

# **Reglamento General de Protección de Datos**

## **GESTIÓN DE PROYECTOS INFORMÁTICOS**

### **ALUMNOS**

Ángel Cardoso Parreño  
Alexander Andonov Aracil  
Daniel Gozálvéz Sánchez  
Gregorio Berná Domenech  
Alfonso Izura Concellón

### **PROFESOR**

Francisco José Mora Lizán

# Contenidos

<b>1</b>	<b>Conceptos generales/Definiciones</b>	<b>2</b>
1.1	Datos de carácter personal . . . . .	2
1.2	Tipos y usos de datos . . . . .	2
1.3	Portabilidad de los datos personales . . . . .	3
1.4	CEPD y AEPD . . . . .	3
<b>2</b>	<b>Participantes</b>	<b>4</b>
2.1	Aspectos generales a tener en cuenta por el responsable . . . . .	4
<b>3</b>	<b>Derechos</b>	<b>6</b>
3.1	Legislación . . . . .	6
3.2	Derechos del Interesado . . . . .	6
<b>4</b>	<b>Procedimiento y documentos a emplear para el registro de datos</b>	<b>7</b>
4.1	Procedimientos de los interesados . . . . .	7
4.2	Documentación para el debido cumplimiento del RGPD . . . . .	8
4.2.1	Documentos obligatorios . . . . .	8
4.2.2	Documentos circunstancialmente obligatorios . . . . .	9
4.3	Evaluación de Impacto . . . . .	9
<b>5</b>	<b>Obligaciones y Sanciones</b>	<b>10</b>
5.1	Proporcionar información a los interesados. . . . .	10
5.1.1	¿Que debe proporcionarse? . . . . .	10
5.1.2	¿Quien debe informar? . . . . .	11
5.1.3	¿Cuándo y cuándo no se debe informar? . . . . .	11
5.1.4	¿A través de que? . . . . .	12
5.2	Incumplimiento de la legislación relativa a la protección de datos de carácter personal y sanciones . . . . .	12
5.2.1	Infracciones leves . . . . .	12
5.2.2	Infracciones graves . . . . .	13
5.2.3	Infracciones muy graves . . . . .	13
5.3	Consentimiento del tratamiento de los datos de carácter personal. . . . .	14
5.4	Datos relativos a menores de edad. . . . .	14
5.5	Cumplimiento . . . . .	15
<b>6</b>	<b>Referencias</b>	<b>15</b>

# 1 Conceptos generales/Definiciones

El Reglamento General de Protección de datos (RGPD) es el reglamento europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos. Entró en vigor el 24 de mayo de 2016 y fue aplicada el 25 de mayo de 2018.

Es una normativa a nivel de la Unión Europea, por lo que cualquier empresa o aquellas empresas que tengan negocios en la Unión Europea, que manejen información personal de cualquier tipo, deberán acogerse a ella.

## 1.1 Datos de carácter personal

Los datos de carácter personal son cualquier información referente a personas físicas identificadas o identificables, pudiendo ser identificable toda persona cuya identidad pueda determinarse mediante un identificador o mediante el uso de uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de las personas.

Los datos de carácter personales que hayan sido anonimizados, cifrados o presentados con un seudónimo, pero que puedan utilizarse para volver a identificar a una persona, siguen siendo datos personales y se inscriben en el ámbito de aplicación del RGPD.

## 1.2 Tipos y usos de datos

Los datos personales se pueden usar para la identificación de cualquier usuario que se inscriba para el uso de nuestra aplicación.

Se pueden utilizar los siguientes datos personales:

- Nombre y apellidos.
- Domicilio.
- Dirección de correo electrónico.
- Número de documento nacional de identidad.
- Datos de localización.
- Dirección de protocolo de internet.

- El identificador de una cookie.
- El identificador de la publicidad del teléfono.
- Los datos en poder de un hospital o médico.

Se pueden utilizar los siguientes datos especialmente protegidos:

- Datos personales de origen étnico o racial.
- Opiniones políticas.
- Creencias religiosas o convicciones filosóficas.
- Afiliación sindical.
- Datos genéticos.
- Datos biométricos.
- Datos relativos a la salud o la vida sexual.
- Orientación sexual.

### **1.3 Portabilidad de los datos personales**

La portabilidad de los datos de carácter personal consiste en que el interesado tendrá derecho a que los datos de carácter personal se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

El interesado tendrá derecho a recibir los datos personales que le pertenezcan y 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.

### **1.4 CEPD y AEPD**

El comité Europeo de Protección de Datos (CEPD) es un organismo de la Unión Europea responsable de la aplicación del RGPD. Ayudará a garantizar que el Reglamento de protección de datos se aplica de forma coherente en toda la UE y trabajará para garantizar la cooperación efectiva entre las APD.

La Agencia Española de Protección de Datos (AEPD) es la organización española que vela por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

Las funcionalidades de la AEPD son:

1. Sensibilizar a responsables y encargados del tratamiento acerca del cumplimiento de sus obligaciones según la normativa de protección de datos.
2. Promover, dictaminar y aprobar la elaboración de códigos de conducta de acuerdo a la normativa.
3. Recomendaciones de adecuación de los tratamientos a la LOPD.
4. Realizar auditorías de protección de datos.
5. Requerir medidas de corrección.
6. Cancelación de los datos.
7. Notificar a responsables y encargados del tratamiento cuando se produzca una infracción de la normativa de protección de datos.
8. Acceder a las instalaciones de responsables y encargados para ejercer sus funciones de investigación.
9. Establecer limitaciones temporales del tratamiento de datos o su completa prohibición.
10. Autorizar las transferencias internacionales de datos.

## **2 Participantes**

En dicho documento se habla de dos participantes los interesados que normalmente son los consumidores de un servicio y los responsables que son aquellos que proveen dicho servicio.

### **2.1 Aspectos generales a tener en cuenta por el responsable**

#### **Independencia de la localización**

A la hora del tratamiento de datos por parte del responsable debe ser consciente que dicho reglamento es aplicado independientemente de la si dicho responsable se encuentra fuera de la unión siempre y cuando el interesado al que preste dicho servicio se encuentre residiendo en la Unión.[1]

### **Tratamiento información anónima**

La información anónima, la cual es aquella que no permita la identificación del interesado por medio de la misma no necesita estar sujeta al reglamento de protección de datos ya sea con fines estadísticos o de investigación.[2]

### **Tratamiento información personas fallecidas**

Para los datos de las personas fallecidas tampoco es necesario aplicar esta regulación en materia de su tratamiento de datos.[3]

### **Seudonimización**

En el tratamiento de datos el reglamento por parte del responsable debe ser posible el establecimiento de seudonimización permitiendo al responsable aun así realizar un análisis general de los mismos. Además dicho responsable deberá indicar cuales son las personas autorizadas para acceder a dichos datos.[4]

### **Cookies e identificadores temporales**

En ciertas situaciones la cookies o otros identificadores temporales pueden ser utilizadas para elaborar perfiles de personas físicas por lo que cabe tratarlos como datos sujetos a esta legislación.[5]

### **Consentimiento**

El consentimiento del almacenamiento de dicha información incluidas las mencionadas anteriormente deben transmitirse de manera clara al usuario el cual debe ser capaz de modificarlas. La ley deja claro que el silencio, casillas ya marcadas o la inacción NO corresponden consentimiento. También se deja claro que se debe manifestar abiertamente los datos que se están recogiendo de manera lícita y leal.[6]

### **Demostración**

Una vez se ha dado el consentimiento el responsable debe ser capaz de demostrar que efectivamente el interesado a dado su aprobación para el tratamiento de sus datos.[7]

### **Interés legítimo**

A la hora de almacenar dichos datos debe existir un interés legítimo por parte del responsable que justifique el almacenamiento de dichos datos.[8]

**Datos personales** La legislación hace especial incapie en la protección de aquellos datos relacionados con derechos o libertades fundamentales considerando orígenes étnicos y raciales como parte de estos datos. Al ser estos de carácter especial el reglamento establece que solo se podrán utilizar para fines relacionados con la salud.[9]

## 3 Derechos

### 3.1 Legislación

La legislación actual que vela por la protección de los derechos de carácter personal es el Reglamento General de Protección de Datos (RGPD).

Este lleva en vigencia desde el 27 de Abril de 2016.

En esta legislación se contemplan varios derechos que tienen como objetivo dar control al interesado sobre sus datos de carácter personal:

### 3.2 Derechos del Interesado

- **Derecho de Información y Acceso:**

Se otorga al usuario el derecho a poder acceder a sus datos personales y a conocer el tratamiento que sufren estos datos para verificar la validez del tratamiento.

Además, el interesado puede solicitar los fines por el que sus datos están siendo tratados, los destinatarios de sus datos.

- **Derecho de Rectificación:**

Se le debe otorgar al interesado la capacidad de poder rectificar. Además, el responsable esta obligado a responder a estas solicitudes en un periodo de un mes y explicar, en caso de que no se realizar la solicitud, los motivos de este hecho.

- **Derecho de retirar el consentimiento:**

El interesado tiene el derecho de poder retirar su consentimiento en cualquier momento. La retirada del consentimiento debe ser igual de fácil que otorgarlo. Además, el responsable tener la obligación de que el interesado sepa que ha otorgado su consentimiento.

- **Derecho de oposición:**

El interesado tiene el derecho de oponerse al tratamiento de sus datos de carácter personal, sobre todo si los tratamientos tienen fines de mercadotecnia o son tratados de manera ilícita.

Si los datos están siendo tratados de manera lícita y están siendo tratado con el objetivo de una interés público el responsable debe demostrar que los intereses del tratamiento son superiores a los del interesado.

Los tratamientos automáticos también tendrán las mismas reglas.

- **Derecho a la limitación del tratamiento:**

El interesado tendrá el derecho de solicitar la limitación del tratamiento respecto a sus

datos de carácter personal.

La limitación del tratamiento influye en el control que tiene el responsable sobre los datos, evitando la modificación o el borrado de los datos.

Este derecho se puede aplicar en los siguientes casos:

1. Si el interesado demuestra la injusticia o la ilegalidad en la exactitud de los datos.
2. Si el tratamiento es ilícito o el interesado se oponga a la supresión de los datos.
3. Si el responsable no necesita los datos pero el interesado si los necesite.

- **Derecho al Olvido:**

El interesado tendrá el derecho de solicitar inmediatamente la supresión de sus datos de carácter personal si se cumplen alguna de las siguientes condiciones:

1. Los datos personales ya no son necesarios para los fines por los que se recogieron.
2. Si el interesado retira su consentimiento y este no se base en un fundamento jurídico.
3. Si el interesado se ha opuesto al tratamiento de sus datos.
4. Si los datos han sido tratados ilícitamente.
5. Si los datos deben suprimirse para cumplir una obligación legal.

## 4 Procedimiento y documentos a emplear para el registro de datos

### 4.1 Procedimientos de los interesados

Por lo general no existen documentos formales que se deban seguir a la hora de que los usuarios puedan ejercer sus derechos por lo que es responsabilidad de las empresas realizar dichos procedimientos de manera transparente al usuario.

El reglamento expone que se debe poder identificar a dicho usuario para que sea capaz de ejercer dichos derechos y siempre y cuando la empresa no aporte un motivo de fuerza mayor por el cual no se puedan conocer dichos datos ya sea por se parte de la confidencialidad de la propia empresa o porque conocer dicha información compromete la confidencialidad de los demás datos.



## 4.2 Documentación para el debido cumplimiento del RGPD

La estructura de la mayoría de documentos necesarios para el debido cumplimiento del RGPD, no esta establecida explícitamente, con lo cual dejan flexibilidad a su estructuración pero no a su contenido y propósito.

Si un interesado requiere información relacionada al tratamiento de sus datos personales (a la que tiene derecho como se comenta en los siguientes apartados). Tiene derecho a recibir dicha información presentada de una manera estructurada y de uso común de manera que dicha lectura sea mecánica e interoperable.

### 4.2.1 Documentos obligatorios

1. Política de Privacidad: Constata los datos personales que se recogen de los usuarios, el motivo de su recogida y como se garantiza su privacidad.
2. Aviso de Privacidad: Con el objeto de informar a los usuarios sobre los alcances y condiciones generales del tratamiento de sus datos personales.
3. Aviso de Privacidad de los Empleados: Con el objeto de informar a los empleados sobre los alcances y condiciones generales del tratamiento de sus datos personales.
4. Política de Retención de Datos: Es el protocolo establecido para el periodo de retención de información.
5. Registro de Retención de Datos: Enumera hasta que fecha se almacenarán los datos personales.
6. Formulario de Consentimiento del Interesado: Utilizado para obtener el consentimiento para tratar los datos personales de los interesados con una finalidad específica.
7. Formularios de Consentimiento Paterno: Utilizado para obtener el consentimiento del tutor/tutora legal de un menor para tratar con sus datos personales.
8. Registro de EIPD: Agrupa las evaluaciones de impacto relacionadas con la privacidad y cuyo objetivo es identificar y analizar cómo la privacidad de los datos puede verse afectada por determinadas acciones.
9. Acuerdo de Tratamiento de Datos del Proveedor: Establece los límites y condiciones bajo los cuales un proveedor puede procesar datos personales en nombre de la compañía.
10. Procedimiento de Respuesta a la Violación de Seguridad de Datos: Describe como reaccionar ante violaciones de seguridad de datos personales e intentar mitigarlas.

11. Notificación de brechas de datos personales: Accesible a través de la sede electrónica de la AEPD, notifica a esta autoridad de control de una brecha de datos personales.
12. Formulario de Notificación de Violación de Seguridad de Datos a los Afectados: Cuando se produce una brecha de datos es necesario notificar a las entidades o personas involucradas.

#### **4.2.2 Documentos circunstancialmente obligatorios**

1. Descripción del puesto de Delegado de Protección de Datos:
  - El tratamiento es llevado a cabo por una autoridad u organismo público
  - El tratamiento de las operaciones de tratamiento requieren un seguimiento regular a gran escala
  - El tratamiento de incluye datos especialmente sensibles
2. Registro de actividades de tratamiento: Se documentan los flujos de datos personales que circulan dentro de una entidad. Deben estar disponibles para su presentación a la autoridad de control, si esta los requiere.
  - La empresa tiene más de 250 empleados
  - El tratamiento de los datos personales puede ocasionar un riesgo para los derechos y libertades de los interesados
  - El tratamiento de los datos no es ocasional
  - El tratamiento incluye datos penales
  - El tratamiento incluye datos especialmente sensibles
3. Cláusulas Contractuales para la Transferencia de Datos Personales a Responsables
  - Si el responsable trabaja fuera del Área Económica Europea
4. Cláusulas Contractuales para la Transferencia de Datos Personales a Encargados:
  - Si el encargado trabaja fuera del Área Económica Europea

### **4.3 Evaluación de Impacto**

Una evaluación de impacto es una revisión realizada cuando el tratamiento de datos incluye un alto riesgo de que dicha información comprometa libertades o derechos de personas físicas.

Esta evaluación debe evaluar el origen, la naturaleza, la particularidad y la gravedad de los riesgos presentes. Una vez realizado se deben tomar las medidas pertinentes para asegurar que

dicha información cumple con el reglamento.

Si es dado el caso en el cual dicho tratamiento no puede otorgar las suficientes garantías, el responsable deberá consultar a una autoridad en el control de los datos antes del tratamiento de dichos datos.

Para evitar cargas excesivas en el apartado administrativo y financiero, el reglamento establece que dichas consultas solo deben hacerse en casos con un alto riesgo por el tipo de datos tratados o cuando se utiliza una nueva tecnología que previamente no ha sido sometida a este procedimiento. En estos casos recoge que es fundamental la medidas, garantías y mecanismos previstos para mitigar el los posibles riesgos.[10]

## 5 Obligaciones y Sanciones

### 5.1 Proporcionar información a los interesados.

#### 5.1.1 ¿Que debe proporcionarse?

Antes de la entrada en vigor del Reglamento General de Protección de Datos (RGPD), la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) estipulaba las siguientes obligaciones en torno a la información que se ha de facilitar a las personas interesadas:

- La existencia del fichero o tratamiento, su finalidad y destinatarios.
- El carácter obligatorio o no de la respuesta, así como de sus consecuencias.
- La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- La identidad y datos de contacto del responsable del tratamiento.

Con la entrada en vigor del Reglamento General de Protección de Datos se añaden requisitos adicionales de los que se ha de informar a las personas interesados, incorporando, en líneas generales, los siguientes detalles:

- Los datos de contacto del Delegado de Protección de Datos
- La base jurídica o legitimación para el tratamiento
- El plazo o los criterios de conservación de la información
- La existencia de decisiones automatizadas o elaboración de perfiles

- La previsión de transferencias a Terceros Países
- El derecho a presentar una reclamación ante las Autoridades de Control

Y, en caso de que los datos obtenidos no se obtuvieran directamente del propio interesado:

- El origen de los datos
- Las categorías de los datos

### **5.1.2 ¿Quien debe informar?**

La obligación de informar a las personas interesadas sobre las circunstancias relativas al tratamiento de sus datos recae sobre el Responsable del Tratamiento.

### **5.1.3 ¿Cuándo y cuándo no se debe informar?**

La información se debe poner a disposición de los interesados en el momento en que se soliciten los datos, previamente a la recogida o registro, si es que los datos se obtienen directamente del interesado.

Si los datos no se obtuvieran directamente del interesado, por proceder de alguna cesión legítima, o de fuentes de acceso público, el Responsable informará a las personas interesadas dentro de un plazo razonable, pero en cualquier caso:

- antes de un mes desde que se obtuvieron los datos personales
- antes o en la primera comunicación con el interesado
- antes de que los datos, en su caso, se hayan comunicado a otros destinatarios

Esta obligación se debe cumplir sin necesidad de requerimiento alguno, y el responsable deberá poder acreditar con posterioridad que la obligación de informar ha sido satisfecha.

El único contexto en el que se puede no informar al interesado es cuando este ya dispone de la información, si es información obtenida directamente del interesado.

Si los datos no proceden del interesado, no es necesario informar cuando:

- la comunicación resulte imposible o suponga un esfuerzo desproporcionado

- el registro o la comunicación esté expresamente establecido por el Derecho de la Unión o de los Estados miembros
- cuando los datos deban seguir teniendo carácter confidencial por un deber legal de secreto

#### **5.1.4 ¿A través de que?**

Como los procedimientos de recogida de información pueden ser muy variados, la forma en la que se informa a los interesados debe adaptarse a las circunstancias de cada una de estas. Puede ser a través de un formulario en papel, formulario web, entrevista telefónica, registro de aplicaciones móviles, etc.

Dependiendo del medio usado, las características como extensión, legibilidad, espacio, etc. pueden variar, pero en cualquier caso, la información a las personas interesadas debe proporcionarse:

- con un lenguaje claro y sencillo
- de forma concisa, transparente, inteligible y de fácil acceso

## **5.2 Incumplimiento de la legislación relativa a la protección de datos de carácter personal y sanciones**

Podemos dividir las infracciones en tres magnitudes, cada una con sus rangos de sanciones correspondientes: leves, graves y muy graves.

### **5.2.1 Infracciones leves**

Estas infracciones pueden costar entre 900 y 40.000 euros. Son consideradas infracciones leves las siguientes:

- No remitir a la Agencia Española de Protección de Datos las notificaciones previstas legalmente.
- No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos.
- El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos sean recabados del propio interesado.
- La transmisión de los datos a un encargado del tratamiento sin dar cumplimiento a los deberes formales establecidos en la ley.

### 5.2.2 Infracciones graves

Estas infracciones pueden costar entre 40.001 y 300.000 euros. Son consideradas infracciones graves las siguientes:

- Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el “Boletín Oficial del Estado” o diario oficial correspondiente.
- Tratar datos de carácter personal sin recabar el consentimiento de las personas afectadas, cuando el mismo sea necesario conforme a lo dispuesto en la Ley.
- Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la Ley y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy grave.
- La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal.
- El impedimento o la obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación y oposición.
- El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos no hayan sido recabados del propio interesado.
- El incumplimiento de los restantes deberes de notificación o requerimiento al afectado impuestos por la ley.
- Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad
- No atender los requerimientos o apercibimientos de la Agencia Española de Protección de Datos o no proporcionar a aquélla cuantos documentos e informaciones sean solicitados por la misma.
- La obstrucción al ejercicio de la función inspectora.
- La comunicación o cesión de los datos de carácter personal sin contar con legitimación para ello, salvo que la misma sea constitutiva de infracción muy grave.

### 5.2.3 Infracciones muy graves

Estas infracciones pueden costar entre 300.001 y 600.000 euros. Son consideradas infracciones muy graves las siguientes:

- La recogida de datos en forma engañosa o fraudulenta.

- Tratar o ceder los datos de carácter personal salvo en los supuestos en que la ley lo autoriza o violentar algunas prohibiciones específicas de la ley.
- No cesar en el tratamiento ilícito de datos de carácter personal cuando existiese un previo requerimiento del Director de la Agencia Española de Protección de Datos para ello.
- La transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia Española de Protección de Datos salvo en los supuestos en los que no sea necesario porque así lo indique la ley.

### **5.3 Consentimiento del tratamiento de los datos de carácter personal.**

El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. 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. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta.

### **5.4 Datos relativos a menores de edad.**

En el artículo 7 de la Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales se establece que el tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años. Para menores de 14 años, el consentimiento para la utilización de los datos personales de este se otorgará por sus padres o tutores legales, teniendo el responsable del tratamiento hacer esfuerzos razonables para verificar que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.

## 5.5 Cumplimiento

Como se ha visto, es obligatorio el cumplimiento del Reglamento General de Protección de Datos y su incumplimiento es penado por ley, por ello, habrá que garantizar su cumplimiento para evitar pérdidas monetarias de gran calibre, como se ha visto en apartados anteriores.

## 6 Referencias

[1] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 Artículo 22, 23, 24 y 25.

[2] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 Artículo 26.

[3] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 Artículo 27.

[4] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 Artículo 28 y 29.

[5] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 Artículo 30.

[6] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 Artículo 32 y 39.

[7] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 Artículo 42.

[8] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 Artículo 47 y 49.

[9] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 Artículo 51.

[10] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 Artículo 84, 89 y 90.