
# Guía de Protección de Datos por Defecto

*octubre de 2020*

# RESUMEN EJECUTIVO

Esta guía desarrolla de forma práctica la aplicación de la protección de datos por defecto, o PDpD, en los tratamientos de datos personales a partir de lo establecido en el artículo 25 del RGPD y la guía publicada por el Comité Europeo de Protección de Datos “Guidelines 4/2019 on Article 25 Data Protection by Design and by Default”.

Las medidas de PDpD giran en torno a la aplicación racional del principio de minimización de datos, bajo los criterios de adecuación, pertinencia y necesidad con relación a los fines en el diseño de las distintas fases del tratamiento, tal como establece el artículo 25.2.

Este documento identifica las estrategias que han de guiar la aplicación de la PDpD, como son la optimización, la configurabilidad y la restricción en el tratamiento de datos personales por defecto. A continuación, se desarrollan las medidas específicas para la implementación de la PDpD con relación a la cantidad de datos personales recogidos, la extensión del tratamiento, el periodo de conservación y la accesibilidad de los datos. Finalmente, se recogen los requisitos de documentación y auditoría con relación a la PDpD.

Los destinatarios son los responsables de tratamiento y Delegados de Protección de Datos, además de aquellas unidades o departamentos que, dentro de la entidad responsable, tienen a su cargo el diseño, selección, desarrollo, despliegue, y explotación de aplicaciones y servicios. También está dirigido a aquellos con el rol de encargados, desarrolladores o suministradores, en la medida que proporcionan productos y servicios a responsables, y busquen que éstos cumplan con los requisitos de PDpD establecidos en el RGPD.

**Palabras clave**: RGPD, responsabilidad proactiva, protección de datos por defecto, protección de datos desde el diseño, riesgo, minimización de datos.

# ÍNDICE


I. OBJETIVO Y DESTINATARIOS 4

II. INTRODUCCIÓN 5

III. APLICACIÓN DE LA PROTECCIÓN DE DATOS POR DEFECTO 7

IV. OPTIMIZACIÓN DEL TRATAMIENTO 9

A. Análisis del Tratamiento 9

B. Casos de uso 11

C. Relaciones entre tratamientos 12

D. Adaptación del tratamiento 13

V. CONFIGURABILIDAD 15

A. Configurabilidad de un tratamiento 15

B. Configurabilidad en los componentes 17

C. Control del usuario 18

VI. RESTRICCIÓN POR DEFECTO 20

VII. MEDIDAS DE PROTECCIÓN DE DATOS POR DEFECTO 21

A. Cantidad de datos personales recogidos. 21

B. La extensión de su tratamiento. 21

C. El periodo de conservación. 22

D. La accesibilidad de los datos 22

E. Aplicación práctica de las medidas a implantar: opciones de configuración 22

VIII. DOCUMENTACIÓN Y AUDITORÍA 24

IX. CONCLUSIONES 27

X. ANEXO I: RGPD 28

A. Artículo 6.4 28

B. Artículo 25 Protección de datos desde el diseño y por defecto 28

C. Considerando 78 28

XI. ANEXO II: LISTA DE OPCIONES DE CONFIGURACIÓN 30

XII. BIBLIOGRAFÍA 39

# I. OBJETIVO Y DESTINATARIOS

El objetivo de este documento es proporcionar una guía práctica para la aplicación de medidas concretas de protección de datos por defecto.

Como se establece en el segundo apartado del artículo 25 del Reglamento (UE) 2016/679, General de Protección de Datos (en adelante RGPD), corresponde al responsable del tratamiento la implementación de las medidas de Protección de Datos por Defecto (en adelante, PDpD).

Esta guía va dirigida a los Delegados de Protección de Datos y, específicamente, a aquellas unidades o departamentos que, dentro de la entidad responsable del tratamiento, tienen a su cargo el diseño, selección, desarrollo, despliegue y uso de aplicaciones y servicios.

En el caso de que la entidad responsable utilice los servicios de terceros para la implementación efectiva de un tratamiento, el responsable tiene la obligación, de acuerdo con el artículo 28 del RGPD, de "*elegir únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del Reglamento y garantice la protección de los derechos del interesado.*".

En este sentido, el responsable deberá tener en mente su obligación de aplicar la protección de datos desde el diseño y por defecto a la hora de seleccionar tanto a los encargados de tratamiento como a los proveedores de productos y soluciones que utilicen para su tratamiento. Por otro lado, el considerando 78 del RGPD, insta a los desarrolladores de productos, servicios y aplicaciones a que, aunque no tengan la consideración de responsables o encargados del tratamiento, consideren el derecho a la protección de datos cuando desarrollen y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos.

De este modo, esta guía también está dirigida a encargados, desarrolladores o suministradores que quieran que sus productos o servicios permitan a los responsables cumplir con los requisitos de PDpD establecidos en el RGPD.

No obstante, hay que recordar que el criterio para establecer la responsabilidad en un tratamiento se basa en determinar quién especifica los fines perseguidos y los medios utilizados. Cuando el encargado, o el suministrador de sistemas/soluciones, incluya en sus productos tratamientos colaterales de datos personales de los usuarios finales (por ejemplo, para "mejorar el servicio", "depurar el sistema", "ofrecer publicidad", "hacer seguimiento del uso de licencias", "mantenimiento de la solución", etc.) podría estar asumiendo, en estos casos, la consideración de responsable del tratamiento.

## II. INTRODUCCIÓN

El artículo 25 del RGPD establece que los principios, derechos y obligaciones relativos a la protección de datos recogidos en dicho Reglamento han de tenerse en cuenta 'desde el diseño y por defecto'. En este sentido, una aplicación demostrable de la protección de datos por defecto se convierte en una de las medidas de responsabilidad proactiva que permite acreditar el cumplimiento de las obligaciones establecidas en la norma.

Si bien el cumplimiento de las exigencias previstas en el Reglamento es obligatorio con independencia de la naturaleza y tamaño de la entidad responsable del tratamiento, el RGPD se muestra flexible a la hora de seleccionar las medidas para garantizar este cumplimiento, pudiendo optar por diferentes aproximaciones y alternativas a la hora de implementar la dimensión de PDpD.

La configuración 'por defecto' de aplicaciones, productos y servicios es algo común en el desarrollo y puesta en producción de sistemas a la hora de determinar su funcionamiento. En el RGPD se ha fijado la obligación que tienen los responsables de garantizar una protección de la PDpD de los datos personales objeto de tratamiento en línea con dicha configuración 'por defecto'.

El apartado 2 de dicho artículo establece que:

> *"El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la* ***cantidad*** *de datos personales recogidos, a la* ***extensión*** *de su tratamiento, a su* ***plazo*** *de conservación y a su* ***accesibilidad****. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas."*

Los parámetros de las distintas opciones de configuración que definen la implementación del tratamiento han de ser establecidos por el responsable. En algunos casos, dependiendo de la naturaleza del tratamiento, en el diseño que haya realizado el responsable algunas de esas opciones de configuración podrían estar puestas a disposición del usuario.

A su vez, el documento "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default"[1] (Directrices sobre el artículo 25 Protección de datos desde el diseño y por defecto) del Comité Europeo de Protección de Datos (en adelante la Guía del CEPD) manifiesta en el apartado 2.2 "Protección de datos por defecto" que la PDpD hace referencia a las elecciones realizadas con respecto a los valores de configuración u opciones de tratamiento fijadas en los sistemas y procedimientos que implementan el tratamiento y que determinan la cantidad de los datos personales recopilados, el alcance de su procesamiento, el período de su conservación y su accesibilidad**.**

El RGPD exige del responsable una configuración por defecto de los tratamientos que sea respetuosa con los principios de protección de datos, abogando por un procesamiento mínimamente intrusivo: mínima cantidad de datos personales, mínima extensión del tratamiento, mínimo plazo de conservación y mínima accesibilidad a datos personales. Todo ello, además, sin que sea necesaria la intervención del interesado para garantizar que estos mínimos están establecidos. De ahí que la PDpD no se limita a requisitos sobre

[1] Publicadas en versión draft en https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_es

el programas o dispositivos, sino que afecta también al propio diseño del tratamiento, con independencia del soporte en el que se desarrolle el mismo.

En el párrafo 47 de la misma Guía se manifiesta que las medidas de seguridad siempre se han de incluir por defecto:

> *La seguridad de la información debe estar siempre por defecto en todos los sistemas, transferencias, soluciones y opciones cuando se tratan datos de carácter personal.*

Esto significa que, aunque el riesgo del tratamiento para los derechos y libertades sea escaso[2], el responsable no puede ignorar el establecimiento de medidas de seguridad. Ahora bien, a la hora de elegir las medidas concretas de seguridad que se han de implementar, el proceso de selección de cada una de ellas ha de estar guiado por un análisis de riesgos para los derechos y libertades de las personas físicas, tal y como se establece en el artículo 32 del RGPD.

El RGPD no pretende ser exhaustivo en las medidas que hay que implementar por el solo hecho de que exista un tratamiento de datos personales. Para ello incluye el concepto de la PDpD, para abarcar todas aquellas medidas y garantías de "*configuración por defecto*" que, independientemente del riesgo, es necesario establecer por "*la naturaleza, el ámbito, el contexto y los fines del tratamiento*"[3].

Como cualquier otra medida de responsabilidad proactiva, la PDpD hay que abordarla integrada con el resto de las garantías establecidas en el RGPD y como parte integral de los procedimientos y de la cultura de la organización.

Por un lado, como subraya la Guía del CEPD, la PDpD está relacionada con la protección de datos desde el diseño, ya que las medidas de PDpD han de ser tenidas en cuenta desde la concepción del tratamiento e implementadas mediante las medidas y garantías de protección de datos identificadas en el diseño de la solución.

La selección de medidas y garantías para la PDpD tienen influencia sobre los requisitos que se establecen sobre los dominios de seguridad (confidencialidad, disponibilidad, integridad y autenticidad) desde un punto de vista de "seguridad por defecto". Sin embargo, ha de tenerse en cuenta que la seguridad por defecto, en determinadas situaciones, puede entrar en tensión con la PDpD. Un ejemplo concreto es llevar al exceso las actividades de monitorización o autenticación de usuarios de forma tal que la información personal obtenida del usuario pueda representar un riesgo[4] para los derechos y libertades de los usuarios cuyos accesos al sistema, producto o servicio se pretende gestionar.

Finalmente, la PDpD está relacionada con la transparencia, pues solo conociendo las características del tratamiento, el usuario estará en disposición de decidir, libremente y con conocimiento de las posibles consecuencias, ir más allá de la configuración inicial más respetuosa con la privacidad, seleccionando aquellas opciones de la aplicación, producto o servicio que afecten significativamente a esta.

---

[2] El riesgo del tratamiento, por muy escaso que sea, nunca será nulo.

[3] Artículo 24.1 del RGPD

[4] Un riesgo para sus derechos y libertades en cuanto a se realice una observación o evaluación sistemática y exhaustiva de aspectos personales.

## III. APLICACIÓN DE LA PROTECCIÓN DE DATOS POR DEFECTO

En el apartado 2.2 de la Guía del CEPD se realiza un análisis del apartado 2 del artículo 25 de RGPD. La opinión fijada por el Comité Europeo de Protección de Datos con relación a la implementación de medidas de PDpD se centra en tres estrategias:

- **Optimizar**: La optimización del tratamiento persigue analizarlo desde el punto de vista de la protección de datos, lo que supone aplicar medidas con relación a la cantidad de datos recogidos, la extensión del tratamiento, su conservación y accesibilidad.
- **Configurar**: Esta estrategia debe permitir que el tratamiento sea configurable con relación a los datos personales mediante valores (ajustes) disponibles en las aplicaciones, dispositivos o sistemas que lo implementan. Parte de esa configurabilidad ha de estar bajo el control del usuario.
- **Restringir**: La restricción garantiza que, por defecto, el tratamiento es lo más respetuoso posible con la privacidad, de modo que, las opciones de configuración han de estar ajustadas, por defecto, en aquellos valores que limiten la cantidad de datos recogidos, la extensión del tratamiento, su conservación y accesibilidad.

Estas tres estrategias están vinculadas con las correspondientes estrategias de minimizar y controlar definidas en la Guía de Protección de Datos desde el Diseño de la AEPD, como además se explicita en el apartado 2.2 de la Guía del CEPD.

En la Guía del CEPD se subraya que las medidas de PDpD han de estar alineadas con las adoptadas en el marco de la protección de datos desde el diseño, orientadas específicamente a la aplicación del principio de minimización de datos, y que dichas medidas han de seleccionarse en función de su adecuación para la consecución de ese objetivo en los términos señalados anteriormente. Además, se explicita que solo se procesen los datos personales que son necesarios para el propósito específico del tratamiento. Explícitamente se hace referencia a los artículos 5.1.b, c, d y e del RGPD. En particular, el artículo 5.1.c del RGPD establece el principio de minimización como que los datos personales serán *"adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados"*.

A su vez, en la Guía del CEPD se manifiesta que el hecho de que se necesiten datos personales para cumplir un propósito no significa que se puedan llevar a cabo todos los tipos de operaciones en el tratamiento de dichos datos y con cualquier frecuencia. Esto supone que el tratamiento ha de ser analizado en sus distintas fases y en cada una de ellas se tratarán los datos mínimos imprescindibles para la operación que se efectúe en cada fase, la extensión de las fases en las que se trate el dato será la mínima necesaria, el periodo de conservación de la información será el menor posible y la accesibilidad a los datos personales será la mínima imprescindible, tal y como se establece en el artículo 25.2 del RGPD:

> *Art.25.2 …Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad.*

La aplicación del principio de minimización no es algo trivial, pues requiere estudiar, justificar y establecer qué datos son necesarios para el tratamiento. Los datos necesarios se determinan mediante un análisis del conjunto de datos con relación a la eficacia que es necesario alcanzar para cumplir con los propósitos del tratamiento. Dicho análisis, en la extensión de los sujetos implicados y en la extensión de los datos tratados de cada sujeto, dependerá del tipo de tratamiento. Por ejemplo, con relación a la extensión de personas afectadas, la ciencia estadística establece que el universo de sujetos necesario para

obtener el nivel e intervalo de confianza deseado en un tratamiento no implica el acceso a los datos de toda la población, sino que existen procedimientos analíticos para establecer el volumen necesario[5].

Sin embargo, es un error realizar una aplicación del principio de minimización que comprometa el propósito tratamiento. Por ejemplo, con relación a la extensión de datos tratados de un sujeto, diseñar una evaluación clínica que recoja información insuficiente de tal forma que no sea posible alcanzar un diagnóstico del individuo con los niveles de precisión adecuados, no solo no cumpliría con el principio de minimización, sino que iría incluso en contra del principio de lealtad del tratamiento, al ser inviable poder cumplir con el propósito declarado. Por lo tanto, la aplicación del principio de minimización implica un análisis objetivo y racional del tratamiento.

[5] Por ejemplo, para realizar un análisis de una población de 40 millones con un nivel de confianza del 99% y un intervalo de confianza del 1% podrían ser necesarios los datos de menos de 20.000 personas (https://www.surveysystem.com/sscalc.htm, https://www.calculator.net/sample-size-calculator.html)

# IV. OPTIMIZACIÓN DEL TRATAMIENTO

La optimización de los tratamientos es una actividad fundamental en cualquier entidad con el objeto de conseguir la mejora continua en su eficacia y eficiencia. En este apartado solo se tratará dicha optimización desde el punto de vista de la protección de datos de carácter personal, visión que debería estar integrada en el proceso global de calidad de la entidad.

Para la adopción de cualquier medida de responsabilidad proactiva es imprescindible analizar la actividad de tratamiento, dividirlo en sus fases, determinar las operaciones de tratamiento realizadas en cada una de ellas, conocer las particularidades de cada fase y optimizarla, al menos desde el punto de vista de protección de datos. Como se ha indicado anteriormente, esta tarea no es exclusiva de la PDpD, sino que forma parte de la estrategia para la aplicación racional de las medidas de responsabilidad proactiva.

La optimización del tratamiento para la implementación de la PDpD hay que realizarla llevando a cabo las siguientes actividades, que en algún caso se realizarán en paralelo:

- Una descomposición y análisis del tratamiento en fases
- La definición de casos de uso
- El estudio de la relación entre tratamientos realizados por un mismo responsable.
- La optimización del tratamiento

## A. ANÁLISIS DEL TRATAMIENTO

Para una adecuación correcta de las medidas PDpD, el responsable debe analizar el tratamiento que pretende llevar a cabo. El análisis debe ir más allá que considerar el tratamiento como una caja negra. Hay que identificar dentro de él aquellas operaciones singulares que se llevan a cabo y la relación entre ellas.

Las operaciones que pueden formar parte de un tratamiento, y que son de interés para protección de datos, están definidas, de forma no exhaustiva, en el artículo 4.2 del RGPD como:

> *… recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.*

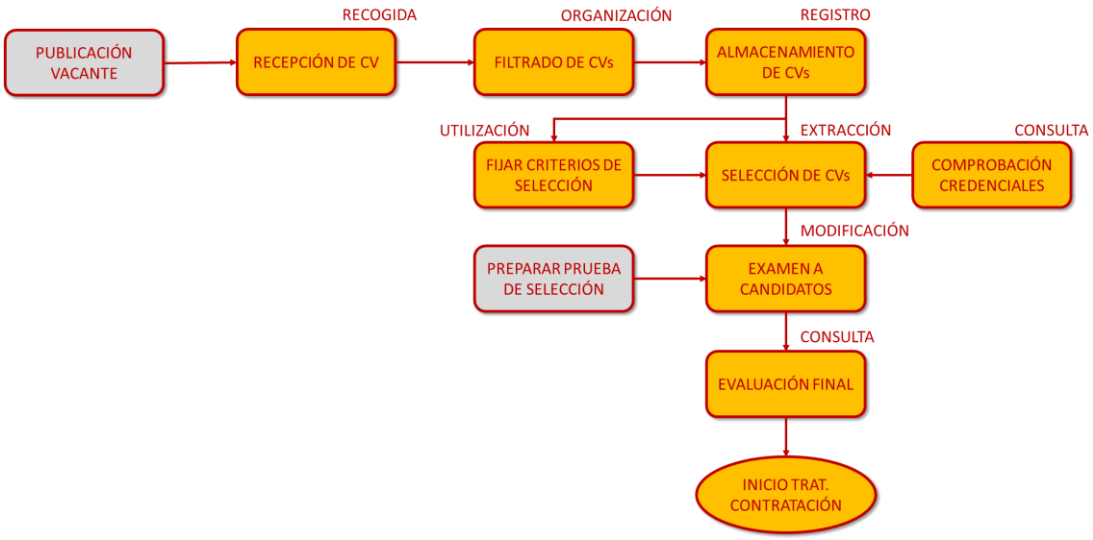

Figura 1. Ejemplo simplicado de una actividad de tratamiento relativa a la selección de personal. En este caso, se marca para cada fase la operación u operaciones realizadas. En sombreado se encuentran aquellas fases que, en este ejemplo, no tratarían datos de carácter personal.

Las actividades de tratamiento se estructuran en fases que implementan operaciones. No obstante, cabe la posibilidad de que, como parte de un tratamiento, existan fases que no traten datos personales de modo que, y en un principio, dichas fases serían transparentes desde el punto de vista de protección de datos[6].

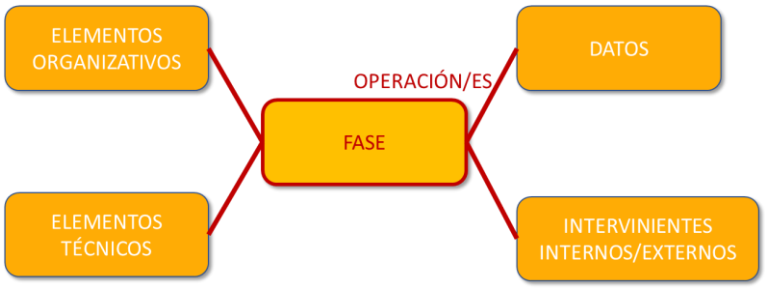


Figura 2. Elementos que configuran las fases de un tratamiento

La implementación de las operaciones en cada fase en la que se estructura el tratamiento se puede realizar con medidas organizativas y/o elementos técnicos. Las medidas organizativas, que pueden incluir aspectos como los roles asignados a cada persona, la distribución física de las instalaciones (por ejemplo, el aislamiento de zonas de entrevista) o la generación y destrucción de informes físicos, pueden ser incluso más importantes y efectivas que los componentes técnicos.

Las operaciones de un tratamiento pueden implementarse mediante componentes desarrollados *ad-hoc*, es decir, específicamente para ese tratamiento o a través de componentes estándar o adaptaciones de desarrollos *ad-hoc* de otros tratamientos. Estos componentes pueden ser desde aplicaciones, servidores, sistemas operativos, componentes de red, librerías, entornos de desarrollo, etc. También pueden ser componentes de terceros, estándares o simplemente componentes a disposición del responsable, que se reutilizan para un nuevo propósito. Entre estos se encuentran incluso componentes que pueden tener un carácter más organizativo que técnico, como servicios de atención al cliente.

En estos casos, normalmente se utiliza el término componentes *off-the-shelf*[7], que significa componentes preexistentes que se "toman de la estantería". Componentes *off-the-shelf* son aquellos prefabricados, diseñados para otro propósito específico, que provienen incluso de usos anteriores por la misma entidad, o de propósito general, que se incorporan a la implementación de un tratamiento.

En el RGPD se establece que, a la hora de establecer la configuración por defecto, el responsable del tratamiento ha de tener en cuenta los requisitos de necesidad para el propósito específico perseguido por el tratamiento. Por lo tanto, en el análisis que se realice de la actividad de tratamiento, se ha de determinar la pertinencia y necesidad de realizar todas y cada una de las distintas fases/operaciones de tratamiento de datos personales que se hayan identificado.

[6] Aunque las fases que no traten datos de carácter personal o no afecten de forma colateral a lo establecido en el RGPD sí tengan influencia en el análisis de la eficacia y eficiencia del tratamiento, no entraría dentro de las competencias del RGPD evaluar la adecuación de dichas fases de forma estricta.

[7] Término que también se utiliza en la Guía del CEPD

En definitiva, es obligatoria una revisión crítica de cada fase y su propósito para aplicar el principio de minimización.

## B. CASOS DE USO

Los tratamientos pueden ser muy sencillos y lineales, en los que las opciones de configuración por defecto sean muy limitadas, pero también podemos encontrarnos ante tratamientos complejos que pueden ofrecer diferentes funcionalidades para adaptarse a usuarios de distintos perfiles o con necesidades concretas. El ajuste del servicio puede depender de distintas circunstancias: servicios normales o premium, adecuación a un público menor de edad, adulto o de tercera edad, presencia de servicios de valor añadido, etc. Los distintos ajustes del servicio son los que configuran diferentes casos de usos.

Dependiendo del tipo de servicio que precisa el usuario, o que el responsable le pretende ofrecer en el marco de un mismo tratamiento, será necesario recabar y procesar una distinta extensión de datos personales. Un ejemplo, simplificado, podría ser los distintos casos de uso de una app bancaria:


Figura 3. Descomposición en fases del tratamiento en una app bancaria simplificada.

En el ejemplo anterior se muestra un tratamiento en el que se pueden plantear varios casos de uso según la funcionalidad deseada por el usuario final:

- Gestión de la cuenta, en la que se precisa una identificación.
- Pagos, en la que además de la identificación, es necesario la comunicación con un interfaz de pagos.
- Localización de oficinas, que necesita el acceso a la posición actual.
- Recepción de ofertas por proximidad, que precisa de una geolocalización continua del interesado.

En función de los casos de uso el responsable ha de tratar una extensión distinta de datos personales, entre otros la identificación del usuario, los interfaces con las pasarelas de pago, la geolocalización puntual o la geolocalización continua. Esto implica que el tratamiento ha de ser configurable en el tipo y extensión de dichos datos y que dicha configuración ha de estar condicionada por el caso de uso elegido por el usuario en cada momento. No se deberían recabar por defecto los datos que serían necesarios para un potencial uso de todas las funcionalidades futuras, incluidas las que podrían ser a elección por el usuario. Por ejemplo, en el caso de recogida de datos en un formulario web para la reservar plaza en un servicio, por ejemplo, de reparación, en el que es posible que se rechace la solicitud por falta de disponibilidad, no se deberían recoger inicialmente más datos de los necesarios para hacer la reserva, y no datos adicionales que se emplearían

para proporcionar el servicio en el caso de que existan vacantes. En su caso, estos se deberían solicitar una vez garantizada la disponibilidad.

Otros tratamientos en los que se pueden encontrar diferentes casos de uso son, entre otros:

- En una red social, en función del grado de la difusión de información personal que desea el usuario.
- En pulseras de fitness, en función de los servicios seleccionados: entrenamiento, seguimiento, estadísticas, salud…
- En apps para el seguimiento de epidemias, con relación a los servicios de diagnóstico o seguimiento.
- En dispositivos para telemedicina, en función del tratamiento deseado.
- En plataformas y apps en entornos educativos y de formación, dependiendo del tipo de formación o evaluación.
- Etc.

Los casos de uso de un tratamiento están vinculados a finalidades específicas e identifican y agrupan opciones de configuración del tratamiento de forma que, la elección de un caso de uso por parte del responsable, o del usuario, determina el valor de una serie de opciones de configuración.

Los casos de uso han de ser determinados por el responsable, que es quien define las distintas finalidades del tratamiento, y tendrá que establecer los compromisos entre privacidad, usabilidad, funcionalidad y seguridad. El responsable tendrá que evaluar la adecuación de los casos de uso que ha definido a la realidad y necesidades de los usuarios, así como su adaptación en función de que el contexto del tratamiento cambie en el tiempo. Atendiendo al mismo principio de minimización, esta evaluación ha de ser lo menos intrusiva posible desde el punto de vista de protección de datos. Por ejemplo, se podría considerar intrusivo y desproporcionado realizar el seguimiento automático de los hábitos de uso de los usuarios con este propósito, mientras que la realización de encuestas de utilización sería una forma menos intrusiva. Un aspecto importante a tener en cuenta en la definición de los casos de uso es considerar las necesidades de los sujetos que pertenezcan a colectivos vulnerables, especialmente menores de edad.

Los casos de uso definidos por el responsable han de poder ser ajustados por el usuario.

En ningún caso, los casos de uso definidos por el responsable podrán plantear al usuario un dilema del tipo *"lo tomas o lo dejas"* para acceder al servicio contratado y que, de esa forma, se ejerza algún tipo de imposición para el tratamiento de datos personales que exceden lo necesario. No podrá denegarse el acceso a un servicio simplemente porque el usuario haya optado por una configuración restrictiva con relación a la cantidad de datos tratados o la extensión del tratamiento[8].

### C. RELACIONES ENTRE TRATAMIENTOS

En una entidad será común que varios tratamientos puedan acceder a los mismos conjuntos de datos y hacer uso de servicios[9] comunes de recogida de datos, de proceso, o de comunicación. Estos componentes que implementan operaciones y son compartidos entre tratamientos en muchos casos son sistemas heredados[10]. En otros casos, como puede ser la implementación de apps en sistemas móviles, los tratamientos se desarrollan

[8] En línea con lo establecido en el apartado 3.1.2 de la guía "Guidelines 05/2020 on consent under Regulation 2016/679" del CEPD

[9] Con implementación organizativa, como puede ser un mostrador físico de atención al cliente, como tecnológica, una página web.

[10] Un sistema o aplicación de computadora que todavía se está utilizando debido a los costos de reemplazo o rediseño.

utilizando componentes estándar de terceros compartidos entre varias aplicaciones que hacen un uso común de acceso a servicios de proceso de datos[11].

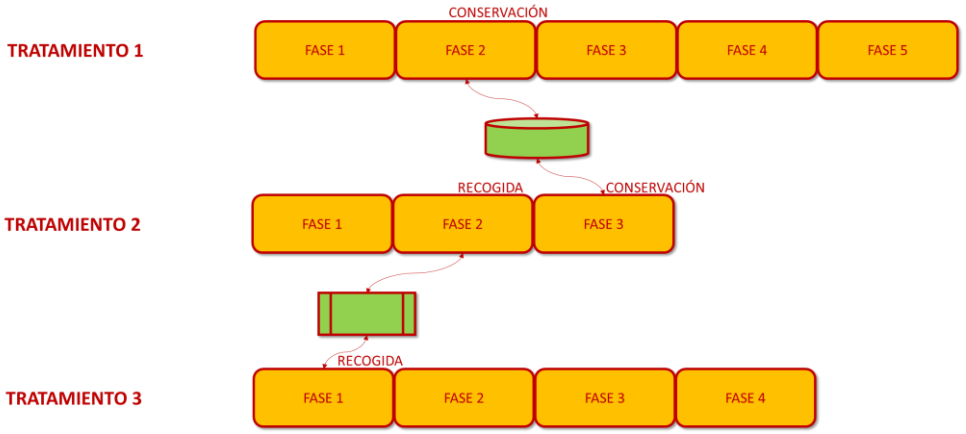


Figura 4. En este caso, los tratamientos 1 y 2 incluyen fases de conservación de datos personales, que se implementan en los servicios de bases de datos de la entidad, mientras que los tratamientos 2 y 3 incluyen fases de recogida de datos implementandas sobre las mismas librerías de captura de datos (por ejemplo, una API en Android).

El responsable debe analizar cada tratamiento en el contexto de la organización para identificar las necesidades de configuración sobre los servicios comunes a distintos tratamientos para, por ejemplo y dependiendo de su tipo concreto:

- Determinar los datos mínimos necesarios para cada tratamiento, independientemente de los que se encuentren disponibles.
- Realizar una separación lógica y/o física de datos personales utilizados en cada tratamiento.
- Gestionar los derechos de acceso de acuerdo con cada tratamiento.
- Establecer un espacio independiente, que podría ser lógico o físico dependiendo de los casos, para los tratamientos de datos sensibles.

Este análisis está muy relacionado con la aplicación del artículo 6.4 del RGPD y los límites que se manifiestan en el apartado 2.2 de la Guía del CEPD, en el sentido que los responsables deben tener cuidado de no extender los límites de los "propósitos compatibles" y tener en mente qué procesos estarán dentro de las expectativas razonables de los sujetos de los datos.

### D. ADAPTACIÓN DEL TRATAMIENTO

Junto con las actividades de análisis, determinación de casos de uso y selección de componentes compartidos, es necesario estudiar cada una de las fases o etapas del tratamiento, para cada uno de los casos de uso definidos por el responsable, y determinar:

- La necesidad de la fase, de cara a determinar si es superflua o evitable desde el punto de vista del tratamiento de datos personales.
- La minimización aplicable, estableciendo:

[11] En relación a los riesgos para la protección de datos que puede suponer, consultar el: Avance del estudio de IMDEA NETWORKS y UC3M: "Análisis del Software Pre-instalado en Dispositivos Android y sus Riesgos para la Privacidad de los Usuarios" https://www.aepd.es/sites/default/files/2019-09/nota-tecnica-IMDEA-android.pdf

    - El conjunto mínimo de datos personales que han de ser tratados en dicha fase y que han de ser los estrictamente necesarios para las operaciones específicas a las que dan soporte.
    - la necesidad de los datos inferidos, si los hay.
    - si la fase puede ser implementada sin utilizar datos de carácter personal.
- El periodo de conservación durante el que es necesario retener los datos personales.
- Los criterios de acceso para aplicaciones, servicios y personas:
    - Qué roles definidos en la entidad han de tener qué privilegios de acceso y a qué datos.
    - Qué roles externos a la entidad se han definido y con qué privilegios de acceso y a qué datos.
- La capacidad de control que se va a dar al usuario sobre las opciones anteriores.

# V. CONFIGURABILIDAD

## A. CONFIGURABILIDAD DE UN TRATAMIENTO

Un servicio, sistema o aplicación es "no configurable" cuando en su diseño e implementación existen unos parámetros fijos que determinan de forma inalterable la forma en la que se va a ejecutar el tratamiento, bien porque ha adquirido una implementación no configurable o la ha configurado con valores fijos. En estos casos, se dice que la funcionalidad está *"wired-in"* o cableada.

Cuando el tratamiento es configurable implica que ha sido diseñado con un conjunto de opciones susceptibles de ser alteradas por el responsable o incluso por el usuario. Por ejemplo, es posible configurar la recogida de datos de geolocalización, la información almacenada en los registros de actividad, los permisos de acceso al contenido del dispositivo, la información de identidad que se solicitará a un usuario del sistema, la posibilidad de cifrar las comunicaciones, el uso de los identificadores de publicidad, etc. Además, cada opción de configuración puede estar definida mediante un conjunto de parámetros[12], por ejemplo, en el caso de configurar el registro de actividad de la aplicación, además de un parámetro para activar dicho registro de forma general, podrían existir parámetros para determinar el tiempo máximo de conservación, las acciones sometidas a registro, la granularidad del registro a nivel de tipos de acceso, la información de tiempo o de identificación del usuario y del dispositivo, etc.

A la hora de la implementación habrá parámetros que podrán tomar cualquier valor, mientras que otros estarán limitados a un rango de valores. A su vez, dichos parámetros tomarán unos valores iniciales por defecto. El conjunto de las distintas opciones, sus parámetros y valores por defecto son establecidos por el responsable como requisitos del servicio, sistema o aplicación.

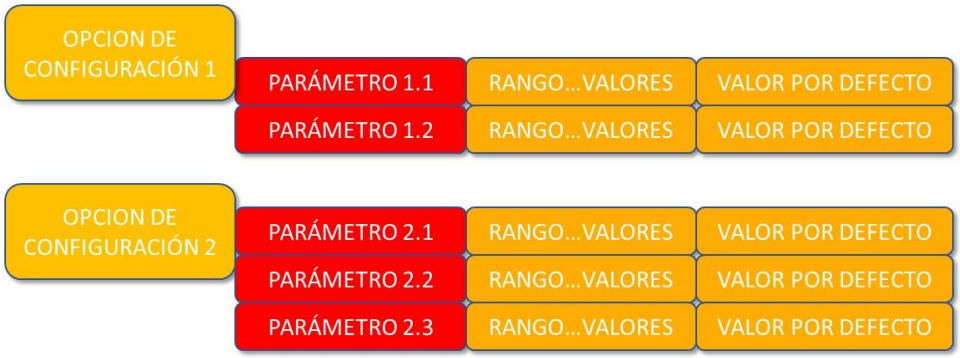


Figura 5 Listado de opciones de configuración, parámetros, rangos y valores por defecto

Atendiendo a la PDpD, el responsable del tratamiento debe establecer los requisitos de configurabilidad en cada una de sus fases, en función del análisis que se ha realizado sobre él y los casos de uso que han sido identificados. Dichos requisitos hay que trasladarlos al diseño e implementación del tratamiento.

La configuración por defecto determina el uso habitual del servicio y las características del tratamiento siempre que el responsable no ofrezca al usuario la posibilidad de

[12]En el caso de que se tenga la opción de configurar el cifrado de las comunicaciones, o la opción de cifrar los datos almacenados, existirán varios parámetros que podrían ser fijados, como, por ejemplo, el tipo de algoritmo, el tamaño de bloque, la longitud de la clave, características de robustez de la clave, posibilidad de reutilización de claves, mecanismos de generación de valores aleatorios, etc.

personalizarlo o que, haciéndolo, el usuario no haga uso de ella. La configuración "por defecto" estará formada por el conjunto de pares "parámetro-valor" preseleccionados o preasignados en un sistema, aplicación o servicio, que condicionan, en todo o en parte, el modo de funcionamiento de este.

La configurabilidad tiene cuatro aspectos:

- La identificación de los requisitos de configurabilidad, que se integrarán como parte de los requisitos de privacidad desde el diseño del tratamiento y se traducen en la determinación y selección de un conjunto de opciones de configuración, entendidas estas como el conjunto de parámetros susceptibles de ser modificados y sus posibles valores, incluido el valor fijado por defecto, que determinan el comportamiento del sistema, aplicación, producto o servicio. Será necesario pues:
  - La identificación de los parámetros configurables
  - Los rangos de valores disponibles técnicamente
  - El valor por defecto asignado a cada parámetro
- Determinar cuáles de las opciones de configuración estarán bajo el control exclusivo del responsable y con qué límites.
- En el caso de que ciertas opciones de configuración, por la naturaleza del tratamiento, estén bajo control del usuario, es necesario determinar cuáles de las opciones de configuración son las consideradas y con qué límites.
- Determinar si los componentes *off-the-shelf* con los que se va a construir el tratamiento cumplen con dichos requisitos de configurabilidad y ajustar su valor.

Este aspecto de la configurabilidad debe valorarse especialmente cuando se tratan datos de menores o datos de colectivos de personas que se encuentren en situaciones de vulnerabilidad (víctimas de violencia de género, personas en riesgo de exclusión social, etc.). Por ejemplo, posibilitar que los accesos a servicios de asistencia a víctimas no aparezcan en los registros de llamadas o en el historial del dispositivo.

Finalmente, la determinación de opciones de configuración y de casos de uso ha de ser información de entrada en la etapa de análisis de riesgos para los derechos y libertades de las personas físicas, para así establecer cómo pueden afectar a la privacidad de los usuarios los valores asignados a los diferentes parámetros, así como las posibles consecuencias de su modificación posterior por parte de éstos o de la posible manipulación por terceros[13]. Los usuarios han de estar informados de las consecuencias y los riesgos de configuración de forma clara y concisa de modo que les permita tomar una decisión informada respecto al impacto sobre su privacidad.

Elegir la configuración por defecto no es algo trivial. Para ello hay que determinar:

- Los distintos casos de uso del tratamiento que se ofrecen al usuario en base a las finalidades perseguidas.
- Los datos mínimos, en cada una de las fases y para cada uno de los distintos casos de uso identificados.
- Cuál de los posibles casos de uso disponible se configurará como caso de uso por defecto.
- Los parámetros de configuración y sus valores en función del caso de uso seleccionado por defecto.

[13] Por ejemplo, un tratamiento puede permitir al usuario activar las opciones de geolocalización, entonces hay que analizar el riesgo de que un tercero pueda gestionar o acceder a dicha geolocalización.

Un parámetro configurable no aceptará cualquier valor, sino que los valores posibles estarán limitados a un rango o un conjunto acotado de opciones de configuración[14]. Sin embargo, el grado de configurabilidad debe ser lo suficientemente amplio para que ofrezca opciones reales de configuración al responsable o usuario del sistema. Además, puede que los distintos parámetros configurables no sean independientes unos de otros y que haya vinculaciones técnicas entre ellos. Por lo tanto, la configurabilidad de un determinado parámetro no se mide por un "sí" o un "no", sino por un determinado grado de configurabilidad que, en ocasiones, puede requerir de un análisis de dependencias entre parámetros, como podría ser el caso en la configuración de los sistemas de autenticación o seguridad.

La configuración por defecto afecta también a las medidas organizativas, como se manifiesta el apartado 2.2 de la Guía del CEPD.

Entre los requisitos adicionales deseables, tal y como se manifiesta en la Guía del CEPD, se encuentra que los valores y opciones de tratamiento deberían ser universales para todas las instancias del modelo de aplicación, dispositivo o servicio puesto en marcha por el responsable y que deberían optarse por aproximaciones "*out-of-the-box"* en la puesta en funcionamiento de los sistemas, minimizando el tratamiento de datos personales y sin necesidad de pasar por un largo proceso de configuración antes de su uso.

### B. CONFIGURABILIDAD EN LOS COMPONENTES

La utilización de componentes de terceros (ya tratados en el apartado IV.A "Análisis del Tratamiento") puede limitar la capacidad del responsable, o el encargado en la medida que pueda afectarle para la correcta ejecución del requisitos fijados por responsable, para la aplicación de los requisitos de configurabilidad. Por lo tanto, es importante determinar, para estos componentes, qué valores están prefijados y son inalterables, qué parámetros sí son configurables y el valor por defecto con el que están configurados, así como el conjunto de posibles valores que podrían tomar.

El problema que los componentes estándar pueden presentar en un tratamiento es que se desarrollaron con un objetivo y finalidad que pueden ser distintos, incluso completamente distintos, del que se plantea en el tratamiento en el que los utiliza el responsable. De ahí que, un aspecto clave del proceso de configuración es averiguar si dichos componentes realizan actividades de tratamiento que no son necesarias para el tratamiento analizado. Es decir, si están implementando funcionalidades adicionales y no configurables, que generan efectos colaterales como, por ejemplo, comunicaciones a terceros, recogida de datos de tráfico, logs, etc.

En la selección de los componentes, el responsable ha de tener en cuenta la utilización de PETs o "Privacy Enhancing Technologies". PETs son un conjunto organizado y coherente de soluciones TIC que implementan estrategias y patrones de privacidad, entre ellas características de configurabilidad de los tratamientos.

En el caso de que dichos componentes estándar no cumplan con los principios de minimización se tendrá que analizar la base legitimadora del tratamiento y, en su caso, la posibilidad de desactivar las funcionalidades adicionales y llegado el caso, la eventualidad de no utilizarlos y optar por otro componente alternativo.

[14] Esta limitación puede ser técnica, por ejemplo, la longitud de una clave no podrá tener un valor infinito, sino un valor máximo. O también puede ser una limitación funcional, por ejemplo, se puede limitar la configurabilidad de las contraseñas a sólo aquellas que cumplan con determinados requisitos de robustez.

## C. CONTROL[15] DEL USUARIO

Una vez que un parámetro relativo a un tratamiento es configurable, hay que determinar si corresponde dar control al usuario sobre su configuración. Por ejemplo, un servicio que permite a los buscadores indexar datos de los usuarios bajo ciertas condiciones de configuración, podría permitir determinar al usuario la extensión de los datos indexables, individualmente o por categorías.

No siempre es necesario dar control al usuario sobre las opciones de configuración. Al contrario, en algunos casos no es apropiado y no se debería dar esa opción. Por ejemplo, no se debería permitir al usuario establecer su propio rol de acceso al sistema, sino que esta tarea debería descansar en el administrador.

El control del usuario significa que éste tenga posibilidad de tomar decisiones sobre las acciones de configuración, pero también implica transparencia e información sobre el resultado y consecuencias de las opciones que éste puede elegir.

En ese caso, es importante que el usuario esté adecuadamente informado y comprenda las consecuencias, en lo que a su privacidad, derechos y libertades se refiere, de elegir una u otra configuración o modificar los valores establecidos por defecto (por ejemplo, en los casos en que el usuario quiere ampliar las finalidades iniciales del tratamiento con funcionalidades extendidas). Una información adecuada ha de ir en línea con las expectativas que sobre el sistema tiene o se han creado al usuario. Además, el usuario ha de tener información relevante sobre la accesibilidad por terceros a sus datos personales y sobre el momento en que esta se está produciendo, como, por ejemplo, recibir información de que se está realizando una captura continua de su geolocalización mediante un icono en la pantalla[16]. Esta información debe facilitar al sujeto el ejercicio de los derechos para lo cual será necesario, además, disponer de herramientas adecuadas y ágiles.

La forma de implementar los efectos de los cambios de configuración elegidos por el usuario debe ser un aspecto perfectamente establecido por el responsable para poder informar al usuario del momento preciso en que sean efectivos, así como las acciones adicionales que pudiera tener que realizar (por ejemplo, reinicializar el sistema). Estas tendrían que ser lo menos traumáticas posible para el usuario, evitando consecuencias como, por ejemplo, la pérdida de datos o de características de personalización previamente configuradas.

En este sentido, es necesario tener en cuenta que un exceso de información o de opciones de configuración necesarias para poner en marcha y poder utilizar el sistema pueden conducir al usuario a la toma de decisiones erróneas que podrían afectar a sus derechos y libertades. Es necesario ponderar el volumen y frecuencia de los cambios junto con el volumen de información proporcionada al usuario. Por ello, y en aras de la usabilidad, una forma adecuada de evitar, o al menos limitar, la fatiga informativa que supone un elevado número de preguntas de configuración es ofrecer al usuario la posibilidad de elegir entre casos de uso que agrupen opciones de configuración. De este modo, se ofrece un modo de interacción fluido y se evita agobiar al usuario final con una infinidad de preguntas que responder y opciones que seleccionar.

La información facilitada sobre las distintas funcionalidades de los casos de uso debe hacer consciente al usuario de qué datos (y sus metadatos asociados) van a ser necesarios

[15] El termino inglés utilizado habitualmente es “intervenability” que se podría traducir también por capacidad de participación, intervención, fiscalización o influencia.

[16] El artículo 13 del RGPD establece "Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación..."

para que el sistema, aplicación, producto o servicio pueda proporcionar y gestionar esa funcionalidad concreta.

El empleo de casos de uso permite una aproximación en dos capas al control del tratamiento por parte del usuario: una primera para seleccionar casos generales de uso y una segunda para la configuración en detalle de cada uno de ellos.

En cualquier caso, si una modificación tiene lugar, debe ser posible revertir el cambio a los valores iniciales prestablecidos y recuperar la configuración "*privacy friendly*" establecida en origen de una forma fácil, sencilla e intuitiva.

Las acciones del usuario que cambien las opciones de configuración han de ser activas, conscientes e informadas y no se pueden confundir con cualquier otra. Para ello, se remite a la guía sobre el consentimiento[17] publicada por el CEPD.

[17] Guidelines 05/2020 on consent under Regulation 2016/679"
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

## VI. RESTRICCIÓN POR DEFECTO

El caso de uso que, siendo lo más restrictivo por defecto, permita acceder a la funcionalidad básica del sistema (funcionalidad inicial, valores de fábrica, …) siempre ha de estar disponible y seleccionado inicialmente sin necesidad de ningún cambio por parte del responsable o del usuario.

El caso de uso por defecto ha de ser el que cumpla, de la forma más restrictiva posible, el principio de minimización. Los responsables del tratamiento deben seleccionar las opciones de configuración adecuadas de forma que se asegure que sólo se recopilarán los datos estrictamente necesarios para alcanzar el propósito del tratamiento que se ha habilitado. Hay que tener presente que este caso de mínima intrusión puede no ser único y que, en función de la complejidad del tratamiento, podrían existir varios casos de uso restrictivos. En esa circunstancia, el responsable deberá justificar la elección de aquel que se haya establecido por defecto.

El usuario tendrá que modificar la configuración por defecto si quiere ampliar el tratamiento de datos personales más allá de la base legal en la que se basa el tratamiento principal para el que se ha realizado la configuración “por defecto” o si las nuevas funcionalidades implican propósitos no compatibles con el propósito original para el que inicialmente se recopilaron los datos personales.

En aplicación del principio de lealtad o “fairness” establecido en el artículo 5.1.a del RGPD, el responsable del tratamiento ha de garantizar que no se emplean “patrones oscuros” o “dark patterns”, esto es, interfaces de usuario diseñadas para influir, a través de manipulaciones psicológicas y de forma encubierta, en las elecciones del interesado, al menos, con relación al tratamiento de sus datos personales. Un ejemplo de este tipo de patrones es ofrecer al usuario una finalidad atractiva en función de su análisis comportamental para enmascarar una transferencia de datos a un tercero con fines que no han sido claramente definidos[18].

[18] Una explicación sobre los “dark patterns” se puede encontrar en https://en.wikipedia.org/wiki/Dark_pattern y ejemplos en la dirección www.darkpatterns.org.

## VII. MEDIDAS DE PROTECCIÓN DE DATOS POR DEFECTO

Como se describía en el capítulo “III Aplicación de la protección de datos por defecto”, para implementar las estrategias de PDpD es necesario adoptar medidas sobre:

- La cantidad de datos personales recogidos.
- La extensión del tratamiento.
- El periodo de conservación.
- La accesibilidad de los datos.

Estas medidas de PDpD se agrupan a través de opciones de configuración que permiten determinar la extensión del tratamiento. Dentro de las opciones de configuración están aquellas que permitirán al responsable configurar el tratamiento, las que estén bajo el control del usuario en su “panel de privacidad” y los requisitos de configuración de los componentes compartidos.


Figura 6. Estrategias de PDpD, medidas y opciones de configuración

Y para facilitar la aplicación práctica de la PDpD, en el último apartado de este capítulo se facilita información, con carácter orientativo, sobre las características de las opciones de configuración que podrían ser incluidas en un tratamiento.

### A. CANTIDAD DE DATOS PERSONALES RECOGIDOS.

Como se señala en la Guía del CEPD, el término “cantidad” implica factores cualitativos y cuantitativos de los datos. El responsable del tratamiento deberá considerar el volumen de datos personales tratados, el nivel de detalle, las diferentes categorías, la sensibilidad (categorías especiales de datos) y los tipos de datos personales requeridos y necesarios para llevar a cabo una operación de tratamiento, incluyendo tanto los datos recogidos como los generados o inferidos a partir de estos.

### B. LA EXTENSIÓN DE SU TRATAMIENTO.

La implementación de la PDpD implica que las operaciones de tratamiento sobre los datos personales realizadas por el responsable se limitarán a lo estrictamente necesario para cumplir con el propósito declarado.

En consecuencia, cuando el tratamiento se estudia como un conjunto de fases, hay que asegurar que las operaciones que se realizan en cada una de ellas sean únicamente las necesarias, y sobre los datos necesarios, para el cumplimiento de la finalidad de dicha fase. En particular, el responsable y, en los casos oportunos, el usuario, han de poder configurar la extensión del tratamiento en cada fase, en particular en función de los casos de uso.

### C. EL PERIODO DE CONSERVACIÓN.

Las limitaciones al periodo de conservación están vinculadas con la extensión del tratamiento ya que la conservación de los datos es, en sí, una operación de tratamiento. Sin embargo, por su especificidad, se analiza de forma independiente.

La aplicación del principio de minimización sobre el periodo de conservación establece que, si un dato personal no se necesita más después de ejecutar una fase del tratamiento, el dato deberá ser suprimido (lo que podría suponer en algunos casos el bloqueo[19] o la anonimización). Cualquier retención deberá ser objetivamente justificable y fundamentada. Por ejemplo, en los casos en los que es necesario utilizar captchas en sitios web que tratan información biométrica para detectar robots, como el movimiento del ratón, hay que justificar la conservación de esa información para su uso en fases posteriores del tratamiento.

### D. LA ACCESIBILIDAD DE LOS DATOS

Como manifiesta la Guía del CEPD, el responsable del tratamiento deberá establecer quién puede acceder a los datos personales, tanto en lo que respecta al personal dentro de la organización como a terceros, ya sean otras entidades y organismos o incluso sistemas automatizados como motores de búsqueda, servidores en la nube, o cualquier otro sistema aplicación o servicio que acceda a los datos utilizados en el tratamiento. El grado de accesibilidad a los datos ha de estar establecido basándose en un análisis de necesidad para cumplir con el propósito del tratamiento.

Este análisis se deberá realizar para cada una de las fases del tratamiento y se implementará mediante:

- Una definición de roles y responsabilidades de los miembros de la organización.
- Una política de control de privilegios de acceso como parte de las medidas organizativas adoptadas.
- La incorporación de mecanismos de control de acceso a la información que implementen la política definida y que serán en parte de carácter organizativo y de tipo técnico.

El responsable debe limitar la accesibilidad de los datos personales por defecto y, cuando sea necesario, consultar al sujeto de los datos personales antes de publicarlos o hacerlos accesibles de algún modo a un número indefinido de personas. Para ello, el tratamiento ha de ser configurable por el responsable, y en su caso por el usuario, para ajustar el grado de accesibilidad a los distintos casos de uso.

A la hora de implementar las operaciones sobre los datos, los tratamientos pueden utilizar componentes estándar. En la práctica será muy común que distintos tratamientos compartan dichos componentes estándar y accedan a servicios compartidos con otros tratamientos en tareas de recogida, conservación y transmisión de datos. Por lo tanto, es necesario poder configurar (limitar) la posible comunicación de datos con otros tratamientos que no sea necesaria para la finalidad original del mismo.

### E. APLICACIÓN PRÁCTICA DE LAS MEDIDAS A IMPLANTAR: OPCIONES DE CONFIGURACIÓN

En el Anexo II se desarrolla una lista, con carácter orientativo, de aquellas opciones en las que un tratamiento podría ser configurable para implementar las medidas con relación

[19] https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673#a3-4

a la cantidad de datos personales utilizados, la extensión del tratamiento, el periodo de conservación, la accesibilidad de los datos y cualquier otra circunstancia en el proceso del tratamiento susceptible de incidir en la privacidad de los usuarios.

Asociados a cada una de esas opciones de configuración el responsable deberá determinar los parámetros específicos[20], estableciendo los rangos o posibles valores que los parámetros podrán aceptar, así como cuál de esos parámetros o valores esté fijado por defecto, en función de los casos de uso.

Por lo tanto, los requisitos de configurabilidad del tratamiento contendrán la lista de opciones, detallando parámetros, rangos y valores por defecto. Estos requisitos se aplicarán desde el diseño, tanto para el desarrollo de componentes *ad-hoc* como para la utilización o adquisición de componente estándar, así como para la definición de parte de la interfaz con el usuario.

Las opciones que puedan ser configurables por el usuario formarán parte de su "panel de privacidad" pudiendo este modificar a discreción el valor por defecto originalmente configurado para estas opciones. Es importante volver a señalar que no todas las opciones de configuración deben estar disponibles al usuario, o a todos los tipos de usuario, y su determinación quedará circunscrita al proceso de definición de los requisitos de configurabilidad del tratamiento[21].

Es importante destacar que no todas las opciones presentadas en la lista son aplicables a todos los casos, ni que se contemplan todas las posibles opciones de configuración que puede tener un tratamiento dado. Para cada tratamiento concreto la lista desarrollada en el Anexo II tendrá que adaptarse, y en algunos casos extenderse. Por ello, la lista también estará disponible en una hoja de cálculo en el microsite de Innovación y Tecnología de la AEPD, para poder ser explotada por responsables, encargados y desarrolladores y actualizada de forma más ágil.

[20] Como ya se había señalado en una nota al pie previa, en el caso de que se tenga la opción de configurar el cifrado de las comunicaciones, o la opción de cifrar los datos almacenados, existirán varios parámetros que podrían ser fijados, como, por ejemplo, el tipo de algoritmo, el tamaño de bloque, la longitud de la clave, características de robustez de la clave, posibilidad de reutilización de claves, mecanismos de generación de valores aleatorios, etc.

[21] Como se ha señalado anteriormente, hay casos en los que el rol del usuario no debe ser poder alterado por él mismo.

## VIII. DOCUMENTACIÓN Y AUDITORÍA

Como establece el principio de responsabilidad proactiva en el artículo 24.1 del RGPD, las medidas y garantías de PDpD han de estar documentadas y recoger la información suficiente para permitir, de forma satisfactoria y demostrable, acreditar el cumplimiento del RGPD. Esta documentación ha de permitir la trazabilidad de las decisiones tomadas y de las comprobaciones realizadas siguiendo los principios de minimización antes señalados.

Formando parte de la documentación del tratamiento ha de encontrarse la documentación relativa a los componentes estándar, que el responsable tiene la obligación de asegurar que es completa y suficiente[22] para justificar la decisión de haber incluido el componente en el tratamiento. En particular, cuando dicho componente estándar corresponda a un servicio desarrollado por un tercero, el responsable ha de garantizar que se describe en la documentación la información necesaria para determinar la correcta aplicación del principio del PDpD en dicho sistema, producto o servicio.

En definitiva, el tratamiento ha de ser auditable a lo largo de su ciclo de vida, incluyendo la etapa de retirada de este.

La auditoría para determinar la correcta aplicación de la PDpD se integrará dentro de un plan de auditoría de protección de datos y este, a su vez, dentro del plan de auditoría general del tratamiento que podría abarcar objetivos más allá del RGPD.

La PDpD forma parte de las condiciones de cumplimiento estricto del RGPD que no está sujeta ni condicionada por el resultado de un análisis de riesgos para los derechos y libertades, como, entre otros, la existencia de una base jurídica que legitime el tratamiento o las obligaciones de información establecidas en los artículos 13 y 14. Por lo tanto, los controles a analizar en el caso de una auditoría que incluya la PDpD no serán seleccionados como consecuencia de un análisis de riesgos para los derechos y libertades.

A continuación, se enumeran, de forma enunciativa y no exhaustiva, los controles básicos que deberían ser tomados en consideración para determinar el cumplimiento del tratamiento con relación a la PDpD. Como se ha dicho anteriormente, esta lista de verificaciones debe considerarse circunscrita a una auditoría de PDpD de forma aislada que deberá quedar integrada en el marco global de una auditoría de protección de datos:

1. Comprobar que está disponible en la entidad responsable la documentación necesaria para aplicar PDpD de forma objetiva; en particular, la definición de roles y obligaciones de los miembros de la organización, la política de control de accesos, la política de información y cualquier otra documentación significativa.
2. Comprobar que la entidad tiene implementados procedimientos que garanticen el cumplimiento de las políticas anteriores y que están operativos.
3. Comprobar que está disponible la información básica relativa al tratamiento, en particular, sobre la naturaleza, el ámbito, el contexto y los fines, así como el análisis de proporcionalidad y necesidad.
4. Tener documentado un análisis del tratamiento desde el punto de vista de la PDpD.
    a. Comprobar que el análisis de tratamiento se ha descompuesto en fases e identificar para cada fase las operaciones, la implementación organizativa y técnica, los datos personales y los intervinientes internos y externos

[22] La información comercial o la contenida en las acciones publicitarias no puede considerarse información completa y suficiente.

   b. Los componentes estándar están identificados.
   c. Igualmente, han de estar identificadas las interacciones, servicios, sistemas y operaciones compartidos con otros tratamientos.
   d. Cada fase se ha estudiado para su optimización con relación a la necesidad, la minimización, la conservación, los accesos y los controles.
   e. Se han definido los casos de uso del tratamiento y los criterios tenidos en cuenta por el responsable para su determinación.
   f. En particular, en la definición de los casos de uso se han tenido en cuenta la protección de la privacidad de sujetos de colectivos vulnerables, especialmente menores.
5. Comprobar que el ciclo de vida de los datos está ajustado a los casos de uso.
6. Comprobar que el responsable ajusta los casos de uso a la operativa real y necesidades del usuario y que comprueba la evolución de esta operativa en el tiempo.
7. Comprobar que el responsable no obliga al usuario a aceptar un tratamiento más intrusivo (mayor cantidad de datos o una mayor extensión en las operaciones) como condición para acceder a un servicio.
8. Comprobar que las opciones de configuración están correctamente identificadas y definidas con relación a:
   a. Tipo de medidas de PDpD (la cantidad de datos personales recogidos, la extensión del tratamiento, el periodo de conservación, la accesibilidad de los datos u otros),
   b. Parámetros configurables y rango de valores asociados con un juego de alternativas lo suficientemente amplio.
   c. Valores por defecto asociados a cada parámetro.
   d. Dependencias de los parámetros de configuración y posibles conflictos entre los valores seleccionados, incluso con otras opciones.
   e. Qué roles (responsable o tipos de usuario) tienen control sobre las opciones de configuración y límites de dicho control.
9. Comprobar que los requisitos de configurabilidad establecidos por el responsable se han trasladado desde el diseño y se encuentran correctamente implementados.
   a. Comprobar que existe una decisión justificada sobre las opciones no-configurables, identificando las razones de funcionalidad o legales que lo motivan.
   b. En particular, comprobar qué componentes *off-the-shelf* cumplen los requisitos de configuración establecidas en la documentación y, en su caso, determinar las limitaciones de configuración que tienen y cómo afectan al tratamiento[23].
10. Comprobar la posibilidad de coexistencia de configuraciones alternativas en distintas instancias de la aplicación sobre diferentes dispositivos.

[23] Por ejemplo, para el caso de implementar un blog corporativo, si se utiliza una herramienta desarrollada por un tercero (Wordpress, Blogger, SharePoint, etc), en cada caso la configuración por defecto será distinta y tendrá que ser evaluada.

11. Comprobar que se han implementado medidas de seguridad.
12. Comprobar que el caso de uso por defecto es el que cumple de forma más restrictiva con el principio de minimización.
13. Comprobar que las opciones de cambio de la configuración que se ofrecen al usuario proporcionan explicaciones que permitan al usuario tomar una decisión informada
    a. Comprobar que el usuario recibe información suficiente de los efectos y consecuencias de los cambios de configuración como para tomar una elección consciente. Por ejemplo, en el caso de optar por un cifrado de más baja protección a cambio de poder acceder o tener un mayor rendimiento, informar de las posibles consecuencias de dicho cambio.
    b. En particular, proporcionar información sobre el momento en el que los cambios de configuración se hacen efectivos.
    c. Comprobar que no se emplean "*dark patterns*" para manipular el proceso de elección del usuario o influir de forma encubierta en su decisión respecto al alcance del tratamiento.
14. Comprobar que un cambio de configuración requiere una acción consciente, libre e intencionada del usuario.
15. Comprobar la posibilidad de revocar elecciones en cualquier momento con la misma facilidad con la que fueron seleccionadas.
16. Comprobar que el usuario puede retornar a la configuración inicial más restrictiva en caso de elección de cambio de la configuración.
17. Comprobar que un cambio de configuración por acción del usuario, sobre todo si es un cambio hacia condiciones de tratamiento más restrictivas en cuanto minimización, no afecta negativamente al usuario.
18. Comprobar que la documentación relevante relativa a la implementación de las medidas de PDpD se han trasladado a la etapa de gestión de riesgos para los derechos y libertades y, en particular, a la gestión de riesgos de seguridad.
19. Comprobar que la documentación relevante de la implementación de la PDpD ha sido utilizada para configurar la política de información y trasparencia proporcionada al usuario.

Conforme a lo establecido el control número 6: *"el responsable ajusta los casos de uso a la operativa real y necesidades del usuario y que comprueba la evolución de esta operativa en el tiempo"*, el listado anterior ha de considerarse como un mínimo genérico de controles a revisar y ser susceptible de ser ampliado para tratamientos específicos. Debido a la evolución del entorno del tratamiento, de las actualizaciones de este y el posible impacto social, que puede ser impredecible, es necesario adaptar de forma continua los casos de uso definidos en el tratamiento y, en consecuencia, los controles de verificación necesarios.

# IX. CONCLUSIONES

El artículo 25 del RGPD establece la PDpD como una de las medidas de responsabilidad proactiva, integrada con el resto de las garantías establecidas en el RGPD, y pudiendo optar por diferentes aproximaciones y alternativas a la hora de implementar la dimensión de PDpD.

Aunque este documento está centrado en la forma de abordar las obligaciones del artículo 25 con relación a la PDpD, todas las acciones relativas a la implementación de la PDpD en un tratamiento hay que abordarlas integradas con el resto de la medidas y garantías establecidas en el RGPD.

Tanto responsables de tratamiento de datos personales, como encargados y desarrolladores en la medida de sus obligaciones, deben tener presentes las medidas de PDpD. De un lado los desarrolladores deberían proporcionar soluciones técnicas que incluyan la posibilidad de establecer configuraciones por defecto respetuosas con los principios del RGPD y de otro lado responsables, y encargados en la medida que ofrecen servicios para ejecutar sus instrucciones, deben seleccionar soluciones que cumplan con estos requisitos y exigir a los desarrolladores el cumplimiento de los mismos.

El RGPD exige del responsable una configuración por defecto de los tratamientos que sea respetuosa con los principios de protección de datos, abogando por un procesamiento mínimamente intrusivo: mínima cantidad de datos personales, mínima extensión del tratamiento, mínimo plazo de conservación y mínima accesibilidad a datos personales.

Estos mínimos se han de establecer “por defecto”, es decir, la PDpD ha de aplicarse siempre que tenga lugar un tratamiento de datos personales independientemente de la naturaleza del tratamiento realizado. El establecimiento de medidas de privacidad por defecto no se deriva del resultado de un análisis de riesgos para los derechos y libertades, sino que son medidas y garantías que es necesario establecer, en cualquier caso.

Los paneles de privacidad para los usuarios deberán facilitar la configurabilidad ofreciendo una aproximación en dos niveles a través de casos de uso y opciones de configuración específicas. Además, la información al usuario sobre las consecuencias de sus elecciones ha de ser completa y transparente. Igualmente convendría que dichos paneles y el modo de ofrecer la información fueran de algún modo estándar, tanto en la utilización de iconos, como en la distribución de las opciones de configuración en la interfaz de usuario de cara a mejorar la transparencia y la usabilidad.

La aplicación de la PDpD ha de ser demostrable, lo que implica que su implementación ha de estar justificada, documentada y ser auditable. Con relación a ello, el tercer párrafo del artículo 25 del RGPD establece que:

> *3.Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.*

La utilización de certificaciones aprobadas con arreglo al artículo 42 del RGPD es una de las formas que tendría el responsable para demostrar el cumplimiento de la aplicación de medidas de PDpD.

# X. ANEXO I: RGPD

## A. ARTÍCULO 6.4

4. Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:

a. cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;

b. el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;

c. la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;

d. las posibles consecuencias para los interesados del tratamiento ulterior previsto;

e. la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización

## B. ARTÍCULO 25 PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.

## C. CONSIDERANDO 78

78. La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas

apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos.

## XI. ANEXO II: LISTA DE OPCIONES DE CONFIGURACIÓN

Lista, no exhaustiva y con carácter orientativo, de aquellas opciones en las que un tratamiento podría ser configurable para implementar las medidas con relación a la cantidad de datos personales utilizados, la extensión del tratamiento, el periodo de conservación, la accesibilidad de los datos y cualquier otra circunstancia en el proceso del tratamiento susceptible de incidir en la privacidad de los usuarios.

| | **Opciones de configuración agrupadas por tipo de medida** | **Opciones que podrían ser fijadas en el tratamiento por el responsable** | **Opciones que podrían incluirse en el panel de privacidad** | **Opciones de configuración de podrían establecerse en los componentes off-the-shelf** |
|---|---|---|---|---|
| **Cantidad de datos personales** | | | | |
| | Operación en modo anónimo. | X | X | |
| | Operación sin necesidad de crear cuenta de usuario. | X | X | |
| | Operación con distintas cuentas de usuario sobre el mismo dispositivo para el mismo interesado. | X | X | |
| | Operación con distintas cuentas de usuario sobre distintos dispositivos para el mismo interesado y tratamiento. | X | X | |
| | Identificación mediante herramientas y tecnologías que refuerzan la privacidad como las credenciales basadas en atributos, las pruebas de conocimiento cero, … | X | X | |
| | Agregación de datos: en el tiempo, en el espacio, por colectivos… | X | | |
| | Calibración de la granularidad de los datos: p.ej. disminuir la frecuencia de recogida de datos de localización, de medida, etc.. | X | | |
| | Generalización de los datos: emplear rangos para edad, direcciones postales para direcciones. | X | | |

| | | | | |
|---|---|---|---|---|
| | Graduación de la extensión de los datos recogidos en función de los casos de uso | X | | |
| | Alternativas y voluntariedad en la información de contacto reclamada al usuario: e-mail, postal, teléfono… | X | X | |
| | Técnicas de seguimiento en el tratamiento (cookies, etiqueta de pixeles, fingerprint, etc.) | X | X | |
| | Configuración de identificadores unívocos (tracking IDs), la programación de su reinicialización y el aviso de tiempos de activación. | X | X | |
| | Metadatos del dispositivo recogidos del dispositivo (consumo de batería, S.O., versiones, lenguajes, etc.). | X | X | |
| | Metadatos incluidos en los soportes tratados o generados (en documentos, fotos, videos, etc.) | X | X | |
| | Información recogida sobre la conexión de internet del usuario (dispositivo con el que se conecta, dirección IP, datos de sensores del dispositivo, aplicación utilizada, registro de navegación y búsqueda, registro de fecha y hora de solicitud de página web, etc.) e información sobre elementos cercanos al dispositivo (puntos de acceso Wi-Fi, antenas de servicio de telefonía móvil, dispositivos bluetooth activados, etc.). | X | X | |
| | Información recogida sobre la actividad del usuario en el dispositivo: encendido, activación de aplicaciones, uso de teclado, ratón, etc. | X | X | |
| | Mecanismos de recogida escalonada de la información necesaria para el tratamiento. Retrasar la recogida de datos hasta la fase en que sean necesarios. | X | | |
| | Tipo y volumen de nuevos datos inferidos a partir de procesos automatizados como el machine learning u otras técnicas de inteligencia artificial. | X | | |
| | Enriquecimiento de datos y la vinculación con conjuntos de datos externos | X | | |
| | Activación y desactivación a voluntad de los sistemas de recogida de datos (cámaras, micrófonos, GPS, bluetooth, wifi, movimiento, etc.). | X | X | |

| | | | | |
|---|---|---|---|---|
| | Establecer una programación temporal de cuándo los sensores (p.ej. cámaras, micrófonos, etc.) pueden estar operativos. | X | X | |
| | Incorporación de mecanismos de ofuscación para evitar el tratamiento de datos biométricos en fotos, video, teclado, ratón, etc. | X | X | |
| | Bloqueadores físicos (como las pestañas para cubrir las lentes de las cámaras, bloqueadores de altavoces, etc.). | X | X | |
| | Utilización de máscaras de privacidad o pixelado en los sistemas de videovigilancia. | X | | |
| **Extensión del tratamiento** | | | | |
| | Definición y diseño de los tratamientos para minimizar la cantidad de copias temporales de datos que se generen y reducir al máximo los tiempos de conservación, las transferencias y comunicaciones | X | | |
| | Seudonimización atendiendo a las operaciones de tratamiento que puedan existir en cada fase o etapa. | X | | |
| | Procesamientos de carácter local y aislado, incluida la posibilidad de almacenamiento local. | X | | |
| | Tratamiento adicional de los metadatos recogidos – ficheros log. | X | | |
| | Ejercicio de derechos de oposición, limitación o supresión. | X | X | |
| | Configuración del tratamiento para perfilado o decisiones automáticas (caso cookies) | X | | |
| | Posibilidad de configurar todas las operaciones optativas de tratamientos para finalidades no imprescindibles: por ejemplo, tratamiento de datos para mejora del servicio, análisis de uso, personalización de anuncios, detección de patrones de uso, etc. | X | X | |
| | Configuración de un borrado seguro de ficheros temporales, principalmente aquellos situados fuera del dispositivo del usuario y fuera de los sistemas del responsable | X | | |
| | Incorporación de una opción de reinicialización de los datos de usuario para retomar la relación desde cero | X | X | |

| | | | | |
|---|---|---|---|---|
| | Configuración de la opción de enriquecimiento de datos | X | | |
| | Contemplar mecanismos para auditar la existencia de Dark Patterns | X | | |
| | Apartado específico para las opciones de configuración relacionadas con datos sensibles | | X | |
| | Panel de ayuda y transparencia con ejemplos de uso y posibles riesgos y consecuencias para los derechos y libertades del usuario | | X | |
| | Incorporación de un medio específico (botón o enlace) de retorno a la configuración inicial con valores por defecto | | X | |
| **Periodo de almacenamiento** | | | | |
| | Configuración de borrado de datos de sesión tras su cierre. | X | X | |
| | Configuración de plazos máximos para el cierre de sesión en la aplicación o dispositivos. | X | X | |
| | Plazos de conservación de perfiles de usuario. | | X | |
| | Configuración de la gestión de copias temporales. | X | | |
| | Control del borrado de copias de temporales. | | X | |
| | Eliminación del rastro del usuario en el servicio: “derecho al olvido”. | X | X | |
| | Identificación, dentro del registro de expedientes de datos recogidos de las secciones, o datos dentro de secciones, que puedan ser anonimizables. | X | | |
| | Programación de mecanismos de bloqueo y borrado automático. | X | | |
| | Programación de mecanismos automáticos de borrado de salidas a dispositivos de impresión. | X | | |

| | | | | |
|---|---|---|---|---|
| | Configuración de plazos de conservación de datos históricos en el servicio: p.ej., en los sitios de compra, últimos artículos, ultimas consultas, etc. | X | X | |
| | Incorporación de mecanismos genéricos de anonimización. | X | | |
| **Accesibilidad de los datos** | | | | |
| | Información de perfil del interesado mostrada a usuario y terceros: nombre, pseudónimo, teléfono, etc. | X | X | |
| | Información del interesado que se muestra a terceros: p.ej. divulgación selectiva de elementos del CV, la historia clínica, etc. | X | | |
| | Información de estatus del interesado accesible a terceros. P.ej. en las aplicaciones de mensajería, información sobre disponibilidad, escritura de mensaje, recepción de mensaje, lectura de mensaje, … | X | X | |
| | Clasificación y etiquetado de las operaciones de tratamiento, las secciones de los documentos y/o datos dentro de secciones, que puedan ser gestionados mediante una política de control de accesos. | X | | |
| | Organización, clasificación y etiquetado de la aplicación o servicio de acuerdo con la sensibilidad de datos, secciones u operaciones de tratamiento. | X | | |
| | Posibilidad de definición y configuración de perfiles de acceso y asignación granular de privilegios | X | | |
| | Bloqueos automáticos de sesión. | X | X | |
| | Asignación de perfiles de acceso a los datos de acuerdo con los roles de los usuarios para cada fase del tratamiento. | X | | |
| | Diseño del espacio de trabajo (zonas aisladas de entrevista, ficheros físicos no accesibles, carpetas no transparentes, pantallas no expuestas a terceros o con filtros de privacidad, cascos para los teléfonos, locutorios, políticas de mesas limpias, etc.) | X | | |

| | | | | |
|---|---|---|---|---|
| | Parámetros de gestión de la información como dónde se almacenan y procesan los datos, si se hace en claro o utilizando un sistema de cifrado, los mecanismos de control de acceso implementados, si existen múltiples copias de los datos, incluidas instancias borradas de forma no segura, que pueden ser accedidas por terceros. | X | | |
| | Control del cifrado de almacenamiento de los datos | X | X | |
| | Control del cifrado de comunicación de los datos | X | X | |
| | Procedimientos de gestión de acceso a dispositivos compartidos de impresión/salida donde pueden quedar documentos abandonados por el usuario. | X | | |
| | En su caso, prohibición de impresión. | X | | |
| | Control del borrado de salidas de impresión | | X | |
| | Procedimientos de gestión de dispositivos de almacenamiento portátil para su formateo periódico | X | | |
| | La retención o eliminación de la información de sesión, en aplicaciones, sistemas compartidos, comunicaciones o sistemas proporcionados al empleado o al usuario final. | X | | |
| | El tipo y cantidad de metadatos recogidos en la documentación generada por las utilidades del sistema (procesadores de texto, herramientas de dibujo, cámaras y videos, etc.) | X | | |
| | En el envío de mensajes, configurar la incorporación de hilos de la conversación, así como configurar la posibilidad de confirmación de envío múltiples destinatarios. | X | | |
| | Mecanismos de para evitar la indexación en Internet | X | | |
| | Medidas organizativas y técnicas para revisión y filtrado de información que se va a hacer pública. | X | | |
| | Sistemas de anonimización y/o seudonimización de textos a difundir. | X | | |

| | | | | |
|---|---|---|---|---|
| | Parámetros de gestión de los elementos de conectividad de los dispositivos (Wifi, Bluetooth, NFC, etc.). | X | | |
| | Alertas sobre el estado de conectividad de los dispositivos. | X | X | |
| | Controles para evitar la comunicación de los identificadores unívocos del dispositivo (Advertising-ID, IP, MAC, número de serie, IMSI, IMEI, etc.) | X | | |
| | Mecanismos de control de acceso a sistemas pasivos (como tarjetas contactless) con la incorporación de protocolos de autenticación de terminales o con medidas físicas para evitar el acceso electromagnético. | X | | |
| | Controles de accesibilidad a contenidos del usuario en redes sociales. | X | | |
| | Incorporación de controles para recoger acciones afirmativas y claras de confirmación antes de hacer públicos los datos personales, de forma que la diseminación esté bloqueada por defecto. | X | | |
| | Configuración de avisos y recordatorios a los interesados sobre qué políticas de difusión y comunicación de la información están establecidas. | X | X | |
| | Definición y configuración de permisos de acceso sobre conjuntos de datos (bases de datos, sistemas de fichero, galerías de imágenes, …) y elementos de captación de información como sensores (cámaras, GPS, micrófonos, etc.) del dispositivo e información sobre elementos cercanos al dispositivo (puntos de acceso Wi-Fi, antenas de servicio de telefonía móvil, dispositivos bluetooth activados, etc.). | X | | |
| | Definición y configuración de las políticas de permisos de acceso a datos entre aplicaciones y librerías, como en el caso de los teléfonos móviles. | X | | |
| | Definición de perfiles de acceso en base a privilegios u otro tipo de barreras tecnológicas y procedimentales que impidan la vinculación no autorizada de fuentes de datos independientes. | X | | |
| | Contenido registrado en los logs (quién, cuándo, a qué, qué acción, para qué propósito, … se accede a los datos). | X | | |
| | Definición de sistemas automáticos de alerta ante eventos concretos. | X | | |

| | | | | |
|---|---|---|---|---|
| | Trazabilidad de la comunicación de datos entre responsables, encargados y subencargados. | X | | |
| | Opciones de seguridad configurables (aparte de las opciones de cifrado). | X | | |
| | Permitir configuraciones de acceso diferentes en función de distintos dispositivos. | X | | |
| | Configurar sistemas de alerta por accesos anómalos a los datos. | X | | |
| | Configuración de algunos de los parámetros de seguridad, en particular las claves y cómo balancear la relación seguridad/rendimiento/funcionalidad en función de la robustez deseada por el usuario. | | X | |
| | Control del ámbito de distribución de la información que se distribuye en el entorno de la aplicación (redes sociales, redes laborales, etc.). | | X | |
| | Configuración de la recepción de avisos cuando la información se está haciendo accesible a terceros. | | X | |
| | Control de los metadatos incorporados en la información generada o distribuida. | | X | |
| | Mecanismo del “derecho al olvido” de la información publicada en redes sociales u otros sistemas. | | X | |
| | Opciones de elección respecto a dónde se almacenan los datos personales, ya sea en dispositivos locales o remotos y, en este último caso, otros parámetros como encargados o países. | | X | |
| | Histórico de perfiles y entidades que han accedido a su información. | | X | |
| | Información sobre el acceso a sus datos por usuarios autorizados | | X | |
| | Información sobre los últimos cambios llevados a cabo y el perfil que ha realizado el cambio | | X | |

| | | | | |
|---|---|---|---|---|
| | Configurabilidad de controles de acceso por funcionalidades prestadas. | | | X |
| | Configurabilidad de separación lógica de grupos de datos. | | | X |
| | Configurabilidad de separación física de grupos de datos. | | | X |
| | Deshabilitación o anulación selectiva de funcionalidades. | | | X |
| **General** | | | | |
| | En el caso de que el servicio sea multidispositivo, posibilidad (no obligación) de aplicar criterios generales de privacidad aplicable a todos ellos y en una única acción. | X | X | |
| | Recordatorios, iconos y avisos de todas aquellas acciones que afectan a la privacidad de la información: cambios de configuración, acceso a los datos por parte de terceros como captura de video, sonido, posición, etc. | X | X | |

## XII. BIBLIOGRAFÍA


- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

  https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&qid=1592307014433&from=ES

- Guidelines 4/2019 on Article 25 Data Protection by Design and by Default

  https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_es

- "Recommendations on shaping technology according to GDPR provisions. Exploring the notion of data protection by default", dic 2018. European Union Agency for Cybersecurity (ENISA).

  https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2