

Análisis de Cumplimiento RGPD

(Estudio de Caso Fitness)

Introducción

Este ejercicio evalúa su capacidad para aplicar los **Principios Generales del Reglamento General de Protección de Datos (RGPD)**, específicamente la Licitud, la Limitación de la Finalidad, la Minimización de Datos y la necesidad de realizar una Evaluación de Impacto (AIPD).

Debe analizar una estrategia de marketing de una empresa de comercio electrónico y determinar su nivel de cumplimiento, proponiendo soluciones concretas.

Caso de Estudio: E-commerce "HealthyLife"

La empresa ficticia "HealthyLife" vende ropa deportiva y suplementos nutricionales en línea. Para "mejorar la experiencia del cliente" y lanzar una nueva línea de productos, la Gerencia de Marketing ha decidido implementar la siguiente estrategia al momento del registro de un nuevo cliente:

- 1. Recogida de Datos Adicionales:** Al registrarse, los clientes deben proporcionar obligatoriamente su **talla de ropa y su peso corporal actual**.
- 2. Uso de Datos (Sin Consentimiento Específico):** Utilizarán el correo electrónico proporcionado durante la compra para enviar **correos electrónicos semanales con dietas y planes nutricionales personalizados** basados en el peso corporal. Estos planes son generados por un algoritmo.

El Aviso Legal y la Política de Privacidad mencionan únicamente que los datos serán usados para "procesar pedidos y enviar información promocional de productos".

Tareas para el Alumno

Basándose en los principios del RGPD estudiados (Licitud, Minimización, Limitación de la Finalidad), responda y justifique las siguientes preguntas:

Tarea 1: Identificación de Incumplimientos (Licitud, Minimización, Finalidad)

Identifique y explique detalladamente qué principios del RGPD se están infringiendo con la estrategia actual de "HealthyLife".

1. Principio de Minimización de Datos:

- *¿Qué datos recogidos son excesivos o no pertinentes para la finalidad principal (procesar pedidos y enviar promociones de ropa/suplementos)?*
- *Justifique por qué el Peso Corporal se considera un dato sensible o excesivo en este contexto.*

2. Principio de Limitación de la Finalidad:

- *¿Cuál es el fin inicial para el que se recogen los datos (según la Política de Privacidad)?*
- *¿El envío de "dietas personalizadas" es compatible con el fin inicial? Explique por qué esta nueva finalidad requiere un tratamiento separado.*

3. Principio de Licitud y Transparencia:

- *¿Bajo qué base legal (consentimiento, interés legítimo, etc.) se intenta tratar el dato del "Peso Corporal" y el envío de las "dietas personalizadas"?*
- *Explique por qué el consentimiento genérico de "enviar información promocional" no es lícito ni transparente para justificar el envío de planes nutricionales.*

Tarea 2: Propuesta de Estrategia de Cumplimiento y Consentimiento

Modifique la estrategia de "HealthyLife" para que cumpla con los principios identificados en la Tarea 1.

1. **Minimización de Datos:** Proponga un enfoque para el dato del **Peso Corporal**. ¿Se debe eliminar la recogida? Si la empresa insiste en ofrecer dietas, ¿qué dato alternativo y menos invasivo podría solicitar para segmentar los planes (ej. "Objetivo: Perder peso" o "Nivel de actividad")?
2. **Licitud y Limitación de la Finalidad:** Diseñe cómo deben obtener el **Consentimiento Válido y Específico** para enviar los "Planes Nutricionales Personalizados". Detalle qué

información debe aparecer en la casilla de consentimiento y por qué debe ser una acción **voluntaria y separada** de la aceptación de la política de privacidad (p. ej., utilizando una casilla *checkbox* no marcada por defecto).

Tarea 3: Evaluación de Impacto (AIPD/DPIA)

Determine si la empresa "HealthyLife" debe realizar una Evaluación de Impacto de Protección de Datos (AIPD o DPIA) antes de implementar su nueva estrategia.

1. **Obligación Legal:** Determine si la recogida del **Peso Corporal** y su uso para la **segmentación algorítmica** de dietas se considera un tratamiento de alto riesgo.
2. **Justificación:** Justifique su respuesta basándose en los criterios que obligan a realizar una AIPD (p. ej., tratamiento de datos sensibles a gran escala, elaboración de perfiles o decisiones automatizadas con efectos jurídicos).

Formato de Entrega: El ejercicio debe presentarse como un informe de consultoría que desarrolle cada una de las tareas de forma clara y justificada.