

ATTO DI NOMINA A RESPONSABILE DEL TRATTAMENTO (ART. 28 GDPR)

FAC-SIMILE · Edizione aggiornata ad agosto 2026

Documento a cura della redazione di DB Agenzie Italia — dbagenzieitalia.it

AVVERTENZA

Questo è un fac-simile generico, redatto a scopo informativo e divulgativo. Non è un parere legale, non è calibrato su un caso concreto e non sostituisce l'assistenza di un professionista.

La materia è tecnica e le conseguenze di un atto incompleto ricadono su entrambe le parti: la soluzione migliore resta sempre rivolgersi a uno studio legale specializzato in protezione dei dati o a un responsabile della protezione dei dati, che possa cucire il documento sui trattamenti effettivamente svolti, sui sistemi utilizzati e sui trasferimenti eventualmente coinvolti.

Le parti tra parentesi quadre vanno compilate. Le note in corsivo sono spiegazioni per chi compila e vanno cancellate dal documento definitivo.

Tra:

[DENOMINAZIONE], con sede in [indirizzo, CAP, città], C.F./P. IVA [____], in persona di [nome e cognome], PEC [____] — di seguito «Titolare»

e

[DENOMINAZIONE / NOME E COGNOME], con sede in [indirizzo, CAP, città], C.F./P. IVA [____], PEC [____] — di seguito «Responsabile»

PREMESSO CHE

- fra le Parti è in essere il contratto del [data] avente ad oggetto [servizi di marketing digitale / gestione dei social / realizzazione e manutenzione del sito / gestione delle campagne pubblicitarie] (di seguito il «Contratto»);
- l'esecuzione del Contratto comporta il trattamento, da parte del Responsabile, di dati personali di cui il Titolare è titolare del trattamento;
- il Titolare intende designare il Responsabile ai sensi dell'articolo 28 del Regolamento (UE) 2016/679 (di seguito il «Regolamento»);
- il Responsabile presenta garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, come dichiarato all'art. 4 e documentato nell'Allegato B;

Le Parti convengono quanto segue. Il presente atto costituisce parte integrante del Contratto e prevale su di esso in caso di contrasto in materia di protezione dei dati personali.

Art. 1 — Oggetto e descrizione del trattamento

1.1 Il Titolare designa il Responsabile per il trattamento dei dati personali necessario all'esecuzione del Contratto.

1.2 Materia, durata, natura, finalità del trattamento, tipi di dati personali e categorie di interessati sono descritti nell'Allegato A, che costituisce parte integrante del presente atto.

1.3 Il Responsabile non tratta i dati personali per finalità proprie e non li utilizza per attività svolte a favore di terzi.

Nota per chi compila — L'Allegato A non è un accessorio: l'articolo 28 del Regolamento richiede espressamente che l'atto specifichi materia, durata, natura, finalità, tipo di dati e categorie di interessati. Un atto che rinvia genericamente al contratto senza descrivere il trattamento è incompleto.

Art. 2 — Istruzioni documentate

2.1 Il Responsabile tratta i dati personali soltanto su istruzione documentata del Titolare. Costituiscono istruzioni documentate il presente atto, il Contratto e le successive indicazioni impartite per iscritto.

2.2 Il Responsabile informa immediatamente il Titolare qualora ritenga che un'istruzione ricevuta violi il Regolamento o altre disposizioni in materia di protezione dei dati, e può sospendere l'esecuzione dell'istruzione fino a chiarimento.

2.3 Qualora il Responsabile sia tenuto a un trattamento in forza del diritto dell'Unione o dello Stato membro, ne informa il Titolare prima del trattamento, salvo che il diritto lo vieti per motivi di interesse pubblico.

Art. 3 — Riservatezza e persone autorizzate

3.1 Il Responsabile garantisce che le persone autorizzate al trattamento si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

3.2 Il Responsabile limita l'accesso ai dati alle sole persone che ne abbiano necessità per l'esecuzione del Contratto, con i permessi minimi necessari, e ne tiene evidenza.

3.3 Il Responsabile impartisce alle persone autorizzate istruzioni adeguate e ne verifica periodicamente la comprensione.

Art. 4 — Misure di sicurezza

4.1 Il Responsabile adotta le misure tecniche e organizzative adeguate a garantire un livello di sicurezza appropriato al rischio, ai sensi dell'articolo 32 del Regolamento. Le misure adottate sono descritte nell'Allegato B.

4.2 Le misure comprendono, in relazione ai rischi propri delle attività digitali: gestione degli accessi con credenziali individuali e autenticazione a più fattori ove disponibile; cifratura delle comunicazioni; separazione fra ambienti di prova e di produzione; copie di sicurezza e verifica della loro ripristinabilità; procedure per la gestione degli incidenti; aggiornamento dei sistemi utilizzati.

4.3 Il Responsabile riesamina periodicamente l'adeguatezza delle misure e informa il Titolare di ogni modifica sostanziale.

Nota per chi compila — L'Allegato B va compilato con le misure realmente adottate, non con un elenco di buone intenzioni. È il documento che, in caso di controllo o di incidente, dimostra che la valutazione è stata fatta: un elenco copiato e mai applicato produce l'effetto opposto a quello desiderato.

Art. 5 — Sub-responsabili

5.1 Il Responsabile non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del Titolare.

5.2 Il Titolare rilascia autorizzazione generale al ricorso ai sub-responsabili elencati nell'Allegato C. Il Responsabile informa il Titolare di eventuali modifiche riguardanti l'aggiunta o la sostituzione di sub-responsabili con preavviso di [n.] giorni, dando al Titolare la possibilità di opporsi.

5.3 Il Responsabile impone ai sub-responsabili, mediante contratto, obblighi di protezione dei dati non meno onerosi di quelli previsti dal presente atto, e risponde nei confronti del Titolare dell'inadempimento degli stessi.

Nota per chi compila — L'Allegato C è il punto che le agenzie compilano peggio. Rientrano fra i sub-responsabili i fornitori di hosting, le piattaforme di invio delle email, i sistemi di gestione dei contatti, gli strumenti di archiviazione e collaborazione, i servizi di analisi. Non elencarli non li fa sparire: li rende soltanto non autorizzati.

Art. 6 — Assistenza al Titolare

6.1 Il Responsabile assiste il Titolare, con misure tecniche e organizzative adeguate e nella misura in cui ciò sia possibile, per dare seguito alle richieste di esercizio dei diritti degli interessati.

6.2 Il Responsabile trasmette al Titolare senza ritardo, e comunque entro [n.] giorni lavorativi, ogni richiesta ricevuta direttamente da un interessato, astenendosi dal darvi autonomo seguito salvo istruzione contraria.

6.3 Il Responsabile assiste il Titolare nel garantire il rispetto degli obblighi in materia di sicurezza, notifica delle violazioni, valutazione d'impatto e consultazione preventiva, tenendo conto della natura del trattamento e delle informazioni a sua disposizione.

6.4 L'assistenza di cui al presente articolo è compresa nel corrispettivo del Contratto, salvo che richieda un impegno straordinario, nel qual caso è compensata secondo le tariffe ivi previste.

Art. 7 — Violazioni dei dati personali

7.1 Il Responsabile informa il Titolare senza ingiustificato ritardo e comunque entro [n.] ore dalla conoscenza di una violazione dei dati personali che riguardi i dati trattati per conto del Titolare.

7.2 La comunicazione contiene almeno: descrizione della natura della violazione, categorie e numero approssimativo di interessati e di registrazioni coinvolti, probabili conseguenze, misure adottate o proposte, punto di contatto per ulteriori informazioni.

7.3 Il Responsabile documenta la violazione e coopera con il Titolare per la gestione dell'evento, restando in capo al Titolare ogni valutazione in ordine alla notifica all'autorità di controllo e alla comunicazione agli interessati.

Nota per chi compila — Le [n.] ore del comma 7.1 non sono un dettaglio: il titolare ha un termine stretto per notificare all'autorità di controllo, e quel termine decorre da quando viene a conoscenza della violazione. Un termine di ventiquattro o quarantotto ore per il responsabile è la scelta più diffusa.

Art. 8 — Trasferimenti verso Paesi terzi

8.1 Il Responsabile non trasferisce dati personali verso Paesi terzi o organizzazioni internazionali senza previa autorizzazione scritta del Titolare, salvo che vi sia obbligato dal diritto applicabile.

8.2 I trasferimenti autorizzati alla data del presente atto, e le relative garanzie, sono indicati nell'Allegato C.

8.3 Il Responsabile informa il Titolare di ogni modifica che incida sulle garanzie applicabili ai trasferimenti in essere.

Nota per chi compila — Molti strumenti di uso quotidiano nel marketing digitale comportano trasferimenti verso Paesi terzi. Ignorare l'articolo 8 non elimina il problema: lo lascia soltanto non documentato, il che è la condizione peggiore in caso di controllo.

Art. 9 — Dimostrazione della conformità e verifiche

9.1 Il Responsabile mette a disposizione del Titolare le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dall'articolo 28 del Regolamento.

9.2 Il Responsabile consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da un incaricato da questi designato, con preavviso di almeno [n.] giorni, durante l'orario di lavoro e senza pregiudizio per la riservatezza dei dati di altri clienti.

9.3 Le verifiche possono svolgersi al massimo [n.] volte l'anno, salvo che siano conseguenti a una violazione dei dati o a una richiesta dell'autorità di controllo.

9.4 I costi di verifiche eccedenti quanto previsto al comma precedente sono a carico del Titolare.

Art. 10 — Registro dei trattamenti

10.1 Il Responsabile tiene, ove tenuto ai sensi dell'articolo 30, paragrafo 2, del Regolamento, il registro delle categorie di attività di trattamento svolte per conto del Titolare, e ne fornisce copia su richiesta.

Art. 11 — Cancellazione o restituzione dei dati

11.1 Alla cessazione del Contratto, e comunque su richiesta del Titolare, il Responsabile, a scelta di quest'ultimo: restituisce i dati personali in formato strutturato e di uso comune, oppure li cancella, unitamente alle copie esistenti.

11.2 L'operazione è completata entro [n.] giorni ed è confermata per iscritto al Titolare.

11.3 È fatta salva la conservazione dei dati nella misura in cui sia richiesta dal diritto dell'Unione o dello Stato membro, limitatamente a quanto necessario e per il tempo previsto.

11.4 Le copie di sicurezza contenenti dati personali sono cancellate secondo il ciclo di rotazione indicato nell'Allegato B, e il Responsabile ne dà atto nella conferma di cui al comma 11.2.

Nota per chi compila — Il comma 11.4 affronta una questione pratica quasi sempre ignorata: la cancellazione immediata dalle copie di sicurezza non è tecnicamente possibile in molti sistemi. Dichiarare il ciclo di rotazione è più corretto che promettere una cancellazione istantanea che non avverrà.

Art. 12 — Responsabilità e durata

12.1 Ciascuna Parte risponde secondo quanto previsto dall'articolo 82 del Regolamento.

12.2 Il presente atto ha efficacia dalla sottoscrizione e per tutta la durata del Contratto. Gli obblighi che per loro natura sono destinati a permanere restano efficaci anche dopo la cessazione.

12.3 Le eventuali limitazioni di responsabilità previste dal Contratto non si applicano agli obblighi derivanti dal presente atto nella misura in cui ciò sia inderogabilmente escluso dalla normativa applicabile.

Art. 13 — Legge applicabile e foro competente

13.1 Il presente atto è regolato dalla legge italiana e dal Regolamento.

13.2 Per ogni controversia è competente in via esclusiva il Foro di [____], fermi restando i diritti degli interessati e le competenze delle autorità di controllo.

Luogo e data: [____]

Il Titolare	Il Responsabile
_____	_____

Allegato A — Descrizione del trattamento

Compilare con riferimento ai trattamenti effettivamente svolti. Le righe che non ricorrono vanno eliminate, non lasciate in bianco.

Elemento	Contenuto
Materia del trattamento	[es. gestione dei contatti raccolti tramite il sito e le campagne]
Durata	[per tutta la durata del Contratto]
Natura e finalità	[raccolta, registrazione, conservazione, consultazione, comunicazione a piattaforme, cancellazione — per le finalità di ____]
Tipi di dati personali	[dati anagrafici e di contatto, dati di navigazione e identificativi online, dati relativi agli acquisti, contenuto delle comunicazioni ricevute]
Categorie particolari di dati	[nessuna / indicare quali e con quale base giuridica]
Categorie di interessati	[clienti, potenziali clienti, iscritti alla newsletter, visitatori del sito, utenti dei social]
Sistemi e strumenti utilizzati	[piattaforma del sito, strumento di invio email, sistema di gestione dei contatti, piattaforme pubblicitarie, strumenti di

Elemento	Contenuto
	analisi]
Luogo del trattamento	[]

Allegato B — Misure tecniche e organizzative

Indicare le misure realmente adottate. Le voci non applicabili vanno cancellate.

Ambito	Misura adottata
Controllo degli accessi	[credenziali individuali, autenticazione a più fattori, revisione periodica dei permessi]
Gestione delle credenziali	[gestore di password, divieto di condivisione su canali non protetti]
Cifratura	[protocollo sicuro sui siti, cifratura dei dispositivi, cifratura degli archivi]
Copie di sicurezza	[frequenza, luogo, ciclo di rotazione, verifica di ripristinabilità]
Separazione degli ambienti	[ambiente di prova senza dati reali o con dati resi anonimi]
Aggiornamenti	[frequenza degli aggiornamenti di sicurezza dei sistemi utilizzati]
Gestione degli incidenti	[procedura, referente, tempi di comunicazione]
Formazione	[periodicità della formazione delle persone autorizzate]
Dispositivi	[protezione dei dispositivi, cancellazione sicura in caso di dismissione]
Cancellazione	[procedura di cancellazione e tempi]

Allegato C — Sub-responsabili autorizzati e trasferimenti

Sub-responsabile	Servizio	Dati trattati	Luogo del trattamento	Garanzie per i trasferimenti
[fornitore di hosting]	[ospitalità del sito e della base dati]	[]	[]	[non applicabile / clausole contrattuali tipo / decisione di adeguatezza]
[piattaforma di invio email]	[invio delle comunicazioni]	[]	[]	[]
[sistema di gestione dei contatti]	[archiviazione dei contatti]	[]	[]	[]
[piattaforme pubblicitarie]	[campagne e pubblici]	[]	[]	[]
[strumenti di analisi]	[misurazione]	[]	[]	[]
[archiviazione e collaborazione]	[gestione dei file di progetto]	[]	[]	[]

Prima di firmare: verifica finale

- L'Allegato A descrive materia, durata, natura, finalità, tipi di dati e categorie di interessati?
- L'Allegato B contiene le misure realmente adottate e non un elenco copiato?
- L'Allegato C elenca tutti i fornitori che accedono ai dati, compresi hosting, invio email e strumenti di archiviazione?
- I trasferimenti verso Paesi terzi sono stati verificati e documentati?
- Il termine per la comunicazione delle violazioni è compatibile con gli obblighi del Titolare?
- È previsto come si procede alla cancellazione dalle copie di sicurezza?
- L'atto è allegato al contratto principale e vi si fa espresso riferimento?
- Le persone autorizzate al trattamento sono state effettivamente istruite?

Avvertenza finale

Questo documento è un fac-simile generico a scopo informativo, redatto dalla redazione di DB Agenzie Italia sulla base della normativa vigente alla data di agosto 2026. Non costituisce un parere legale, non è personalizzato sul caso concreto e non sostituisce l'assistenza di un professionista abilitato.

La materia della protezione dei dati è tecnica e le conseguenze di un atto incompleto ricadono su entrambe le parti: la soluzione migliore resta sempre rivolgersi a uno studio legale specializzato o a un responsabile della protezione dei dati, che possa verificare i trattamenti effettivamente svolti, i sistemi utilizzati e i trasferimenti coinvolti.

DB Agenzie Italia non risponde dell'uso che viene fatto di questo documento né delle conseguenze derivanti dalla sua adozione senza adeguata verifica professionale.