CORSO IA CON CLAUDE · DISPENSA PER L'ALLIEVO

Account personale o sottoscrizione aziendale

Chi controlla i dati, chi risponde davanti alla legge, chi paga il conto

ORA	DURATA	MODULO
04 di 12	60 minuti	2 — Governance

Gianluca Bonomo · www.gianlu.it · info@gianlu.it

Indice

Indice 2
Come usare questa dispensa 3
1. La scena che si ripete in ogni azienda 4
1.1 Perché succede: non è cattiva volontà 4
1.2 Che cosa si rischia davvero 5
2. Chi decide che fine fanno i dati 6
2.1 Sugli account personali decide l'utente 6
2.2 Sui prodotti aziendali decide l'azienda 7
2.3 Titolare e responsabile: il punto che conta per il GDPR 7
2.4 Che cosa chiedere di vedere, in concreto 7
2.5 Dove finiscono fisicamente i dati 8
3. I piani a confronto 8
3.1 Il calcolo che convince la direzione 9
3.2 Cinque domande da fare al proprio IT prima di partire 10
4. La console: il pezzo che cambia tutto 10
4.1 I ruoli 11
4.2 Perché conta il giorno in cui qualcuno se ne va 11
4.3 Le tre cose da mettere per iscritto prima di comprare 11
4.4 Che cosa vede l'amministratore, e che cosa no 12
5. Esercitazione pratica dell'ora 13
Le domande che arrivano in aula 13
Glossario 15
Per approfondire 16

Come usare questa dispensa

Questa dispensa raccoglie, in forma scritta e ordinata, tutto quello che vediamo insieme durante l'ora di lezione. Non devi studiarla a memoria: serve a farti ritrovare le cose con calma, dopo, quando l'aula è finita e ti resta una domanda in sospeso.

È pensata per chi parte da zero. Ogni termine tecnico viene spiegato la prima volta che compare, e a fine dispensa trovi un glossario con tutte le parole nuove. Se una pagina ti sembra difficile, saltala e torna indietro dopo: nessun concetto di questa dispensa richiede conoscenze informatiche precedenti.

> **COME SONO FATTI I RIQUADRI**
>
> **In parole semplici** (azzurro): la spiegazione senza tecnicismi, quella da portarsi a casa se si ricorda una cosa sola.
>
> **Attenzione** (oro): un errore frequente, un rischio, una cosa da non fare.
>
> **Esempio** (grigio): un caso concreto, preso dalla vita di tutti i giorni o dal lavoro in azienda.

Obiettivo dell'ora

Capire perché far usare ai collaboratori account personali è un rischio per l'azienda, che cosa cambia con una sottoscrizione aziendale e come si imposta una governance minima ma seria.

Che cosa saprai fare alla fine

- Spiegare alla direzione perché la differenza non è il prezzo.
- Sapere chi decide se le conversazioni alimentano l'addestramento.
- Riconoscere il ruolo di titolare e responsabile del trattamento.
- Scrivere le tre regole minime di una policy aziendale sull'IA.

1. La scena che si ripete in ogni azienda

Non c'è nessun cattivo in questa storia. È proprio questo che la rende difficile da affrontare.

L'azienda non ha comprato nulla. I collaboratori, però, hanno scoperto che l'intelligenza artificiale fa risparmiare ore. Così ognuno si arrangia: chi usa il piano gratuito, chi si paga l'abbonamento personale, chi usa il telefono aziendale con un account privato.

Funziona benissimo. Ed è esattamente questo il problema.

> **IL RISCHIO NON È IL DIPENDENTE SLEALE**
>
> È quello **diligente e di corsa**: quello che ha una scadenza, apre un chatbot, incolla il foglio con i dati dei clienti e ottiene in trenta secondi un report perfetto.
>
> Ha fatto bene il suo lavoro. E ha portato fuori dal perimetro aziendale dei dati che nessuno sa più dove siano.

È la **Shadow AI** di cui abbiamo parlato nella seconda ora. L'azienda non sa quali documenti siano usciti, non può controllarne l'uso e, in caso di contestazione, non può dimostrare di aver fatto il necessario per proteggerli.

1.1 Perché succede: non è cattiva volontà

Chi incolla il testo di un contratto in un assistente personale non sta aggirando una regola: quasi sempre non sa che ce ne sia una. Sta facendo il suo lavoro con lo strumento più veloce che ha a disposizione.

È la stessa dinamica che negli anni scorsi ha portato i file aziendali sui servizi di archiviazione personali e le conversazioni di lavoro sulle applicazioni di messaggistica private. La risposta che ha funzionato allora è la stessa che funziona oggi: **dare un'alternativa aziendale prima di vietare quella personale**.

Quello che dice l'azienda	Quello che succede davvero
«Non si usano strumenti di IA»	Si usano lo stesso, dal telefono personale, e l'azienda non lo sa
«Si usa solo lo strumento aziendale»	Funziona, se lo strumento aziendale c'è ed è altrettanto comodo
«Si usa lo strumento aziendale, e queste sono	È l'unica formulazione che le persone ricordano e

Quello che dice l'azienda	Quello che succede davvero
le tre cose da non caricare mai»	applicano

IL DATO DA TENERE A MENTE

In azienda il rischio non nasce quasi mai da chi vuole fare danni: nasce da chi vuole fare in fretta.

Una policy costruita per il primo caso è inutile. Una costruita per il secondo funziona.

1.2 Che cosa si rischia davvero

Le conseguenze di un uso non governato non sono ipotesi da manuale: sono quattro situazioni concrete, e nessuna richiede malafede per verificarsi.

1. **La perdita di riservatezza su un'informazione commerciale.** Il preventivo che state preparando, il margine su una commessa, la strategia per una gara. Non serve che finiscano a un concorrente: basta che siano usciti dal perimetro aziendale senza una base contrattuale.
2. **La violazione di un obbligo verso un terzo.** Molti contratti e accordi di riservatezza vietano espressamente di trasferire il materiale a soggetti non autorizzati. Un fornitore di servizi non coperto dal contratto è un soggetto non autorizzato.
3. **Il trattamento illecito di dati personali.** Caricare un curriculum, una busta paga o l'elenco dei clienti su un servizio senza contratto adeguato è un trattamento privo di base giuridica. Con tutto ciò che comporta in caso di reclamo.
4. **Il danno reputazionale.** È quello che le direzioni temono di più, e l'unico che non si ripara con un pagamento.

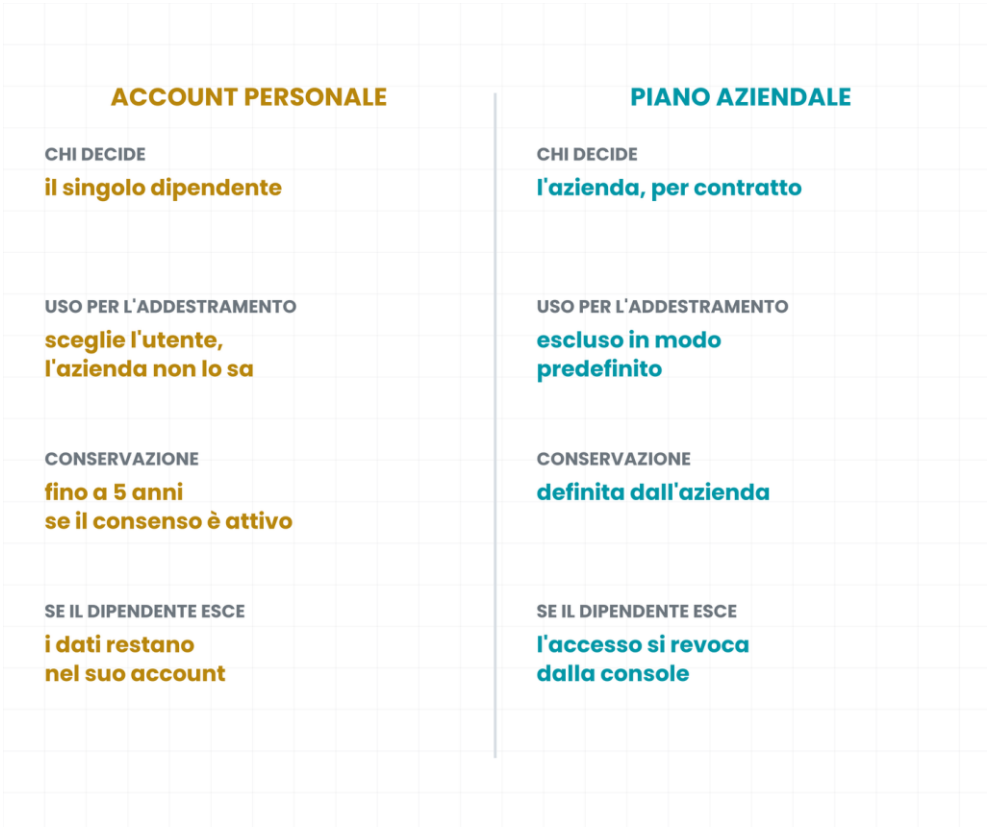
IL PUNTO CHE SORPRENDE SEMPRE

Nessuna di queste quattro situazioni richiede che il fornitore si comporti male o subisca un attacco.

Bastano un documento caricato sull'account sbagliato e un contratto che quel caricamento non copre.

2. Chi decide che fine fanno i dati

È il punto centrale dell'ora, e quasi nessuno lo conosce con precisione.



Le stesse quattro domande, due risposte molto diverse.

2.1 Sugli account personali decide l'utente

Sui piani destinati alle persone (gratuito, individuale a pagamento e le sue varianti) esiste una **scelta dell'utente**: si può consentire o negare che le proprie conversazioni vengano usate per migliorare i modelli. La scelta si fa nelle impostazioni e si può cambiare in qualsiasi momento.

La conseguenza pratica riguarda anche i tempi di conservazione: se il consenso è attivo, i contenuti possono essere conservati per un periodo molto più lungo rispetto a chi non lo ha dato.

> **IL PUNTO CHE RIGUARDA L'AZIENDA**
>
> L'azienda **non può sapere** che cosa ha scelto ciascun dipendente sul proprio account personale. Né può imporlo, né verificarlo.
>
> Ma resta comunque l'azienda a rispondere, se in quelle conversazioni sono finiti dati personali di clienti o dipendenti.

2.2 Sui prodotti aziendali decide l'azienda

Sui prodotti commerciali — i piani aziendali e l'accesso tramite interfaccia di programmazione — la regola predefinita è opposta: **i dati non vengono usati per addestrare i modelli**, salvo che sia l'azienda stessa a scegliere diversamente.

Non è un'impostazione che il singolo può cambiare di nascosto: è la condizione contrattuale con cui il servizio viene fornito all'organizzazione.

2.3 Titolare e responsabile: il punto che conta per il GDPR

C'è un secondo aspetto, meno noto e più importante. Con una sottoscrizione aziendale il rapporto giuridico cambia forma.

- L'**azienda cliente** è il *titolare* del trattamento: decide finalità e modalità, e dà le istruzioni.
- Il **fornitore** agisce come *responsabile*: tratta i dati soltanto per conto del cliente e secondo le sue istruzioni.

È esattamente la struttura che il GDPR richiede quando un trattamento viene affidato all'esterno. Con un account personale quella struttura non esiste: il contratto è fra il fornitore e il singolo dipendente, e l'azienda non ne è parte.

> **DETTO IN UNA FRASE**
>
> Con l'account personale l'azienda ha il **rischio** senza il **controllo**. Con la sottoscrizione aziendale ha entrambi.

2.4 Che cosa chiedere di vedere, in concreto

Quando si valuta un fornitore, «i dati sono al sicuro» non è una risposta. Questi quattro documenti esistono e si possono chiedere: se non arrivano, è già un'informazione.

1. **L'accordo sul trattamento dei dati.** È il contratto previsto dall'articolo 28 del GDPR fra titolare e responsabile. Senza quello, l'azienda sta trattando dati personali fuori dalle regole.
2. **L'elenco dei sub-responsabili.** Chi altro tocca i dati, a che titolo e in quale paese. Serve per sapere dove finiscono davvero.
3. **Le condizioni sull'addestramento.** Devono dire per iscritto che i contenuti dei clienti non vengono usati per addestrare i modelli, e in quali casi eventualmente sì.

4. **I tempi di conservazione.** Per quanto restano i contenuti, che cosa succede alla chiusura del contratto, come si chiede la cancellazione.

> **LA DOMANDA CHE CHIUDE IL DISCORSO**
>
> «Me lo mandate per iscritto?»
>
> Vale per qualsiasi fornitore, non solo per l'intelligenza artificiale. Ciò che un commerciale dice a voce non protegge nessuno.

2.5 Dove finiscono fisicamente i dati

La domanda arriva sempre, e merita una risposta precisa: i dati vengono elaborati sui server del fornitore, che per i grandi operatori del settore si trovano in larga parte fuori dall'Unione europea, tipicamente negli Stati Uniti.

Questo non rende il trattamento illegittimo: significa che deve essere **governato**. Il GDPR prevede strumenti precisi per il trasferimento verso paesi terzi, e il fornitore serio li dichiara nel contratto.

- **Le clausole contrattuali standard**, approvate dalla Commissione europea: sono lo strumento più diffuso e vanno allegate al contratto.
- **Le decisioni di adeguatezza**, quando esistono per il paese di destinazione: semplificano molto la posizione del titolare.
- **Le misure supplementari**, come la cifratura dei dati in transito e a riposo, che il fornitore deve descrivere.

> **LA DOMANDA OPERATIVA**
>
> Non è «i dati restano in Italia?» — quasi mai è così, e nemmeno per la maggior parte dei servizi informatici che usate già.
>
> È «quale base giuridica copre il trasferimento, e me la mostrate?». A questa, un fornitore in regola risponde con un documento.

3. I piani a confronto

Che cosa si compra davvero passando da un account personale a uno aziendale.

Piano	Per chi	Che cosa dà all'azienda
Free	Per provare, individuale	Nulla: nessuna garanzia contrattuale, nessun controllo.
Pro	Individuale, a pagamento	Più capacità d'uso per la persona. Resta un account personale: l'azienda non lo governa e non lo vede.
Team	Il primo piano aziendale	Console di amministrazione, ruoli, fatturazione unica, progetti condivisi, accesso con le credenziali aziendali.
Enterprise	Organizzazioni grandi	Controlli avanzati, integrazione con i sistemi d'identità, condizioni contrattuali su misura, contratto annuale.

ORDINI DI GRANDEZZA, NON PREVENTIVI

Al momento della verifica, il piano individuale costa intorno ai **20 dollari al mese**; il primo piano aziendale intorno ai **25 dollari per utente al mese**, con uno sconto pagando annualmente, da un minimo di due postazioni.

Questi numeri servono a dare la **scala**, non a fare un preventivo: controlla sempre il listino aggiornato e la disponibilità per l'Italia.

Il confronto giusto, comunque, non è fra venti e venticinque euro. È fra venticinque euro al mese e il costo di una violazione di dati: notifica al Garante, eventuale comunicazione agli interessati, sanzione, tempo perso e danno reputazionale.

3.1 Il calcolo che convince la direzione

La domanda che arriva dalla direzione è sempre la stessa: perché dovremmo pagare, se funziona già gratis? Il calcolo, fatto bene, è breve.

Voce	Ordine di grandezza
Dieci postazioni aziendali per un anno	qualche migliaio di euro
Una violazione di dati personali: notifica, istruttoria, tempo del personale interno, eventuale consulenza legale	decine di migliaia di euro, anche senza sanzione
Sanzione amministrativa nei casi più gravi	percentuali del fatturato annuo
Il tempo che un reparto perde rifacendo lo stesso lavoro, perché nessuno condivide istruzioni e materiali	difficile da quantificare, e per questo quasi sempre ignorato

COME IMPOSTARE LA CONVERSAZIONE

Non presentatela come la spesa per uno strumento: presentatela come **il contratto che vi mette in regola** su un trattamento di dati che è già in corso, che l'azienda lo sappia o no.

La domanda vera non è «ci serve?», ma «lo stanno già usando?». La risposta, in quasi tutte le aziende, è sì.

3.2 Cinque domande da fare al proprio IT prima di partire

Sono domande brevi, e le risposte determinano quanto lavoro c'è davvero da fare. Vale la pena porle prima di fissare tempi con la direzione.

1. **Abbiamo già un sistema di identità aziendale** (accesso unico, gestione centralizzata degli account)? Se sì, la gestione delle licenze è quasi immediata; se no, va previsto un lavoro in più.
2. **Chi toglie gli accessi quando una persona esce?** Se non c'è già una procedura, questo è il momento di scriverla: vale per tutti gli strumenti, non solo per questo.
3. **Abbiamo un registro dei trattamenti aggiornato?** Va aggiunta una voce. È un adempimento breve, ma è il primo che verrà chiesto in caso di controllo.
4. **Chi firma il contratto sul trattamento dei dati?** Deve essere chi ha i poteri per farlo, non chi attiva le licenze.
5. **Che cosa diciamo ai lavoratori, e quando?** L'informativa va data **prima** dell'attivazione, non dopo.

LA BUONA NOTIZIA

Nessuna di queste cinque cose è specifica dell'intelligenza artificiale: sono gli stessi adempimenti che servono per qualsiasi servizio esterno.

Se l'azienda li ha già fatti per la posta elettronica o per l'archivio in cloud, qui si tratta di aggiungere una riga, non di ricominciare.

4. La console: il pezzo che cambia tutto

La differenza più concreta fra un account personale e uno aziendale non è nelle funzioni di Claude: è in quello che ci sta intorno.



Un punto solo da cui si governano licenze, ruoli e accessi.

4.1 I ruoli

- **Owner** — possiede l'organizzazione, gestisce la fatturazione, decide le impostazioni generali.
- **Admin** — gestisce gli utenti, i permessi e i progetti condivisi.
- **Member** — usa Claude dentro le regole ricevute.

4.2 Perché conta il giorno in cui qualcuno se ne va

È la domanda che in aula mette in imbarazzo più di ogni altra. Su un account personale ci sono mesi di lavoro: bozze, analisi, listini, forse dati di clienti. L'azienda non può entrarci, non può recuperarli e non può cancellarli.

Con una console, invece, l'accesso si revoca da un pannello, e il materiale che stava nei progetti condivisi resta all'azienda.

4.3 Le tre cose da mettere per iscritto prima di comprare

Acquistare le licenze è la parte facile. Quello che fa la differenza sono tre documenti brevi, che possono stare in una pagina ciascuno.

1. **La policy d'uso.** Che cosa si può caricare, che cosa non si può caricare mai, a chi si chiede nei casi dubbi. Deve essere leggibile in tre minuti, altrimenti non la legge nessuno.

2. **L'informativa ai lavoratori.** La normativa italiana chiede che i lavoratori, e le loro rappresentanze, siano informati quando l'azienda adotta sistemi di intelligenza artificiale che incidono sul lavoro.
3. **La procedura di uscita.** Che cosa succede agli accessi e ai contenuti quando una persona lascia l'azienda o cambia ruolo.

> **L'ORDINE GIUSTO**
>
> Prima si dà uno strumento aziendale, poi si scrivono le regole, poi si chiede di non usare quelli personali.
>
> Se si comincia dal divieto, la Shadow AI non sparisce: impara solo a nascondersi meglio.

4.4 Che cosa vede l'amministratore, e che cosa no

È la domanda che i dipendenti fanno per primi, e che merita una risposta netta perché riguarda la loro riservatezza: che cosa può vedere chi gestisce la console?

Tipicamente si vede	Tipicamente non si vede
Chi ha un account attivo e chi no	Il contenuto delle singole conversazioni, salvo funzioni specifiche di conservazione attivate esplicitamente e dichiarate
Quanto viene usato, in forma aggregata	Che cosa ha chiesto una determinata persona in un determinato momento
Quali progetti condivisi esistono e chi vi partecipa	Le conversazioni private di un collaboratore dentro il suo spazio personale

> **IL PUNTO GIURIDICO DA NON SBAGLIARE**
>
> Qualunque funzione permetta di risalire all'attività di una singola persona ricade nella disciplina italiana sui controlli a distanza (articolo 4 dello Statuto dei lavoratori) e va gestita di conseguenza: accordo sindacale o autorizzazione, e informativa preventiva.
>
> Il modo più semplice di evitare il problema è non attivare ciò che non serve, e dire chiaramente alle persone che cosa è attivo.

Dirlo in anticipo, e per iscritto, ha anche un effetto pratico: toglie il sospetto che è la prima causa per cui le persone continuano a usare i propri account personali.

5. Esercitazione pratica dell'ora

Una configurazione simulata. Sono tre righe: sono anche la differenza fra un'adozione governata e una Shadow AI.

Domanda	La vostra risposta
Chi è Owner? Chi è Admin? Chi li sostituisce se sono assenti?	.....
Quali categorie di documenti si possono caricare?	.....
Quali non si possono caricare **mai**?	.....
Che cosa succede quando una persona lascia l'azienda?	.....
Chi si occupa di formare chi entra?	.....

L'ORDINE GIUSTO DELLE MOSSE

Prima si dà uno strumento aziendale. **Poi** si vieta quello personale.

Fatto al contrario, il divieto non elimina la Shadow AI: la rende solo invisibile.

Le domande che arrivano in aula

Sono le stesse in ogni corso. Vale la pena avere pronta una risposta breve e onesta, anche per quando le farà un collega.

«Ma i nostri dati li leggono davvero?»

Sui prodotti aziendali, in modo predefinito, i contenuti non vengono usati per addestrare i modelli: è una condizione contrattuale, non una cortesia.

Questo non significa però che i dati restino in casa: vengono comunque elaborati sui server del fornitore. Per questo servono il contratto e la valutazione, non la fiducia.

«E se un dipendente usa di nascosto il suo account personale?»

È il caso più frequente, ed è anche il motivo per cui il divieto da solo non funziona.

La responsabilità verso il Garante resta dell'azienda, che in quel caso non ha né visibilità né prova di aver fatto il necessario: è esattamente la posizione peggiore possibile.

«Possiamo dare il piano aziendale solo ad alcuni reparti?»

Sì, ed è spesso la scelta più sensata per partire: si comincia da chi tratta i dati più delicati o da chi ne trarrebbe più vantaggio.

L'importante è che la policy valga per **tutti**, anche per chi non ha ancora la licenza. Altrimenti si sta solo spostando il problema.

«Di chi è la responsabilità, dell'IT o della direzione?»

Di entrambi, e non è una risposta diplomatica. L'IT gestisce accessi e sicurezza; la direzione decide che cosa si può fare con i dati dell'azienda e se ne assume la responsabilità.

Il ruolo che manca quasi sempre è il terzo: qualcuno che formi le persone. Senza quello, gli altri due lavorano a vuoto.

Glossario

Le parole che incontri in questa dispensa, spiegate in una riga. Tienilo a portata di mano: torneranno in tutte le ore successive del corso.

Termine	Che cosa significa
Console di amministrazione	Il pannello da cui l'azienda gestisce utenti, ruoli, licenze e impostazioni di sicurezza.
Responsabile del trattamento	Chi tratta dati personali per conto del titolare e secondo le sue istruzioni.
Shadow AI	Uso di strumenti di IA non autorizzati, all'insaputa dell'azienda.
SSO	Accesso unico: si entra nei servizi con le credenziali aziendali, senza password separate.
Titolare del trattamento	Chi decide finalità e modalità del trattamento dei dati personali, e ne risponde.

Per approfondire

Le fonti usate per costruire questa dispensa. Sono tutte pubbliche e consultabili: se un dato ti interessa, vai alla fonte e verificalo. È esattamente quello che chiediamo di fare anche all'intelligenza artificiale.

La politica sui dati del fornitore

Il centro privacy di Anthropic distingue in modo esplicito i prodotti consumer da quelli commerciali: sui secondi, in modo predefinito, i dati non sono usati per addestrare i modelli.

I piani e i prezzi

La pagina dei piani e il centro assistenza di Claude riportano prezzi, numero minimo di postazioni e funzioni incluse. Cambiano: vanno verificati.

La normativa

Regolamento (UE) 2016/679 (GDPR) per i ruoli di titolare e responsabile; legge 23 settembre 2025, n. 132 per gli obblighi verso i lavoratori.

Il libro di riferimento del corso

Gianluca Bonomo, *Niente paura, è solo IA. La guida completa per capirla, usarla e restare umani*.

UNA NOTA SULLE DATE

Le norme sull'intelligenza artificiale cambiano in fretta. I dati normativi di questa dispensa sono verificati a **settembre 2026**. Prima di usarli in una decisione aziendale, controlla sempre la fonte ufficiale: il calendario dell'AI Act è già stato modificato una volta.