



# UNIVERSIDAD MARIANO GÁLVEZ DE GUATEMALA

## FACULTAD DE INGENIERÍA EN SISTEMAS DE INFORMACIÓN PROGRAMA DE POSGRADOS

### INFOGRAFIA DE GDPR

**Autor:**

**Guerrero Hernandez, Diego Guerrero – [dguerreroh@miumg.edu.gt](mailto:dguerreroh@miumg.edu.gt)**

**Profesor**

**Evelyn Yesenia Lobos Barrera**

**Curso**

**Marco legal y regulatorio – Tercer Trimestre - 2025**

**Guatemala, junio 2025**

## Contenido

Google Gemini .....	3
Análisis .....	3
Pasos para el cumplimiento .....	4
Comentario .....	5
Microsoft copilot .....	6
Análisis .....	6
Pasos para el cumplimiento .....	7
Comentario .....	9
CHATGPT .....	10
Análisis .....	10
Pasos a seguir el cumplimiento.....	12
Comentario .....	15
Infografía .....	16

# Google Gemini

## Análisis

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, conocido como el Reglamento General de Protección de Datos (RGPD), tiene como objetivo principal proteger los datos personales de las personas físicas dentro de la Unión Europea y regular la libre circulación de dichos datos. El documento enfatiza que la protección de los datos personales es un derecho fundamental.

### Puntos clave del Reglamento

- **Alcance territorial:** El reglamento se aplica al tratamiento de datos personales de individuos que residen en la UE, incluso si el responsable o encargado del tratamiento no está establecido en la Unión. Esto ocurre cuando las actividades de tratamiento están relacionadas con la oferta de bienes o servicios a dichos individuos o con la observación de su comportamiento dentro de la UE.
- **Definiciones:** El reglamento define "datos personales" como cualquier información sobre una persona física identificada o identifiable. El concepto de "tratamiento" abarca cualquier operación o conjunto de operaciones realizadas con datos personales, ya sean automatizadas o no, como la recogida, registro, organización y conservación.
- **Principios de tratamiento:** El tratamiento de datos debe ser **lícito** y **leal**. La transparencia es clave, lo que significa que la información sobre el tratamiento debe ser accesible y fácil de entender. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que se tratan.
- **Consentimiento:** El consentimiento debe ser un **acto afirmativo claro** que refleje una manifestación de voluntad libre, específica, informada e inequívoca del interesado. El silencio, las casillas pre-marcadas o la inacción no se consideran consentimiento válido.
- **Derechos de los interesados:** Se refuerzan los derechos de los interesados, incluyendo la capacidad para pedir a la autoridad de control acceso a sus datos, su rectificación o supresión, la limitación de su tratamiento y el derecho a oponerse al tratamiento.
- **Autoridades de control:** El reglamento establece que las autoridades de control deben tener los mismos poderes efectivos en todos los Estados

miembros, incluidos los de investigación, corrección y sanción. La finalidad es asegurar una supervisión y una aplicación coherentes del reglamento en toda la UE.

- **Transferencias de datos:** El documento establece que la transferencia de datos personales a países no pertenecientes a la UE o a organizaciones internacionales no debe menoscabar el nivel de protección garantizado en la Unión. Se permiten transferencias si la Comisión ha constatado que el tercer país garantiza un nivel de protección de datos adecuado.

El RGPD busca unificar y fortalecer la protección de datos en la UE, eliminando la fragmentación y la inseguridad jurídica que existía con la directiva anterior (Directiva 95/46/CE), la cual deroga.

## Pasos para el cumplimiento

Una empresa debe seguir varios pasos clave para cumplir con el Reglamento General de Protección de Datos (RGPD) y gestionar de forma adecuada los datos personales. Estos pasos incluyen:

### 1. Concienciación y Evaluación

- **Designar un Responsable de Protección de Datos (DPO):** Si la empresa cumple ciertos criterios (por ejemplo, si el tratamiento de datos es a gran escala o implica categorías especiales de datos), debe nombrar un DPO para supervisar el cumplimiento.
- **Realizar un inventario de datos:** Identificar qué datos personales se recopilan, cómo se utilizan, dónde se almacenan y con quién se comparten.
- **Analizar la base jurídica:** Determinar la base legal para el tratamiento de cada tipo de dato (por ejemplo, consentimiento, interés legítimo o cumplimiento de un contrato).
- **Evaluación de Impacto:** Realizar una Evaluación de Impacto sobre la Protección de Datos (EIPD) si el tratamiento de datos puede suponer un alto riesgo para los derechos y libertades de los interesados.

---

## **2. Implementación de políticas y procedimientos**

- **Obtener un consentimiento válido:** Asegurarse de que el consentimiento sea **libre, específico, informado y una manifestación de voluntad clara** del interesado.
  - **Revisar y actualizar contratos:** Ajustar los contratos con proveedores y socios para incluir las cláusulas de protección de datos.
  - **Establecer medidas de seguridad:** Implementar medidas técnicas y organizativas para proteger los datos, como el cifrado, la seudonimización y el control de acceso.
  - **Crear políticas internas:** Desarrollar políticas claras sobre el tratamiento de datos para los empleados, así como procedimientos para manejar las solicitudes de los interesados (derechos ARSULIPO: Acceso, Rectificación, Supresión, Limitación, Portabilidad y Oposición).
- 

## **3. Mantenimiento y Rendición de Cuentas**

- **Documentar el cumplimiento:** Mantener registros de todas las actividades de tratamiento de datos y de las medidas de seguridad adoptadas para demostrar el cumplimiento del RGPD.
- **Notificar violaciones de datos:** Establecer un plan de respuesta para notificar a la autoridad de control y a los afectados en caso de una violación de seguridad de datos.
- **Formación continua:** Capacitar a los empleados sobre la importancia de la protección de datos y sus responsabilidades bajo el RGPD.
- **Monitoreo y revisión:** Revisar y actualizar regularmente las políticas y procedimientos para asegurar que siguen siendo efectivos.

## **Comentario**

Considero que la información de la información de Google Gemini es bastante clara, deja bien especificado los pasos y el análisis que realizo

# Microsoft copilot

## Análisis

El **Reglamento (UE) 2016/679**, mejor conocido como **Reglamento General de Protección de Datos (RGPD o GDPR)**, es la norma clave de la Unión Europea sobre protección de datos personales y privacidad. Entró en vigor el **25 de mayo de 2018** y su objetivo principal es dar a las personas más control sobre sus datos, así como establecer obligaciones claras para quienes los tratan.

Aquí tienes un desglose de sus puntos más relevantes:

### Objetivos principales

- **Proteger los derechos y libertades fundamentales** de las personas, especialmente el derecho a la protección de sus datos.
- **Armonizar la normativa** de protección de datos en todos los Estados miembros de la UE.
- **Adaptar las reglas** al entorno digital y a los flujos globales de información.

### Derechos clave para los ciudadanos

- **Derecho de acceso**: saber qué datos personales se están tratando.
- **Derecho de rectificación**: corregir información inexacta.
- **Derecho de supresión** (“derecho al olvido”): solicitar la eliminación de datos cuando ya no sean necesarios.
- **Derecho a la portabilidad**: recibir los datos en un formato estructurado y transferirlos a otro responsable.
- **Derecho a la limitación u oposición del tratamiento**: detener o restringir el uso de datos bajo ciertas condiciones.
- **Protección frente a decisiones automatizadas**, incluido el perfilado.

### Obligaciones para responsables y encargados de tratamiento

- **Base jurídica** para procesar datos (consentimiento, contrato, interés legítimo, etc.).
- **Transparencia**: informar de forma clara y sencilla sobre el tratamiento.

- **Seguridad:** aplicar medidas técnicas y organizativas para proteger datos.
- **Notificación de brechas:** informar a la autoridad competente y, en algunos casos, a los afectados.
- **Evaluaciones de impacto** en casos de alto riesgo.
- **Nombramiento de un Delegado de Protección de Datos (DPO)** en ciertos supuestos.

### Alcance extraterritorial

Aplica **también a empresas fuera de la UE** si tratan datos de personas que se encuentren en la UE, por ejemplo, ofreciendo bienes o servicios o monitoreando su comportamiento.

### Sanciones

- Multas administrativas de **hasta 20 millones de euros** o el **4 % de la facturación anual global**, la cifra que sea mayor.

## Pasos para el cumplimiento

### Pasos para el cumplimiento del GDPR

#### 1. Diagnóstico inicial

- Auditar qué datos personales se recogen, de quién, para qué y dónde se almacenan.
- Identificar si hay transferencias internacionales de datos.

#### 2. Definir bases legales de tratamiento

- Documentar si el tratamiento se basa en **consentimiento, contrato, interés legítimo, obligación legal**, etc.
- Asegurarse de que cada tratamiento tiene una justificación válida.

#### 3. Actualizar políticas y avisos de privacidad

- Redactar avisos claros y transparentes.

- Explicar qué datos se recogen, por qué, durante cuánto tiempo y con quién se comparten.

#### **4. Establecer procedimientos para derechos de los interesados**

- Crear canales para ejercer derechos: acceso, rectificación, supresión, oposición, portabilidad y limitación.
- Definir plazos y responsables para responder.

#### **5. Seguridad de la información**

- Implementar medidas técnicas (cifrado, contraseñas robustas, backups seguros).
- Adoptar medidas organizativas (formación del personal, control de accesos).

#### **6. Gestión de brechas de seguridad**

- Tener un protocolo para detectar, evaluar y notificar incidentes.
- Notificar a la autoridad de control en un máximo de 72 horas cuando sea necesario.

#### **7. Evaluaciones de impacto (DPIA)**

- Realizar análisis de riesgos cuando el tratamiento pueda afectar gravemente la privacidad (p. ej., uso de IA o vigilancia).

#### **8. Nombrar Delegado de Protección de Datos (DPO), si aplica**

- Obligatorio en administraciones públicas, tratamientos a gran escala o gestión de datos sensibles.

#### **9. Contratos con proveedores**

- Firmar acuerdos de encargado de tratamiento que incluyan cláusulas de protección de datos.

#### **10. Formación continua y cultura de protección de datos**

- Sensibilizar a empleados sobre su papel en el cumplimiento.
- Mantener el cumplimiento como un proceso vivo, no un proyecto puntual.

## Comentario

El análisis realizado por Copilot fue más robusto y profundo que el realizado por la IA de Gemini, deja en claro más aspectos haciendo énfasis en más clasificaciones o apartados para dejarlo mas claro, incluso en los pasos a seguir da datos importantes como las multas en caso de un incumplimiento, la información proporcionada es muy buena.

# CHATGPT

## Análisis

### Contexto y Finalidad

El RGPD fue aprobado el **27 de abril de 2016** y entró en vigor el **25 de mayo de 2018**, sustituyendo la Directiva 95/46/CE. Su objetivo principal es:

- **Proteger los datos personales** de las personas físicas.
  - **Unificar las normas** en toda la Unión Europea (armonización).
  - **Garantizar la libre circulación de datos** dentro del mercado único europeo sin que la protección de datos sea un obstáculo.
- 

### 💡 Principios Fundamentales

El RGPD establece principios que deben cumplirse en todo tratamiento de datos:

1. **Licitud, lealtad y transparencia** – El tratamiento debe ser legítimo, claro y comprensible.
  2. **Limitación de la finalidad** – Los datos deben recogerse con fines específicos, explícitos y legítimos.
  3. **Minimización de datos** – Solo se pueden tratar los datos estrictamente necesarios.
  4. **Exactitud** – Los datos deben ser veraces y actualizarse.
  5. **Limitación del plazo de conservación** – No guardar más tiempo del necesario.
  6. **Integridad y confidencialidad** – Seguridad frente a accesos no autorizados.
  7. **Responsabilidad proactiva (accountability)** – El responsable debe demostrar cumplimiento.
- 

### 👤 Derechos de los Interesados

El Reglamento refuerza los derechos de los ciudadanos europeos sobre sus datos personales:

- **Derecho de acceso** (saber qué datos se tratan).

- **Derecho de rectificación.**
  - **Derecho de supresión o “derecho al olvido”.**
  - **Derecho a la limitación del tratamiento.**
  - **Derecho a la portabilidad de los datos.**
  - **Derecho de oposición** al tratamiento, especialmente contra la mercadotecnia directa.
  - **Derecho a no ser objeto de decisiones automatizadas** (incluida la elaboración de perfiles) que produzcan efectos jurídicos significativos.
- 

## **Responsables y Encargados**

El RGPD define claramente roles:

- **Responsable del tratamiento:** decide fines y medios del tratamiento.
  - **Encargado del tratamiento:** procesa los datos en nombre del responsable.
  - Ambos deben implementar **medidas técnicas y organizativas adecuadas** (cifrado, seudonimización, control de accesos, evaluaciones de impacto, etc.).
- 

## **Bases de Licitud del Tratamiento**

Los datos solo pueden tratarse si existe una base jurídica válida:

- Consentimiento explícito.
  - Ejecución de un contrato.
  - Obligación legal.
  - Interés vital del interesado o de otra persona.
  - Misión realizada en interés público o en ejercicio de poderes públicos.
  - Interés legítimo del responsable, siempre que no prevalezcan los derechos del interesado.
-

## Sanciones

El RGPD introduce un régimen sancionador fuerte:

- Multas administrativas de hasta **20 millones de euros** o el **4% de la facturación anual global** (la que sea mayor).
  - Diferentes niveles de sanciones según la gravedad de la infracción.
- 

## Alcance Territorial

Se aplica no solo a organizaciones de la UE, sino también a empresas **fuerza de la UE** que:

- Ofrezcan bienes o servicios a residentes de la UE.
- Monitorean su comportamiento (ej. cookies, perfiles online)

## Pasos a seguir el cumplimiento

### 1. Diagnóstico Inicial

- **Auditoría de datos:** Identificar qué datos personales se recopilan, cómo se usan, dónde se almacenan y con quién se comparten.
  - **Mapa de datos:** Documentar los flujos de datos internos y externos.
  - **Clasificación:** Distinguir entre datos comunes y categorías especiales (salud, biométricos, etc.).
- 

### 2. Definir Bases Legales del Tratamiento

- Determinar la **base jurídica** aplicable en cada caso: consentimiento, contrato, obligación legal, interés legítimo, interés público o vital.
  - Garantizar que el **consentimiento** sea libre, informado, explícito y verificable.
-



### 3. Implementar Principios de Protección

- **Minimización de datos:** Recoger solo lo necesario.
  - **Limitación de conservación:** Definir plazos claros de almacenamiento y supresión.
  - **Seguridad:** Aplicar medidas técnicas y organizativas (cifrado, seudonimización, backups seguros).
  - **Privacidad por diseño y por defecto:** Incorporar la protección de datos desde la planificación de procesos, productos y servicios.
- 



### 4. Derechos de los Interesados

- Establecer procedimientos internos para responder a:
    - Acceso, rectificación, supresión (“derecho al olvido”).
    - Limitación del tratamiento.
    - Portabilidad.
    - Oposición.
    - Exclusión de decisiones automatizadas.
  - Garantizar respuesta en **máx. 1 mes**.
- 



### 5. Nombrar un Delegado de Protección de Datos (DPO)

- Obligatorio en:
    - Autoridades u organismos públicos.
    - Empresas cuya actividad principal implique monitorización sistemática a gran escala.
    - Empresas que traten datos sensibles a gran escala.
  - El DPO asesora, supervisa y actúa de enlace con la autoridad de control.
-

## 6. Documentación y Registro

- Mantener un **registro de actividades de tratamiento** (obligatorio para empresas de +250 empleados o si tratan datos sensibles/riesgosos).
  - Elaborar **políticas de privacidad** claras y accesibles.
  - Revisar y actualizar contratos con terceros (encargados de tratamiento) para incluir cláusulas de protección de datos.
- 

## 7. Gestión de Brechas de Seguridad

- Establecer un **protocolo de notificación** de incidentes.
  - Comunicar a la autoridad de control en un máximo de **72 horas** tras detectar la brecha.
  - Notificar a los interesados si hay alto riesgo para sus derechos.
- 

## 8. Transferencias Internacionales

- Verificar que las transferencias de datos fuera del EEE cuenten con garantías adecuadas (cláusulas tipo, decisiones de adecuación, normas corporativas vinculantes).
- 

## 9. Formación y Concienciación

- Capacitar a empleados sobre buenas prácticas de seguridad y privacidad.
  - Realizar campañas internas para fomentar la cultura de protección de datos.
- 

## 10. Evaluación Continua

- Realizar **evaluaciones de impacto (DPIA)** cuando el tratamiento implique alto riesgo.
- Revisar y mejorar continuamente las políticas y medidas adoptadas.

## Comentario

En mi criterio ChatGPT cuenta con una información más entendible que las otras inteligencias artificiales, aunque la estructura comparándola con copilot es muy similar, estas dos para mi son las mejores del mercado actualmente.

Explican bien el análisis sobre el decreto y los pasos a seguir para hacer que la empresa cumpla este reglamento, hacen énfasis por subtítulos para que se entienda mejor y dan detalles específicos en cada aspecto de los temas que involucran el decreto.

## Infografía

# REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD)

## OBJETIVO

Proteger los datos personales y garantizar la libre circulación de los datos en la Unión Europea



## PRINCIPIOS FUNDAMENTALES

- |  |                              |
|--|------------------------------|
| 1 Licitud, lealtad y transparencia     | • Acceso                     |
| 2 Limitación de la finalidad           | • Rectificación              |
| 3 Minimización de datos                | • Limitación del tratamiento |
| 4 Exactitud                            | • Portabilidad               |
| 5 Limitación del plazo de conservación | • Oposición                  |
| 6 Integridad y confidencialidad        |                              |
| 7 Responsabilidad proactiva            |                              |



## DERECHOS DE LOS INTERESADOS

- |                              |                            |
|------------------------------|----------------------------|
| • Acceso                     | • Consentimiento           |
| • Rectificación              | • Ejecución de un contrato |
| • Supresión                  | • Obligación legal         |
| • Limitación del tratamiento | • Intereses vitales        |
| • Portabilidad               | • Interés público          |
| • Oposición                  | • Interés legítimo         |



## RESPONSABLES Y ENCARGADOS

Medidas técnicas y organizativas adecuadas



## SANCIONES

Hasta 20 millones de euros o el 4% de facturación anual global  
(si es mayor)

## ALCANCE TERRITORIAL

Organizaciones en la UE o que ofrecen bienes o servicios a personas en la UE