# INFORME TÉCNICO DE CUMPLIMIENTO RGPD

Evaluación comparativa: ChatGPT, Microsoft 365 Copilot y Azure OpenAI

Fecha: Octubre 2025

Autor: José Fuentes / Área Técnica IT Netview Soluciones Digitales S.L.

## 1. Contexto

La organización está evaluando la integración de herramientas de inteligencia artificial (IA) para apoyar la productividad y el análisis de información. Este informe analiza el cumplimiento del RGPD (Reglamento General de Protección de Datos) en el uso de ChatGPT (OpenAI), Microsoft 365 Copilot y Azure OpenAI.

## 2. Descripción técnica de las soluciones

Comparativa de las soluciones según su infraestructura, tipo de servicio y nivel de control sobre los datos:

| Solución | Infraestructura | Naturaleza del servicio | Control del entorno |
|---|---|---|---|
| ChatGPT (público) | OpenAI (EE.UU.) | SaaS externo | Bajo |
| ChatGPT Enterprise | OpenAI Cloud (UE/EE.UU.) | SaaS empresarial | Medio |
| Microsoft 365 Copilot | Tenant M365 (UE) | Integrado en M365 | Alto |
| Azure OpenAI | Azure Tenant (UE) | API gestionada | Muy alto |

### ChatGPT (OpenAI) — Cumplimiento RGPD

#### a) Dónde se procesan los datos

- OpenAI (empresa estadounidense) aloja y procesa los datos **en EE. UU.**
- Aunque cumple con el **EU–U.S. Data Privacy Framework (julio 2023)**, sigue siendo un **encargado de tratamiento externo** fuera del espacio europeo.

#### b) Uso de tus datos (muy importante)

| Versión | Tratamiento de datos | Uso en entrenamiento |
|---|---|---|
| **ChatGPT gratuito o Plus (usuario personal)** | Los datos se almacenan y pueden revisarse para mejorar los modelos | ✅ Sí, salvo que lo desactives manualmente |
| **ChatGPT Team o Enterprise** | Datos **aislados y no utilizados** para entrenamiento | ❌ No se usan en modelos futuros |
| **API de OpenAI (Azure OpenAI o API directa)** | Por defecto **no entrenan con tus datos**, solo para inferencia | ❌ No |

**Si usas la versión pública (chat.openai.com) y subes documentos con datos personales, estarías INCUMPLIENDO RGPD, salvo anonimización previa o consentimiento explícito.**

### c) Revisión técnica

Para verificar el estado:

1. Ve a **Settings → Data Controls** en ChatGPT.
2. Desactiva "Training data sharing".
3. Si usas cuenta profesional, revisa el **Data Processing Addendum (DPA)** firmado con OpenAI.

---

## 3 Microsoft Copilot (Microsoft 365 Copilot / Azure OpenAI)

### a) Dónde y cómo procesa los datos

- Copilot en Microsoft 365 **se ejecuta dentro del tenant de Microsoft 365 del cliente**, usando **el mismo entorno que Outlook, SharePoint y OneDrive**.
- Los datos **no salen de tu entorno Microsoft 365**.
- Microsoft actúa como **encargado del tratamiento** bajo el **Data Protection Addendum (DPA)** de Microsoft.
- Está **certificado bajo RGPD, ISO 27001, SOC 2, FedRAMP, etc.**

### b) Uso de datos para entrenamiento

| Servicio | Uso de datos para mejorar modelos | Comentario |
|---|---|---|
| **Microsoft 365 Copilot** | ❌ No usa tus datos corporativos ni de usuarios para entrenamiento | Los modelos base (GPT) ya están entrenados y solo ejecutan inferencias |
| **Azure OpenAI Service** | ❌ No usa los datos para entrenar modelos de OpenAI | Los datos se quedan en tu suscripción Azure |
| **GitHub Copilot** | ⚠️ El código puede usarse para mejorar el modelo salvo exclusión contractual (depende del plan) | No recomendable para datos sensibles |

### c) Seguridad añadida

- Los **tokens de salida (respuestas generadas)** también se tratan dentro del marco de tu tenant.
- No se almacenan fuera de tu organización.
- Microsoft aplica **data residency** (por ejemplo, Europa → datos en datacenters de la UE).

---

## Comparativa técnica–legal directa

| Criterio | ChatGPT (web o app pública) | ChatGPT Team/Enterprise | Microsoft Copilot (M365) |
|---|---|---|---|
| Ubicación del tratamiento | EE. UU. (OpenAI) | Data residency configurable | Datacenters UE (según tenant) |
| Control de datos | Limitado | Control medio (acuerdo empresarial) | Total (dentro de M365 tenant) |
| Uso para entrenamiento | ✅ Sí (por defecto) | ❌ No | ❌ No |
| Cumplimiento RGPD | ❌ Riesgoso si hay datos personales | ✅ Cumple con DPA | ✅ Cumple RGPD, ISO, SOC |
| Integración con sistemas internos | Manual | Limitada | ✅ Nativa con OneDrive, Outlook, SharePoint |
| Riesgo de fuga de datos | Alto | Bajo | Muy bajo |

**Conclusión:**
Desde el punto de vista de **cumplimiento RGPD y seguridad**,
**Copilot en Microsoft 365 es la opción más segura y legalmente sólida** para tratar documentos corporativos o personales.
ChatGPT público **solo sería aceptable si los datos están anonimizados o no sensibles.**

---

### 5 Recomendaciones prácticas para IT y cumplimiento

1. **Clasifica la sensibilidad de los datos** (público / interno / confidencial / personal).
2. **Anonimiza** antes de subir a cualquier IA externa.
3. **Desactiva entrenamiento y logging** en ChatGPT (Settings → Data Controls).
4. **Verifica el DPA firmado con Microsoft** en el portal de cumplimiento (`https://servicetrust.microsoft.com`).
5. **Revisa auditorías periódicas** de acceso (Azure AD Sign-ins → App Copilot).
6. **Incluye cláusulas de IA** en las políticas internas (quién puede usar IA, con qué fines, y en qué entorno).

## 3. Análisis de cumplimiento RGPD

Se analizan los aspectos clave: base jurídica, ubicación de los datos, uso para entrenamiento y medidas de seguridad.

### 3.1 Base jurídica y rol del responsable

ChatGPT público depende del consentimiento explícito o del interés legítimo, mientras que Microsoft y Azure actúan como encargados de tratamiento bajo contrato (DPA) compatible con RGPD.

### 3.2 Transferencia internacional de datos

ChatGPT público implica transferencia a EE.UU.; Copilot y Azure OpenAI mantienen los datos en la UE, conforme al DPA de Microsoft.

### 3.3 Uso de datos para entrenamiento

Solo ChatGPT público utiliza datos de usuario para entrenamiento. Copilot y Azure OpenAI no usan datos corporativos para mejorar los modelos.

### 3.4 Medidas técnicas y organizativas

Microsoft Copilot y Azure OpenAI ofrecen cifrado, control de identidades (Azure AD), auditoría y residencia de datos en la UE.

**Análisis de cumplimiento RGPD**

**A) Base jurídica y rol del responsable**

| Criterio RGPD | ChatGPT Público | ChatGPT Enterprise | Copilot | Azure OpenAI |
|---|---|---|---|---|
| **Responsable del tratamiento** | OpenAI | OpenAI (con DPA empresarial) | Microsoft (encargado del tratamiento) | Cliente (responsable) / Microsoft (encargado) |
| **Base jurídica** | Consentimiento o interés legítimo (limitado) | Contrato empresarial | Contrato de servicios M365 | Contrato Azure + DPA |
| **Adecuación al RGPD** | ❌ Insuficiente sin consentimiento y anonimización | ⚠️ Parcialmente adecuado | ✅ Cumple RGPD | ✅ Cumple RGPD |

**B) Localización y transferencia internacional de datos**

| Criterio | ChatGPT Público | ChatGPT Enterprise | Copilot | Azure OpenAI |
|---|---|---|---|---|
| **Ubicación del procesamiento** | EE. UU. | UE/EE. UU. (según contrato) | Datacenters regionales (UE) | Datacenters regionales (UE o cliente) |
| **Transferencia fuera del EEE** | ✅ Sí | ⚠️ Posible | ❌ No (si tenant UE) | ❌ No (si región UE) |
| **Mecanismos de garantía** | Privacy Framework EE. UU.–UE | Cláusulas contractuales tipo | DPA Microsoft | DPA Microsoft |

**C) Uso de datos para entrenamiento y retención**

| Criterio | ChatGPT Público | ChatGPT Enterprise | Copilot | Azure OpenAI |
|---|---|---|---|---|
| **Uso de datos para entrenamiento** | ✅ Sí (por defecto) | ❌ No | ❌ No | ❌ No |

| Criterio | ChatGPT Público | ChatGPT Enterprise | Copilot | Azure OpenAI |
|---|---|---|---|---|
| **Retención de entradas/salidas (logs)** | 30 días (según política) | Control configurable | Dentro del tenant (según políticas M365) | Dentro del tenant (según retención configurada) |
| **Posibilidad de anonimización** | Manual | Parcial | Total (según políticas internas M365) | Total (control IT) |

**D) Medidas técnicas y organizativas**

| Aspecto | ChatGPT Público | ChatGPT Enterprise | Copilot | Azure OpenAI |
|---|---|---|---|---|
| **Cifrado en tránsito/reposo** | TLS | TLS | TLS + cifrado reposo (BitLocker / EKM) | TLS + cifrado reposo (Azure Key Vault) |
| **Gestión de identidades** | Usuario externo | SSO empresarial opcional | Azure AD | Azure AD |
| **Auditoría / logging** | Limitado | Parcial | Completo (Microsoft 365 Compliance Center) | Completo (Azure Monitor / Defender) |
| **Residencia de datos garantizada (UE)** | ❌ No | ⚠️ Parcial | ✅ Sí | ✅ Sí |
| **Certificaciones** | SOC 2, ISO 27001 | SOC 2, ISO 27001 | ISO 27001, SOC, GDPR DPA, FedRAMP | ISO 27001, SOC, GDPR DPA, FedRAMP |

## 4. Evaluación de riesgos

Identificación de riesgos principales y medidas de mitigación recomendadas:

• Exposición de datos personales al usar ChatGPT público → Mitigar con anonimización o uso restringido.

• Transferencias internacionales → Verificar DPA y residencia de datos.
• Falta de control sobre entrenamiento → Usar versiones empresariales.
• Riesgos de acceso no autorizado → Implementar MFA y revisiones periódicas.

## 5. Conclusiones

**Copilot y Azure OpenAI cumplen plenamente con el RGPD y ofrecen el mayor control y seguridad. ChatGPT público no es recomendable para datos personales o confidenciales. Se recomienda centralizar el uso de IA bajo políticas corporativas de seguridad.**

## 6. Medidas recomendadas

1. Firmar el DPA de Microsoft.
2. Configurar residencia de datos en la UE.
3. Activar auditorías en Microsoft Purview.
4. Prohibir ChatGPT público con datos reales.
5. Anonimizar datos sensibles antes de su uso.
6. Revisar accesos trimestralmente.
7. Documentar roles y responsabilidades en la DPIA.

## 7. Checklist DPIA

Complete la siguiente lista para evaluación interna:

[ ] ¿Existe una base jurídica documentada para el uso de IA?

[ ] ¿Se han firmado los contratos/DPA con proveedores (Microsoft/OpenAI)?

[ ] ¿Los datos se almacenan y procesan dentro de la UE?

[ ] ¿Se impide el uso de ChatGPT público con información personal?

[ ] ¿Se han implementado controles de acceso y MFA?

[ ] ¿Se realizan auditorías periódicas de uso de IA?

[ ] ¿Se informa a los usuarios del tratamiento de datos mediante IA?

[ ] ¿Se ha documentado la DPIA en el registro de actividades?

**Anexo: referencias normativas y técnicas**

- Reglamento (UE) 2016/679 — RGPD
- Directrices 4/2022 del Comité Europeo de Protección de Datos sobre IA
- Cláusulas Contractuales Tipo (2021/914/UE)
- EU–U.S. Data Privacy Framework (julio 2023)
- Microsoft Data Protection Addendum (DPA)
- OpenAI Data Processing Terms (2024)
- ISO/IEC 27001:2022 y SOC 2 Type II

# Ejemplos concretos de exposición y consecuencias

## 1 Principio general del riesgo

Cuando subes documentos o texto a ChatGPT **fuera de un entorno controlado** (por ejemplo, chat.openai.com), estás:

- **Transfiriendo datos personales** a un tercero (OpenAI, EE. UU.).
- **Perdiendo control sobre el almacenamiento, uso y eliminación** de esos datos.
- **Posiblemente violando el principio de minimización y limitación de finalidad** del RGPD.

Aunque OpenAI afirma aplicar medidas de seguridad, **los datos pueden conservarse durante un periodo limitado** y **ser revisados o utilizados para entrenamiento** si no se ha desactivado expresamente.

Esto, para una empresa europea, **equivale a una transferencia internacional sin garantías adecuadas**, lo cual es una **infracción directa del RGPD (art. 44-49)**.

---

## 2 Riesgos principales al subir información personal o sensible

| Tipo de riesgo | Descripción | Impacto potencial |
|---|---|---|
| **Pérdida de confidencialidad** | Los datos podrían almacenarse en servidores externos o ser revisados por personal autorizado de OpenAI. | Divulgación no autorizada de información protegida. |
| **Transferencia internacional no autorizada** | Los datos viajan a EE. UU. sin cláusulas contractuales tipo ni consentimiento válido. | Infracción del RGPD (arts. 44-46). |
| **Reutilización de datos** | Los textos pueden emplearse para entrenar modelos de lenguaje o mejorar servicios. | Tratamiento fuera de la finalidad original. |
| **Fuga de secretos empresariales o confidenciales** | Información estratégica o contractual puede filtrarse o reidentificarse. | Daños reputacionales, pérdida de ventaja competitiva. |

| Tipo de riesgo | Descripción | Impacto potencial |
|---|---|---|
| **Incumplimiento de deber de confidencialidad profesional** | Si se trata de información médica, judicial o notarial. | Responsabilidad disciplinaria o penal. |
| **Imposibilidad de ejercer derechos ARCO (acceso, rectificación, supresión)** | No puedes garantizar el borrado real de los datos subidos. | Falta de control efectivo sobre los datos personales. |

**A. Informes médicos o historiales clínicos**

**Ejemplo:** un técnico o administrativo copia en ChatGPT un informe para "resumirlo" o "traducirlo".
Contiene: nombre, diagnóstico, historial médico, medicación, número de historia clínica.

**Riesgo:**

- ChatGPT almacena temporalmente el texto.
- El dato de salud es **categoría especial (art. 9 RGPD)**: su tratamiento requiere garantías reforzadas y consentimiento explícito.
- Posible infracción grave → sanciones de hasta **20 millones € o el 4 % de la facturación**.
- Además, violación del **secreto médico**.

**Medidas correctivas:**

- Prohibir subir datos de salud a herramientas no certificadas.
- Usar versiones on-premise o Azure OpenAI bajo control sanitario (HDS, ISO 27799).

**B. Escrituras notariales o contratos de compraventa**

**Ejemplo:** un empleado sube una escritura para "extraer nombres de partes y fechas" o redactar un resumen jurídico.
Contiene: nombres, DNI, direcciones, valores económicos, firmas.

**Riesgo:**

- Transferencia de datos identificativos y patrimoniales a EE. UU.

- Posible **quiebra del secreto notarial o de la confidencialidad contractual**.
- Pérdida de validez del documento por incumplir la cadena de custodia digital.
- Exposición de datos de terceros (comprador/vendedor).

**Medidas correctivas:**

- Usar IA local o Copilot con datos almacenados en SharePoint protegido.
- Sustituir datos reales por seudónimos en pruebas.

**C. Acuerdos empresariales o NDAs**

**Ejemplo:** un directivo pide a ChatGPT "resumir este acuerdo de confidencialidad con nuestro proveedor alemán".
Contiene: cláusulas estratégicas, precios, procesos internos.

**Riesgo:**

- Fuga de secretos comerciales (art. 2 Ley 1/2019 de Secretos Empresariales).
- Posible incumplimiento del propio NDA al divulgar información a terceros (OpenAI).
- Pérdida de confianza de socios o clientes.

**Medidas correctivas:**

- Implementar política interna: "ningún documento contractual se introduce en herramientas no aprobadas".
- Usar Copilot o Azure OpenAI (controlado, sin entrenamiento externo).

**D. Documentos judiciales o denuncias**

**Ejemplo:** un abogado o gestor copia en ChatGPT el texto de una sentencia o demanda para "resumir el caso".
Contiene: nombres, direcciones, antecedentes, número de procedimiento, delitos.

**Riesgo:**

- Violación del secreto profesional y de la confidencialidad judicial (art. 301 CP).
- Posible identificación indirecta de las partes o testigos.
- Transferencia internacional no autorizada de datos judiciales.

**Consecuencia:**

- Infracción grave del RGPD y del Código Deontológico.
- Sanciones y apertura de expediente en el Colegio Profesional.

**Medidas correctivas:**

- Prohibir subir documentos judiciales a IA pública.
- Usar herramientas aprobadas por el Consejo General del Poder Judicial o entornos seguros internos.

---

### 🔽 Evaluación del impacto (resumen DPIA)

| Escenario | Tipo de dato | Riesgo RGPD | Nivel | Mitigación necesaria |
|---|---|---|---|---|
| Subir informe médico | Datos de salud | Art. 9 RGPD | 🔴 Alto | Prohibir uso; anonimizar; IA certificada sanitaria |
| Subir escritura notarial | Identificativos y patrimoniales | Art. 6, 32 RGPD | 🔴 Alto | Anonimizar, entorno seguro |
| Subir NDA o acuerdo comercial | Datos confidenciales | Art. 5 RGPD | 🟠 Medio-alto | Política interna de uso y cifrado |
| Subir documentos judiciales | Datos sensibles / penales | Art. 10 RGPD | 🔴 Alto | Solo en entornos certificados, IA on-premise |

José Fuentes

CIO