ESEMPIO SINTETICO — NON È LA VALUTAZIONE DI UN CLIENTE

Europe Cyber-Safe

Passaporto IA per deployer — dichiarazione di autovalutazione

Organizzazione	Agenzia Creativa Esempio S.r.l. (15 dipendenti)	**Riferimento**	SAMPLE-0002
Compilata il	2026-10-30	**Compilata da**	director@example.com
Questionario	v1.1-EU-it (EU, it) · `55e04c6dac584fdd`		

> **Autovalutazione compilata dall'organizzazione. Le risposte non sono state esaminate da Europe Cyber-Safe né da altri. Il presente report non costituisce consulenza legale.**

Il report descrive la situazione alla sola data di compilazione.

Valutazione per area

Ogni area è valutata in base alle risposte date: rosso se almeno una risposta attiva il rosso, altrimenti giallo se almeno una risposta è gialla o mancante, altrimenti verde. Non viene prodotto alcun punteggio complessivo.

Area	Valutazione
D1 Inventario dell'IA	ROSSO
D2 Protezione dei dati	ROSSO
D3 Governance e policy	ROSSO
D4 Sorveglianza umana	GIALLO
D5 Gestione dei fornitori	GIALLO
D6 Risposta agli incidenti di IA	GIALLO

Azioni

Prima le aree in rosso, poi le azioni più rapide.

#	Area	Azione	Impegno
1	D1	Designi un responsabile dell'inventario e lo indichi nella policy sull'uso dell'IA.	un'ora
2	D1	Inserisca un controllo trimestrale dell'inventario nel calendario del responsabile designato.	un'ora
3	D2	Aggiunga all'informativa privacy una sezione sull'uso dell'IA che indichi le finalità e le categorie di fornitori; la pubblichi e ne informi il personale.	un'ora
4	D2	Diffonda a tutto il personale l'elenco dei dati da non inserire e lo affigga dove gli strumenti vengono utilizzati.	un'ora

ESEMPIO SINTETICO — NON È LA VALUTAZIONE DI UN CLIENTE

5	D2	Registri per ogni strumento l'ubicazione dei dati e il meccanismo di trasferimento sulla base della documentazione del fornitore; se i dati escono dal SEE, accerti il meccanismo (una decisione di adeguatezza, oppure le clausole contrattuali tipo dell'UE con una valutazione d'impatto del trasferimento).	un'ora
6	D2	Per ogni strumento, individui il comando di cancellazione o l'impegno contrattuale alla cancellazione; se non esiste né l'uno né l'altro e sono coinvolti dati personali, dismetta lo strumento.	un'ora
7	D3	Designi un responsabile delle decisioni sull'IA e metta per iscritto le tre domande che pone prima di approvare uno strumento (quali dati, quali condizioni, chi controlla i risultati).	un'ora
8	D1	Completi l'inventario dell'IA utilizzando il modello; chieda a ogni responsabile di team quali strumenti usano lui e il suo team, comprese le estensioni del browser e le app per smartphone.	un giorno
9	D1	Smetta subito di inserire dati personali in strumenti con condizioni per consumatori o sconosciute. Sposti tale uso su un piano business con un accordo di nomina a responsabile del trattamento, oppure vi rinunci.	un giorno
10	D1	Controlli le impostazioni IA di ciascun prodotto principale (trascrizione delle riunioni, riepiloghi, completamento automatico) e le aggiunga all'inventario; decida quali disattivare.	un giorno
11	D2	Applichi il modello di valutazione preliminare DPIA a ogni strumento che tratta dati personali; effettui una DPIA completa quando la valutazione preliminare lo indica.	un giorno
12	D3	Adotti il modello di policy sull'uso dell'IA (due pagine), la faccia firmare al titolare, la diffonda a tutto il personale e registri chi l'ha vista.	un giorno
13	D3	Organizzi per tutto il personale una sessione di sensibilizzazione sull'IA di un'ora (presentazione modello) e conservi il registro presenze.	un giorno
14	D3	Controlli i cinque principali contratti con i clienti e le indicazioni sull'IA del suo ordine o della sua associazione professionale, cercando clausole su riservatezza e IA; registri il risultato.	un giorno
15	D4	Informi il personale sui tipi di errore dell'IA usando la nota di una pagina; includa un esempio reale tratto dal suo settore.	un'ora
16	D4	Concordi una convenzione semplice (una nota a piè di pagina, un campo, una cartella) per contrassegnare i risultati rilevanti prodotti con l'aiuto dell'IA.	un'ora
17	D5	Controlli la dichiarazione sull'uso dei dati di ciascun fornitore; attivi l'opt-out o passi a un piano che escluda l'addestramento; registri il risultato nell'inventario.	un'ora
18	D5	Raccolga per ciascun fornitore la pagina sulla sicurezza o le prove del trust center e le conservi insieme all'inventario.	un'ora
19	D5	Designi chi riceve le comunicazioni dei fornitori; scriva una nota di uscita di un paragrafo per ogni strumento critico (come esportare, come interrompere).	un'ora
20	D6	Aggiunga gli incidenti di IA alla procedura esistente per incidenti o reclami, con tre esempi e un referente designato.	un'ora

ESEMPIO SINTETICO — NON È LA VALUTAZIONE DI UN CLIENTE

21	D6	Designi il responsabile delle decisioni sulle violazioni dei dati e tenga a portata di mano il modulo di notifica delle violazioni della sua autorità di protezione dei dati e un modello di registro delle violazioni (l'art. 33 GDPR richiede di documentare ogni violazione).	un'ora
22	D6	Attivi i log delle attività negli strumenti con piano business; dove non è possibile, tenga un semplice registro condiviso per gli usi che coinvolgono dati personali o riservati.	un'ora
23	D4	Introduca una fase di controllo affidata a una persona designata per tutti i risultati dell'IA destinati ai clienti o che incidono sugli archivi; la renda parte della normale procedura di approvazione.	un giorno
24	D5	Ottenga le condizioni business o l'accordo di nomina a responsabile del trattamento di ciascun fornitore; se non esistono, smetta di inviare dati personali a quel fornitore.	un giorno
25	D5	Sposti gli strumenti di IA su account gestiti dall'azienda con MFA; li aggiunga alla checklist di uscita del personale.	un giorno
26	D6	Per ogni strumento critico, provi una volta l'esportazione e annoti come disattivare l'accesso; conservi i documenti essenziali al di fuori dello strumento.	un giorno
27	D4	Documenti la fase di controllo, la base giuridica e i controlli sui bias effettuati; stabilisca se l'uso rientra nell'Allegato III dell'AI Act e pianifichi gli obblighi per i deployer applicabili dal 2 dicembre 2027.	una settimana

Risposte date

D1 Inventario dell'IA — ROSSO

ID	Domanda	Risposta	Livello
D1-1	Ha censito tutti gli strumenti di IA utilizzati in azienda, compresi gli account gratuiti che il personale usa sui propri dispositivi o con le proprie credenziali?	Nessun elenco	rosso
D1-2	Qualche strumento dell'inventario riceve dati personali di clienti, pazienti, committenti o dipendenti?	Sì - in almeno uno strumento con condizioni per consumatori, o le cui condizioni sono sconosciute	rosso
D1-3	C'è una persona designata responsabile di mantenere aggiornato l'inventario e di approvare i nuovi strumenti?	No	giallo
D1-4	Le funzionalità di IA integrate nei prodotti che già utilizza (e-mail, CRM, contabilità, browser, strumenti per riunioni, telefoni) sono incluse nell'inventario?	Non so	giallo
D1-5	Quando è stato confrontato per l'ultima volta l'inventario con gli strumenti effettivamente usati dal personale?	Mai, oppure non esiste un inventario	rosso

ESEMPIO SINTETICO — NON È LA VALUTAZIONE DI UN CLIENTE

D2 Protezione dei dati — ROSSO

ID	Domanda	Risposta	Livello
D2-1	La sua informativa privacy comunica a clienti e personale che vengono usati strumenti di IA, per quali finalità e con quali fornitori?	No	rosso
D2-2	Per gli strumenti che trattano dati personali, ha effettuato una valutazione d'impatto sulla protezione dei dati (DPIA) o una valutazione preliminare documentata che ha concluso che non è necessaria?	No	rosso
D2-3	Il personale dispone di un elenco scritto di ciò che non deve mai essere inserito in uno strumento di IA (ad esempio dati dei pazienti, numeri di carte di pagamento, identificativi dei clienti, password)?	Comunicato a voce, nulla di scritto	giallo
D2-4	Sa dove ciascun fornitore conserva e tratta i suoi dati e se questi escono dallo Spazio economico europeo (SEE)?	Per alcuni strumenti	giallo
D2-5	Può cancellare, o far cancellare dal fornitore, i dati conservati in ciascuno strumento di IA quando smette di usarlo o quando un interessato lo richiede?	Non so	giallo

D3 Governance e policy — ROSSO

ID	Domanda	Risposta	Livello
D3-1	Esiste una policy scritta sull'uso dell'IA, che il personale ha visto e che indica che cosa è consentito e che cosa no?	Redatta ma non diffusa	giallo
D3-2	Chi decide se un nuovo strumento o una nuova funzionalità di IA può essere usato per finalità aziendali?	La direzione, in modo informale	giallo
D3-3	La policy elenca gli usi vietati - ad esempio prendere decisioni sulle persone senza controllo umano, o generare contenuti presentati come scritti da una persona quando ciò sarebbe ingannevole?	Sì	verde
D3-4	Tutto il personale che usa strumenti di IA ha ricevuto negli ultimi 12 mesi una formazione di sensibilizzazione sui limiti all'inserimento dei dati, sui tipi di errore e sulla policy?	Parte del personale	giallo

D3-5	I contratti con i clienti o committenti, le regole professionali o l'autorità di vigilanza del suo settore limitano il modo in cui può usare l'IA con le loro informazioni, e tali limiti vengono rispettati?	Esistono limitazioni e non siamo sicuri di rispettarle	rosso

D4 Sorveglianza umana — GIALLO

ID	Domanda	Risposta	Livello
D4-1	I risultati dell'IA vengono controllati da una persona competente prima di arrivare a un cliente, in un archivio o in una decisione che riguarda una persona?	Di solito	giallo
D4-2	Il personale che usa strumenti di IA conosce i tipi di errore che questi strumenti commettono - fatti e citazioni inventati, informazioni non aggiornate, errori presentati con sicurezza, distorsioni (bias)?	Parte del personale	giallo
D4-3	È possibile stabilire a posteriori quali documenti, e-mail o registrazioni sono stati prodotti con l'aiuto dell'IA?	A volte	giallo
D4-4	Una persona designata risponde di una decisione presa con l'aiuto dell'IA esattamente come di una decisione umana?	Sì	verde
D4-5	Usa l'IA per decisioni su selezione del personale, credito, prezzi, idoneità, prestazioni o altre decisioni che riguardano singole persone?	Sì, con un controllo umano effettivo e una base documentata	giallo

D5 Gestione dei fornitori — GIALLO

ID	Domanda	Risposta	Livello
D5-1	Per ogni fornitore di IA che tratta i suoi dati, dispone di un contratto o di condizioni che includono un accordo di nomina a responsabile del trattamento (art. 28 GDPR)?	Per alcuni	giallo
D5-2	Sa se ciascun fornitore usa i suoi input per addestrare o migliorare i propri modelli, e ha esercitato l'opt-out dove possibile?	Non noto	giallo
D5-3	Ha visionato prove di sicurezza indipendenti per ciascun fornitore (ad esempio certificazione ISO/IEC 27001, report SOC 2, uno schema nazionale di riferimento, sintesi di un penetration test)?	No	giallo

D5-4	L'accesso a ciascuno strumento di IA è controllato con account aziendali, autenticazione a più fattori e disattivazione quando il personale lascia l'azienda?	In parte	giallo
D5-5	Se un fornitore modificasse le proprie condizioni, subisse una violazione o cessasse l'attività, lo verrebbe a sapere, e ha un modo per smettere rapidamente di usarlo?	No	giallo

D6 Risposta agli incidenti di IA — GIALLO

ID	Domanda	Risposta	Livello
D6-1	Il personale sa che cosa costituisce un incidente di IA (ad esempio dati personali incollati in uno strumento, un risultato dannoso o errato preso per buono, una notifica di violazione da parte di un fornitore) e come segnalarlo?	In modo informale	giallo
D6-2	Sarebbe in grado di rispettare il termine di 72 ore previsto dal GDPR per la notifica alla sua autorità di protezione dei dati se dati personali fossero esposti tramite uno strumento di IA?	Non so	giallo
D6-3	Negli ultimi 12 mesi ha avuto un incidente di IA, o ha svolto un'esercitazione a tavolino (tabletop) su un incidente di IA?	Sì	verde
D6-4	Conserva registrazioni sufficienti (chi ha usato quale strumento, quando, per che cosa) per indagare a posteriori su un incidente di IA?	In parte	giallo
D6-5	Potrebbe smettere di usare uno specifico strumento di IA entro un giorno lavorativo, se fosse compromesso, senza perdere documenti aziendali essenziali?	In parte	giallo

Indicazioni di riferimento

- AI Act, art. 26 (obblighi dei deployer dei sistemi di IA ad alto rischio) e Allegato III; per gli usi di cui all'Allegato III tali obblighi si applicano dal 2 dicembre 2027 ai sensi del Regolamento (UE) 2026/1744
- Regolamento sull'intelligenza artificiale (AI Act, Regolamento (UE) 2024/1689), art. 4 (alfabetizzazione in materia di IA), applicabile dal 2 febbraio 2025 e modificato dal Regolamento (UE) 2026/1744: fornitori e deployer devono adottare misure per favorire l'alfabetizzazione in materia di IA del personale e delle altre persone che utilizzano sistemi di IA per loro conto
- AI Act, art. 50 (trasparenza: informare le persone che stanno interagendo con un sistema di IA; rendere noti i contenuti generati o manipolati dall'IA), applicabile dal 2 agosto 2026
- ISO/IEC 27001:2022; schemi nazionali di riferimento (ad esempio Framework Nazionale per la Cybersecurity e la Data Protection / indicazioni ACN, BSI IT-Grundschutz, CyberFundamentals); autenticazione a più fattori e controlli su ingressi e uscite del personale
- Commissione europea, AI literacy - Questions and Answers (2025)
- Parere 28/2024 dell'EDPB su taluni aspetti della protezione dei dati relativi al trattamento dei dati personali nel contesto dei modelli di IA (dic. 2024); indicazioni sull'IA della sua autorità nazionale di protezione dei dati (ad esempio il Garante per la

protezione dei dati personali)
- Normativa nazionale sul lavoro e norme sulle rappresentanze dei lavoratori in materia di controllo e di IA nella selezione e nella gestione del personale; AI Act, Allegato III, punto 4 (gli usi in ambito occupazionale sono ad alto rischio)
- ENISA, Multilayer Framework for Good Cybersecurity Practices for AI (2023); NCSC/CISA e agenzie partner, Guidelines for secure AI system development (nov. 2023)
- Direttive UE sulla parità di trattamento (2000/43/CE, 2000/78/CE, 2006/54/CE) e normativa nazionale antidiscriminazione (discriminazione diretta e indiretta)
- GDPR, art. 22 (processo decisionale automatizzato relativo alle persone fisiche); linee guida del Gruppo di lavoro Articolo 29 sul processo decisionale automatizzato e sulla profilazione (WP251 rev.01)
- GDPR, artt. 33-34 (notifica all'autorità di controllo entro 72 ore quando sussiste un rischio per le persone; documentazione di ogni violazione); Linee guida 9/2022 dell'EDPB sulla notifica delle violazioni dei dati personali
- GDPR, art. 35 (valutazione d'impatto sulla protezione dei dati); linee guida in materia di DPIA del Gruppo di lavoro Articolo 29 (WP248 rev.01, fatte proprie dall'EDPB); elenco dei trattamenti soggetti a DPIA della sua autorità nazionale
- GDPR, Capo V (artt. 44-49): decisioni di adeguatezza; clausole contrattuali tipo (decisione della Commissione 2021/914); Raccomandazioni 01/2020 dell'EDPB sulle misure supplementari
- Regolamento generale sulla protezione dei dati (GDPR), artt. 12-14 (informazioni da fornire agli interessati)
- Indicazioni ENISA sulla gestione degli incidenti; indicazioni sulle segnalazioni del CSIRT nazionale; direttiva NIS2, art. 23, obblighi di segnalazione (per i soggetti che rientrano nell'ambito di applicazione)
- ISO/IEC 42001:2023, sistemi di gestione dell'IA (ruoli, valutazione d'impatto, ciclo di vita, fornitori)
- ISO/IEC 27001:2022 Allegato A 8.15 (logging) e 8.16 (attività di monitoraggio)
- NIST AI Risk Management Framework 1.0 (Govern, Map, Measure, Manage) e il relativo Generative AI Profile (NIST AI 600-1)
- OWASP Top 10 for LLM Applications 2025 (prompt injection, divulgazione di informazioni sensibili, catena di fornitura)
- Indicazioni ENISA sulla sicurezza della catena di approvvigionamento ICT; direttiva NIS2, art. 21(2)(d), sicurezza della catena di approvvigionamento (per i soggetti che rientrano nell'ambito di applicazione)

I riferimenti alle indicazioni sono fonti pubbliche elencate per comodità; ne controlli la versione aggiornata prima di farvi affidamento. La presente dichiarazione non costituisce consulenza legale né una certificazione.