



GUÍA

10 Tendencias en Compliance

que todos los responsables legales de cumplimiento deberían saber

2025

1 Endurecimiento normativo y evolución del RGPD



Revisión del RGPD

Se esperan revisiones puntuales del **RGPD** por la **Comisión Europea**. Algunas obligaciones se relajarán, pero, por el contrario, se prevé una **mayor presión inspectora**.

Aumento de sanciones y resoluciones ejemplarizantes

Por parte de **autoridades** como las de control y protección de datos (**AEPD, CNIL y Garante italiano**).

Transparencia algorítmica

Más exigencias sobre **decisiones automatizadas** y **explicabilidad** (art. 22 RGPD), en conexión con el **Reglamento de IA (RIA)**.

2 Integración del Reglamento de IA y Privacidad



Obligaciones de evaluación de impacto conjunta (IA + protección de datos)

Ya no basta una **EIPD**, ahora deberíamos ser capaces de integrarla en un **único documento** cuando utilicemos sistema de **alto riesgo IA** (ej. scoring de empleados, evaluación de estudiantes, selección automatizada de personal, IA médica, etc.).

Gobernanza ética de IA

Marcos que integren **compliance, privacidad, ciberseguridad y RSC**.

Superposición regulatoria

Coordinación entre el **RGPD, RIA, DSA, DMA, NIS2 y normas sectoriales** (sanidad, finanzas, laboral, etc.).



3 Gobierno del dato: eje estratégico y regulatorio



El dato deja de ser solo un activo: pasa a ser un **riesgo jurídico y reputacional** si no se gobierna bien.

Cohesión entre normativas: **RGPD, ENS, ISO 27001, RIA, ESG, sectoriales (sanitario, financiero...)**.

Catálogos de datos y **Políticas de clasificación y conservación.**

Calidad, integridad y trazabilidad de los datos. Identificación de **responsables de dato ("data owners")**, controles de acceso y reglas de uso.

4 Auditorías, accountability y prueba del cumplimiento



Auditorías

Mayor demanda de auditorías **internas** y **externas**.

Dashboards

Implementación de **dashboards de cumplimiento** (visión en tiempo real) y **registros automatizados**. Permite tomar decisiones rápidas.

Superposición regulatoria

Énfasis en la **trazabilidad** y **prueba documental** del cumplimiento ("demuestra que cumples").



5 Traslado contractual del riesgo a proveedores y socios



Cláusulas

Más **robustas** sobre tratamiento de datos por **encargados** y **subencargados**.

Exigencias

En **transferencias internacionales** (medidas adicionales, evaluaciones TIA).

Revisión

Profunda de **contratos** para cubrir usos de **IA**, **datos sintéticos**, **entrenamiento de modelos**, etc.

6 Diligencia debida en la cadena de suministro



Cláusulas anticorrupción, ant blanqueo y de respeto a los derechos humanos

Se **extienden** los requerimientos contractuales de compliance a toda la cadena.

Programa de compliance activo

O al menos **adherirse** al programa del cliente principal.

Declaraciones responsables y due diligence

Autodeclaraciones firmadas + derecho a auditar por parte de la matriz o cliente.



7 Datos sensibles y nuevos tratamientos de alto riesgo



Datos sensibles y nuevos tratamientos de alto riesgo

Datos biométricos, genéticos y de salud, especialmente con IA, Apps y wearables.

Telemedicina, diagnóstico y recomendación de tratamientos IA

Neuroderechos bajo la lupa por riesgos éticos y legales.

Nuevas exigencias

Sobre geolocalización, control biométrico y videovigilancia con IA.

8 Compliance como cultura organizativa



Integración de compliance

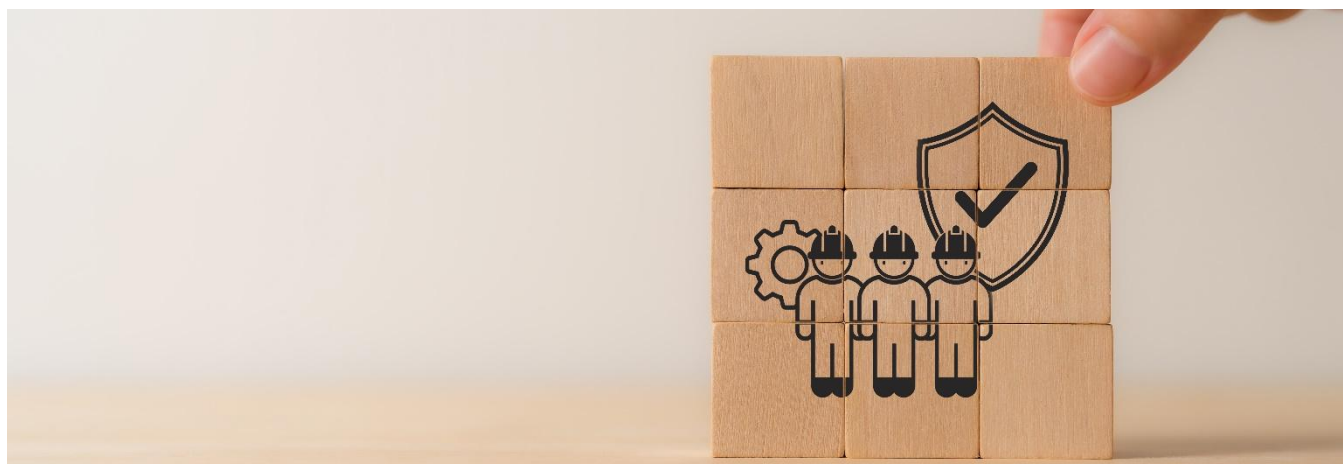
De privacidad, penal, laboral, medioambiental y de IA en un **sistema único**. **Cumplimiento transversal** no estanco.

Mayor implicación

Del **Consejo de Administración** y **directivos** en cultura de cumplimiento ("tone from the top").

Certificaciones

De **compliance** y **protección de datos** como herramienta competitiva (ej. UNE 19601, ISO 27001, Esquema Nacional de Seguridad).



9 Nuevos riesgos por el uso de IA generativa



LLMs (Large Language Model)

Uso de **LLMs** en **entornos empresariales** (tratamiento de datos personales, confidenciales, sujeto a derechos PI y secretos de empresa en prompts).

Riesgos legales, éticos y de seguridad

Por parte de **autoridades AEPD, CNIL y Garante italiano, AESIA**, etc.

Políticas y formación

Sobre el **uso responsable** de IA en RRHH, marketing, jurídico, etc.

10 Comunicación, concienciación y formación



DPO y CO

Se refuerzan los roles del DPO y del Compliance Officer como formadores transversales, agentes de cambio cultural y referentes internos en ética digital.

Campañas internas

Creación de campañas internas de **cumplimiento, privacidad y ética de datos** adaptadas a perfiles (ej. ventas, IT, RRHH). El "formato power point + política PDF" ya no funciona.

Formaciones

Formaciones sobre **DSA, DMA, IA, NIS2, privacidad y ESG**, cada vez más demandadas en planes de compliance global.





CECA MAGÁN

ABOGADOS

#EstiloCeca



Contacto

info@cecamagan.com
www.cecamagan.com