Guia de compliment d'IA 2026

Guia de compliment de la IA per a empreses i particulars (2026): AI Act, DSA i RGPD

> **Què és això.** Un dossier pràctic i verificat sobre el que les autoritats europees i espanyoles exigiran a qualsevol que faci servir intel·ligència artificial, tingui un lloc web o tracti dades. Està pensat perquè un empresari, un autònom o un particular sàpiga què li aplica, què miraran amb lupa els reguladors, on hi ha les trampes i com preparar-se sense gastar de més ni espantar-se de menys.
>
> **Avís.** Això és informació rigorosa, no assessorament jurídic individual. El marc legal del 2026 és en moviment (ho assenyalem on toca). Tancament d'aquesta edició: juny del 2026.

---

1. TL;DR: això em afecta?

Resposta curta: **gairebé segur que sí, però probablement menys del que tems i d'una manera diferent de la que creus.**

- **Fas servir IA a la teva empresa** (un chatbot, una eina que redacta, que puntua currículums, que genera imatges)? T'aplica el **Reglament europeu d'IA (AI Act)**, gairebé sempre en la seva versió més lleugera, i el **RGPD** si aquella IA toca dades personals.
- **Tens un lloc web o una aplicació on altres publiquen** (comentaris, ressenyes, un mercat en línia, un fòrum)? T'aplica el **Reglament de Serveis Digitals (DSA)**, normalment només en les seves obligacions bàsiques.
- **Ets autònom o professional i crees contingut amb IA** (vídeos, veus, imatges)? T'apliquen les **obligacions de transparència** (revelar que és contingut sintètic). En **ús purament personal i no professional**, l'AI Act no t'imposa aquelles obligacions de "responsable del desplegament", però continuen vigents les prohibicions i altres normes (drets d'autor, honor, protecció de dades).

Les tres normes conviuen i es complementen. No tries una: t'apliquen les que corresponguin alhora. La resta del dossier és el mapa per saber quines i què fer.

---

2. El marc en una pàgina

Norma	Què regula	A qui apunta sobretot
AI Act (Reglament UE 2024/1689)	L'**ús i la comercialització de sistemes d'IA**, per nivells de risc	Qui fabrica IA (proveïdor) i qui la fa servir professionalment (responsable del desplegament)
DSA (Reglament UE 2022/2065)	Els **serveis digitals intermediaris** i la moderació de continguts de tercers	Allotjaments, mercats en línia, plataformes, cercadors
RGPD (Reglament UE 2016/679)	El **tractament de dades personals** (també quan ho fa una IA)	Qualsevol que tracti dades de persones

Idea clau: l'**AI Act** mira *què fa el sistema d'IA*; el **RGPD** mira *quines dades personals toca*; el **DSA** mira *què passa amb el contingut que pengen tercers al teu servei*. Un mateix projecte pot activar les tres normes.

---

3. La línia de temps (i el termini que es va moure)

L'AI Act s'aplica de manera **escalonada** (article 113). El que ja és obligatori i exigible:

Data	Què entra en joc	Estat
1 ago 2024	Entrada en vigor	Sense obligacions encara
2 feb 2025	**Pràctiques prohibides (art. 5) + alfabetització en IA (art. 4)**	✅ En vigor i exigible
2 ago 2025	Obligacions dels **models de propòsit general (GPAI)**, governança i **règim sancionador (arts. 99-100)**	✅ En vigor
2 ago 2026	**Alt risc de l'Annex III** + **transparència (art. 50)** + avaluacions d'impacte + entorns de prova	Data per defecte
2 ago 2027	Alt risc integrat en **productes regulats (Annex I)**	Data per defecte

> 🔴 **Caixa: el termini que es va moure**
>
> Aquí hi ha el matís que gairebé ningú explica bé. La Comissió Europea va proposar el novembre del 2025 el **"Digital Omnibus"** (COM(2025)836), un paquet que **proposa retardar l'entrada en vigor del règim d'alt risc**:
>
> - **Annex III** (biometria, ocupació, educació, serveis essencials, etc.): del 2 ago 2026 a **finals del 2027** (les fonts apunten al 2 dic 2027).
> - **Annex I** (IA dins de productes regulats): del 2 ago 2027 a **2028** (al voltant del 2 ago 2028).
>
> Però atenció: a juny del 2026 això és una **proposta en tramitació legislativa** (procediment 2025/0359(COD)), **no dret vigent**: el text encara no s'ha adoptat de manera definitiva ni publicat al Diari Oficial de la UE, i les dates exactes poden canviar durant la negociació. L'Omnibus "mou el rellotge, no l'arquitectura": no canvia les obligacions de fons, només quan comencen.
>
> **Què fer amb això:** planifica de manera conservadora cap a l'agost del 2026, perquè el retard encara no és segur, però guanya marge sabent que probablement tindràs més temps del que diu el calendari per defecte. Verifica la data definitiva abans de prendre decisions importants. Font: Digital Omnibus, Comissió Europea.

El que realment és important per avui: **les prohibicions i l'obligació de formació ja estan en vigor des del febrer del 2025.** No són futur.

---

4. AI Act per nivells de risc

L'AI Act classifica els sistemes d'IA en quatre nivells. La teva primera tasca és saber en quin cau cada eina que fas servir.

🚫 Risc inacceptable (prohibit), art. 5

Vuit pràctiques prohibides des del febrer del 2025, sense possibilitat de mitigació. Les que afecten més les empreses:

- Manipulació subliminal o aprofitament de vulnerabilitats per alterar el comportament de manera perjudicial.
- **Puntuació social** (social scoring) de persones.
- **Reconeixement d'emocions a la feina i en centres educatius** (excepte per raons mèdiques o de seguretat).
- **Categorització biomètrica** per característiques sensibles (raça, religió, orientació, etc.).
- Creació de bases de dades de reconeixement facial per **scraping massiu** d'internet o càmeres.

Si alguna eina de la teva empresa fa alguna d'aquestes coses, no es "mitiga": es retira.

⚠️ Alt risc (Annex III + Annex I)

Sistemes en vuit àmbits sensibles: biometria, infraestructures crítiques, **educació**, **ocupació i RRHH** (cribatge de currículums, decisions de promoció), serveis essencials (inclosa la **puntuació creditícia**), aplicació de la llei, migració i justícia. Si en fabrices un, les obligacions són importants: gestió de riscos, governança de dades, documentació tècnica, registre de logs, supervisió humana, robustesa, avaluació de conformitat, **marcatge CE** i registre en una base de dades de la UE.

Si només el fas servir (ets "responsable del desplegament"), les teves obligacions són més acotades però reals: fer-lo servir segons les instruccions, **supervisió humana** designada, conservar **logs (mínim 6 mesos)**, **informar els representants dels treballadors** i, en certs casos, fer una **avaluació d'impacte en els drets fonamentals (FRIA, art. 27)**.

💬 Risc limitat (transparència), art. 50

El nivell on caurà la majoria de les pimes. Obligació principal: **avisar**.

- Un **chatbot** ha d'identificar-se com a IA ("estàs parlant amb un assistent automàtic").
- Qui **fabrica** un sistema que genera contingut sintètic ha de marcar-lo en format llegible per màquina (art. 50.2). Qui **publica un deepfake** ha de **revelar que ha estat generat o manipulat amb IA** (art. 50.4), amb matisos per a obres creatives, satíriques o artístiques.

Aquestes obligacions de transparència s'apliquen des de **l'agost del 2026**. Atenció: el retard del Digital Omnibus afecta el **règim d'alt risc** (capítol III), no aquestes obligacions de l'art. 50 (llevat d'una transició concreta per a sistemes generatius ja al mercat). Avançar-les és bona pràctica i sovint ja ho exigeix la normativa de consumidors.

✅ Risc mínim

Filtres antispam, videojocs, recomanadors trivials. Sense obligacions específiques de l'AI Act.

> **Models de propòsit general (GPAI):** si fas servir ChatGPT, Claude, Gemini o similars, *tu* no ets el seu proveïdor, de manera que les obligacions GPAI (documentació tècnica, resum de dades d'entrenament, política de drets d'autor i, per als més potents, red-teaming i informe d'incidents) recauen en l'empresa que els fabrica, no en tu. A tu t'afecta com a *deployer* del nivell que correspongui a l'ús.

---

5. DSA: tinc una “plataforma”? (i per què probablement no)

El DSA fa més por de la que hauria a les pimes. El que de debò importa:

- **Lloc web corporatiu sense contingut de tercers:** el DSA **no t’aplica**, perquè no ets un “servei intermediari” (el DSA només regula qui allotja o transmet contingut de tercers). Les teves obligacions vénen del RGPD i de la normativa de consumidors, no del DSA.
- **Lloc web amb comentaris o ressenyes:** et converteixes en “allotjament”. Obligacions bàsiques: **mecanisme de notificació i retirada de contingut il·lícit** (notice & action, art. 16) i **motivar** quan elimines alguna cosa (art. 17).
- **Mercat en línia o fòrum:** ets “plataforma en línia”, però aquí hi ha l’alleujament: l’**article 19 eximeix les microempreses i les petites empreses** (menys de 50 empleats i menys de 10 M€) de les obligacions més pesades (sistema formal de reclamacions, resolució extrajudicial, informes de transparència). **No t’eximeix** del notice & action ni de motivar les retirades.
- **Plataforma molt gran (VLOP):** des de 45 milions d’usuaris a la UE. Auditories, avaluació de riscos, supervisió directa de la Comissió. No és el teu cas si estàs llegint això.

Sancions: fins al **6% de la facturació mundial anual** (art. 74). Per a les grans plataformes (VLOP) les imposa la Comissió Europea; per a la resta de serveis intermediaris, les fixen les autoritats nacionals (art. 52), també fins a aquell 6%. El DSA s’aplica **plenament des del 17 de febrer del 2024**.

> **Dada que gairebé ningú explica:** a Espanya, l’autoritat del DSA és la **CNMC** (Coordinador de Serveis Digitals), però la Comissió Europea **va demandar Espanya davant el Tribunal de Justícia de la UE el maig del 2025** (IP/25/1081) perquè la CNMC encara **no té plenes potestats sancionadores**. El DSA és directament aplicable igualment, però el règim administratiu de multes a Espanya és pendent. Traducció: l’obligació existeix, el pal nacional encara s’està muntant.

No confonguis el DSA amb el RGPD (dades) ni amb el DMA (grans plataformes i competència): són normes diferents.

---

6. Qui vigila i què miraran amb lupa

Autoritats:

Autoritat	Àmbit
AI Office (Comissió Europea)	Models de propòsit general (GPAI); coordinació UE
AESIA (Agència Espanyola de Supervisió de la IA, la Corunya)	Pràctiques prohibides, alt risc general, transparència
AEPD	Dades personals, **biometria**, decisions automatitzades (art. 22 RGPD)
CNMC	DSA i dimensió competitiva dels algorismes

La AESIA existeix i és operativa (creada pel RD 729/2023), i ja va tancar el **primer entorn de proves regulatori d'IA de la UE**. La seva potestat sancionadora plena depèn de la futura **Llei orgànica espanyola de bon ús i governança de la IA**, que a juny del 2026 continua **en tramitació, no en vigor**.

Focus de fiscalització (el que miraran primer):

1. Pràctiques **prohibides** (puntuació social, biometria, manipulació). Ja sancionable.
2. **Transparència**: chatbots i deepfakes sense avisar.
3. Sistemes d'**alt risc sense conformitat** (RRHH, scoring) sense documentació ni supervisió humana.
4. **Intersecció amb el RGPD**: base legal, decisions automatitzades, avaluacions d'impacte.
5. **Reclamacions d'afectats**: sovint, la inspecció comença per una queixa.

---

7. Sancions: quant fa mal

AI Act (art. 99), xifres verificades:

Conducta	Règim general (l'import major)	Pimes (l'import menor)
Pràctiques prohibides (art. 5)	**35 M€ o 7%** de la facturació mundial	el menor dels dos
Incomplir altres obligacions	**15 M€ o 3%**	el menor dels dos
Donar informació incorrecta a les autoritats	**7,5 M€ o 1%**	el menor dels dos

Dos matisos importants i poc coneguts: el tram d'informació incorrecta és de l'**1%** (no 1,5%, com repeteixen algunes fonts), i per a **pimes i startups s'aplica l'import més baix** dels dos (al revés que per a les grans). Detall a l'article 99.

DSA: fins al **6%** de la facturació mundial anual (la Comissió Europea per a les grans plataformes; les autoritats nacionals per a la resta de serveis intermediaris).

RGPD: fins a **20 M€ o el 4%**. A Espanya, l'AEPD va resoldre el 2024 centenars de procediments sancionadors; la IA figura entre els seus reptes declarats.

---

8. Les trampes (errors típics que es sancionen)

Ordenades per gravetat regulatòria:

1. **IA en RRHH sense avaluació.** Cribar currículums o decidir ascensos amb IA és alt risc: exigeix base legal, avaluació d'impacte i supervisió. Fer-ho a cegues és triple infracció.
2. **Decisions automatitzades sense intervenció humana real** (art. 22 RGPD). La persona ha de poder entendre i anul·lar el sistema, no signar el que digui la màquina.
3. **Biometria sense base legal reforçada** (art. 9 RGPD). En l'àmbit laboral, a Espanya el consentiment del treballador no es considera vàlid per la relació de poder.
4. **Chatbot que no avisa que és IA** (art. 50).
5. **Fer servir una IA de tercers sense contracte d'encarregat de tractament (DPA) signat** abans de posar-hi dades personals. La responsabilitat recau en tu, no en el proveïdor.
6. **Scraping massiu de dades personals per a IA** sense test de ponderació. L'Opinió 28/2024 del Comitè Europeu de Protecció de Dades és clara: l'interès legítim no guanya automàticament.
7. **Deepfakes i contingut sintètic sense etiquetar.**
8. **No informar la plantilla** d'un ús d'IA que els afecta (art. 64 de l'Estatut dels Treballadors + arts. 13-14 RGPD).
9. **"IA-washing"**: vendre capacitats que el sistema no té (publicitat deslleial).
10. **Copiar la política d'IA d'una altra empresa.** Incompleix el principi de responsabilitat proactiva i agreuja la sanció si hi ha inspecció.

---

9. Bones vs. males pràctiques

Aspecte	Malament	Bé
Inventari d'IA	Informal, "ja sé el que faig servir"	Registre amb proveïdor, finalitat, dades i base legal per eina
Decisions automàtiques	Sense revisió humana possible	Persona designada que pot anul·lar + canal d'impugnació visible
Chatbot	Es presenta com a persona	"Soc un assistent d'IA" des del primer missatge
Contingut amb IA	Sense etiqueta	Etiqueta visible + marcatge tècnic en metadades
Proveïdor d'IA	API sense DPA signat	DPA signat abans de la primera crida amb dades personals
Formació	"Ja saben fer servir la IA"	Registre signat, proporcional al risc, actualitzat
Supervisió	"El sistema és molt bo"	Persona que entén i pot anul·lar; documentat
Incidents	Esperar la queixa del client	Protocol: detectar, avaluar, notificar a l'AEPD en 72 h

El fil conductor és el **principi de responsabilitat proactiva (accountability)**: no n'hi ha prou amb complir, cal **poder demostrar-ho i justificar-ho** davant l'autoritat amb documentació viva.

---

10. Com preparar la teva empresa: llista de verificació per fases

Bloc A. Inventari (fes-ho ja). Llista de tota eina d'IA que fas servir: proveïdor, per a què, quines dades toca, base legal i si té DPA signat.

Bloc B. Base legal i contractes (abans de tractar dades). Una base legal del RGPD (art. 6) per a cada tractament; **DPA signat** amb cada proveïdor d'IA (OpenAI, Anthropic i Google ho ofereixen); comprova el mecanisme de transferència internacional (marc UE-EUA o clàusules contractuals tipus).

Bloc C. Avaluacions d'impacte (abans de desplegar). Fes una **DPIA** si hi ha perfilació, categories especials o decisions automatitzades significatives. Afegeix una **FRIA** (art. 27) si ets un **organisme públic**, una **entitat privada que presta serveis públics**, o fas servir IA d'alt risc per **avaluar la solvència o la puntuació creditícia** de persones o per a **assegurances de vida i salut** (Annex III.5).

Bloc D. Transparència (abans de l'agost del 2026). Avís de "estàs parlant amb IA" en chatbots; etiqueta del contingut generat amb IA; mecanisme per impugnar decisions automatitzades.

Bloc E. Formació (art. 4, ja en vigor). Formació documentada i signada per empleat, proporcional al risc del seu lloc. No exigeix certificació oficial, però sí deixar constància.

Bloc F. Supervisió i registres (continu). Logs de decisions, supervisió humana real documentada, revisió anual de l'inventari i protocol d'incidents (notificació a l'AEPD en 72 h si hi ha bretxa).

---

11. Per a particulars i autònoms

No només les empreses estan al punt de mira:

- **Creadors de contingut amb IA (a títol professional):** l'obligació de **revelar el contingut sintètic** (art. 50) t'arriba quan publiques deepfakes, veus o imatges generades en el marc d'una activitat professional. L'ús purament personal i domèstic queda en gran mesura fora de l'AI Act, tot i que no d'altres normes.
- **Deepfakes sense consentiment:** a més de la transparència, certs usos (sexuals, suplantació) estan prohibits o tipificats. La futura llei espanyola reforça això.
- **Drets d'autor:** generar amb IA no et dona automàticament la titularitat, i fer servir obres alienes per crear pot tenir conseqüències.
- **Autònoms que fan servir IA amb dades de clients:** t'apliquen les mateixes regles del RGPD i del DPA amb el proveïdor que a una empresa.

---

12. Glossari ràpid

- **Proveïdor:** qui fabrica o comercialitza el sistema d'IA.
- **Responsable del desplegament (deployer):** qui fa servir el sistema d'IA en la seva activitat. La majoria de les empreses.
- **GPAI:** model d'IA de propòsit general (els grans models generatius).
- **DPIA:** avaluació d'impacte en protecció de dades (RGPD, art. 35).
- **FRIA:** avaluació d'impacte en els drets fonamentals (AI Act, art. 27).
- **DPA:** contracte d'encarregat de tractament (RGPD, art. 28).
- **VLOP:** plataforma en línia molt gran (DSA).
- **Accountability:** responsabilitat proactiva, poder demostrar el compliment.

Fonts

> Per als números d'article i les sancions, la font que mana és sempre el **text oficial a EUR-Lex / DOUE**. Les pàgines d'anàlisi (com artificialintelligenceact.eu) s'inclouen només com a suport divulgatiu, no com a font normativa.

Primàries (AI Act) - Reglament (UE) 2024/1689, text consolidat (inclou arts. 5, 27, 50, 99 i 113): https://eur-lex.europa.eu/eli/reg/2024/1689/oj?locale=es - Calendari d'aplicació (AI Act Service Desk, Comissió Europea): https://ai-act-service-desk.ec.europa.eu/en/ai-act/timeline/timeline-implementation-eu-ai-act - Digital Omnibus, proposta COM(2025)836 (Comissió Europea): https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal

Suport divulgatiu (no oficial) - AI Act Explorer (anàlisi per articles, arts. 27/50/99): https://artificialintelligenceact.eu/es/

DSA - Reglament (UE) 2022/2065, text en espanyol: https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:32022R2065 - Política DSA (Comissió Europea): https://digital-strategy.ec.europa.eu/en/policies/digital-services-act - Llista de VLOP/VLOSE: https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops - CNMC, Coordinador de Serveis Digitals: https://www.cnmc.es/en/sectores-que-regulamos/servicios-digitales-dsa - Demanda de la Comissió a Espanya (IP/25/1081): https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1081

Espanya / RGPD - AESIA (web oficial): https://aesia.digital.gob.es/es - RD 729/2023 (estatut AESIA): https://www.boe.es/buscar/doc.php?id=BOE-A-2023-18911 - AEPD, guia d'adequació al RGPD de tractaments amb IA: https://www.aepd.es/guias/adecuacion-rgpd-ia.pdf - AEPD, orientacions sobre IA agèntica: https://www.aepd.es/guias/orientaciones-ia-agentica.pdf - EDPB, Opinió 28/2024 (models d'IA i protecció de dades): https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf

Casos - Multa del Garante italià a OpenAI (15 M€, desembre del 2024). Font primària: comunicat del *Garante per la protezione dei dati personali* (https://www.garanteprivacy.it). Cobertura de premsa (secundària): https://www.euronews.com/next/2024/12/20/italys-privacy-watchdog-fines-openai-15-million-after-probe-into-chatgpt-data-collection

---

Edició tancada al juny del 2026. El marc normatiu és en evolució (en particular, el Digital Omnibus i la llei orgànica espanyola d'IA). Verifica les dates i l'estat de tramitació abans de prendre decisions amb impacte legal. Informació general, no assessorament jurídic individual.