de herramientas para que a la hora de desarrollar una aplicación no se nos pase absolutamente nada y poder tener claro los pasos a seguir a la hora del desarrollo.

Profesionalmente estas herramientas nos van a ayudar a cumplir con las actuales normativas de protección de forma más fácil y efectiva.

En el trabajo se va a analizar la regulación de la protección de datos de carácter personal en España.

En primer lugar, es necesario tener en cuenta la estrecha relación existente entre el derecho al honor y a la intimidad, tal como se establece en el artículo 18.1 de la Constitución Española. Una vez que comprendamos claramente esta conexión, procederemos a examinar la Ley Orgánica 3/2018, de 5 de diciembre, relativa a la protección de datos personales y garantías de los derechos digitales, así como el Reglamento (UE) 2016/679. Además, también se hará mención de la Ley Orgánica anterior de protección de datos para observar su evolución, es decir, la Ley Orgánica 15/1999, de 13 de diciembre, y al Real Decreto 1720/2007, de 21 de diciembre, que aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre.

Se va a explorar el ámbito objetivo de aplicación de la protección de datos, es decir, qué datos se incluyen y cuáles quedan excluidos. En segundo lugar, detallaremos la normativa que afecta a la protección de datos tanto para personas físicas como jurídicas, incluyendo el proceso de obtención de consentimiento para el tratamiento de datos, y subrayando las diferencias entre menores y adultos en lo que respecta a la obtención de dicho consentimiento. También, abordaremos las figuras del responsable del tratamiento de datos y del encargado del tratamiento de datos. Finalmente, examinaremos la Agencia Española de Protección de Datos, su marco regulatorio y sus funciones principales, con especial énfasis en su papel en la garantía del cumplimiento de la ley.

Tras estudiar y analizar lo anterior, enfocaremos el estudio hacia el análisis de los derechos de las personas sobre la protección de datos. Se estudiarán los derechos PARSOL (Portabilidad, Acceso, Rectificación, Supresión, Supresión y Limitación del acceso). Después, ya dentro de cada uno de los derechos describiremos su concepto y el modo y plazo para ejercerlos.

Continuaremos analizando los derechos por separado, estudiaremos la forma de ejercer estos derechos ante el responsable de tratamiento de datos y el procedimiento para ejercerlo ante la Agencia Española de Protección de datos.

Para terminar este trabajo haremos un resumen de los factores a tener en cuenta a la hora de desarrollar las aplicaciones y como asegurarnos que cumplimos con todos los puntos de la ley de protección de datos, así como relacionando cada punto anterior con alguna experiencia profesional y/o ejemplo comparativo en distintos campos de la forma de aplicación de la protección de datos

3. Estado del arte y Crítica

El estado del arte actual de la protección de datos es muy cambiante, igual que las nuevas tecnologías, ya que estas segundas están obligando a adaptar las leyes para proteger a todos los individuos y que nuestros datos estén siempre asegurados, para que nos hagamos una idea, la evolución en esta materia empieza en 1992 con la LORTAD, ley orgánica de 29 de octubre, 7 años después en 1999 surgió su primera evolución la LOPD, la Ley Orgánica de 13 de diciembre a la cual haremos referencia varias veces durante el estudio, en 2007 salió el RDLOPD, Real Decreto 1720/2007 que fue el real decreto que aprobó y desarrollo la LOPD como hemos comentado anteriormente. En 2016 surgió el RGPD, se aprueba el Reglamento General de Protección de datos a nivel europeo para homogeneizar la normativa europea sobre protección de datos, siendo Aprobada y desarrollada en 2017 con PLOPD, Proyecto de Ley Orgánica de Protección de datos. Y el 25 de mayo de 2018 el RGPD pasa a ser aplicable. Aun no hay una nueva normativa desarrollada, pero los expertos dicen que ya vamos tardes, pues hay nuevas tecnologías que ponen a prueba estos datos personales.

Para el desarrollo de este trabajo nos vamos a fijar como ya he mencionado en la Ley Orgánica de Protección de Datos y en el Reglamento General de Protección de Datos anteriormente mencionados, Así como las distintas guías que pone a nuestra disposición la AEPD, como su marco organizativo y régimen jurídico, o la explicación más sencilla que tiene de explicar los distintos Derechos que tenemos.

Igualmente consultaremos distintos BOE como el número 294 de 06/12/2018 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, como también el BOE número 298, de 14 de diciembre de 1999: Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de Carácter Personal.

4. Asignaturas relacionadas

Al tratarse de un Trabajo Final de Grado relacionado con la rama de Sistemas de la Información es lógico que esté relacionado con asignaturas del departamento de organización de empresas, en especial está muy ligada a Deontología y Profesionalismo y Gestión de las tecnologías de la información ya que las leyes de protección de datos son de obligatorio cumplimiento para cualquier empresa.

5. Metodología

La metodología utilizada para desarrollar este trabajo ha sido la del estudio del Derecho y la jurisprudencia de las distintas leyes de protección de datos, así como el análisis de como afecta al desarrollo de nuevas aplicaciones para dispositivos Android e iOS.

Esta metodología consiste en estudiar y analizar las distintas normativas tanto a nivel legislativo español como a nivel legislativo europeo y analizar cómo se adaptarían a nuestro campo. Esto quiere decir que deberemos adaptarla con lenguaje más científico y técnico con tal de acercar y facilitar la comprensión y aplicación de de estas leyes al profesional y poder implementarlas correctamente.

Comenzaremos nuestro enfoque a partir de la recopilación, actualización y clasificación exhaustiva de toda la normativa vigente. Desde la perspectiva de la aplicación territorial del Derecho, nos centraremos en la legislación directamente aplicable en el territorio español. Esta legislación abarca desde las disposiciones más generales, como las leyes orgánicas, los Reglamentos comunitarios y las Directivas, hasta las disposiciones reglamentarias y de aplicación, como los Reales Decretos y las Órdenes Ministeriales.

Posteriormente se va a estudiar y analizar jurídicamente la norma en vigor y que nos afecta ahora mismo, teniendo como fin la extracción de conclusiones sobre aplicación concreta y medidas que debemos tomar al programar nuestras aplicaciones. En esta fase es donde se consultará y revisarán otros recursos bibliográficos (Documentación de la Unión Europea, Actas de congresos, B.O.E., etc.).

El siguiente paso consiste en juntar todos los datos obtenidos previamente y realizar propuestas para comprender la regulación y poderla aplicar a nuestros futuros proyectos en el campo de la programación. Para ello también se recomienda estar muy atento a las futuras necesidades de adaptación de las normativas y cómo evolucionan, puesto que en los últimos años la normativa ha evolucionado bastante, incluyendo nuevos derechos y obligaciones.

Se pretende con esta metodología finalizar estableciendo una serie de herramientas para los desarrolladores y para las empresas, con el fin primero de proteger mejor los datos personales de los interesados, como para que los desarrolladores comprendan y tengan mas claro tanto la importancia de los datos personales como las medidas que se deben adoptar la desarrollar una nueva aplicación en Android e iOS

6. Tiempos empleados en el desarrollo del TFG

En este punto voy a exponer cual ha sido el trabajo realizado y el tiempo dedicado a cada parte de este trabajo fin de grado, desde el inicio hasta el final.

Pasos	Tarea	Tiempo empleado
1	Primer análisis del alcance del TFG y un primer índice de contenidos que consideraba que debía tener	4 horas
2	Realización de los primeros puntos (Motivación, Asignaturas relacionadas, Introducción)	2 horas
3	Análisis del estado del arte actual	5 horas
4	Recopilación de material bibliográfica, tanto usado como no usado (BOE, Leyes orgánicas, guías, recomendaciones, ETC.)	24 horas
5	Lectura y comprensión de los documentos	35 horas
6	Extracción de la información a utilizar, resumen de los documentos y escrito en el trabajo	120 horas
7	Trabajo en el caso ejemplo del aplicativo móvil de carga de coches eléctricos	5 horas
8	Adaptación de las normativas a nuestro trabajo	20 horas
9	Desarrollo del diagrama de flujo de la aplicación ejemplo	2 horas
10	análisis y estudio de como implementar los distintos derechos en las aplicaciones móviles, y explicación para acercárselo a los desarrolladores	2 horas
11	Estudio y uso de las aplicaciones proporcionadas por la AEDP para añadirlas al trabajo	5 horas
12	Desarrollo del checklist guía para los desarrolladores	15 horas
13	Desarrollo de una pagina de protección de datos de ejemplo para que sirva de guía a los desarrolladores.	20 horas

7. Ámbito objetivo y subjetivo de la Ley Orgánica 3/2018

El primer párrafo de la Ley Orgánica 3/2018 ya nos dice que:

"*La protección de datos de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución española*"[2], ya que en este artículo se hace referencia que, a la hora de utilizar la informática, se debe garantizar el honor y la intimidad personal y familiar de los ciudadanos, y el pleno ejercicio de sus derechos.

Es decir, a la hora de programar nuevas tecnologías y aplicaciones, deberemos tener que proteger siempre al usuario, y sus datos personales y garantizar que el interesado tenga un control total y absoluto sobre sus datos.

El Tribunal constitucional señaló en su Sentencia 94/1998, de 4 de mayo que nos encontramos ante un derecho fundamental a la protección de datos, por el que debemos asegurar que se debe garantizar a la persona el control sobre cualquiera de sus datos personales, para evitar su uso ilícito o lesivo para la dignidad:

"*Este no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, sino que consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona*"[3]

Desde el punto de vista legislativo, la concreción y desarrollo del derecho fundamental de protección de datos de las personas físicas se originó con la aprobación de la Ley Orgánica 5/1992, del 29 de octubre, que regulaba el tratamiento automatizado de datos personales, comúnmente conocida como LORTAD. Posteriormente, la Ley Orgánica 5/1992 fue sustituida por la Ley Orgánica 15/1999, del 5 de diciembre, de protección de datos personales, con el propósito de adaptar nuestra legislación a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.[4]

La idea de la Directiva 95/46/CE fue de crear unas normas y aunar los diferentes criterios europeos, para que así, tengamos todos los mismos derechos y sea más sencillo y claro cuales son nuestros derechos. A la hora de acercárselo a un profesional, siempre va a ser mas claro que toda una región (región europea en nuestro caso) use las mismas normativas y los mismos instrumentos, que tener que estar preparando la aplicación dependiendo de cada país.

Los objetivos de la Ley Orgánica 3/2018 se pueden resumir en:

a) *Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a*

[2] BOE 294, de 6 de diciembre de 2018
[3] BOE número 137, de 9 de junio: Sala segunda. Sentencia 94/1998, de 4 de mayo.
[4] BOE número 137, de 9 de junio: Sala segunda. Sentencia 94/1998, de 4 de mayo.

la protección de datos de las personas físicas en lo que respecta al tratamiento de sus datos.[5]

b) *Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución*.[6]

Destaca también en esta ley que se incluye por primera vez la regulación de las personas fallecidas, permitiendo a las personas vinculadas al fallecido por razones familiares o de hecho o sus herederos puedan solicitar el acceso, rectificación o supresión de sus datos.

8. Términos referentes a Protección de datos

De acuerdo con el Real Decreto 1720/2007, de 21 de diciembre deberemos tener en cuenta las siguientes definiciones para saber de lo que estamos hablando en todo momento

a) **Accesos autorizados:** Autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.
b) **Afectado o interesado**: Persona física titular de los datos que sean objeto de tratamiento.
c) **Bloqueo de datos**: La identificación y reserva de los datos de carácter personal con el fin de impedir su tratamiento.
d) **Cancelación**: Procedimiento mediante el cual el responsable pone fin al uso de sus datos. Implicará el bloqueo de los datos excepto para su puesta a disposición de Administraciones públicas, Jueces y Tribunales.
e) **Cesión o comunicación de datos**: Tratamiento de datos que supone su revelación a una persona distinta del interesado.
f) **Consentimiento del interesado:** Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
g) **Dato disociado:** Aquél que no permite la identificación de un interesado

[5] BOE número 294, de 06/12/2018 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
[6] BOE número 294, de 06/12/2018 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

h) **Datos de carácter personal:** Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.
i)
j) **Datos accesibles al publico:** Son todos aquellos datos que pueden encontrarse a disposición del público en general. Su acceso y conocimiento no se encuentra limitado por norma legal alguna, y suelen estar recogidos en Diarios y Boletines Oficiales, medios de comunicación, censos, anuarios, bases de datos públicas, repertorios y anuarios legales y de jurisprudencia, archivos de prensa, repertorios telefónicos y análogos, así como los datos publicados referentes a grupos de personas en los que su agrupación lo es en función de categorías o actividades y grupos profesionales y que contengan exclusivamente los nombres, títulos profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo
k) **Datos de carácter personal relacionados con la salud:** Las informaciones que hagan referencia a su salud, pasa, presente y futura, física o mental del individuo, poniendo especial importancia en porcentaje de discapacidad y a información genética.
l) **Destinatario:** Persona física o jurídica, pública o privada u órgano administrativo al que se le revelen datos.
m) **Derechos de Acceso:** autorizaciones concedidas a un usuario para la utilización de los diversos recursos de un sistema, normalmente informático.
n) **Encargado del tratamiento:** La persona física o jurídica, pública o privada u órgano administrativo que en solitario o junto otros trate datos personales por cuenta del responsable del tratamiento o responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito.
o) **Fichero:** Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de se creación, almacenamiento, organización y acceso.
p) **Persona identificable:** Toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.
q) **Responsable del fichero:** Persona física o jurídica, de naturaleza publica, privada u órgano administrativo, que solo o conjuntamente otros, decida la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.
r) **Terceros:** Persona física o jurídica, publica o privada, u órgano administrativo distinta del afectado o interesado, responsable del

tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los daros bajo autoridad directa del tratamiento o del encargado del tratamiento.

s) **Tratamiento de datos:** Cualquier operación y procedimiento técnico, sea o no automatizado, que permita la obtención, grabación, conservación, elaboración, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de las comunicaciones, consultas interconexiones y transferencias.

t) **Transferencia de datos:** El transporte de los datos entre sistemas informáticos por cualquier medio de transmisión. Así como el transporte de soporte de datos por correo o por cualquier otro método convencional.

9. Personas físicas

A la vista del artículo 1 de la LOPD, se puede observar que la ley solo regula el tratamiento de datos personales a las personas físicas disponiendo lo siguiente: "*La ley tiene por objeto garantizar y proteger el tratamiento de datos personales, las libertades públicas y derechos fundamentales de las personas físicas*"[7].

Entendemos por persona física los seres humanos que son capaces de adquirir derechos y contraer obligaciones, y tienen unos atributos concretos, que son: Persona jurídica, capacidad, nombre, domicilio, estado civil, patrimonio y nacionalidad.

Esto ayudará mucho a la hora de comprender y acercar al profesional las leyes de protección de datos, ya que solo les afectan a personas que sean identificables. Por ejemplo, un usuario que se registre en nuestra aplicación sabremos que es una persona física, con su móvil, y que se representa a si mismo.

Cuando hacemos referencia a "personas físicas", nos referimos a individuos que son identificables o ya han sido identificados. Se considera una persona física identificable a cualquier individuo cuya identidad pueda determinarse a través de un número de identificación o uno o varios elementos específicos relacionados con su identidad física, fisiológica, psicológica, económica, cultural o social. Esta definición se basa en los términos establecidos en el artículo 2.a de la Directiva 95/46/CE.

Para llevar a cabo el procesamiento de datos personales, será necesario obtener siempre el consentimiento del individuo afectado o interesado. Según lo definido en el artículo 3 de la Ley Orgánica de Protección de Datos (LOPD), se entiende por "interesado" a la persona física que es la titular de los datos sujetos al procesamiento. El "consentimiento" se refiere a una expresión de voluntad que debe ser libre, inequívoca,

[7] Artículo 1 Ley Orgánica de Protección de Datos 3/2018, de 5 diciembre

específica e informada, a través de la cual el interesado autoriza el tratamiento de sus datos personales.

Quiere decir que a la hora de que el interesado declare que esta de acuerdo con el tratamiento de los datos personales, los datos que le exigiremos serán siempre acorde con la ley, de su persona, pudiendo así pedir responsabilidades o identificarle en caso necesario.

A parte de todo esto también se debe tener en cuenta que los menores de edad también tienen sus derechos sobre protección de datos. Estos están regulados de una forma diferente, igual que en otros aspectos de la legislación no tienen la capacidad necesaria ni la voluntad para ejercer sus derechos.

Hasta la aprobación de la RLOPD de la LOPD a los menores se les aplicaban las mismas normas. Con la aprobación de la RLOPD en el artículo 13 se establecen una serie de condiciones sobre el consentimiento de los menores para el tratamiento de sus datos personales.

Para la obtención de datos personales de menores de edad, se hará una distinción entre menore de hasta 13 años y los menores mayores de 14 años. El artículo 13.1 del RLOPD establece lo siguiente: "*Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria y potestad de la tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores legales*"8.

Hay que tener en cuenta también que este consentimiento afectará solamente a los datos que le afecten directamente y que hay situaciones que se requerirá la asistencia de los padres o tutores legales, poniendo como ejemplo el ámbito sanitario, ya que la mayoría de edad medica se establece en los 16 años, De esta manera, se establece que un menor de 16 años no tiene la capacidad para otorgar su consentimiento al tratamiento de sus datos personales médicos. En cuanto al consentimiento de menores en un contexto general, el Reglamento de la Ley Orgánica de Protección de Datos (RLOPD) es explícito en que no se pueden utilizar los datos de un menor con el propósito de obtener información sobre su núcleo familiar, excepto en lo que respecta a los datos de identidad y dirección de su representante legal. Esto se hace con el fin de obtener el consentimiento del representante legal para el tratamiento de los datos cuando el menor carece de capacidad para hacerlo por sí mismo.

Para evitar falsificación en los consentimientos. El artículo 13.4 del RLOPD establece que el responsable del fichero o del tratamiento llevarán a cabo procedimientos para verificar y garantizar a la edad del menor y el consentimiento de sus representantes.

[8] Real decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Estos mecanismos deben ir acompañadas de garantías que eviten la falsificación como puede ser un documento identificativo.

Por ejemplo, si vamos a desarrollar una aplicación en torno a la carga de coches eléctricos, como la legislación española impide el poder conducir coches a menores de 18 años, se podrá rechazar cualquier intento de menor de intentar registrarse. Sin embargo, si estamos realizando una aplicación para un ámbito escolar, necesitaríamos tratar los datos del alumno menor de edad al menos para la realización de la función docente, tal y como se indica en Ley Orgánica, o para la relación contractual de las matriculas escolares o si hay un interés legitimo que prevalezca sobre intereses y derechos de los interesados

10. Personas Jurídicas

Las personas jurídicas son entidades que, a pesar de no tener una existencia física individual, poseen personalidad jurídica y están sujetas a derechos y responsabilidades legales. Como se mencionó anteriormente, dado que están excluidas, las personas jurídicas enumeradas en el artículo 35 del Código Civil no disfrutarán de las protecciones establecidas por la ley. Por lo tanto, se deduce que las personas jurídicas no tienen derecho al reconocimiento de la protección de datos, a menos que existan datos que permitan identificar a personas físicas relacionadas con ellas.

11. Responsable del tratamiento de datos y Encargado del tratamiento de datos

Otro aspecto subjetivo que se enmarca en la aplicación de la Ley Orgánica de Protección de Datos (LOPD) involucra al responsable del fichero o tratamiento de datos, así como al encargado del fichero o tratamiento de datos. Como se explicó previamente, el responsable del tratamiento se define en el artículo 3.d de la LOPD como "aquella persona física o jurídica, de carácter público o privado, o entidad administrativa que toma decisiones acerca de la finalidad, contenido y uso del tratamiento de datos".

La distinción fundamental entre el responsable del tratamiento y el encargado del tratamiento radica en que el primero es quien toma decisiones con respecto a la creación del fichero, su contenido y su propósito. En otras palabras, el responsable del tratamiento es la entidad que decide realizar operaciones o procedimientos con los datos personales de un fichero del cual no es titular.

Por último, la definición de responsable del tratamiento establece que tanto personas físicas como personas jurídicas y órganos administrativos pueden desempeñar este rol. Cuando se trata de personas físicas, no suele haber complicaciones, ya que son fácilmente identificables. Sin embargo, en el caso de personas jurídicas, ya sean de naturaleza privada o pública, así como órganos administrativos, la situación se vuelve más compleja. Esto se debe a que, para atribuirles la responsabilidad, deben cumplir con ciertas obligaciones y deberes, lo que conlleva la necesidad de designar a una persona física identificable que asuma estas responsabilidades en nombre de la entidad jurídica o el órgano administrativo correspondiente.

Por otro lado, atendiendo a artículo 3.g) de la LOPD, el encargado del tratamiento entendemos que hablamos de la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trate datos personales por cuenta del responsable del tratamiento. Esta definición la complementa la RLOPD en su artículo 5.i, que define al encargado del tratamiento como persona física o jurídica, pública o privada, u órgano administrativo que trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero.

A parte, en el artículo 12 de la LOPD establece la actuación del encargado del tratamiento. El cargo deberá estar formalizado mediante un contrato por escrito o algún otro método que se acredite su celebración y contenido. También se establece que el encargado solo tratará los datos personales siguiendo instrucciones ofrecidas por el responsable del tratamiento, quedando claro que estos datos no los utilizará para fines distintos a los indicados en el contrato ni los comunicará a terceros.

Estas dos figuras deberán adoptar medidas de seguridad para el tratamiento de datos según establece el artículo 9 de la LOPD: “Adoptar medidas de índole técnica y organizativa necesaria que garantice la seguridad de los datos de carácter personal y eviten su alteración, perdida, tratamiento o acceso no autorizado.

La regulación de la relación entre el responsable y el encargado del tratamiento debe establecerse a través de un contrato o un acto jurídico similar que los vincule.

Una de las novedades en el RGPD es la posibilidad de, unilateralmente, establecer esta relación por parte del responsable. En cualquier caso, de be tratarse de un acto jurídico que establezca y defina la posición del encargado del tratamiento.

Este contrato debe al menos contener los siguientes puntos para considerarse valido:

- Objeto duración, naturaleza y la finalidad del tratamiento.

- Tipo de datos personales y categoría de interesados.
- Obligación del encargado de tratar los datos personales únicamente siguiendo instrucciones del responsable.
- Condiciones para que el responsable pueda dar autorización previa, especifica o general, a las subcontrataciones
- Asistencia al responsable, siempre que sea posible, en la atención al ejercicio de los derechos de los interesados

La AEDP y las autoridades autonómicas dedicadas a este fin han creado directrices para regular la relación entre el responsable y encargados de protección de datos.

El encargado de tratamiento de datos debe saber y conocer el tipo de servicio que debe realizar, y para ello es preciso que las instrucciones sean claras y concretas. El encargado tendrá que notificar la responsable, en el caso que haya que realizar comunicaciones a otros países sobre los datos tratados.

Existe un deber de confidencialidad por parte del encargado del tratamiento y las personas que estén autorizadas a tratar los datos de carácter personal, y todo eso debe estar por escrito en el contrato.

12. Agencias de protección de Datos

La Agencia Española de Protección de Datos, en adelante AEDP, es según su web, "*La autoridad estatal de control independiente encargada de velar por el cumplimiento de la normativa de protección de datos. Garantiza y tutela el derecho fundamental a la protección de datos de carácter personal de los ciudadanos*".[9]

La AEDP es un órgano de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con independencia de las Administraciones Públicas en el ejercicio de sus funciones. Se regula por su propia normativa y la podemos encontrar también en su página web. Estas normativas son:

- Reglamento (UE) 2016/679 del parlamento europeo y del consejo del 27 de abril de 2016.

[9] AEDP: https://www.aepd.es/es/la-agencia/transparencia

- Corrección de errores del Reglamento (UE) 2016/679 del parlamento europeo y del consejo del 27 de abril de 2016.
- Ley Orgánica 3/2018, de 5 de diciembre, de protección de Datos personales y garantía de los derechos digitales.
- Real decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de Agencia Española de Protección de Datos.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del sector Público.

Las tareas que lleva a cabo la AEDP son las de registrar y resolver reclamaciones y denuncias, el registro y consulta de ficheros con su posterior autorización de transferencia, así como resolver las consultas que plantean los ciudadanos en la página web.

La AEDP tiene también a disposición de todo profesional herramientas como Facilita RGPD que permite a pequeñas pymes el poder conocer fácilmente que hacer con los datos personales de escaso riesgo. A través de tres pantallas con distintas preguntas te ofrece una guía de cómo tratar los datos.

Otra herramienta bastante interesante que nos ofrece la AEDP es Evalúa-Riesgo RGPD V2. Se trata de una herramienta que tiene como objeto servir de ayuda a responsables y encargados de identificar los factores de riesgo para los derechos y libertades de los interesados cuyos datos están presentes en el tratamiento de datos.

Para que nos hagamos una idea, en 2022 Facilita RGPD tuvo 56586 accesos, y de acumulados lleva mas de 1 millón. Por otro lado, Evalua-Riesgo tuvo en 2022 101897 accesos y de acumulados apenas lleva 108031[10]. Esto es debido a que es una herramienta mucho más nueva.

Por otra parte, también tenemos al Comité Europeo de Protección de Datos que fue creado en 2018. Según ellos mismos son: "*El Comité Europeo de Protección de Datos (CEPD) es un organismo europeo independiente. Es la organización coordinadora que reúne a las autoridades nacionales de protección de datos de los países del Espacio Económico Europeo*"[11].

De lo que se encarga este comité es de velar por el cumplimiento del RGPD de forma coherente y garantice la cooperación también en materia de ley.

El CEPD también pone a nuestro servicio y al del profesional unas guías de Directrices y buenas practicas para el cumplimiento del RGPD

[10] Memoria 2022 AEDP
[11] https://edpb.europa.eu/about-edpb/who-we-are/edpb-chairmanship_es

13. Derechos específicos de las personas físicas en materia de Protección de Datos y su ejercicio

La denominación "Derechos PARSOL" proviene de la reducción de las siglas de los seis derechos, en nuestro caso los siguientes:

- Derecho a la Portabilidad
- Derecho de Acceso
- Derecho de Rectificación
- Derecho de Supresión
- Derecho de Oposición
- Derecho a la Limitación del tratamiento

Sin embargo, hay que mencionar que estos derechos cambiaron hace relativamente poco, anteriormente y mucha gente aun los confunde existían los derechos ARCO que se trataban de los derechos de Acceso, Rectificación, Cancelación y Oposición, sin embargo, con las nuevas tecnologías y los nuevos desafíos sociales estos derechos se especificaron un poco mas en los derechos PARSOL que están recogidos en los artículos del 15 al 22 del Reglamento (UE) 2016/679.

13.1 Derecho de Acceso

El derecho de acceso consiste en tener la posibilidad de dirigirte al responsable del tratamiento para conocer si está utilizando y para que tus Datos personales. Además, se le podrá pedir la siguiente información al responsable del tratamiento:

- Fines del tratamiento.
- Las categorías de datos personales que se trate.
- Los destinatarios o las categorías de destinatarios a los que se les comunica los datos personales
- De ser posible, el plazo de conservación de los datos, y de no ser posible, los criterios para determinar estos plazos
- La existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento.
- El derecho a presentar una reclamación.
- Cuando los datos no se hayan obtenido del interesado, cualquier información disponible sobre su origen
- La existencia de decisiones automatizadas y la información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento.

- Cuando se transfieran los datos a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia

13.2 Derecho de rectificación

El Derecho de rectificación es el que tienen los interesados a que el responsable del tratamiento rectifique aquellos datos que no sean correctos o sean inexactos o estén incompletos, sin dilación indebida. Para ser más exactos el artículo 16 dice lo siguiente: El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernen. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional".

13.3 Derecho de supresión

El derecho de supresión establece que la persona interesada tiene el derecho de solicitar al responsable del tratamiento que elimine sus datos personales. El responsable del tratamiento está obligado a llevar a cabo esta eliminación de manera inmediata cuando se cumpla alguna de las siguientes circunstancias:

- Los datos personales ya no sean necesarios en relación con los fines que fueron recogidos o tratados de otro modo
- El interesado reitere el consentimiento en que se basa el tratamiento de conformidad y este no se base en otro fundamento jurídico.
- El interesado se oponga al tratamiento con arreglo al artículo 21.1 y no prevalezcan otros motivos legítimos para el tratamiento
- Los datos hayan sido tratados ilícitamente
- Los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.
- Los datos personales se hayan obtenido en una relación con oferta de servicios de la sociedad de la información.

Además, si los datos personales se han hecho públicos y el responsable del tratamiento está obligado a eliminarlos, deberá tomar medidas razonables, incluyendo medidas técnicas, teniendo en cuenta la tecnología y el costo de implementación, con el fin de informar a otros responsables que estén tratando los datos personales sobre la solicitud del individuo interesado.

Los casos anteriores no se aplicarán cuando:

- Para ejercer el derecho a la libertad de expresión e información

- Para el 5cumplimiento de una obligación legal que requiere el tratamiento de datos impuesta por el derecho de la Unión de los Estados miembros que se aplique el responsable de tratamiento, o para el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos al responsable.
- Por razones de interés público en el ámbito de la salud pública de conformidad con el art. 9.2 y el 9.3.
- Con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89.1, en la medida que el derecho indicado en apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos.

13.4 Derecho a la limitación del tratamiento

El derecho a la limitación del tratamiento supone que, a petición del interesado, sus datos se dejen de tratar. La limitación la puede solicitar cuando la persona interesada ha ejercido su derecho de ratificación u supresión y mientras el responsable determina si pega atender la solicitud.

Para ello el artículo 18 dice lo siguiente:

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

- El interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de estos.
- El tratamiento sea ilícito y el interesado se oponga al a supresión de3 los datos personales y solicite en su lugar la limitación de su uso.
- El responsable de tratamiento ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesita para la formación, ejercicio o la defensa de reclamaciones.
- El interesado se haya opuesto al tratamiento en virtud del articulo 21(derecho de supresión), mientras se verifican los motivos legítimos del responsable prevalecen sobre los del interesado.

Una vez que los datos personales han sido restringidos según lo explicado anteriormente, dichos datos solo podrán ser procesados, a excepción de su almacenamiento, bajo las siguientes circunstancias: con el consentimiento del individuo afectado, con el propósito de llevar a cabo acciones legales, defenderse en procedimientos legales o formular reclamaciones, o en aras de proteger los derechos de otra persona física o jurídica o por razones de interés público.

Por último, todo aquel interesado que haya obtenido la limitación de sus datos mediante este derecho deberá ser informado por el responsable antes del levantamiento de dicha limitación.

13.5 Derecho a la portabilidad de los datos

Este derecho es un nuevo derecho que se añadió en el Reglamento (UE) 2016 679 que complementa al derecho de Acceso. El artículo 20 especifica lo siguiente:

El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:

- El tratamiento está basado en el consentimiento como arreglo al articulo 6.1.a o el artículo 9.2.a, o en un contrato con arreglo al artículo 6.
- El tratamiento se efectúe por medios automatizados[12]

Además, al ejercer el derecho de portabilidad de datos, la persona interesada tiene el derecho de solicitar que sus datos personales se transmitan directamente de un responsable del tratamiento a otro cuando esto sea técnicamente factible. Es importante destacar que el ejercicio de este derecho no afecta al artículo 17 y no se aplicará en situaciones en las que el tratamiento de datos sea necesario para cumplir una tarea en el interés público o en el ejercicio de poderes públicos otorgados al responsable del tratamiento.

Por último, el derecho de portabilidad de los datos no afectará negativamente a los derechos y libertades de otros.

13.6 Derecho de Oposición

Es el derecho del interesado a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que sus datos personales sean objeto de tratamiento basado en una misión de interés público o en el interés legítimo. Para ser más concreto el artículo 20 establece lo siguiente:

El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernen sean objeto de tratamiento basado en lo dispuesto en e l artículo 6.1.e o f. incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del

[12] Reglamento (UE) 2016 679

tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

También se establece que cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida que esté relacionada con la mercadotecnia.

A más tardar, en el momento de la primera comunicación con el interesado, el derecho de oposición será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.

Además, en el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.

Por último, cuando los datos personales se utilicen con fines de investigación científica, histórica o estadística de acuerdo con lo establecido en el artículo 89.1, la persona interesada tiene el derecho, por razones relacionadas con su situación particular, a oponerse al tratamiento de sus datos personales, a menos que dicho tratamiento sea esencial para llevar a cabo una tarea realizada por motivos de interés público.

13.7 Procedimientos reglamentarios para ejercitar los derechos

Como podemos ver en el artículo 25 de la RLOPD, se establecen los métodos para ejercer los derechos respecto a los Datos. En este artículo se expone: “el ejercicio de los derechos deberá llevarse a cabo mediante una comunicación dirigida al responsable del fichero que contendrá:

- Nombre y apellidos del Nombre y apellidos del interesado; fotocopia de su documento nacional de identidad, o de su pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica identificativa del afectado eximirá de la presentación de las fotocopias del DNI o documento equivalente.
- Petición en que se concreta la solicitud.
- Dirección a efectos de notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición que formula.

El responsable del tratamiento deberá contestar la solicitud que se le dirija en todo caso, con independencia de que figuren o no datos personales en sus ficheros.

En el caso de que la solicitud no reúna los requisitos especificados, el responsable del fichero deberá solicitar la subsanación de los mismos.

La respuesta deberá ser conforme con los requisitos previstos para cada caso en el presente título.

Corresponderá al responsable del tratamiento la prueba del cumplimiento del deber de respuesta establecido previamente, debiendo conservar la acreditación del cumplimiento del mencionado deber.

El ejercicio de los derechos de acceso, rectificación, cancelación y oposición podrá modularse por raciones de seguridad pública en los casos y con el alcance previsto en las leyes.

Cuando las leyes aplicables a determinados ficheros concretos establezcan un procedimiento especial para la rectificación o cancelación de los datos contenidos en los mismos, se estará a los dispuesto en aquellas. Este ultimo punto esta muy relacionado con nuestro trabajo, debido a que un caso especial puede ser el de las aplicaciones móviles Android e iOS. Dando acceso en una pantalla a los datos al propio usuario y sea el interesado capaz de modificar sus propios datos.

De esta manera podemos establecer que en aplicaciones móviles puede ser mas sencillo ejercer los derechos de Acceso, Rectificación incluso el derecho de Supresión. Ya que, al dar acceso mediante una pantalla al interesado, este podrá ver/modificar e incluso solicitar la eliminación de su perfil mediante un botón.

14. Gestión de datos personales en aplicaciones Android/iOS

Una vez establecida la legislación y conociendo las figuras y en qué consisten los distintos derechos, debemos aplicar estos conocimientos cuando creemos nuestras aplicaciones debiendo tener en cuenta que la protección de datos debe estar totalmente asegurada, ya que si no tanto la Play Store como el Market de iOS no nos dejen publicar las aplicaciones.

Se deben adoptar las medidas organizativas y técnicas precisas para asegurar la protección de los datos de carácter personal objeto de tratamiento: En

todas y cada una de las etapas del diseño y la implementación de la app (privacy by design).

Para desarrollar este punto me acogeré a mi experiencia profesional y a la aplicación que se está desarrollando sobre recarga de coches eléctricos. Aplicación en la que los usuarios se deben registrar y por lo tanto se deben gestionar sus datos personales.

Lo primero y más importante como ya hemos visto tiene que ser la designación de un responsable de tratamiento de datos y un encargado del tratamiento de datos. Normalmente en grandes compañías tienen un departamento legal que son los encargados de representar estas figuras, sin embargo, si las aplicaciones las estamos haciendo en una empresa pequeña, lo lógico sería que el responsable del tratamiento sea la figura de mayor autoridad y el encargado la persona que vaya a tener acceso a la administración de la aplicación y mantenimiento posterior a la puesta en marcha.

Una vez establecidas esas figuras voy a establecer y trabajar dos tipos de aplicaciones: las que Tengan un sistema de usuarios y las que no dispongan de un sistema de usuarios. Como es lógico las aplicaciones que no dispongan de un sistema de usuarios no va a guardar ningún dato personal y nos deberemos asegurar que cuando el usuario cierra la aplicación, se eliminan todos los datos de su conexión.

Por otro lado, y el que va a ser nuestro principal caso de estudio, son las aplicaciones con un sistema de registro de usuarios. Al disponer de este sistema como ya suponemos, tendremos que almacenar datos personales de las personas que se registren.

Según el grupo de trabajo del artículo 29 sobre protección de datos el consentimiento es una de las seis bases jurídicas para el tratamiento de datos personales. Por ello cuando se lleven a cabo actividades que impliquen el tratamiento de datos, el responsable del tratamiento siempre debe detenerse a considerar cual va a ser el fundamento jurídico del tratamiento[13].

En realidad, para que el consentimiento sea considerado una base jurídica válida, es esencial ofrecer al individuo interesado un verdadero control y la capacidad de elección en cuanto a si desea aceptar o rechazar los términos sin restricciones. Al aceptar estos términos, el responsable del tratamiento debe evaluar si el consentimiento cumple con todos los requisitos necesarios para ser

[13] Grupo de trabajo del artículo 29 Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679

considerado válido. El consentimiento se convierte en una herramienta que empodera al interesado, dándole el control sobre si sus datos personales serán objeto de tratamiento o no. Si esto no se cumple, el control resulta ser ilusorio y, en consecuencia, el consentimiento no constituirá una base jurídica válida.[14]

Para que un consentimiento sea válido, el Artículo 4, apartado 11 del RGPD estipula que el consentimiento del interesado es toda manifestación de voluntad:

- Libre
- Especifica
- Informada
- inequívoca por la que el interesado acepta, ya sea mediante una declaración afirmativa, el tratamiento de datos personales que le conciernen

No obstante, al evaluar si el consentimiento se ha otorgado de manera voluntaria, es necesario tener en cuenta las circunstancias específicas en las que el consentimiento está vinculado a la celebración de contratos o a la prestación de un servicio. Esto significa que el consentimiento se considerará inválido en caso de que exista cualquier tipo de influencia indebida o presión ejercida sobre la persona interesada.

Pongo como ejemplo que si desarrollamos una aplicación de carga de coches eléctricos pide a sus usuarios tener activado el GPS para el uso de sus servicios. La aplicación señala también a sus usuarios que utilizara los datos recogidos para fines de publicidad comportamental. En este caso la geolocalización es necesaria para identificar los cargadores más cercanos al usuario, sin embargo, la publicidad comportamental no es necesaria para la prestación de carga de coches eléctricos y va más allá de lo necesario para prestar el servicio básico ofrecido. Dado que los usuarios no pueden utilizar la aplicación sin dar consentimiento a estos fines, no puede considerarse que el consentimiento se haya dado libremente.

El artículo 7 del apartado 4 del RGPD pretende garantizar que el tratamiento de los datos no se camufle o se vincule a la prestación de un contrato o servicio para el cual los datos personales no son necesarios. Cumpliendo de este modo que el tratamiento de los datos para los que se ha solicitado el consentimiento no se convierta directa o indirectamente en una contraprestación de un contrato.

Con todo esto nos estamos refiriendo que a la hora de desarrollar nuestra aplicación deberemos tener siempre claro cuáles son los datos personales que

[14] Grupo de trabajo del artículo 29 Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679

vamos a recoger, como los vamos a recoger, como los vamos a tratar y si de verdad son necesarios o no.

En el ejemplo de la aplicación de carga de coches eléctricos, por ejemplo, deberemos recoger nombre y apellidos, un documento de identidad, cuenta bancaria y país residente, que serán tratados a la hora de poder facturar el servicio prestado. Además, se tendrá acceso a su ubicación GPS para ayudar al usuario a encontrar los puntos de carga más cercanos.

También el grupo de trabajo 29 dice que la legislación sobre protección de datos tiene como fin la protección de los derechos fundamentales, el control de una persona sobre sus datos personales es esencial y existe una firme presunción de que dar el consentimiento a un tratamiento de datos personales que no sea necesario no puede considerarse como un requisito obligatorio para la ejecución de un contrato o la prestación de un servicio.

Por lo tanto, en los casos en que la solicitud de consentimiento esté relacionada con la ejecución de un contrato por parte del responsable del tratamiento, una persona interesada que no quiera que sus datos personales estén disponibles para el tratamiento por parte del responsable corre el riesgo de que se le nieguen los servicios que ha solicitado.

Es decir, retomando el ejemplo anterior. Tras informar al usuario quien será el responsable del tratamiento de los datos y para que, y con que fin se recogen y utilizan sus datos personales, el usuario se niega o no acepta a darnos el permiso. Podremos denegar el servicio.

A la hora de implementar esto es bastante sencillo de cara a un programador. Cuando se acceda por primera vez a la aplicación y el usuario vaya a registrarse.

La medida que tomaremos es a la hora de realizar el registro debemos facilitar una política de privacidad que se debe de aceptar para cumplimentar el registro. En esta Política de privacidad debemos incluir como mínimo lo siguiente:

- Quienes somos
- Que categoría de datos de carácter personal recogeremos
- Por qué deben realizar el procesamiento de datos y para que se van a utilizar
- En caso de cederlo a terceros, una especifica descripción de a quien van a ser cedidos y los derechos de los usuarios, en lo referido a la revocación del consentimiento y la supresión de datos

En caso de que el usuario se negará a aceptar las políticas de privacidad la aplicación deberá devolver al usuario a la pantalla inicial y no haber realizado el

registro. Negando así el acceso a nuestros servicios, en caso del ejemplo a los puntos de carga y a la posibilidad de recargar su coche eléctrico.

También deberemos tener en cuenta a la hora de desarrollar nuestra aplicación el uso de los datos personales de los usuarios que vamos a hacer, y si van a servir para un solo propósito, o para mas de uno. En caso de que fuéramos a utilizar los datos para mas de un fin, deberemos asegurarnos de conseguir el consentimiento de los usuarios para cada fin, ya que como dice el considerando 32 del RGPD: "El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos"[15].

Volviendo a nuestro ejemplo de aplicación sobre recarga de vehículos eléctricos. Pongamos el caso de que surge una colaboración con otra empresa que gestiona postes eléctricos y ahora nuestros usuarios podrán tener acceso a los otros puestos de carga, pero para ello, deberemos transferir sus datos personales a la otra empresa para que les de el alta en su sistema. Como nosotros recogimos sus datos solo para nuestro uso de facturación, deberemos conseguir un nuevo consentimiento para poder transferir sus datos, en caso de que no nos den el consentimiento, el consentimiento anterior no será valido para esta nueva función. Pudiendo llegar negarle el servicio nuevo a los usuarios que no acepten el nuevo tratamiento de datos.

Otro punto muy importante a la hora de recabar en nuestra aplicación el consentimiento a la trata de datos personales del usuario es que no puede obtenerse el consentimiento en la misma acción en la que el usuario acepta los términos y condiciones de la aplicación. Sin embargo y en el marco del RGPD, los responsables del tratamiento si que pueden establecer un flujo de consentimiento que convenga la organización[16].

Como ejemplo si volvemos a nuestra aplicación. El responsable del tratamiento de datos podría generar el siguiente el flujo: Al abrir la aplicación por primera vez nos muestra los términos y servicios para aceptar, posteriormente una pantalla de login y al acceder al registro de usuario, nos muestre la pantalla de protección de datos y la acción para aceptarlos.

Lo que no podríamos hacer nunca, es si abrimos por primera vez, en la misma pantalla nos aparecieran los términos y servicios y la protección de datos, con una sola casilla para aceptar, sin poder decidir si aceptamos el tratamiento de nuestros datos o no.

Por último, en lo referente al consentimiento del tratamiento de datos, el responsable debe ser capaz de demostrar el consentimiento valida del interesado,

[15] Referendo 32 RGPD

[16] Grupo de trabajo del artículo 29 Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679

ya sea manteniendo un registro de las declaraciones con una relación de fecha de cuando se obtuvieron, de manera que pueda probar como se obtuvo el consentimiento. También deberá demostrar la información que se le facilito al interesado en su momento.

Si esto lo aplicamos a nuestro ejemplo de aplicación, sería tan sencillo como a la hora que el usuario se registrase y aceptara la política de protección de datos guardar en una tabla el consentimiento que ha dado (en caso de ser varios consentimientos, establecer distintas columnas para cada permiso aceptado) y una columna del día y la fecha que se aceptan, así como una ultima columna que haga referencia al documento.

De esta forma, si en algún momento la aplicación evoluciona, o se establecen nuevas necesidades de trata de datos personales, sería tan sencillo como a la hora de hacer login, les saltara el pop up con la nueva declaración de trata de datos personales, y tener claro que usuarios han firmado, que han firmado y cuando han firmado el consentimiento al uso de sus datos personales.

Se debe informar también en el documento de política de privacidad los derechos PARSOL antes estudiados:

- Derecho de Portabilidad
- Derecho de accesibilidad
- Derecho de rectificación
- Derecho de supresión
- Derecho de oposición
- Derecho de limitación

Para saber de que forma se pueden aplicar todos estos derechos deberemos tener muy claro el funcionamiento de nuestras aplicaciones, para se va a analizar el cómo podríamos implementar, o afrontar en nuestras aplicaciones los derechos

Derecho de Portabilidad: Para ello deberemos tener en la BBDD todos los datos personales localizados y ordenados de forma que si tenemos el consentimiento se puedan compartir, para ello recomiendo hacer una tabla especifica en la que guardar los datos personales de cada usuario, tabla que solo tendrá acceso el responsable del tratamiento y a la hora de interactuar con otras aplicaciones u otras organizaciones, estos datos sean fáciles de trasladar.

Si ponemos como ejemplo la aplicación sobre carga de coches eléctricos, si tengo un acuerdo con otra empresa para usar también sus puntos de recarga, es probable que está empresa me pida los datos de mi cliente, para darle acceso a sus puntos de carga. Si tenemos en una tabla todos los datos necesarios será más fácil realizar la portabilidad de datos que si nos los tenemos localizados.

La importancia de esta tabla consiste en que debe tener la vista oculta a aquellas personas que no tengan el rol de responsable de tratamiento o encargado del tratamiento ya que se tratan de datos sensibles que otras personas no deberían tener acceso a ellos.

Derecho de accesibilidad: Este apartado al tratarse de una aplicación para dispositivos Android e iOS resulta bastante sencilla de implementar ya que nos bastaría con una pestaña de usuario o perfil, donde se muestren todos los datos personales que la aplicación tiene. Sin embargo, los permisos de aplicación concedidos no suelen aparecer en la pantalla de perfil. Los permisos de acceso que tendrá la aplicación se deberán guardar en el dispositivo de forma que sea sencillo el activarlos o no.

Por defecto en toda aplicación que se desarrolle si necesitamos permisos específicos como acceso a la agenda o a la geolocalización deberemos generar unas alertas que informen al usuario y recojan la aceptación o negación de estos permisos. A la hora de desarrollar la aplicación estos permisos estarán siempre deshabilitados hasta obtener la aceptación por parte del usuario.

Si esto lo aplicamos a nuestro ejemplo de aplicación de carga de coches eléctricos, el permiso de acceso a la ubicación estará deshabilitado, pero la primera vez que el usuario abra la aplicación, deberá salir un cartel, explicándole el por que y para que necesitamos saber su localización y deberá aceptar los permisos. Tras registrarse y realizar el login en la aplicación. Habrá una pantalla que será la de datos del usuario en la cual el usuario podrá ver los datos que ha dado.

Derecho de rectificación: Este derecho va muy ligado al derecho de acceso a la hora de crear una aplicación debido a que la pantalla de datos personales ya la tenemos creada para garantizar el derecho de acceso. En esta misma pantalla se puede añadir un botón de editar datos.

Este botón nos llevará a una nueva pantalla en la cual se podrán editar los datos personales ofrecidos. En caso de requerirlo, necesitaremos también un sistema que permita al usuario adjuntar evidencia de que se tratan de sus datos correctos, como un carné de identidad. Esto cambios no se deben producir solos, así que se debe garantizar una pareja de botones Aceptar y Cancelar por si el usuario se equivoca o ha corregido correctamente sus datos.

Trasladando esto a nuestra aplicación, como hemos comentado antes generaremos una pantalla de edición de datos personales, que será accesible a través de la pantalla de datos personales. Al tratarse de una aplicación de recarga de coches eléctricos y la necesidad de facturar, en caso de cambiar de documentos de identidad o de residencia se deberá adjuntar documento que acredite estos cambios. Esta pantalla tendrá un botón de aceptar que permitirá almacenar los datos cambiados, y uno de cancelar, que permitirá no almacenar estos datos.

Derecho de Supresión: Este derecho en caso de las aplicaciones es un poco más delicado ya que deberemos tener en cuenta varios factores. Lo primero que deberemos tener en cuenta es el del tiempo establecido que hemos informado a la hora de seguir almacenando los datos.

Teniendo en cuenta lo siguiente, deberíamos ser capaces de programar una forma de que el usuario pueda eliminar sus datos y ejercer su derecho a la supresión. Para ello en relación a aplicaciones Android e iOS lo mas sencillo es crear un flujo que permita al usuario eliminar su usuario de nuestro sistema.

Tras notificar su voluntad de eliminar su usuario de nuestro sistema, nosotros podremos tener sus datos almacenados como máximo lo que se hubiese comunicado en la pantalla de Protección de datos que el usuario aceptó durante el periodo que fueran a ser necesarios.

Se debe informar también al usuario en el documento de políticas de privacidad los plazos de conservación de los datos. Estos periodos de conservación deben tener unos plazos razonables y se debe determinar un plazo de inactividad tras el cual la cuenta se considerará expirada. En el caso de la aplicación en la que estoy trabajando en el entorno laboral, tras la petición del usuario de la supresión de datos, los datos los mantendremos ofuscados durante 1 mes en caso de que el afectado nos lo requiera o lo necesitemos tratar por orden judicial o reclamo administrativo, y tras el mes estos datos son totalmente eliminados.

Si esto lo trasladamos a nuestra aplicación sobre recarga de coches eléctricos podemos crear un botón de dar de baja, en la pantalla de Usuario o datos personales. Al pulsar este botón deberemos mostrar un aviso avisando al usuario el periodo que se mantendrán sus datos y si esta de acuerdo con ejercer el derecho de supresión. En nuestro caso los datos del usuario se mantendrán 30 días debido a que al tratarse de una aplicación con facturación debemos asegurarnos de que el ciclo completo mensual se completa y se crea la última factura correctamente.

Tras este periodo nos debemos asegurar de que la base de datos elimina por completo los datos del usuario y no queda ningún dato sensible. Debido a que ya tenemos todos los datos sensibles en la misma tabla, simplemente consistiría en eliminar el registro de esta tabla, y con opción de eliminar en cascada, es decir, que se eliminen también todos los registros.

Derecho de oposición: Este derecho se basa en la decisión del interesado sobre el uso de sus datos basados en una misión de interés público o en el interés legítimo, incluido creación de perfiles. Para ejercer este derecho se puede crear un formulario de contacto con el responsable de tratamiento, en el cual el usuario notifique su decisión a ejercer el derecho de oposición.

Tras esta notificación el responsable de tratamiento debe activar los mecanismos necesarios para evitar que los datos de este usuario vuelvan a ser utilizados, a excepción motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses.

Si esto lo trasladamos a nuestra aplicación sobre coches eléctricos. Habrá que diseñar una pantalla de contacto, que contenga la opción de contacto con el responsable de tratamiento de datos. Una vez recibida la comunicación. El responsable se encargará que solo se utilicen esos datos cuando sean estrictamente necesarios, es decir a la hora de facturar o realizar alguna comunicación al usuario.

Derecho de limitación: Este derecho esta relacionada cuando el usuario ha ejercido su derecho de rectificación o de supresión, mientras estos se resuelven el usuario puede decidir limitar el uso que se hace de sus datos.

En el caso de las aplicaciones en dispositivos móviles Android e iOS nos encontramos que el derecho de rectificación suele ser casi instantáneo, a no ser que se rectifique algún dato que necesite comprobación. Lo mismo pasa con el derecho de supresión, al tratarse de aplicaciones, suele aplicarse al instante en que el usuario comunica su deseo de ejercer el derecho de supresión.

En el caso de que el usuario decida ejercer el derecho de limitación se podrá usar el mismo formulario que para el derecho de oposición, simplemente sería crear un desplegable con el motivo de contacto con el responsable del tratamiento y un cuadro de texto mediante el cual el usuario explicará su decisión.

Desde el momento en que esta decisión es comunicada, el responsable de tratamiento deberá poner en marcha todos los mecanismos para asegurarse que los datos del usuario solo se usen para reclamaciones, para proteger los derechos de otra persona o por razones de interés público. A su vez, el responsable deberá en caso de requerirlo, comunicar la limitación a cada uno de los destinatarios.

En el caso de nuestra aplicación, en caso de que tengamos acuerdo con otras compañías para el uso de sus postes y zonas de recarga, la aplicación deberá ser capaz de comunicar a estos terceros la limitación de datos, así como tener identificados estos terceros.

Otro punto en el cual se deberá poner especial atención es que hoy en día pueden acceder a las aplicaciones personas de cualquier edad, así que deberemos establecer en el registro la diferenciación entre mayores de edad y menores. En caso de que el usuario sea menor de edad habrá que tener en cuenta los límites de minoría de edad fijados por la ley, por ejemplo, en aplicaciones sanitarias, menores de 16 años no deberían tener acceso. En el caso de la aplicación que estoy trabajando en el entorno laboral, la tratarse de recarga de coches eléctricos, y siendo menor de edad no puedes conducir, cuando un menor de 18 años intenta

registrarse, la aplicación deberá rechazar el registro y mostrar que la edad mínima establecida por las leyes es de 18 años.

También habrá que tener elegir el método más restrictivo para el procesamiento de datos, con total respeto a los principios de minimización de datos y restricción a la finalidad. Para ello la mejor solución a la hora de diseñar las aplicaciones sería una primera página de registro donde se exija el año de nacimiento, y si no supera la edad, llevarle a otra página de registro distinta a la que usuaria una persona mayor de edad.

La información de los menores de edad está completamente prohibida usar con fines comerciales.

Por último, hay que abstenerse de conseguir información a través de los niños de su entorno familiar y/o de amigos.

Según el grupo de trabajo 29 el responsable del tratamiento debe ser conocer las distintas legislaciones nacionales, teniendo en cuenta el público al que van dirigidos sus servicios. En particular se debe señalar que el responsable de tratamiento que ofrezca su servicio en mas de un país, no solo debe conocer la legislación del país desde el que opera, sino de todos los países afectados

La mayoría de las APP cuando las instalamos nos suelen pedir unos permisos extras, la mayoría de veces excesivos, como por ejemplo cuando instalamos una aplicación de lector de QR y piden acceso a nuestros contactos. La mayoría de las aplicaciones van a pedir acceso a Contactos de la agenda, Fotos y Datos de localización. Datos muy personales con que pueden:

- Localizarnos al momento
- Sabe lo que hacemos
- Ver quiénes son nuestros amigos

A nivel de aplicaciones que obtengan información sobre la localización de los usuarios, estos datos se considerarán datos de carácter personal y sometidos, por tanto, a la LOPD.

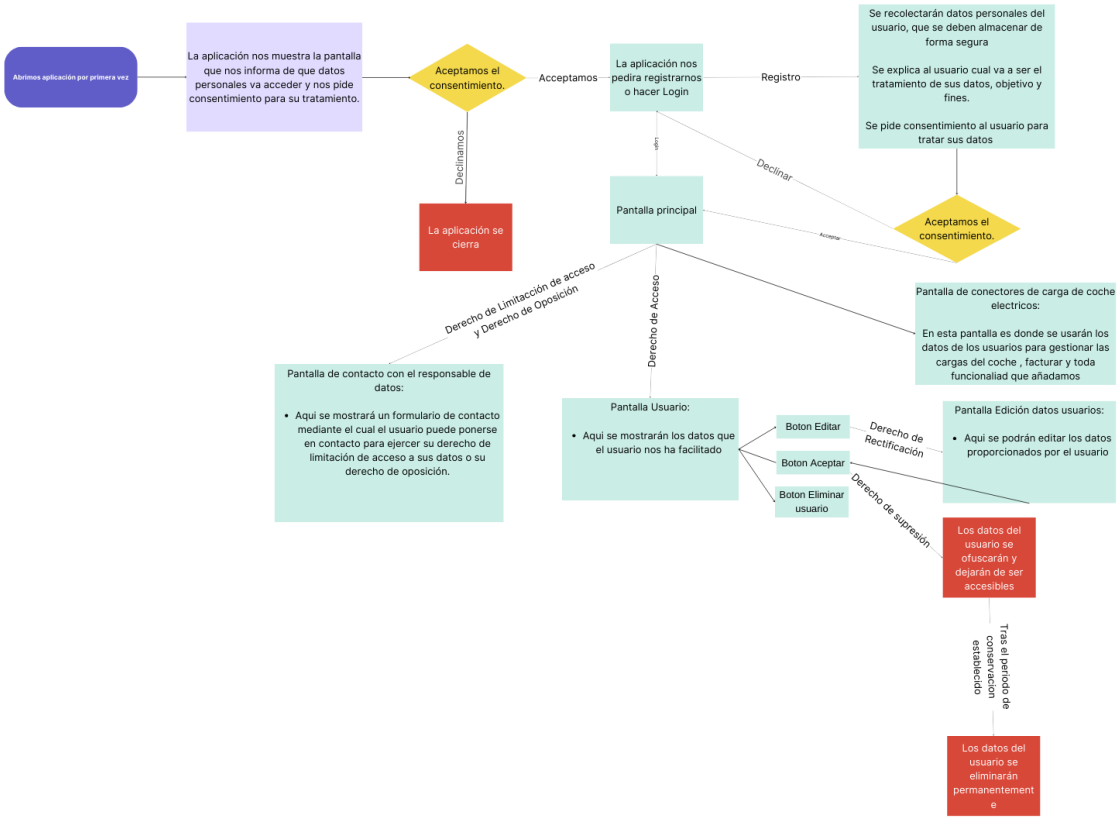
Para cumplir con la Protección de datos en aplicaciones de geolocalización habrá que reunir una serie de requisitos.

- Conseguir el consentimiento previo, especifico e informado del usuario.
- Advertir de los fines para los cuales los datos de localización geográfica van a ser tratados.
- Los servicios de geolocalización deberían estar desactivadas por defecto.
- Facultad de revocar el consentimiento del usuario en cualquier momento.
- Restringir el periodo de validez del consentimiento e indicárselo a los usuarios.
- Respetar y satisfacer los derechos PARSOL.

Podemos concluir indicando que los desarrolladores de aplicaciones móviles están obligados, en cuanto que recogen y tratan datos de carácter personal, al cumplimiento de la LOPD y del RLOPD se les exige:

- Una correcta información al usuario.
- Obtener el consentimiento del mismo.
- Informar sobre derechos PARSOL.
- Adoptar medidas de seguridad adecuadas.
- Definir el periodo de conservación de los datos.

Podemos hacernos una idea de los momentos críticos a la hora de tratar los datos si nos hacemos un diagrama de flujo de lo que va a ser nuestra aplicación



Como podemos observar en el diagrama de flujo de la aplicación que estamos poniendo de ejemplo de recarga de coche eléctrico, puede ayudar mucho al desarrollador ver en que momento se recogen tanto los permisos como los datos personales, ya que normalmente suele ser en momentos distintos. Además de en que pantallas o partes de la aplicación debe llevar cuidado con el tratamiento de los datos personales.

Un ejemplo del texto que podríamos incluir en la pantalla de política de privacidad de datos a la hora de informar al usuario podría ser el siguiente:

POLITICA DE PROTECCIÓN DE DATOS

JOSEDOMINGO, S.L., ha elaborado esta Política de Privacidad para informarte y ser completamente transparente con respecto a toda la información que recopilamos sobre ti, las finalidades para las que lo hacemos y la forma en que puedes controlar tu información personal.

¿Quién es el responsable del tratamiento de tus datos?

RESPONSABLE: JOSEDOMINGO, S.L.

NIF: E55587810

DOMICILIO SOCIAL: Calle Archiduque Carlos 45.

CONTACTO: info@josedmingo.com / 963800000

¿Con qué finalidad tratamos tus datos personales?

En **JOSEDOMINGO, S.L.,** dependiendo de la categoría de interesado en la que te encuentres, tratamos la información que nos facilitas con las siguientes finalidades:

1. USUARIOS

1.1 ACTIVIDADES DE TRATAMIENTO

a. Registro

i. Gestionar el alta de los usuarios en la aplicación.

ii. Gestionar los servicios prestados mediante la aplicación.

A la hora de efectuar el Registro se solicitan los siguientes datos:

- Nombre y apellido
- NIF/NIE/Pasaporte
- Teléfono
- Otro Teléfono
- Email
- Dirección
- CP
- Población
- Provincia
- Información del Vehículo

b. Servicio

i. Geolocalización:

- En caso de que nos permita acceder a su ubicación, esta información se utilizara para facilitarle la ubicación de los puntos de carga en relación con la suya.
- Facilitarle indicaciones en tiempo real en el mapa para llegar a los puntos de carga.

Para este caso en particular, los datos tratados son los siguientes:

- Ubicación aproximada (datos basada en red)
- Ubicación precisa (datos GPS)

ii. Libreta Telefónica:

En caso de que nos permita acceder a su agenda de contactos, su información se utilizará para ponernos en contacto con usted en caso de requerir algún tipo de soporte o aclarar dudas.

iii. Histórico de Recargas:

El objetivo es el de facilitar al usuario información respecto de su actividad de recargas. El tratamiento de esta información se utilizaría para indicar datos que se registran y el plazo de su vigencia en el historial

iv. Reservas y recargas:

- Gestionar las reservas de los puntos de carga.
- Gestionar las recargas desde el móvil.

La información tratada indicará datos personales utilizados para estas actividades.

c. Facturación

Gestionar el pago mediante tarjeta de crédito/debito de las recargas realizadas a través de la aplicación por los usuarios. Los datos utilizados en este apartado se utilizarán para indicar datos de pago

d. Comunicaciones Comerciales

Su finalidad es la de facilitar todo tipo de comunicaciones comerciales por medios electrónicos sobre ofertas de nuestros servicios y/o productos (similares a los inicialmente adquiridos). En esta oportunidad se haría uso del Correo electrónico, fundamentalmente.

e. Contacto

i. Facilitar al usuario la información que nos solicite.

ii. Gestionar las consultas formuladas por los usuarios.

Para este caso en particular, los datos tratados son los siguientes:

- Nombre
- Número de móvil
- Correo electrónico

2.

1. para USUARIOS

- Art. 6.1.b RGPD: ejecución de un contrato en el que el interesado es parte.
- Art. 6.1.a RGPD: consentimiento del propio interesado (geolocalización; acceso libreta telefónica).

- Art. 6.1.f RGPD: Interés legítimo (enviar información solicitada, gestionar las consultas planteada; enviar comunicaciones comerciales).

Los datos que te solicitamos son adecuados, pertinentes y estrictamente necesarios y en ningún caso estás obligado a facilitárnoslos, pero su no comunicación podrá afectar a la finalidad del servicio o la imposibilidad de prestarlo.

¿Por cuánto tiempo conservaremos tus datos personales?

Tus datos, serán conservados el tiempo mínimo necesario para la correcta prestación del servicio ofrecido, así como, para atender las responsabilidades que se pudieran derivar del mismo y de cualquier otra exigencia legal.

¿A qué destinatarios se comunicarán tus datos?

Opción 1: **JOSEDOMINGO, S.L**. no comunicará sus datos a ningún tercero, salvo que se informe de ello expresamente.

Adicionalmente le informamos que determinados datos, en virtud de la normativa vigente o de la relación contractual que mantenga con **JOSEDOMINGO**, S.L., podrán ser comunicados a:

- Los bancos y entidades financieras para el cobro de los servicios contratados y/o productos comprados.
- Administraciones públicas con competencia en los sectores de la actividad de **JOSEDOMINGO,** S.L., cuando así lo establezca la normativa vigente.

Opción 2: **JOSEDOMINGO,** S.L., para una correcta prestación de los servicios, podrá comunicar sus datos para:

Dar acceso o transmitir los datos personales facilitados por el Usuario, a terceros proveedores de servicios con los que **JOSEDOMINGO**, S.L. haya suscrito acuerdos de encargo de tratamiento de datos, y que únicamente accedan a dicha información para prestar un servicio en favor y por cuenta del responsable.

Adicionalmente le informamos que determinados datos, en virtud de la normativa vigente o de la relación contractual que mantenga **JOSEDOMINGO**, S.L., podrán ser comunicados a:

- Los bancos y entidades financieras para el cobro de los servicios contratados y/o productos comprados.

- Administraciones públicas con competencia en los sectores de la actividad de **JOSEDOMINGO**, S.L., cuando así lo establezca la normativa vigente.

¿Cuáles son tus derechos cuando nos facilitas tus datos?

Los derechos de protección de datos que podrás ejercer como interesado, cuando procedan, son:

- Derecho a solicitar el acceso a los datos personales.
- Derecho de rectificación o supresión.
- Derecho de oposición.
- Derecho a solicitar la limitación de su tratamiento.
- Derecho a la portabilidad de los datos.
- Derecho a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de datos.

Los titulares de los datos personales obtenidos podrán ejercer sus derechos de protección de datos personales dirigiendo una comunicación por escrito al domicilio social de **JOSEDOMINGO**, S.L., o al correo electrónico habilitado a tal efecto, responsablepd@josedomingo.com.

Modelos, formularios y más información disponible sobre tus derechos en la página web de la autoridad de control nacional, Agencia Española de Protección de Datos, en adelante, AEPD, www.aepd.es

¿Puedo retirar el consentimiento?

Tienes la posibilidad y el derecho a retirar el consentimiento para cualquier finalidad específica otorgada en su momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento que nos diste inicialmente.

En cualquier momento podrás deshabilitar la funcionalidad de acceso a tu ubicación/localización desde la configuración de tu móvil.

En cualquier momento podrás deshabilitar la funcionalidad de acceso a tu libreta telefónica.

¿Dónde puedo reclamar en caso de que considere que no se tratan mis datos correctamente?

Si consideras que tus datos no son tratados correctamente por **JOSEDOMINGO**, S.L. o que las solicitudes de ejercicio de derechos no han sido atendidas de forma satisfactoria, puede interponer una reclamación ante a la autoridad de protección de datos que corresponda, siendo la AEPD la indicada en el territorio nacional, www.aepd.es.

Seguridad y actualización de sus datos personales

Con el objetivo de salvaguardar la seguridad de tus datos personales, te informamos que **JOSEDOMINGO**, S.L. ha adoptado todas las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos personales suministrados. Todo ello para evitar su alteración, pérdida, y/o tratamientos o accesos no autorizados, tal como exige la normativa, si bien la seguridad absoluta no existe.

Es importante que, para que podamos mantener tus datos personales actualizados, nos informes siempre que se produzca una modificación de los mismos.

Confidencialidad

GESTIÓN INTELIGENTE DE CARGAS, S.L. te informa que tus datos serán tratados con el máximo celo y confidencialidad por todo el personal que intervenga en cualquiera de las fases del tratamiento. No cederemos ni comunicaremos a ningún tercero tus datos, excepto en los casos legalmente previstos, o salvo que el interesado nos hubiera autorizado expresamente.

Para tener todos estos pasos en cuenta y que a la hora de desarrollar una nueva aplicación no se nos pase nada, se ha desarrollado el siguiente checklist como herramienta de ayuda a los equipos de programación:

Paso	Descripción	SI/NO
1	Designación de responsable y encargado del tratamiento de datos.	
2	Pop up comprobando la edad.	

3	Se informa de los derechos PARSOL (Portabilidad, Acceso, Rectificación, Supresión, Ofuscación, Limitación)	
4	Se recogen los datos personales con fines determinados	
5	Se recogen los datos con fines legítimos	
6	Los datos personales se mantienen exactos	
7	Los datos personales se mantienen actualizados	
8	Pantalla de usuario donde ver los datos almacenados y ejercer su derecho de acceso	
9	Pantalla de edición de datos para ejercer su derecho sobre la rectificación de los datos personales inexactos respecto a la finalidad	
10	Opción de eliminar usuario para garantizar el derecho de supresión respecto a la finalidad	
10.1	Se mantienen los datos personales durante más tiempo del necesario respecto a la finalidad	
10.2	Se tratan con fines de archivo público	
10.3	Se tratan con fines de investigación científica	
10.4	Se tratan con fines históricos.	
11	Se tratan con fines estadísticos.	
12	Se han implantado medidas de seguridad para la integridad y seguridad de los datos (Accesos a la BBDD por perfiles, Vistas de tablas ocultas si no tienes el perfil, etc.)	
13	Se solicita el consentimiento de forma clara e independiente. Además de forma inteligible y de fácil acceso.	

14	Se informa al interesado de toda la información relativa al tratamietno	
15	Se informa con antes de recolectar los datos	
16	Se permite retirar fácilmente el consentimiento	
17	Se identifica si el usuario es menor de 14 años y se recaba el consentimiento al titular de la patria y potestad del niño	
18	Se verifica que el consentimiento fue dado por el titular de la patria y potestad	
19	Se tiene un formulario de contacto con el responsable de tratamiento para ejercer derecho de oposición	
20	Se tiene un formulario de contacto con el responsable de tratamiento para ejercer el derecho a la limitación del uso de datos	
21	Se aplican medidas técnicas adecuadas	
22	Las medidas se revisan y actualiza cuando es necesario	
23	Se informa a los destinatarios que serán comunicados los datos	
24	Se informa de plazo de conservación de los datos personales y de los criterios para establecer este plazo.	
25	Se suprimen los datos pasados el plazo de conservación	
26	Se limita el tratamiento de datos durante un plazo para verificar la exactitud de los datos.	
27	Se facilitan lo datos al usuario en un formato estructurado, de uso común y lectura mecánica	

15. Conclusiones

Antes de todo me gustaría aclarar que este trabajo lleva una elevada carga normativa, lo que ha hecho que el informe de turnitin de un alto porcentaje de plagio, pero se trata de las propias normativas o definiciones.

Lo primero de todo quiero dar las gracias a mi tutor Juan Vicente Oltra, porque si no fuera por él, hoy no habría acabado este trabajo. El confió en mí y supo apoyarme desde su posición como profesor y tutor en el camino recorrido con este TFG

Para mi este trabajo ha sido muy difícil de afrontar, no por la complejidad de este, si no por todo lo sucedido alrededor mío, ya que a principio de la pandemia perdí a 2 familiares haciéndome caer en una terrible depresión, agravándola con la muerte de otro familiar hace poco más de 1 año. Haciéndome perder mi trabajo y teniendo que volver a casa de mis padres. A día de hoy aun arrastro esta depresión y no he conseguido sacar fuerzas para poderlo hacer mejor. Sin embargo, Juan Vicente siempre ha estado ahí dándome apoyo y dejándome continuar con el proceso de este trabajo.

Por otro lado, debo admitir que el realizar este trabajo ha sido una experiencia muy bonita este año, porque supone un paso que creí que no podría dar, y el ver que he conseguido sacar fuerzas, investigar, explorar y aprender sobre protección de datos ha sido increíble.

Obviamente voy a recomendar que este trabajo se continue a futuro, ya que las nuevas tecnologías ofrecen retos muy grandes respecto a la protección de datos, ya sea por la propia evolución de las inteligencias artificiales, que ya son capaces de reconocer a personas, lo que podría vulnerar nuestro derecho a la intimidad. Como la tecnología de los ordenadores cuánticos, ya que la tecnología actual en Base de Datos para ofuscar y

encriptar los datos de las personas, se basan en algoritmos que para desencriptar si no tienes la clave tardarías años, sim embargo la con los procesadores cuánticos estas barreras se eliminarían ya que serían capaces de desencriptar en apenas minutos y habría que buscar otros medios para proteger los datos.

Los objetivos alcanzados de este trabajo creo que han sido claramente el poder acercar esta normativa a los desarrolladores, de una forma mas comprensible y accesible, así como la redacción de una guía que servirá para asegurarnos que cumplimos con todo lo que dice la normativa. Se ha creado también un checklist y un diagrama de flujo que los desarrolladores deben tener en cuenta ya que se muestra de forma clara y concisa que medidas se deben tomar para la correcta protección de datos y en que parte de la aplicación es mas sensible el tratamiento de datos personales.

16. Bibliografía

- INE, Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación (TIC) en los Hogares Año 2022
- BOE 294, de 6 de diciembre de 2018
- BOE número 137, de 9 de junio: Sala segunda. Sentencia 94/1998, de 4 de mayo.
- Real Decreto 1720/2007, de 21 de diciembre.
- Ley Orgánica 3/2018, de 5 de diciembre.
- Directiva 94/45/CE.
- Reglamento (UE) 2016/679 del parlamento europeo y del consejo del 27 de abril de 2016.
- Corrección de errores del Reglamento (UE) 2016/679 del parlamento europeo y del consejo del 27 de abril de 2016.
- Real decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de Agencia Española de Protección de Datos.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del sector Público.
- Memoria 2022 AEDP
- directiva 2002/58/CE
- Grupo de trabajo del artículo 29

17. Anexo I

OBJETIVOS DE DESARROLLO SOSTENIBLE

Grado de relación del trabajo con los Objetivos de Desarrollo Sostenible (ODS).

Objetivos de Desarrollo Sostenibles	Alto	Medio	Bajo	No Procede
ODS 1. **Fin de la pobreza.**				**X**
ODS 2. **Hambre cero.**				**X**
ODS 3. **Salud y bienestar.**			**X**	
ODS 4. **Educación de calidad.**			**X**	
ODS 5. **Igualdad de género.**				**X**
ODS 6. **Agua limpia y saneamiento.**				**X**
ODS 7. **Energía asequible y no contaminante.**				**X**
ODS 8. **Trabajo decente y crecimiento económico.**				**X**
ODS 9. **Industria, innovación e infraestructuras.**			**X**	
ODS 10. **Reducción de las desigualdades**.				**X**
ODS 11. **Ciudades y comunidades sostenibles**.				**X**
ODS 12. **Producción y consumo responsables.**				**X**
ODS 13. **Acción por el clima.**				**X**
ODS 14. **Vida submarina.**				**X**
ODS 15. **Vida de ecosistemas terrestres.**				**X**
ODS 16. **Paz, justicia e instituciones sólidas.**				**X**
ODS 17. **Alianzas para lograr objetivos.**				**X**

Reflexión sobre la relación del TFG/TFM con los ODS y con el/los ODS más relacionados.

En este TFG ha sido muy difícil por no decir casi imposible el poderlo relacionar con los Objetivos de Desarrollo sostenible debido a que es un trabajo dedicado a las leyes de protección de datos.

Sin embargo, hay un ODS que se ajusta mucho y es el numero 9: Industria, innovación e infraestructuras debido a que como desarrollamos en nuestro trabajo las políticas de protección de datos deben evolucionar con las nuevas tecnologías y la innovación para no quedarse desactualizadas.

En específico lo podemos relacionar estrechamente con el objetivo 9.c: Aumentar significativamente el acceso a la tecnología de la información y las comunicaciones y esforzarse por proporcionar acceso universal y asequible a internet en los países menos adelantados.

Es cierto que mi trabajo se centra en la normativa europea y española, así que deberíamos realizar un estudio de las normativas del país en el que queremos implementar la protección de datos.

Pese a lo anterior podemos coger como base las normativas europeas y españoles, así como la guía, diagrama y checklist creado como punto de partida, y así poder asegurar una correcta protección de los datos sensibles.

También es cierto que el objetivo 9.4 habla de aquí a 2030, y de cara a esa fecha ya deberíamos tener una nueva normativa de protección de datos y habría que adaptarse a la nueva normativa.

Hay que tener en cuenta que en estos días se está viviendo una revolución en lo que a inteligencia artificial se refiere, y para este tema aún se deben desarrollar muchísimo más las normas de protección de datos. También es cierto que si se garantiza la protección de datos las propias IA's pueden ayudar a cumplimentar el resto de los ODS.

Al tratarse de un análisis de normativa y una propuesta de acercamiento a los profesionales y creación de herramientas útiles a la hora de programar, no se puede relacionar con el ODS 1 ya que esto no ayudará a eliminar la pobreza.

Tampoco veo la relación con el ODS de Hambre 0 al tratarse de un trabajo sobre la protección de Datos.

Sin embargo, Si podría relacionar con el ODS 3: Salud y bienestar, ya que hoy en día es muy común encontrarnos con aplicaciones tanto para mejorar la salud como son las APPS para hacer deporte, como Aplicaciones médicas, mediante las cuales poder ver nuestros resultados médicos, que se nos informe de visitas y/o contacto con nuestros médicos.

también se desarrollaron aplicaciones de rastreo de COVID-19 que al final se demostró que vulneraban los derechos sobre protección de datos, ya que tener una enfermedad es algo privado y perteneciente al campo de los datos personales. Y

desarrollar una aplicación que sea capaz de rastrear con quien te cruzas y si tiene esta enfermedad vulneraba el derecho a la intimidad y privacidad.

En este caso si hubieran tenido una guía y un conocimiento sobre las normativas tanto europea como española podría haberse desarrollado de otra forma o darse cuenta que estaban desarrollando una aplicación que vulneraba los derechos

En todos estos casos hay que tener especial cuidado con el tratamiento de datos, ya que los datos sanitarios son datos personales, así como los datos de geolocalización o los datos que puedan recolectar las distintas aplicaciones deportivas, como pueden ser las pulsaciones.

Un reto al que nos hemos enfrentado en los últimos años ha sido una pandemia mundial, lo que ha hecho que, en la mayoría de los casos, se hayan tenido que descargar aplicaciones para poder seguir los cursos académicos. De esta forma podemos comprender que el ODS 4 de educación de calidad puede estar también relacionado con nuestro tema.

Debido a que muchas de estas aplicaciones han tenido acceso a geolocalizaciones, acceso a la cámara y al micrófono, y la mayoría de las estudiantes suelen ser menores de edad. Hay que tener especial cuidado en que datos se recolectan, como se tratan y del consentimiento adquirido para poder recolectarlos.

Todo esto aprendido se puede llevar a los países menos desarrollados y ayudarlos a evolucionar evitando malas prácticas y protegiendo a las personas de estos países.