AI generativa e implementazione delle normative che hanno impatti sull'ICT

Giancarlo Butti

Ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano.
Referente del Regolamento DORA e Inclusion del Comitato Scientifico del CLUSIT.
Si occupa di ICT, organizzazione e normativa dai primi anni 80. Auditor, security manager ed esperto di privacy. Affianca all'attività professionale quella di divulgatore, tramite articoli, libri, white paper, manuali tecnici, corsi, seminari, convegni. Oltre 170 corsi e seminari presso ISACA/AIEA, ORACLE/CLUSIT, ITER, INFORMA BANCA, CONVENIA, CETIF, IKN, UNIVERSITA DI MILANO, CA FOSCARI, CEFRIEL, ABI…
Già docente del percorso professionalizzante ABI - Privacy Expert e Data Protection Officer e master presso diversi atenei.
Ha all'attivo oltre 800 articoli e collaborazioni con oltre 40 testate.
Ha pubblicato 30 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 31 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT. Socio e già proboviro di ISACA/AIEA è socio del CLUSIT, di DFA, di ACFE e del BCI.
Partecipa a numerosi gruppi di lavoro ed è fra i coordinatori di www.blog.europrivacy.info .
Ha inoltre acquisito le certificazioni/qualificazioni LA BS7799, LA ISO/IEC 27001:2005/2013/2022, LA ISO 22301, LA ISO 20000-1, LA ISO/IEC 42001, CRISC, CDPSE, ISM, DPO , DPO UNI 11697:2017, DPO UNI CEI EN 17740:2024, CBCI, AMBCI.

Note sul copyright

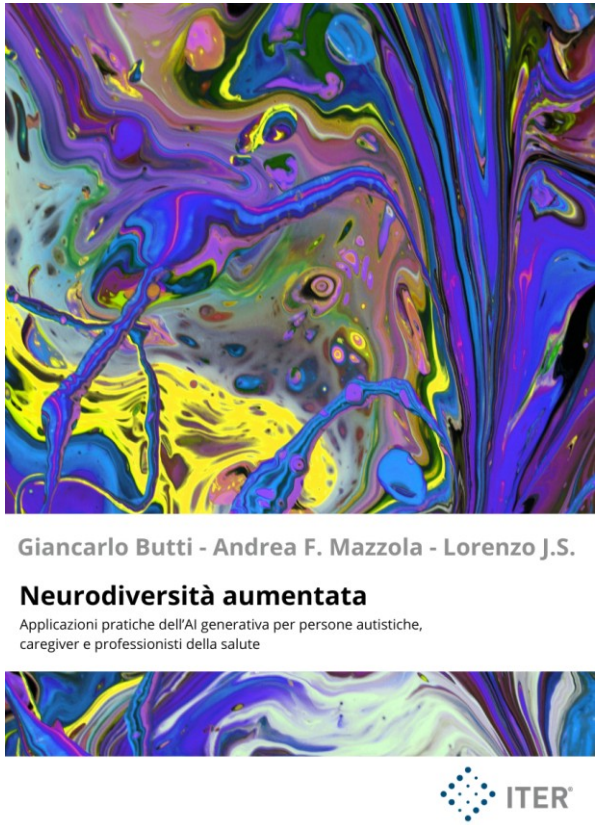
Alcuni testi e applicazioni derivano da queste mie pubblicazioni

https://iterdigital.it/it_it/compliance-4-0/#1759849188556-9a873bd4-14a7
https://iterdigital.it/it_it/ia-e-audit/#1759849267092-0aa1d321-1fd7
https://iterdigital.it/it_it/gestione-rischi-supply-chain/#1759849542919-e116777c-a7f0
https://iterdigital.it/it_it/download/22185/

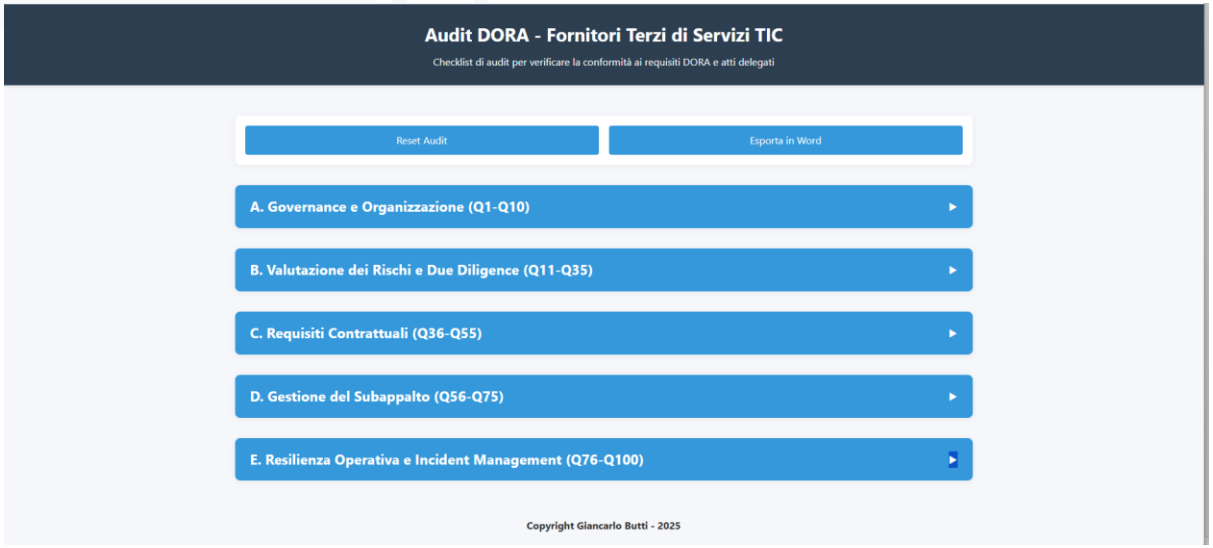
Note sul copyright

IN PREPARAZIONE

Alcuni testi e applicazioni derivano da queste mie pubblicazioni

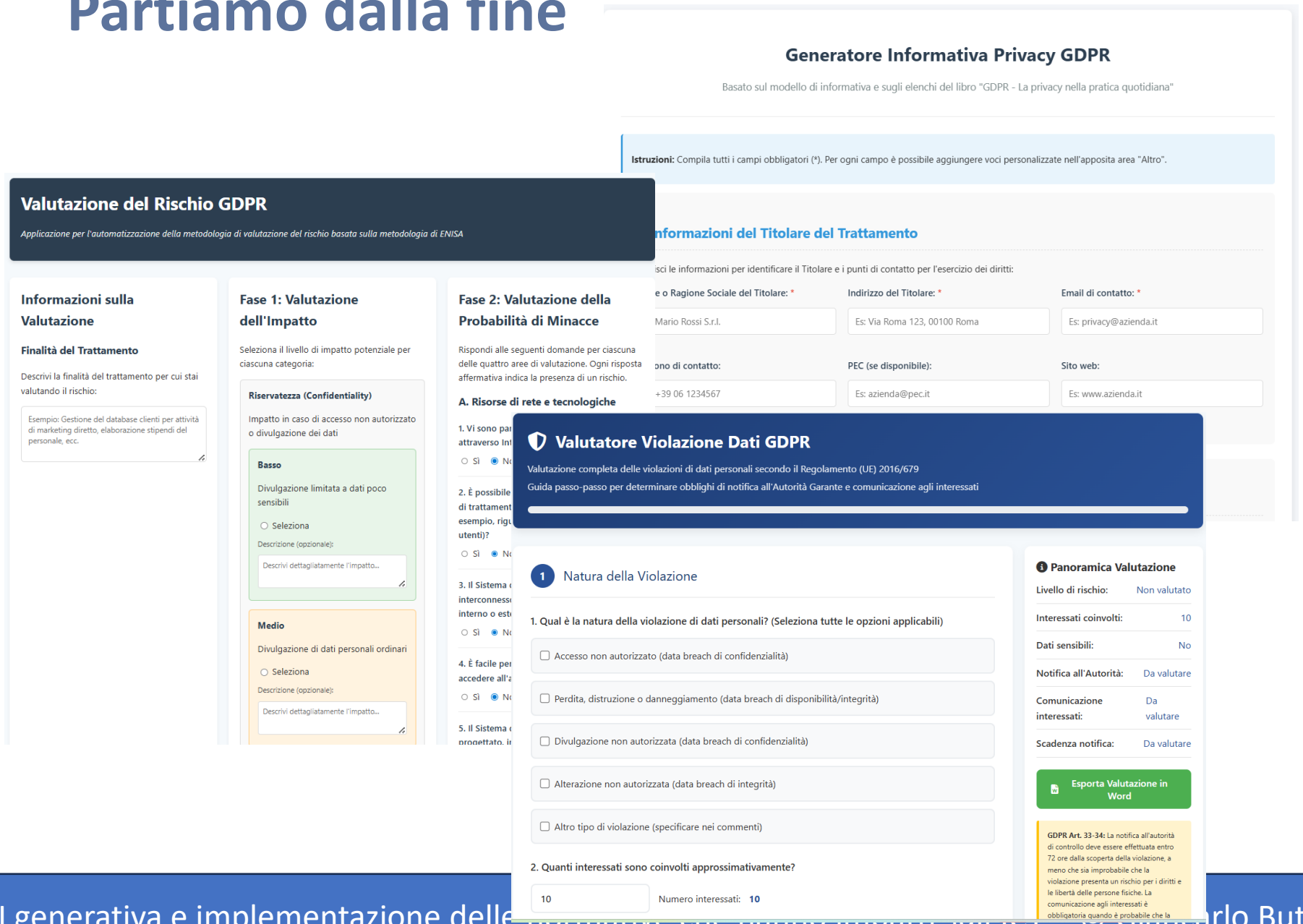


Partiamo dalla fine



https://iterdigital.it/it_it/download-applicazioni/

Partiamo dalla fine



Paradigmi dell'uso di strumenti di AI generativa: esperienza personale

1) La propria esperienza con uno strumento non conta nulla

- L'evoluzione degli strumenti è talmente rapida che quello che conosciamo oggi di uno strumento, dei suoi limiti e delle sue potenzialità può essere obsoleto domani.
- Quindi questi strumenti vanno rianalizzati nel continuo per comprendere cosa è meglio utilizzare in un determinato periodo per un uso specifico.
- È consigliabile mantenersi continuamente aggiornati con l'uso di diversi strumenti e seguendo canali di aggiornamento.

Paradigmi dell'uso di strumenti di AI generativa: esperienza personale

2) Come interagire

- Non è necessario conoscere gli strumenti o porsi quesiti in merito a cosa possono servire.
- È sufficiente chiederlo allo strumento stesso.
- Per la prima volta ci si trova di fronte ad applicazioni che guidano l'utente nel loro uso.
- Non è necessario essere esperti per creare prompt efficaci, perché basta chiedere allo stesso strumento di generarli o chiedere come vuole essere interrogato.
- È possibile chiedere qualunque cosa per superare i limiti apparenti dello strumento, ad esempio quali fonti ha utilizzato, qual è stato il suo ragionamento…

Paradigmi dell'uso di strumenti di AI generativa: esperienza personale

3) Gli strumenti non sono affidabili e quindi:

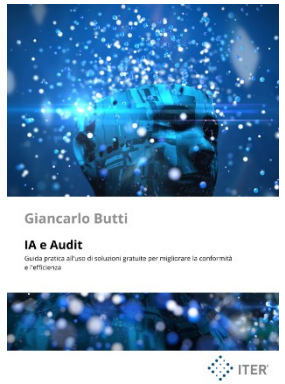
- Vanno usati solo su temi che si padroneggiano
- È utile verificare la risposta di più strumenti
- Vanno individuate strategie per effettuare controlli automatici della validità delle risposte
- Chiedere allo strumento come fare a controllare la risposta

Paradigmi dell'uso di strumenti di AI generativa: esperienza personale

4) Informazioni riservate

- Impostare lo strumento affinché non usi le informazioni caricate per addestrare il modello (se lo consente e si ritiene affidabile il produttore nelle sue affermazioni)
- Anonimizzare le informazioni
- Usare una versione aziendale dei modelli
- Utilizzare modelli in locale

Casi possibili nell’ambito delle attività di audit



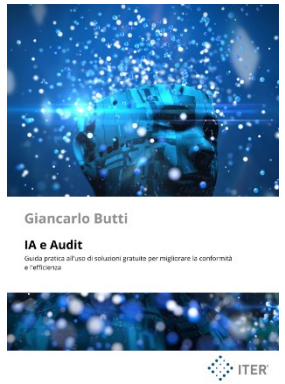
Fase preliminare alle attività di audit

- Che aiuto mi puoi dare per l'esecuzione di un audit
- Come deve essere impostata una richiesta per creare una checklist

Metodologia di audit

- Determinare la dimensione del campione per una popolazione di 5000 elementi e una confidenza del 90%
- Puoi generare del codice per una macro excel che elabori quanto sopra esposto
- Puoi creare del codice per excel al fine di calcolare il numero di campioni da analizzare necessario per avere una confidenza prestabilita?
- Definisci dei criteri con cui valutare i rilievi di un audit
- Definisci dei criteri per valutare il peso di ogni singolo criterio sopra elencato rispetto agli altri, e descrivi le ragioni della tua scelta
- Definisci dei criteri con cui combinare le valutazioni dei singoli rilievi al fine di dare una valutazione complessiva all'audit report. Descrivi le motivazioni delle scelte.

Casi possibili nell’ambito delle attività di audit



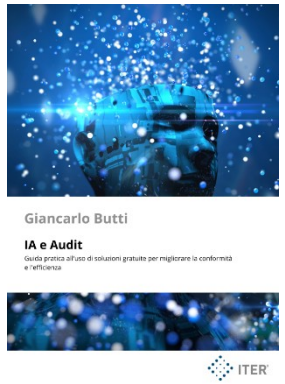
Fase di pianificazione delle attività di audit

- Individua almeno 20 parametri con cui individuare le aree aziendali di maggior rischio, sulle quali eseguire attività di audit
- Per ognuno dei punti sopra riportati elenca una scala di 5 valori che ne permetta la valutazione
- Trasforma i valori qualitativi in range quantitativi
- Individua almeno 20 criteri per identificare quali applicazioni sottoporre ad audit
- Individua almeno 20 criteri per identificare quali processi ICT sottoporre ad audit.

Fase di preparazione dell’audit

- Descrivi come deve svolgersi una attività di audit interno nell'ambito della business continuity
- Come può essere eseguito un audit sulla continuità operativa
- Descrivi un processo ideale per la gestione della business continuity
- Quali sono le fonti che hai utilizzato per descrivere il processo
- Come eseguire al meglio una business impact analysis
- Quali sono i controlli che devo effettuare su una BIA per verificare se è conforme ai requisiti previsti dalla normativa di Banca d'Italia
- Quali sono i controlli che devo mettere in atto per verificare se un piano di continuità operativa sia conforme alle normative EBA e quali sono le normative EBA da prendere in considerazione
- Crea una checklist per svolgere una verifica in ambito business continuity
- Puoi ampliare la checklist ad almeno 100 quesiti
- Crea una checklist di almeno 100 quesiti per un audit sulla business continuity dove nella prima colonna metti il numero della domanda, nella seconda la domanda, oltre ad altre 5 colonne vuote
- Per ogni domanda della checklist precedente predispone 5 risposte che indicano diversi livelli di maturità e compila le colonne della tabella che prima erano vuote
- Genera il codice CSV della precedente tabella
- Crea una checklist per un audit report sulla business continuity basato sulla ISO 22301 per un'azienda manifatturiera di medie dimensioni.

Casi possibili nell’ambito delle attività di audit



Fase di esecuzione di un audit

- Dopo aver individuato i ruoli che in un'azienda sono coinvolti nel processo di gestione della business continuity, genera una serie di domane finalizzate ad intervistare ognuno di loro
- Puoi fare la stessa cosa considerando figure più operative rispetto a quelle elencate in precedenza
- Comportati come un auditor e fammi delle domande considerando che sono il business continuity manager
- Puoi dare un peso alle varie domande e giustificare la tua scelta
- Come deve essere effettuata una verifica sulla conformità di una informativa privacy
- Verifica se la seguente informativa privacy è conforme

Fase di reportistica

- Imposta lo schema di un audit report
- Genera lo schema di un audit report relativo alla business continuity

Implementare e gestire la conformità

CONFRONTO FRA NORMATIVE

- Comparazione fra normative preesistenti e normative attuali
- Comparazione fra DORA e NIS2

SINTESI DI DOCUMENTI NORMATIVI

REQUISITI PREVISTI DA UNA NORMATIVA (tecnici - organizzativi…)

- Fasi della gestione del rapporto di fornitura

CREAZIONE DOCUMENTI: Relazioni contrattuali

- Creazione dei documenti contrattuali
- Definizione degli allegati ad un contratto

Implementare e gestire la conformità

CREAZIONE DOCUMENTI: policy e procedure

- Verifica della conformità di policies e procedure rispetto ad una normativa
- Modulistica
- Strumenti e flussi

FORMAZIONE

GENERARE APPLICAZIONI

- Uso di COLAB

APPLICAZIONI DI CARATTERE GENERALE

- Editing di testi
- Elaborazione di immagini

Gestire i rischi della supply chain

LA GESTIONE DEI FORNITORI

- L'uso degli strumenti di AI per la classificazione dei fornitori

LA GOVERNANCE DELLA GESTIONE FORNITORI

- Uso dell'AI per la gestione della governance dei fornitori
- Uso dell'AI per la creazione di una politica per la gestione dei fornitori

I RISCHI DEI FORNITORI

- Uso dell'AI per la gestione dei rischi

LA VALUTAZIONE PRELIMINARE

- L'uso dell'AI per l'esecuzione della due diligence
- L'uso dell'AI per confrontare i fornitori

Gestire i rischi della supply chain

FASE DI CONTRATTUALIZZAZIONE

- L'uso dell'IA per la fase di contrattualizzazione
- L'uso dell'AI per la gestione delle clausole per la subfornitura

FASE DI MONITORAGGIO E CONTROLLO

- L'uso dell'AI per il monitoraggio della catena di fornitura
- L'uso dell'AI per la gestione di parametri per il monitoraggio

ATTIVITÀ DI AUDIT

- L'uso dell'AI per lo svolgimento delle attività di audit interno
- L'uso dell'AI per le attività di audit sui fornitori

Gestire i rischi della supply chain

LA CHIUSURA DEL RAPPORTO DI FORNITURA

- L'uso dell'AI nella gestione della chiusura del rapporto di fornitura

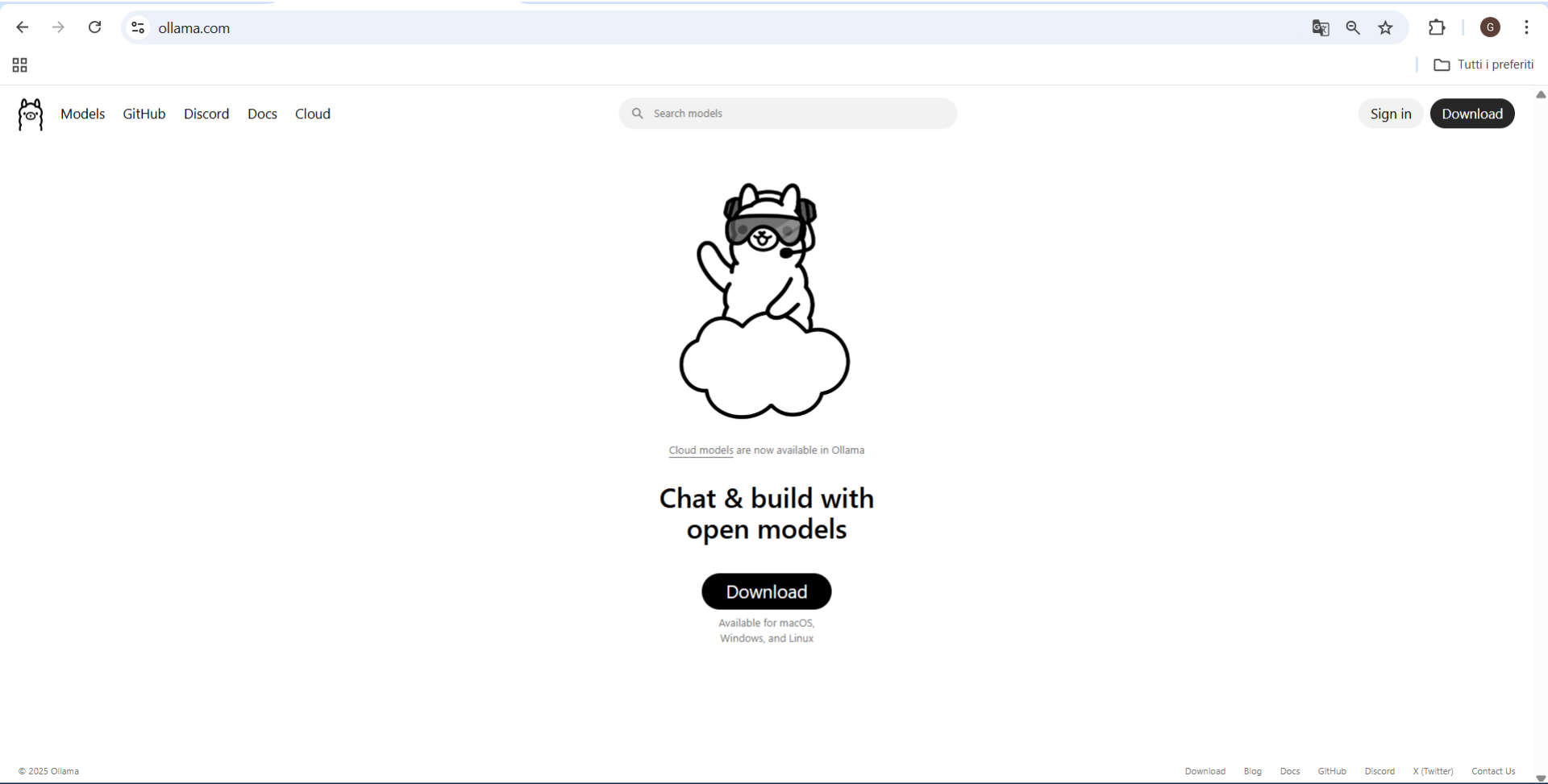
EXIT STRATEGY ED EXIT PLAN

- Uso di strumenti di AI per un Exit Plan finalizzato al rientro
- Uso di strumenti di AI per un Exit Plan finalizzato al passaggio ad un altro fornitore

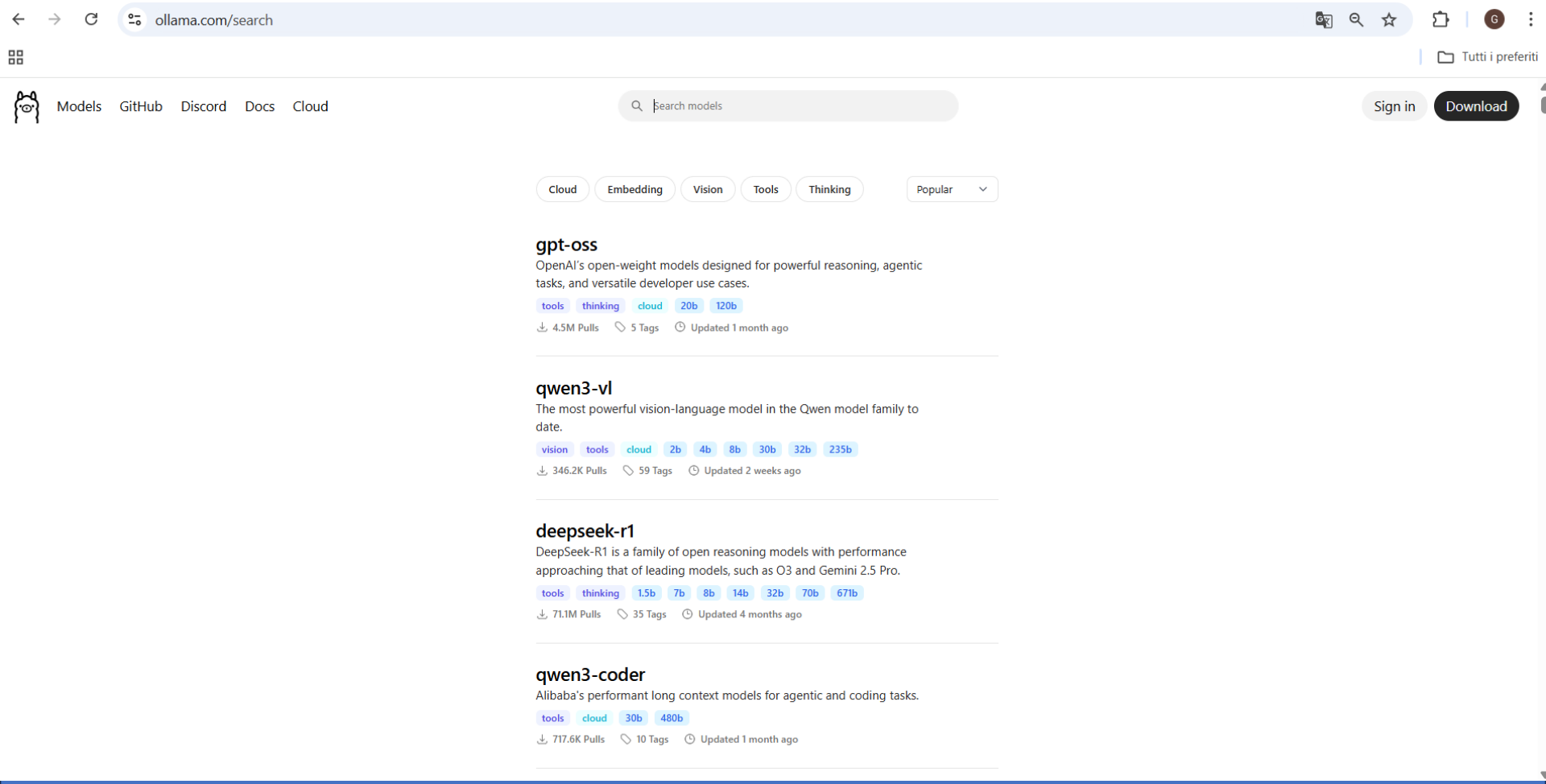
CLOUD

- L'uso dell'AI per la gestione del passaggio alle soluzioni Cloud

Modelli locali



Modelli locali



Modelli locali

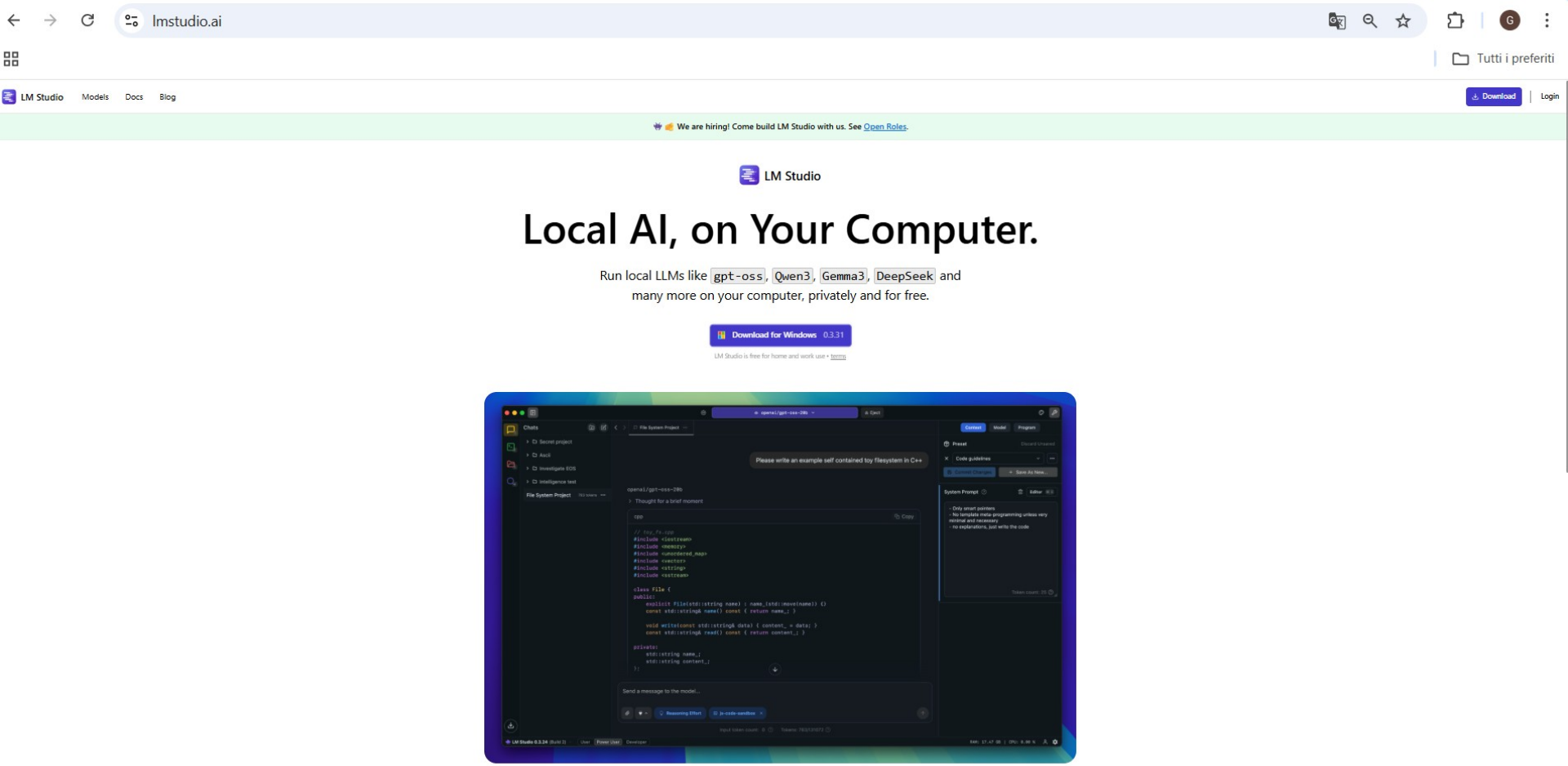
Hardware Progression for Local LLMs

PC Type	OS	CPU	RAM	Storage	GPU	Quantization	Models
Ultra-Budget Laptop	Win 10/11	i3-10th/Ryzen 3	4 GB	256 GB SSD	Intel UHD 630	Q4, Q3	Gemma 270M, TinyLlama 1.1B, Phi-3.5 Mini 3.8B
Entry-Level Laptop	Win 10/11	i5-11th/Ryzen 5	8 GB	512 GB SSD	Iris Xe/Radeon	Q4, Q5	Gemma 2B, Phi-3.5 3.8B, Qwen 3B, LLaMA 1B
Standard Laptop	Win/macOS	i7-12th/Ryzen 7	16 GB	512 GB SSD	Iris Xe/Radeon	Q4, Q5	Phi-4 3.8B, Qwen 7B, Mistral 7B, Gemma 9B
Gaming Laptop (Entry)	Win 11	i7-13th/Ryzen 7	16 GB	1 TB NVMe	RTX 3050/4060	Q4, Q5, Q6	LLaMA 8B, Qwen 8B, Mistral 7B, Phi-4 14B
Gaming Laptop (Mid)	Win 11/Linux	i9-13th/Ryzen 9	32 GB	2 TB NVMe	RTX 4070 12GB	Q5, Q6, Q8	LLaMA 8B Q6, Qwen 14B, Gemma 27B, DeepSeek 32B
Desktop Workstation	Win 11/Linux	Ryzen 9/i9-14th	64 GB	4 TB NVMe	RTX 4090 24GB	Q5, Q6, Q8	LLaMA 70B, Mistral 8x22B, DeepSeek-R1 32B
Mac Studio M3/M4	macOS 13+	M3/M4 Pro 12-16	36-64 GB	1 TB SSD	16-20 core GPU	Q5, Q6, Q8	LLaMA 8B, Qwen 14B, Phi-4 14B, Mistral 7B
Server/Enterprise	Linux Ubuntu	Dual Xeon/EPYC	256 GB	16 TB NVMe	4x A100 80GB	Q4, Q5, FP8	LLaMA 405B, DeepSeek 671B, Mixtral 8x22B

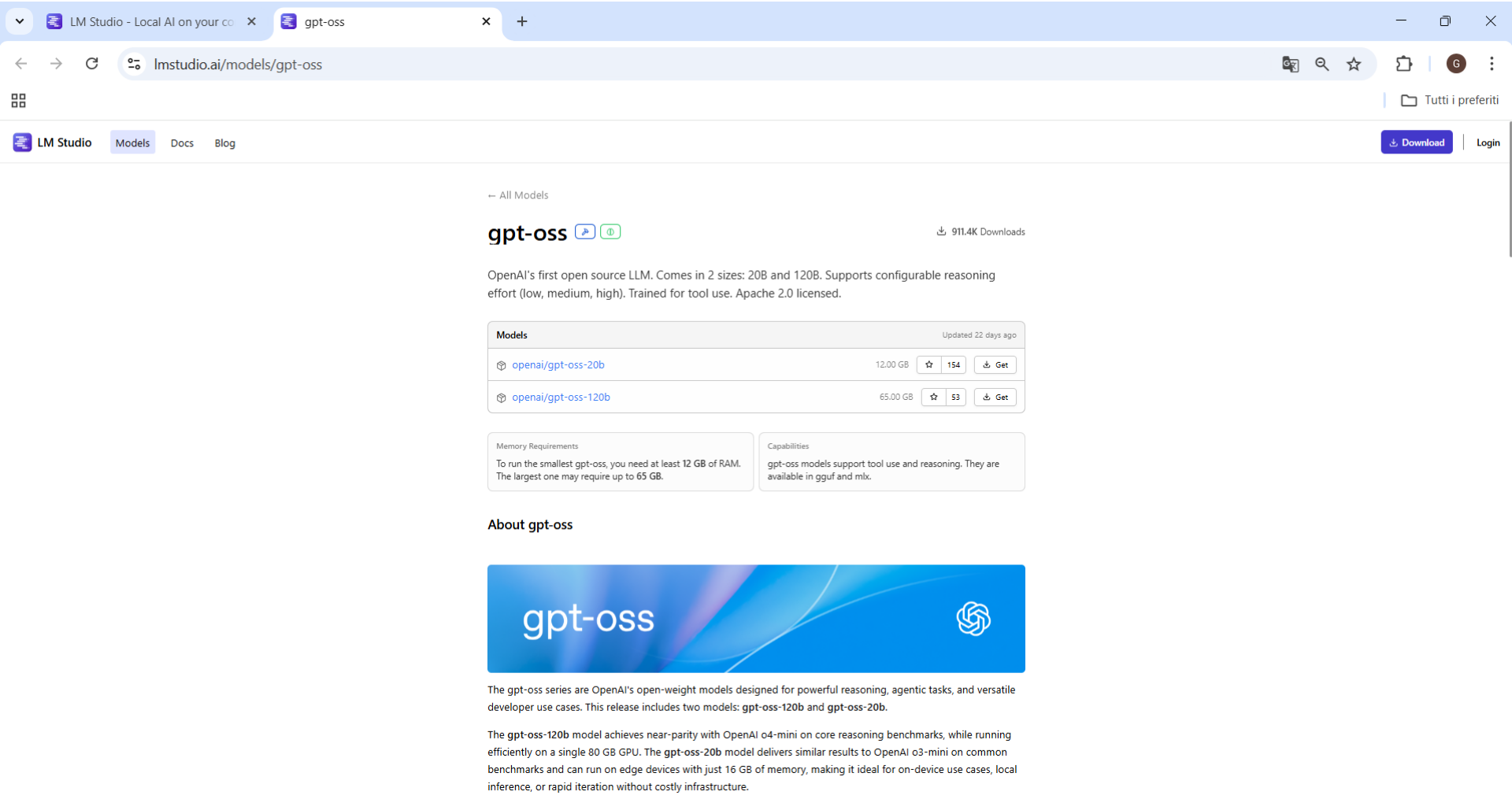
Modelli locali

Modello	Parametri	Dimensione	Comando
DeepSeek-R1	7B	4.7GB	ollama run deepseek-r1
DeepSeek-R1	671B	404GB	ollama run deepseek-r1:671b
LLaMA 3.3	70B	43GB	ollama run llama3.3
LLaMA 3.2	3B	2.0GB	ollama run llama3.2
LLaMA 3.2	1B	1.3GB	ollama run llama3.2:1b
LLaMA 3.2 Vision	11B	7.9GB	ollama run llama3.2-vision
LLaMA 3.2 Vision	90B	55GB	ollama run llama3.2-vision:90b
LLaMA 3.1	8B	4.7GB	ollama run llama3.1
LLaMA 3.1	405B	231GB	ollama run llama3.1:405b
Phi 4	14B	9.1GB	ollama run phi4
Phi 4 Mini	3.8B	2.5GB	ollama run phi4-mini
Gemma 2	2B	1.6GB	ollama run gemma2:2b
Gemma 2	9B	5.5GB	ollama run gemma2
Gemma 2	27B	16GB	ollama run gemma2:27b
Gemma 3	1B	variabile	ollama run gemma3 (AnythingLLM)
Mistral	7B	4.1GB	ollama run mistral
Moondream 2	1.4B	829MB	ollama run moondream
Neural Chat	7B	4.1GB	ollama run neural-chat
Starling	7B	4.1GB	ollama run starling-lm
Code Llama	7B	3.8GB	ollama run codellama
LLaVA	7B	4.5GB	ollama run llava
Granite 3.2	8B	4.9GB	ollama run granite3.2

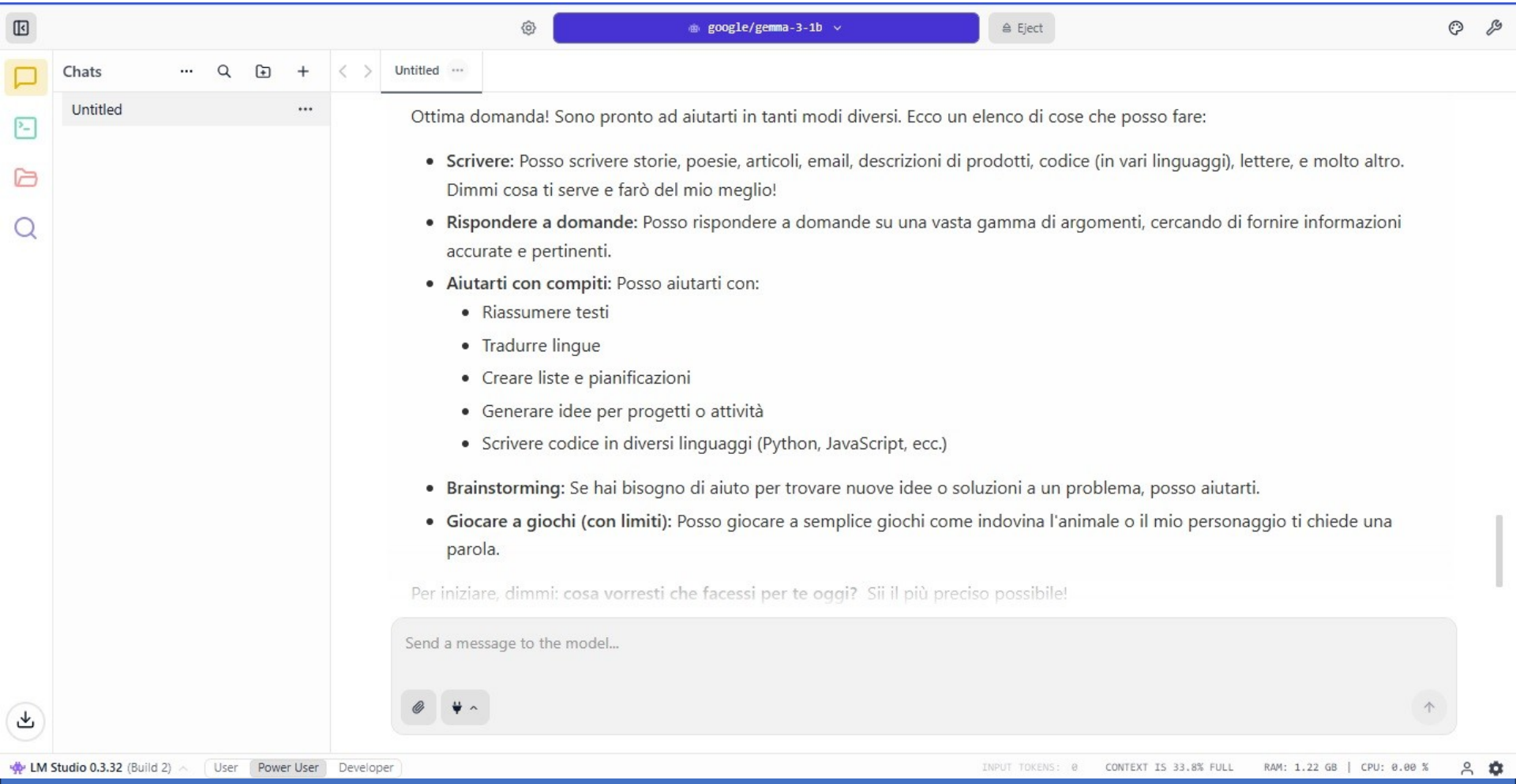
Modelli locali



Modelli locali



Modelli locali



Agenti AI

- Gli agenti AI sono sistemi software che sfruttano l'AI per perseguire obiettivi e completare attività per conto degli utenti. Mostrano capacità di ragionamento, pianificazione e memoria e hanno un livello di autonomia tale da essere in grado di prendere decisioni, apprendere e adattarsi.
- Le loro capacità sono rese possibili in gran parte dalla capacità multimodale dell'AI generativa e dei foundation model dell'AI. Gli agenti AI possono elaborare contemporaneamente informazioni multimodali come testo, voce, video, audio, codice e altro; possono conversare, ragionare, imparare e prendere decisioni. Possono imparare nel tempo e facilitare le transazioni e i processi aziendali. Gli agenti possono collaborare con altri agenti per coordinare ed eseguire workflow più complessi.

Fonte: cloud.google.com

Agenti AI

Monitoraggio continuo della conformità

Gli agenti AI forniscono sorveglianza normativa 24/7, tracciando i cambiamenti nelle normative sulla protezione dei dati attraverso molteplici giurisdizioni. Riducono il tempo di controllo di conformità mensile da 8 ore a 15 minuti, consentendo ai team di conformità di concentrarsi su questioni strategiche piuttosto che su compiti amministrativi ripetitivi.

Agenti AI

Monitoraggio continuo della conformità

Gli agenti AI forniscono sorveglianza normativa 24/7, tracciando i cambiamenti nelle normative sulla protezione dei dati attraverso molteplici giurisdizioni. Riducono il tempo di controllo di conformità mensile da 8 ore a 15 minuti, consentendo ai team di conformità di concentrarsi su questioni strategiche piuttosto che su compiti amministrativi ripetitivi.

Agenti AI

Valutazioni d'impatto sulla protezione dei dati (DPIA)

Un agente dedicato può condurre valutazioni d'impatto complete sulla privacy in sole 3 ore, rispetto alle 2-3 settimane richieste dai processi manuali, con un'accuratezza di individuazione dei rischi potenziata rispetto alle valutazioni tradizionali. L'agente identifica automaticamente i flussi di dati, valuta i rischi associati al trattamento, mappa le misure di protezione e documenta le conclusioni in conformità ai requisiti GDPR. Questo è particolarmente critico poiché il 33% delle aziende europee che utilizzano sistemi di intelligenza artificiale non conduce nemmeno DPIA per i progetti che coinvolgono dati personali.

Fonte: https://verifywise.ai/

Agenti AI

Gestione del rischio dei fornitori terzi

Il DORA richiede un controllo rigoroso dei fornitori di servizi ICT critici, che rappresenta una delle sfide più significative per le istituzioni finanziarie. Invece di analisti che rivedono manualmente centinaia di contratti di fornitori—un processo che può richiedere settimane di lavoro—le organizzazioni implementano sistemi composti da 13-15 agenti AI specializzati, ognuno incaricato di valutare un requisito specifico del DORA (ad esempio, obblighi di continuità, misure di sicurezza, notifica di incidenti). Durante un'implementazione pratica presso un general partner danese, il sistema ha automatizzato il controllo di contratti complessi che coinvolgevano accordi master, addendi e accordi di elaborazione dei dati, riducendo considerevolmente i tempi di revisione e assicurando la coerenza delle valutazioni.deployflow+1

Gli agenti possono anche monitorare continuamente i cambiamenti nelle prestazioni e nella posizione di rischio dei fornitori, identificando potenziali vulnerabilità prima che diventino problemi di conformità. Il 37% dei responsabili della conformità ha identificato l'automazione delle valutazioni del rischio come il principale vantaggio dell'IA nel raggiungimento della conformità.

Fonte: https://deployflow.co/

Classificazione dei sistemi di IA e pratiche di IA vietate

Seguendo un approccio "basato sul rischio", in base al quale tanto maggiore è il rischio, quanto più rigorose sono le regole, la nuova disciplina stabilisce obblighi per fornitori e operatori dei sistemi di IA a seconda del livello di rischio che l'IA può generare:

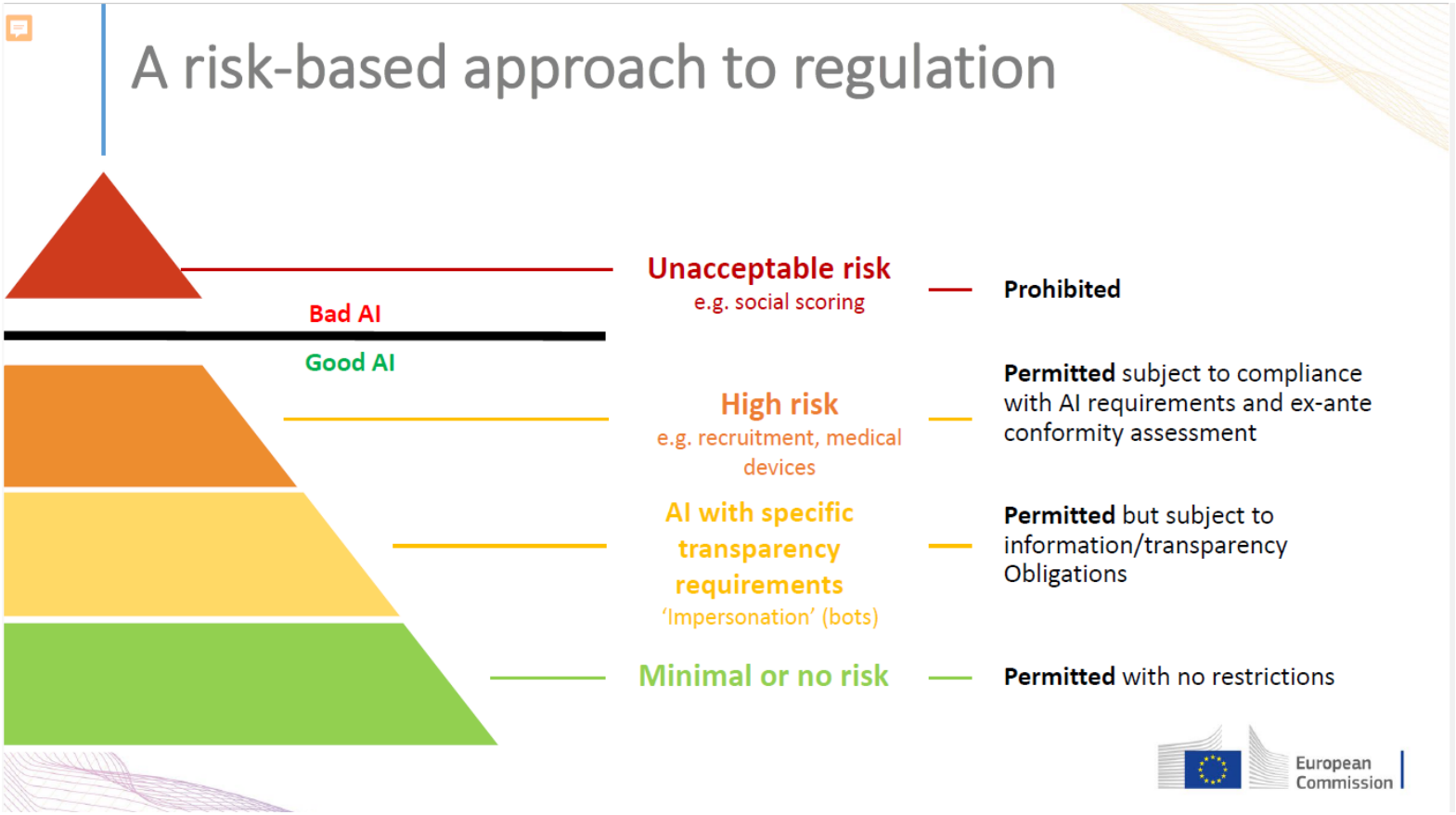
i) un rischio inaccettabile;

ii) un rischio alto;

iii) un rischio basso o minimo.

Sono stabiliti anche obblighi specifici per la trasparenza.

Classificazione dei sistemi di IA e pratiche di IA vietate



Sistemi ad alto rischio nell’ambito di frodi interne

ALLEGATO III

Sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2

Occupazione, gestione dei lavoratori e accesso al lavoro autonomo:

….

b) i sistemi di IA destinati a essere utilizzati per adottare decisioni riguardanti le condizioni dei rapporti di lavoro, la promozione o cessazione dei rapporti contrattuali di lavoro, per assegnare compiti sulla base del comportamento individuale o dei tratti e delle caratteristiche personali o per monitorare e valutare le prestazioni e il comportamento delle persone nell'ambito di tali rapporti di lavoro.

Sistemi ad alto rischio nell'ambito di frodi in ambito scolastico

ALLEGATO III

Sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2

…

3. Istruzione e formazione professionale:….

d) i sistemi di IA destinati a essere utilizzati per monitorare e rilevare comportamenti vietati degli studenti durante le prove nel contesto o all'interno di istituti di istruzione e formazione professionale a tutti i livelli.

Rischi privacy

- mancata individuazione di un trattamento di dati personali:
  - per mancata conoscenza della normativa e della definizione di dato personale o di dato particolare
  - anche tramite inferenza
  - anche se i dati sono originariamente anonimi
- mancati adempimenti in conseguenza di un nuovo trattamento con particolare riferimento agli artt.12-14, 24, 25, 32
- accesso illecito ai dati personali (differenza fra accesso legittimo ed accesso lecito)
- profilazione dei dati personali (articolo 22)
- mancato rispetto dei principi, con particolare riferimento alla minimizzazione
- mancata visibilità delle elaborazioni intermedie (trasparenza black box) di dati personali, che limita il diritto di accesso ai dati

Peculiarità del rischio privacy

Il rischio in ambito privacy ha una doppia valenza:

- È un rischio per i diritti e le libertà delle persone fisiche, non un rischio aziendale e come tale non può essere gestito con i normali criteri
  - ad esempio non è possible accettare un rischio alto o trasferire il rischio
- Si traduce in un rischio aziendale in quanto comporta sanzioni e risarcimenti oltre ad un danno di immagine

Problemi: il rispetto della privacy

«dato personale»: **qualsiasi informazione** riguardante una persona fisica **identificata o identificabile** («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

https://www.mrperugini.it/it/appendici-libri/

Rischi privacy
Profilazione (art. 22 GDPR)

«profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

Grazie per l'attenzione

giancarlo.butti@promo.it

gbutti@clusit.it

338 9230742