Dazr Compliance

Accordo sul trattamento dei dati (DPA)

Ultimo aggiornamento: 7 ottobre 2026 · Contratto ai sensi dell'art. 28 GDPR.

Questa è una traduzione fornita solo a titolo informativo. In caso di differenze tra la presente traduzione e la versione inglese, prevale la versione inglese.

Come funziona

Il presente DPA costituisce parte integrante dei Termini di servizio. Si attiva automaticamente quando viene creato uno spazio di lavoro e vi vengono caricati dati personali. L'organizzazione cliente titolare dello spazio di lavoro è il titolare del trattamento; Dazr è il responsabile del trattamento. Non è richiesta alcuna firma; se la Sua procedura di acquisto richiede una copia controfirmata, scriva a legal@dazr.eu.

1. Definizioni

I termini utilizzati nel presente DPA hanno il significato loro attribuito dal Regolamento (UE) 2016/679 (il GDPR). Per "Dati personali del cliente" si intendono i dati personali che il titolare del trattamento (o i membri o gli auditor che agiscono sotto la sua autorità) inserisce nello spazio di lavoro, compresi i dati personali contenuti in attività di controllo, evidenze, commenti, file, rischi, incidenti, schede dei fornitori, membri e inviti, segnalazioni dal portale pubblico e registro attività.

2. Oggetto, durata, natura e finalità

- Oggetto: il trattamento dei Dati personali del cliente per consentire al titolare di gestire il proprio programma di compliance in materia di sicurezza delle informazioni e protezione dei dati tramite la piattaforma Dazr Compliance.
- Durata: per la durata dell'abbonamento del titolare, più il periodo di tolleranza successivo alla cessazione previsto dai Termini.
- Natura e finalità: hosting, conservazione, trasmissione, consultazione, cancellazione e le operazioni descritte nei Termini e nell'Informativa privacy.
- Tipo di dati personali: dati identificativi dei membri degli spazi di lavoro e degli auditor invitati (email, nome, ruolo); ove applicabile, dati identificativi di chi effettua segnalazioni tramite il portale pubblico e di chi segnala incidenti; dati di contatto del datore di lavoro e metadati operativi caricati dal titolare. Il titolare è responsabile di non caricare categorie particolari di dati salvo che la propria base giuridica lo consenta.
- Categorie di interessati: dipendenti, collaboratori e auditor esterni invitati dal titolare, nonché qualsiasi persona identificata nei contenuti di compliance che il titolare sceglie di caricare.

3. Obblighi del responsabile

1. Trattiamo i Dati personali del cliente soltanto su istruzione documentata del titolare. Le istruzioni consistono nell'utilizzo delle funzioni previste della piattaforma; se riteniamo che un'istruzione violi il GDPR o altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati, ne informiamo il titolare.
2. Garantiamo che le persone autorizzate al trattamento dei Dati personali del cliente si siano impegnate alla riservatezza.
3. Adottiamo tutte le misure richieste ai sensi dell'art. 32 GDPR (sicurezza del trattamento). Le misure attuali sono descritte nella sezione 7.
4. Rispettiamo le condizioni di cui all'art. 28, paragrafi 2 e 4, per ricorrere a sub-responsabili (si veda la sezione 6).
5. Tenendo conto della natura del trattamento e delle informazioni a nostra disposizione, assistiamo il titolare nell'adempimento dei suoi obblighi di dare seguito alle richieste degli interessati, di notificare le violazioni, di effettuare valutazioni d'impatto (DPIA) e consultazioni preventive con le autorità di controllo (art. 28, par. 3,

lett. e) ed f)).

6. Su scelta del titolare, al termine della prestazione dei servizi cancelliamo o restituiamo tutti i Dati personali del cliente e cancelliamo le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri ne preveda la conservazione.
7. Mettiamo a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto dell'art. 28 e consentiamo e contribuiamo alle attività di revisione, comprese le ispezioni (si veda la sezione 9).

4. Obblighi del titolare

- Il titolare garantisce di disporre di una base giuridica ai sensi dell'art. 6 (e, ove pertinente, dell'art. 9) per i dati personali che inserisce nello spazio di lavoro.
- Il titolare è responsabile dell'esattezza dei Dati personali del cliente e di dare seguito alle richieste degli interessati relative al proprio spazio di lavoro (le richieste che riceviamo le inoltriamo al titolare e prestiamo l'assistenza richiesta dall'art. 28, par. 3, lett. e)).
- Il titolare gestisce gli accessi - ruoli dei membri, inviti agli auditor, portale pubblico di segnalazione - tramite i controlli della piattaforma.

5. Trasferimenti internazionali

I Dati personali del cliente sono conservati e trattati su server nell'Unione europea. Vercel, Upstash e Namecheap sono società con sede negli Stati Uniti; qualora una di esse acceda ai Dati personali del cliente da fuori dell'UE, il trasferimento è disciplinato dalle clausole contrattuali tipo della Commissione europea (decisione 2021/914), modulo 3 (da responsabile a responsabile), con le misure supplementari descritte alla sezione 7. I sub-responsabili attuali e le relative regioni dei server sono indicati in /legal/it/subprocessors.

6. Sub-responsabili

1. Il titolare ci autorizza a ricorrere a sub-responsabili per erogare il servizio. L'elenco attuale è su /legal/it/subprocessors.
2. Informeremo il titolare del trattamento di eventuali aggiunte o sostituzioni previste con almeno 30 giorni di anticipo, tramite e-mail al titolare dello spazio di lavoro e a chiunque ci abbia chiesto, scrivendo a privacy@dazr.eu, di esserne informato.
3. Il titolare può opporsi per ragionevoli motivi attinenti alla protezione dei dati. Se non possiamo accogliere l'opposizione, il titolare può recedere dal servizio interessato e ottenere il rimborso pro rata della parte non goduta del periodo di fatturazione in corso.
4. Imponiamo a ogni sub-responsabile, mediante contratto scritto, obblighi in materia di protezione dei dati non meno protettivi di quelli previsti dal presente DPA, e restiamo responsabili nei confronti del titolare per l'adempimento degli obblighi del sub-responsabile.

7. Misure di sicurezza (art. 32)

- Cifratura. I record dello spazio di lavoro sono cifrati con AES-256-GCM dall'applicazione prima della conservazione, in aggiunta alla cifratura a riposo del fornitore di archiviazione, con chiavi derivate (HKDF-SHA-256) da una chiave principale a 256 bit custodita esclusivamente come segreto dell'ambiente di produzione, separata dai dati conservati; la chiave principale può essere sostituita, dopodiché un processo in background cifra nuovamente i record conservati. I file caricati (evidenze, documenti di policy e del profilo, allegati alle segnalazioni di violazioni) sono cifrati a riposo dal fornitore di archiviazione, conservati a indirizzi casuali non indovinabili e consegnati solo dopo un controllo degli accessi; anche i file SBOM del modulo Cyber Resilience Act sono cifrati dall'applicazione. Tutto il traffico avviene tramite HTTPS con HSTS in preload, senza alcuna alternativa in chiaro.
- Controllo degli accessi. Controllo degli accessi basato sui ruoli all'interno della piattaforma (titolare / amministratore / membro / auditor); sessioni auditor a tempo e revocabili. L'accesso operativo è limitato a un

piccolo team di assistenza tramite il portale di assistenza, che per scelta mostra solo metadati.
- Autenticazione. Accesso senza password con Google o Microsoft (OpenID Connect) o con un codice monouso inviato via e-mail; gli auditor confermano un codice monouso inviato via e-mail. Token di sessione firmati con HMAC e di durata limitata. Limitazione delle richieste su ogni endpoint pubblico, compreso l'accesso amministrativo.
- Resilienza e integrità. Un registro delle attività di ogni azione che modifica i dati, che conserva i 2.000-50.000 eventi più recenti a seconda del piano. Backup all'interno dell'UE. L'integrità dei dati conservati è verificata tramite tag di autenticazione AEAD; un testo cifrato alterato produce un errore e non viene restituito.
- Rete e intestazioni. Content-Security-Policy restrittiva con elenco di script inline autorizzati tramite hash, X-Frame-Options restrittivo, X-Content-Type-Options nosniff e HSTS preload.
- Gestione delle vulnerabilità. Le dipendenze sono bloccate a versioni specifiche; monitoriamo gli avvisi di sicurezza e applichiamo le patch con tempi proporzionati alla gravità.

8. Violazione dei dati personali

Se veniamo a conoscenza di una violazione dei dati personali che riguarda i Dati personali del cliente, ne informiamo il titolare dello spazio di lavoro senza ingiustificato ritardo e comunque entro 72 ore dal momento in cui ne siamo venuti a conoscenza (art. 33, par. 2). La notifica descrive, nella misura in cui sono noti: la natura della violazione, le probabili conseguenze, le misure adottate o proposte e il punto di contatto per ulteriori informazioni. Assistiamo il titolare nell'adempimento dei propri obblighi di notifica e comunicazione ai sensi degli artt. 33 e 34.

9. Attività di revisione

Il titolare (o un revisore terzo da esso incaricato) può verificare il nostro rispetto del presente DPA una volta ogni dodici mesi, con un preavviso scritto di almeno 30 giorni e durante l'orario lavorativo, con modalità che non interferiscano in modo irragionevole con la nostra attività e che rispettino la riservatezza dei dati degli altri clienti. Per verifiche ulteriori rispetto a tale limite possiamo addebitare un corrispettivo ragionevole. Se un obbligo di revisione ai sensi dell'art. 28, par. 3, lett. h) può essere soddisfatto con un'attestazione di terzi in nostro possesso, la forniremo in luogo di una verifica in loco.

10. Responsabilità

La responsabilità di ciascuna parte ai sensi del presente DPA è soggetta ai limiti previsti dai Termini di servizio. Tali limiti non si applicano ai danni subiti dagli interessati ai sensi dell'art. 82 GDPR.

11. Durata e cessazione

Il presente DPA resta in vigore finché trattiamo Dati personali del cliente e sopravvive alla cessazione dei Termini di servizio nella misura e per il tempo in cui deteniamo ancora tali dati. Le sezioni 8 (violazione), 9 (revisioni) e 12 (restituzione / cancellazione) sopravvivono alla cessazione.

12. Restituzione e cancellazione

Alla cessazione del servizio, il titolare può esportare i dati dello spazio di lavoro tramite gli strumenti di esportazione della piattaforma durante il periodo di tolleranza di 30 giorni previsto dai Termini. Trascorso tale periodo cancelliamo i Dati personali del cliente; i backup scadono secondo il nostro piano di conservazione. I documenti che siamo tenuti a conservare (ad esempio le fatture ai sensi della normativa italiana) sono conservati solo per la durata di tale obbligo.

13. Ordine di prevalenza

In caso di contrasto tra il presente DPA e i Termini di servizio o l'Informativa privacy, il presente DPA prevale in

materia di trattamento dei dati. Le clausole contrattuali tipo incorporate per eventuali trasferimenti extra UE prevalgono sia sul presente DPA sia sui Termini per le materie da esse disciplinate.

14. Comunicazioni

- A Dazr: privacy@dazr.eu (protezione dei dati) o security@dazr.eu (incidenti).
- Al titolare: l’indirizzo email del titolare dello spazio di lavoro registrato al momento della comunicazione.