

DPA - Nomina responsabile del trattamento - ITA

Contratto di nomina a responsabile del trattamento

ai sensi dell'art. 28 del Regolamento Generale sulla Protezione dei Dati Personali (RGDP) tra

.....

- il Titolare -

[ove applicabile: rappresentante nell'Unione ai sensi dell'art. 27 RGDP:

.....]

.....

- il Responsabile -

[ove applicabile: rappresentante nell'Unione ai sensi dell'art. 27 RGDP:

.....]

1. Oggetto, durata, dati personali trattati e categorie di interessati

(1) Oggetto

- Il presente accordo ha per oggetto la nomina del Responsabile ed il conferimento allo stesso delle istruzioni relative al trattamento dei dati personali. Le attività di trattamento che il Responsabile potrà effettuare sono

limitate a quelle strettamente necessarie per il raggiungimento dello scopo del contratto principale sottoscritto dalle parti in data *[inserire data]*.

[oppure

- Il Responsabile svolgerà, per conto del Titolare, le seguenti attività di trattamento:

.....
.....
.....
.....
.....]

(2) Durata

- La durata di questa nomina è pari alla durata del contratto principale.

[alternativa: specificare la durata]

(3) Categorie di dati personali

- Le categorie di dati personali trattati sono:
 - dati identificativi (e.g. nome, cognome, email)
 - dati statistici o altri dati di navigazione in rete (e.g. dati trattati tramite strumenti analitici etc.)
 - storico acquisti
 - dati di fatturazione, contabilità e pagamenti
 - altri:..... *[specificare in dettaglio, specialmente se il trattamento riguarda dati genetici, biometrici o altri dati "sensibili"]*

(4) Categorie di interessati

- I dati personali raccolti e trattati si riferiscono a:
 - clienti
 - clienti potenziali
 - utenti internet
 - dipendenti, collaboratori
 - consulenti interni
 - agenti e mandatari
 - altri:..... *[specificare]*

2. Trattamento all'interno della UE e dello SEE

(1) Il Responsabile s'impegna a non effettuare alcun trasferimento di Dati Personali

all'estero (*i.e.* al di fuori del territorio dello SEE) se non previa autorizzazione scritta del Titolare e su istruzione documentata e specifica di quest'ultimo.

[opzione 1 no trasferimento]

(2) Le parti si danno reciprocamente atto che il trattamento dei dati personali oggetto del presente accordo non avverrà al di fuori dello SEE.

[opzione 2 solo se uno o più trattamenti hanno luogo extra EU]

(2) Alla data di stipula del presente accordo, il Titolare riconosce di essere stato informato che le seguenti attività di trattamento effettuate dal Responsabile per suo conto, avverranno al di fuori dello SEE. Tali trattamenti, in questa sede specificamente autorizzati dal Titolare, avranno luogo negli stati di seguito elencati e secondo le basi di legittimità del trasferimento stabilite agli artt. 45 e ss. RGDP, come di volta in volta applicabili a ciascun trattamento.

| | A | B | C |
|---|------------------------|-----------------------------------|--|
| 1 | stato | trattamento | base giuridica per il trasferimento |
| 2 | <i>p. es. Svizzera</i> | <i>p. es. servizio di hosting</i> | <i>p. es. decisione di adeguatezza</i> |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |

(Le principali basi di legittimità per il trasferimento dei dati all'estero sono:

- *decisione di adeguatezza della Commissione Europea (art. 45 par. 3);*
- *norme vincolanti d'impresa (art. 46 par. 2 punto b) e art. 47);*
- *clausole contrattuali standard (art. 46 par. 2 punti c) e d);*
- *codici di condotta (art. 46 par. 2 punto e) e art. 40);*
- *meccanismo di certificazione (art. 46 par. 2 punto f) e art. 42).*

occorre selezionare la base di legittimità applicabile a ciascun trattamento che avviene all'estero)

3. Misure tecniche ed organizzative

(1) Prima di dare esecuzione alla presente nomina, il Responsabile sarà tenuto ad implementare tutte le misure tecniche ed organizzative adeguate per la protezione dei dati personali ed a consegnare al Titolare un documento che descrive

dettagliatamente tutte le misure di sicurezza adottate dallo stesso Responsabile, anche con specifico riferimento all'esecuzione del presente contratto. Tali misure sono soggette allo scrutinio del Titolare ed alla sua previa approvazione. Se approvate dal Titolare, tali misure, cristallizzate nel documento di cui al paragrafo precedente, divengono parte integrante e sostanziale di questo contratto di nomina e s'intendono integralmente richiamate nello stesso. Qualora mediante ispezione o revisione il Titolare dovesse constatare la necessità di modificarle, le modifiche saranno apportate di concerto tra le parti.

(2) Il Responsabile garantisce la sicurezza del trattamento ai sensi degli artt. 28 par. 3 punto c) e 32 RGDP, in particolare ai sensi dell'art. 5 par. 1 e par. 2 RGDP. Tali misure devono garantire la sicurezza dei dati ed un livello di protezione adeguato al rischio per la confidenzialità, integrità, disponibilità e resilienza dei sistemi. Ai sensi dell'art. 32 par. 1 RGDP, nel valutare il livello di adeguatezza delle misure di sicurezza deve tenersi conto dello stato dell'arte, i costi di realizzazione, la natura, l'oggetto e gli scopi del trattamento, così come la probabilità di una violazione di dati personali e la gravità dei rischi da essa potenzialmente derivanti per i diritti e le libertà delle persone fisiche.

(3) Le misure tecniche ed organizzative sono soggette a evoluzione e progresso tecnico e tecnologico. Pertanto, il Responsabile può adottare opportune misure alterative adeguate al mutato contesto tecnologico. In tali casi, il livello di sicurezza del trattamento non può essere ridotto. Ogni modifica sostanziale dev'essere documentata.

4. Diritti degli interessati

(1) Il Responsabile d'impegna a cooperare con il Titolare ed a fornire la più ampia assistenza, nei limiti in cui ciò è ragionevole o possibile, al fine di agevolare il Titolare nel riscontro delle richieste degli interessati per l'esercizio dei loro diritti.

(2) In particolare, il Responsabile s'impegna a **(i)** comunicare immediatamente al Titolare ciascuna richiesta pervenutagli dagli interessati in merito all'esercizio dei loro diritti e, se fattibile o del caso, ad **(ii)** assistere il Titolare nel progettare e implementare tutte le misure tecniche ed organizzative necessarie per rispondere a tali richieste.

(3) Fermo restando che la responsabilità di riscontrare e soddisfare le richieste degli interessati grava esclusivamente sul Titolare, il Responsabile può essere

incaricato di evadere alcune specifiche richieste, sempre che ciò non richieda sforzi sproporzionati e su istruzioni specifiche fornite per iscritto dal Titolare.

5. Altri obblighi del Responsabile

In aggiunta alle previsioni di questo contratto, il Responsabile è tenuto a rispettare tutte i requisiti di legge previsti dagli artt. 28-33 RGDP. A tal fine, il Responsabile garantisce quanto segue:

- **Nomina di un Responsabile per la Protezione dei Dati Personali (Data Protection Officer, DPO)**

L'attuale DPO è:

[ESTREMI DI CONTATTO].....

.....

.....

Il Responsabile segnalerà al Titolare senza indebito ritardo ogni cambio di DPO.

[*oppure* Il Responsabile non è tenuto a nominare un DPO. Il sig./La sig.ra [inserire: nome, cognome, settore di appartenenza, telefono, email] funge da persona di riferimento su incarico del Responsabile.]

- [*→ selezionare solo se applicabile*] **Nomina di un Rappresentante nell'Unione**

Essendo il Responsabile stabilito al di fuori della UE e dello SEE,

[ESTREMI DI CONTATTO].....

.....

.....

è nominato/a rappresentante nell'Unione ai sensi dell'art. 27 par. 1 RGDP.

- **Confidenzialità**

Le attività di trattamento regolate da questo contratto di nomina dovranno essere svolte solo da dipendenti, collaboratori o incaricati previamente istruiti dal Responsabile sul corretto trattamento di dati personali e contrattualmente soggetti ad obbligo di confidenzialità ai sensi degli artt. 28 par. 3 (b) e 32 RGDP. Il Responsabile, così come chiunque agisca sotto la sua autorità ed ha abbia accesso a dati personali, non deve trattare dati personali

se non è stato istruito in tal senso dal Titolare, anche a mezzo della presente nomina, salvo che per espressa previsione di legge.

- **Misure tecniche ed organizzative**

Attuazione e rispetto di opportune misure tecniche ed organizzative nel contesto di questo contratto di nomina, ai sensi di quanto specificato dall'art. 32 RGDP. Il Responsabile controlla periodicamente i processi interni e le misure tecniche e organizzative per assicurare che il trattamento nella sua area di competenza sia conforme ai requisiti della normativa sulla protezione dei dati personali e dei diritti degli interessati. Il Responsabile garantisce al Titolare la verificabilità delle misure tecniche e organizzative nell'ambito dei suoi poteri di controllo di cui al punto 7. del presente contratto.

- **Collaborazione con le autorità di controllo**

Il Titolare ed il Responsabile cooperano, su richiesta, con l'autorità di controllo. Il Titolare è immediatamente informato di tutte le ispezioni e misure eseguite dall'autorità di controllo, nella misura in cui esse si riferiscono alle attività svolte in base a questo contratto. Ciò vale anche nel caso in cui il Responsabile sia sottoposto a o coinvolto in una indagine da parte di un'autorità competente in relazione a violazioni di qualsiasi disposizione in materia di trattamento di dati personali nello svolgimento di attività ai sensi di questo contratto. Nella misura in cui il Titolare sia soggetto a ispezione da parte dell'autorità di controllo, sanzione amministrativa pecuniaria, misura cautelare o procedimento penale, pretesa da parte di un interessato o di terzi o qualsiasi altra azione legale in collegamento con il trattamento di dati da parte del Responsabile ai sensi della presente nomina, il Responsabile farà tutto il possibile per sostenere il Titolare.

6. Altri responsabili del trattamento

(1) Il Titolare autorizza fin d'ora il Responsabile a ricorrere a terzi responsabili del trattamento. I sub-responsabili come richiesto dalla normativa, dovranno essere soggetti ai medesimi obblighi contrattuali contenuti nel presente contratto ai sensi dell'art. 28 par. 4 RGDP.

[punto (2) facoltativo, se già esistono sub-responsabili]

(2) Alla data di sottoscrizione del presente accordo, le parti si danno reciprocamente atto che il Responsabile si avvale dei seguenti sub-responsabili, con

i quali s'impegna a concludere accordi contrattuali conformi al dettato dell'art. 28, par. 4 RGDP:

| | A | B | C |
|---|-----------------------------------|------------------------|---|
| 1 | Sub-responsabile (società) | indirizzo/stato | attività di trattamento delegata |
| 2 | | | |
| 3 | | | |

(3) Resta inteso che la comunicazione dei dati ad un terzo responsabile potrà avvenire solo una volta che tutte le condizioni per la nomina di cui al punto (1) del presente paragrafo siano realizzate.

(4) Il Responsabile dovrà mantenere aggiornato un elenco dei sub-responsabili. Qualsiasi modifica a tale elenco deve essere segnalata al Titolare senza indebito ritardo, dando al Titolare la facoltà di opporsi. In caso di opposizione, il Responsabile ha diritto di recedere dal contratto con il Titolare senza preavviso.

(5) Il Responsabile risponde integralmente dell'operato dei sub-responsabili nei confronti del Titolare.

(6) Qualora un sub-responsabile presti la propria opera al di fuori della UE/SEE, il Responsabile deve garantire la liceità del trasferimento dati al di fuori dello SEE, come descritto al punto 2. del presente contratto.

7. Poteri di controllo del Titolare

(1) Il Titolare ha il diritto di svolgere ispezioni o farle svolgere ad un revisore di volta in volta incaricato. Il revisore dovrà valutare il rispetto di questo contratto di nomina da parte del Responsabile nel corso delle proprie attività d'impresa per mezzo di verifiche causali, le quali dovranno di regola essere notificate in anticipo.

(2) Il Responsabile deve permettere al Titolare di verificare l'adempimento alle proprie obbligazioni, come previsto dall'art. 28 RGDP. Su richiesta, il Responsabile fornisce al Titolare ogni informazione necessaria nonché, segnatamente, la prova di aver adottato le misure tecniche ed organizzative.

(3) La prova dell'adozione di tali misure, che potranno riferirsi anche ad attività non rientranti nell'ambito di questo contratto, potrà essere fornita anche per mezzo di

- conformità a codici di condotta approvati ai sensi dell'art. 40 RGDP;
- certificazioni emesse in base ad un meccanismo di certificazione approvato ai sensi dell'art. 42 RGDP;
- attuali certificazioni di revisori, relazioni o estratti di relazioni redatte da organismi indipendenti (p. es. revisori, responsabili della protezione dei dati personali, dipartimento della sicurezza IT, revisori della protezione dei dati)
- idonee certificazioni emesse da revisori della sicurezza IT o della protezione dei dati personali

(4) Il Responsabile può addebitare al Titolare un compenso di entità ragionevole per l'esecuzione delle ispezioni.

8. Assistenza al Titolare

(1) Il Responsabile assiste il Titolare nell'adempimento degli obblighi relativi alla sicurezza dei dati personali, nella segnalazione di violazioni dei dati, nelle valutazioni d'impatto sulla protezione dei dati e nelle consultazioni preventive di cui agli articoli da 32 a 36 RGDP, tra l'altro

- garantendo adeguati standard di protezione mediante misure tecniche e organizzative, tenendo conto della natura, delle circostanze e delle finalità del trattamento, della probabilità di violazioni dei dati e della gravità del rischio per le persone fisiche che ne può derivare
- garantendo l'immediata individuazione delle violazioni
- riferendo senza indebito ritardo al Titolare ogni violazioni di dati
- assistendo il Titolare nell'evadere le richieste degli interessati di esercizio dei loro diritti

(2) Il Responsabile può richiedere al Titolare un compenso ragionevole per servizi di assistenza che non sono compresi nella descrizione dei servizi e che non sono dovuti a errori, violazioni o condotte imputabili al Responsabile.

9. Poteri direttivi del Titolare

(1) Il Responsabile non tratta alcun dato personale ai sensi della presente nomina se non su istruzione documentata del Titolare, salvo che sia obbligato a farlo dal diritto dell'Unione o degli Stati membri.

(2) Nel caso in cui il Titolare richieda una modifica del trattamento dei dati personali previsto dalle istruzioni documentate di cui al punto 2, il Responsabile informa immediatamente il Titolare qualora ritenga che tale modifica possa comportare violazioni delle disposizioni in materia di protezione dei dati. Il Responsabile può astenersi dallo svolgere qualsiasi attività che possa dar luogo a tale violazione.

10. Responsabilità

(1) Ciascuna parte del presente contratto si impegna a risarcire l'altra parte per danni o spese derivanti dal proprio inadempimento colposo del presente contratto, compreso qualsiasi inadempimento colposo commesso dal proprio rappresentante legale, sub-contraenti, dipendenti o altri agenti. Inoltre, ciascuna parte si impegna a tenere indenne l'altra parte da qualsiasi pretesa fatta valere da terzi a causa di o in relazione a qualsiasi violazione colposa commessa dall'altra parte.

(2) Resta ferma la previsione dell'art. 82 RGDP.

11. Distruzione e restituzione dei dati personali

(1) Il Responsabile non crea copie o duplicati dei dati ad insaputa e senza il consenso del Titolare, fatta eccezione per le copie di sicurezza, nella misura in cui siano necessarie a garantire la corretta elaborazione dei dati, nonché per i dati la cui conservazione è prevista dalla legge.

(2) A conclusione della prestazione di servizi, a scelta del Titolare, il Responsabile cancella in maniera conforme alla protezione dei dati o restituisce al Titolare tutti i dati personali raccolti ed elaborati ai sensi della presente nomina, a meno che le disposizioni di legge applicabili non richiedano un'ulteriore conservazione dei dati personali.

(3) In ogni caso, il Responsabile può conservare tutte le informazioni utili a dimostrare la corretta e conforme esecuzione delle attività di trattamento anche oltre la cessazione del contratto.

(4) La documentazione di cui al punto (3) che precede, deve comunque essere conservata dal Responsabile in ottemperanza ai periodi di conservazione previsti dalla legge o altrimenti stabiliti. Il Responsabile può consegnare tale

documentazione al Titolare al termine della durata del contratto per sollevarsi dall'obbligo contrattuale di conservazione.