# ESEMPI DI NOMINE FORMALI

# Clausole Contrattuali (art. 28 e art. 30, co.1 e 2 GDPR)

# Titolare – Responsabile

**FINALITÀ:** Il presente accordo è stipulato fra il Titolare e il Responsabile. Nel caso si configuri un rapporto con un terzo soggetto in qualità di sub responsabile andranno inserite le relative parti anche con separato addendum qualora l’accordo ai sensi dell’art. 28 lo preveda.

# Fac-simile

**Accordo di designazione fra Titolare e Responsabile**

**Art. 28 REGOLAMENTO (UE) 2016/679**

##### TRA

In qualità di TITOLARE DEL TRATTAMENTO, [specificare denominazione, sede, codice fiscale, partita IVA, riferimenti di contatto, eventuale Nome e Cognome del legale rappresentante in caso di persona giuridica],

E

In qualità di RESPONSABILE DEL TRATTAMENTO [specificare denominazione, sede, codice fiscale, partita IVA, riferimenti di contatto, eventuale Nome e Cognome del legale rappresentante in caso di persona giuridica],

di seguito entrambi indicati congiuntamente “le Parti”.

##### ART. 1 TRATTAMENTO DEI DATI PERSONALI

Ai sensi e per gli effetti della normativa in materia di protezione dei dati personali (Reg. UE n. 2016/679, di seguito "GDPR", nonché D. lgs. 196/2003 da ultimo novellato dal D. lgs. 101/2018, di seguito "Codice Privacy") e in relazione alle operazioni che vengono eseguite per lo svolgimento delle attività previste dal [citare il contratto/mandato], [Titolare], in qualità di Titolare, designa [Responsabile], Responsabile del trattamento, ai sensi dell’articolo 28 GDPR.

I trattamenti affidati dal Titolare al Responsabile riguardano [descrivere *le operazioni di trattamento, la tipologia di dati trattati le categorie e numerosità degli interessati*]

I trattamenti effettuati per conto del Titolare dal Responsabile cesseranno al completamento del contratto ovvero, in caso di sua risoluzione, per qualsiasi altro motivo.

*Il* Responsabile fornisce garanzie sufficienti, in particolare in termini di conoscenze specialistiche, affidabilità e risorse, per attuare misure tecniche e organizzative che soddisfino i requisiti normativi sanciti dal GDPR, dal Codice Privacy e da qualsiasi altra norma connessa inerente al trattamento dei dati personali, comprese le misure di sicurezza del trattamento, per garantire la riservatezza e la protezione dei diritti degli interessati.

*Il* Responsabile è tenuto ad assicurare e far assicurare ai propri dipendenti, collaboratori e responsabili ulteriori (qualora autorizzati e nominati), la riservatezza e il corretto trattamento delle informazioni, dei documenti e degli atti amministrativi dei quali venga a conoscenza durante l’esecuzione della prestazione.

In tal senso il Responsabile si impegna a impartire precise istruzioni a tutti i soggetti coinvolti nei trattamenti svolti per conto dello scrivente Titolare. In particolare, il Responsabile si impegna a:

1. adottare e mantenere aggiornato il registro dei trattamenti ai sensi dell’art. 30, co. 2 del GDPR;
2. non mettere in atto, per nessun motivo, trattamenti di dati diversi da quelli autorizzati dal Titolare oggetto del presente contratto/convenzione;
3. fornire agli autorizzati al trattamento (a sub-responsabili) le pertinenti istruzioni;
4. nominare gli autorizzati che svolgono le funzioni di “amministratore di sistema”;
5. collaborare alla eventuale redazione di DPIA su trattamenti affidati alla sua responsabilità dal Titolare;
6. collaborare con il Titolare nelle operazioni di Audit sulla attività del Responsabile, a tal fine impegnandosi a manutenere: il registro dei trattamenti ai sensi dell’articolo 30 c.2; le evidenze documentali delle istruzioni impartite ad addetti e sub responsabili da lui designati e a mantenere aggiornato il catalogo degli asset (comprese le applicazioni utente e quelle di gestione dei sistemi e degli apparati), delle minacce e delle misure di sicurezza adottate e delle loro correlazioni;
7. predisporre e trasmettere, con cadenza annuale e comunque ogni qualvolta ciò appaia necessario, al Titolare una relazione in merito alle misure di sicurezza adottate al fine di renderle e mantenerle sempre adeguate e aggiornate rispetto alla evoluzione delle minacce e sulla base dei riscontri derivanti dalla registrazione continua e puntuale degli incidenti eventualmente occorsi;
8. assistere e garantire il titolare del trattamento, nell’evasione delle richieste e nel rispetto dei tempi previsti, nei rapporti con l’Autorità Garante per la protezione dei dati personali;
9. assistere il Titolare al fine di dare seguito alle richieste per l’esercizio dei diritti degli interessati ai sensi degli artt. 15 a 22 del GDPR, qualora gli interessati esercitino tale diritto verso il Responsabile. In questo caso il Responsabile è tenuto ad inoltrare tempestivamente e comunque nel più breve tempo possibile, le istanze al Titolare al fine di fornire adeguato riscontro agli interessati nei tempi prescritti;
10. garantire al Titolare, su richiesta, l’accesso e la disponibilità permanente ai dati, su formati e strumenti di uso comune che ne garantiscano la fruizione da parte del titolare, consentendo in tal modo la piena continuità dei servizi oggetto del contratto/convenzione e in modo che mai si configuri una situazione da parte del Titolare di diminuzione o di perdita della possibilità di gestire i servizi e relativi dati in autonomia senza dover forzatamente ricorrere Responsabile.

**ART. 2 MISURE DI SICUREZZA DA ADOTTARE**

Tenuto conto della natura, dell’oggetto, del contesto e delle finalità del trattamento, il Responsabile del trattamento deve mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio e il rispetto degli obblighi di cui all’art. 32 del GDPR. Tali misure comprendono tra le altre, se del caso: la pseudonimizzazione e la cifratura dei dati personali; la capacità di assicurare, su base permanente, la riservatezza, l’integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l’accesso dei dati in caso di incidente fisico o tecnico; una procedura per testare, verificare e valutare regolarmente l’efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

A tal fine si impegna ad assistere e assicurare la piena, fattiva e puntuale collaborazione al titolare del trattamento e in particolare al Security IT Manager del Titolare.

1. il Responsabile informa tempestivamente e, in ogni caso senza ingiustificato ritardo dall’avvenuta conoscenza, il Titolare di ogni violazione di dati personali (cd. data breach); tale notifica è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del GDPR, per permettere al Titolare del trattamento, ove ritenuto necessario, di notificare questa violazione all’Autorità Garante per la protezione dei dati personali, entro il termine di 72 ore da quando il Titolare ne viene a conoscenza; nel caso in cui il Titolare debba fornire informazioni aggiuntive all’Autorità di controllo, il Responsabile supporterà il Titolare nella misura in cui le informazioni richieste e/o necessarie per l’Autorità di controllo siano esclusivamente in possesso del Responsabile e/o di suoi sub-Responsabili.
2. Sarà obbligo del Titolare del trattamento vigilare, durante tutta la durata del trattamento, sul rispetto degli obblighi previsti dalle presenti istruzioni e dal GDPR sulla protezione dei dati da parte del Responsabile del trattamento, nonché a supervisionare l’attività di trattamento dei dati personali effettuando audit, ispezioni e verifiche periodiche sull’attività posta in essere dal Responsabile. A tal fine il Responsabile del trattamento metterà a disposizione, su richiesta del titolare del trattamento, tutte le informazioni necessarie per dimostrare il rispetto degli obblighi derivanti dal GDPR, agevolando il contributo alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento o da un altro soggetto da questi incaricato, ivi compresa, se necessario, l'attività di monitoraggio e controllo da parte del DPO e del Security IT Manager (se nominato) sulle misure di sicurezza attuate e sulla loro efficacia, fornendo tutta la documentazione che sarà richiesta e collaborando attivamente alle attività di rilevazione e misura.
3. Comunicare al Titolare il nome e i dati del proprio “Responsabile della protezione dei dati” (DPO), qualora, in ragione dell’attività svolta, ne abbia designato uno conformemente all’articolo 37 del GDPR; il Responsabile della protezione dei dati personali (DPO) del Fornitore/Responsabile collabora e si tiene in costante contatto con il Responsabile della protezione dei dati (DPO) del Titolare.
4. Comunicare al Titolare, al DPO *e al Security Manager (se nominato*) il nome e i riferimenti di contatto del proprio Responsabile della sicurezza IT,

**ART. 3 SUB-RESPONSABILI**

Nel caso in cui, per l’esecuzione delle attività affidate, il Responsabile del trattamento intenda avvalersi di ulteriori soggetti, è tenuto a darne preventiva comunicazione al Titolare del trattamento. Solo previa autorizzazione scritta da parte del Titolare, il Responsabile potrà procedere alla nomina dei sub-responsabili.

##### Tale nomina dovrà avvenire mediante apposito contratto o altro atto giuridico conforme a quanto previsto dall’art. 28 del GDPR, nel quale siano riportati:

##### una descrizione sintetica delle attività delegate,

##### le operazioni di trattamento previste,

##### la tipologia di dati personali trattati,

##### le categorie e la numerosità degli interessati,

##### obblighi equivalenti a quelli imposti dal Titolare al Responsabile.

##### Il Responsabile dovrà inoltre accertarsi che ciascun sub-responsabile offra garanzie sufficienti in termini di competenza, conoscenze specialistiche, affidabilità e risorse per l’adozione di adeguate misure tecniche e organizzative, così da assicurare la conformità del trattamento ai principi del GDPR.

##### Resta inteso che, in caso di inadempimento da parte del sub-responsabile rispetto agli obblighi in materia di protezione dei dati personali, il Responsabile risponde integralmente nei confronti del Titolare per ogni violazione commessa dal sub-responsabile stesso.

##### ART. 4 PENALI

Il Responsabile che agisce in modo difforme o contrario alle legittime istruzioni del Titolare, oppure adotta misure di sicurezza inadeguate rispetto al rischio del trattamento, risponde del danno causato agli “interessati”. In tal caso, il Titolare potrà risolvere il contratto/convenzione, salvo il risarcimento del maggior danno.

Data e Firme

# Clausole Contrattuali (art. 26)

# Contitolarità

**FINALITÀ:** Il presente accordo è stipulato fra due o più Titolari giuridicamente diversi nel rapporto che si viene ad istaurare per il trattamento di dati personali in cui singolarmente o congiuntamente concorrono - ognuno per proprie parti - all’interno di una unica finalità e determinano congiuntamente i mezzi attraverso i quali eseguire i trattamenti. Questi soggetti devono sottoscrivere un accordo, nel quale si dà atto degli impegni e delle responsabilità nell’eseguire trattamenti all’interno del rapporto di contitolarità.

# Fac-simile

**Accordo di contitolarità**

**Art. 26 REGOLAMENTO (UE) 2016/679**

##### TRA

In qualità di TITOLARE 1, [specificare denominazione, sede, codice fiscale, partita IVA, riferimenti di contatto, eventuale Nome e Cognome del legale rappresentante in caso di persona giuridica],

E

In qualità di TITOLARE 2 [specificare denominazione, sede, codice fiscale, partita IVA, riferimenti di contatto, eventuale Nome e Cognome del legale rappresentante in caso di persona giuridica],

E

In qualità di TITOLARE 3 [specificare denominazione, sede, codice fiscale, partita IVA, riferimenti di contatto, eventuale Nome e Cognome del legale rappresentante in caso di persona giuridica],

E

In qualità di TITOLARE “N” [specificare denominazione, sede, codice fiscale, partita IVA, riferimenti di contatto, eventuale Nome e Cognome del legale rappresentante in caso di persona giuridica],

di seguito congiuntamente “i Contitolari”.

##### Premesso che:

* Il GDPR relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, applicabile definitivamente a tutti gli stati membri dal 25 maggio 2018, ha introdotto varie novità, tra le quali assume particolare il principio di accountability, inteso come elemento di responsabilizzazione dei soggetti coinvolti nel trattamento dei dati;
* Il Titolare del trattamento dei dati personali, in continuità con il D.lgs. 196/2003 “Codice in materia di protezione dei dati personali”, come modificato dal D.lgs. 101/2018, rappresenta, nell’ambito del quadro normativo in materia di protezione dei dati, il soggetto a cui competono le decisioni relative alle finalità e ai mezzi del trattamento;
* il GDPR non esclude la possibilità che in talune circostanze uno o più soggetti possano determinare congiuntamente le finalità e i mezzi del trattamento dei dati. In tal senso si esprime l’art. 26 del GDPR che configura tali soggetti quali “contitolari” del trattamento con rispettive responsabilità da ripartire e definire in modo trasparente in un *accordo* interno;
* come evidenziato anche dal parere n. 1/2010 del WP29, sussiste la contitolarità *“quando varie parti determinano, per specifici trattamenti, o la finalità o quegli aspetti fondamentali degli strumenti che caratterizzano il titolare del trattamento”* tenendo conto che *“la partecipazione delle parti alla determinazione congiunta può assumere varie forme e non deve essere necessariamente ripartita in modo uguale”;*
* in relazione a quanto delineato dal parere n. 1/2010 WP29 e in base all’interpretazione letterale dell’art. 26 del GDPR, i rapporti tra contitolari possono quindi articolarsi in modo *asimmetrico,* nel senso che in alcune situazioni i soggetti coinvolti possono determinare in misura diversa le finalità e/o i mezzi e conseguentemente ciascuno di essi risponde solo per una parte del trattamento;

##### Richiamato:

##### *[Richiamare il contratto/progetto/accordo che definiscono la base di liceità, le finalità e le attività di trattamento oggetto dell’accordo per i contitolari]*

##### Considerato che:

* il nuovo quadro normativo e in particolare il GDPR concede ai Titolari del trattamento maggiore autonomia, ma allo stesso tempo maggiori responsabilità in applicazione del principio di accountability che richiede di comprovare*,* anche tramite evidenze, le valutazioni, le scelte e le misure adottate a garanzia della protezione dei dati personali;
* Il GDPR presuppone quindi la definizione di un modello “organizzativo” con ruoli, compiti e responsabilità dei vari attori coinvolti nelle attività, nonché del perimetro di azione di ciascun soggetto per quanto riguarda il trattamento e la gestione di dati personali;

SI CONCORDA QUANTO SEGUE

##### ART. 1 PREMESSE, RICHIAMI E CONSIDERATA

Le premesse, i richiami e i considerata costituiscono parte integrante del presente Accordo.

##### ART. 2 OGGETTO DELL’ACCORDO

Il presente accordo di contitolarità regolamenta l’ambito di azione e le responsabilità dei contitolari del trattamento in merito all’osservanza degli obblighi derivanti dal GDPR, compreso il rapporto con le categorie dei soggetti i cui dati saranno oggetto del trattamento. In particolare, l’accordo ha lo scopo di definire i compiti dei contitolari relativamente alle attività di trattamento dei dati personali riconducibili a ciascuno di essi.

##### ART. 3 ATTIVITÀ DI TRATTAMENTO DEI DATI PERSONALI DI CIASCUN CONTITOLARE

Il GDPR insiste sulla necessità di delineare con chiarezza i ruoli, i compiti e le responsabilità per garantire principalmente i diritti delle persone interessate (soggetti a cui si riferiscono i dati personali). Come descritto in premessa, quando due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento essi sono *contitolari* e in quanto tali sono tenuti, ciascuno per la propria parte, ad adottare le relative misure, tecniche e organizzative, per garantire la protezione dei dati personali. I Contitolari svolgono i propri compiti nel rispetto dei principi di finalità, di proporzionalità e di minimizzazione dei dati personali trattati e trattano i dati degli interessati (persone fisiche) congiuntamente, come di seguito descritto, per una migliore gestione delle attività finalizzate alla realizzazione delle finalità di ciascuno. *A tal fine si specifica quanto segue:*

[*Descrivere i compiti svolti nell’ambito del contratto/progetto/accordo da ciascun contitolare e il relativo livello di responsabilità. È consigliabile indicare anche in forma tabellare, per ciascun titolare, la descrizione delle funzioni svolte che comportano il trattamento dei dati personali, la descrizione sommaria del processo di Trattamento, la modalità di Trattamento, la tipologia di dati, le categorie degli interessati e la loro numerosità (atta ad individuare se trattasi di trattamento su larga scala), le relative operazioni di trattamento*].

**ART. 4 AMBITO DI COMUNICAZIONE**

I contitolari si impegnano ad istruire e autorizzare le persone fisiche facenti parte della propria organizzazione a trattare i dati personali e a nominare, laddove sussistono i presupposti, come responsabili del trattamento i soggetti esterni che potrebbero eventualmente intervenire nelle operazioni di trattamento per conto dei contitolari stessi.

##### ART. 5 INFORMATIVA PRIVACY

[*Indicare il contitolare/i che raccoglie i dati e che si impegna a fornire, in sede di raccolta del dato, le informazioni di cui all’art. 13 del GDPR. Nello specifico indicare anche le modalità in cui la informativa verrà resa (sito web/modulo cartaceo/ affissa in luogo accessibile al pubblico*].

##### ART. 6 ESERCIZIO DEI DIRITTI DELL’INTERESSATO

[*Indicare il/i Titolare/i designato/i a gestire* le richieste di esercizio dei diritti di cui agli artt. 15-22 del GDPR per conto e nell’interesse di tutti i Contitolari e relative dettagliate modalità di esecuzione*].*

##### ART. 7 SICUREZZA DEL TRATTAMENTO

Nel rispetto dei principi di cui all’art. 32 del GDPR i contitolari, nei limiti delle funzioni esercitate e delle rispettive prerogative, tenendo conto anche dello stato dell’arte, dei costi di attuazione, della natura, dell’oggetto, del contesto e delle finalità di trattamento, adottano misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio (es. misure atte a garantire su base permanente la riservatezza, l’integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento). Nel valutare l’adeguato livello di sicurezza i singoli contitolari devono tenere conto dei rischi di perdita; distruzione; modifica; divulgazione non autorizzata; accesso accidentale o illecito a dati personali trasmessi, conservati o comunque trattati. I contitolari, in quanto parti dell’accordo, si impegnano a stabilire, attuare, mantenere e migliorare un sistema di gestione per la sicurezza delle informazioni, sia con riferimento a strumenti, archivi e supporti cartacei, sia con riferimento a strumenti e mezzi digitali e informatici utilizzati.

##### ART. 8 VIOLAZIONE DEI DATI

Ai sensi e per gli effetti dell’art. 33 GDPR, il titolare del trattamento, in caso di violazione di dati personali, notifica la violazione all’autorità di controllo competente senza ingiustificato ritardo e ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora non sia effettuata entro 72 ore, la notifica è corredata dai motivi di ritardo. Ai sensi e per gli effetti dell’art. 34 GDPR, il titolare del trattamento comunica la violazione all’interessato senza ingiustificato ritardo qualora la stessa sia suscettibile di presentare un rischio elevato per i diritti e le libertà fondamentali dell’interessato. Si concorda

[*Indicare il/i Titolare/i designato/i per la gestione delle violazioni dei dati e le modalità con cui ciascun contitolare dovrà comunicare tempestivamente gli eventuali casi di data breach per la valutazione congiunta del fenomeno e per le eventuali comunicazioni al Garante e agli interessati*].

##### Art. 9 DPIA

Per ogni nuova iniziativa che comporti l’utilizzo di nuove tecnologie per il trattamento dei dati, o in caso di modifiche di strumenti del trattamento già adottati (art. 35 s.s. GDPR – art. 23 e 24 D.lgs. 51/2018), i contitolari si impegnano a collaborare per la valutazione dei rischi connessi e delle misure tecniche e organizzative da adottare a tutela dei dati personali. [*Indicare le modalità con cui verranno armonizzate le attività dei diversi Titolari per redigere la DPIA].*

##### ART. 11 CONCLUSIONI

Le parti si impegnano a revisionare il presente accordo in caso di necessità; a tal fine, lo stesso verrà monitorato e revisionato periodicamente per assicurarne l’attualità e l’allineamento alle novità legislative. Il presente accordo viene meno con il conseguimento delle finalità del trattamento da parte dei contitolari o qualora non vi siano più i presupposti di contitolarità. [*Indicare ai sensi dell’articolo 26 comma 2 del GDPR le modalità con cui il contenuto dell’accordo di contitolarità sarà messo a disposizione degli interessati].*

##### Luogo, data, firme

# Nomina per amministratore di sistema

# Fac-simile

|  |  |
| --- | --- |
| LOGO AZIENDA | **ATTO DI NOMINA AD AMMINISTRATORE DI SISTEMA**  ai sensi del Regolamento (UE) 2016/679 e del D.lgs. 196/2003 così come modificato dal D.lgs. 101/2018 |

Egregia/o --------------

Il Titolare del trattamento, facendo seguito ai colloqui intercorsi e tenuto conto del fatto che lei possiede l’esperienza, la capacità, l’affidabilità e i requisiti professionali ai sensi del Provvedimento del Garante della Privacy del 27 novembre 2008 “*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”* (di seguito “il Provvedimento”),

Considerato

* il rapporto di lavoro con lei in essere e della sua qualifica di assegnazione, dei compiti e delle mansioni svolti per la nostra Società;
* le prestazioni da lei effettuate le quali, in via ordinaria, forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo relativo alla sicurezza,

**con il presente atto le conferisce l’incarico di:**

**AMMINISTRATORE DI SISTEMA**

In qualità di: ☐ Dipendente ☐ Consulente esterno

per i trattamenti svolti nella nostra Società relativi alla gestione e alla manutenzione delle risorse informatiche quali software, pc, stampanti, server, accessi a Internet e rete Intranet aziendale. Eventuale gestione di dati.

Nel suo incarico lei dovrà svolgere le seguenti attività*:*

1. gestione e manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali attenendosi al Regolamento Europeo 679/2016 e alle disposizioni del Titolare in tema di protezione dei dati personali;
2. predisposizione e aggiornamento di un sistema di sicurezza informatico idoneo a rispettare le prescrizioni delle normative sulla privacy adeguandolo anche alle eventuali future norme in materia di sicurezza. A titolo esemplificativo, l’Amministratore di Sistema dovrà:

* provvedere alla cifratura e alla pseudonimizzazione dei dati personali contenuti in archivi e dispositivi;
* adottare adeguati programmi antivirus, firewall e altri strumenti software o hardware atti a garantire la massima misura di sicurezza nel rispetto di quanto dettato dalle normative sulla privacy e utilizzando le conoscenze acquisite in base al progresso tecnico software e hardware, verificandone l’installazione, l’aggiornamento e il funzionamento;
* adottare tutti i provvedimenti necessari ad evitare la perdita o la distruzione, anche solo accidentale, dei dati personali e provvedere al ricovero periodico degli stessi con copie di back-up e alla loro conservazione in luogo adatto e sicuro;
* provvedere direttamente (o tramite fornitori esterni) alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati per il loro reimpiego, alla luce del Provvedimento del Garante della Privacy del 13/10/2008 "*Rifiuti di apparecchiature elettriche ed elettroniche (RAAE) e misure di sicurezza dei dati personali*";
* cooperare nella predisposizione dei documenti necessari allo sviluppo dei sistemi di gestione per la parte concernente il sistema informatico e il trattamento informatico dei dati;
* predisporre e implementare le eventuali ulteriori misure tecniche e organizzative di sicurezza per il trattamento informatico dei dati personali e/o sensibili;

1. coordinamento, insieme al Titolare (e/o al Responsabile del trattamento), delle attività operative delle persone della Società nello svolgimento delle mansioni loro affidate per garantire un corretto, lecito e sicuro trattamento dei dati personali nell’ambito del sistema informatico;
2. collaborazione con il Titolare (e/o con il Responsabile del trattamento) per l’attuazione delle prescrizioni impartite dal Garante della Protezione dei Dati Personali;
3. comunicazione tempestiva al Titolare (e/o al Responsabile del trattamento) di qualsiasi situazione di cui sia venuto a conoscenza, nell’espletamento delle attività di esecuzione dell’incarico professionale assegnato, che possa compromettere il corretto trattamento informatico dei dati personali;
4. predisposizione della “*Relazione annuale amministratore di sistema*” al Titolare e/o al Responsabile del trattamento circa le implementazioni maggiormente significative in materia di sicurezza e protezione dei dati personali.

Ogni altra operazione, ancorché eseguibile in virtù dei privilegi di accesso a lei conferiti, dovrà essere autorizzata per iscritto dal Titolare dei dati personali.

Al fine di garantire la protezione dei dati e delle informazioni contenute nelle comunicazioni, è fatto divieto di accedere, manipolare o eseguire operazioni su caselle di posta elettronica o altri account di sistema che contengano o possano contenere dati sensibili, indipendentemente dal contesto operativo.

Alla nostra Società spetta il diritto di adottare provvedimenti adeguati qualora lei ponga in essere dei comportamenti illeciti.

Con l'accettazione e la sottoscrizione della presente designazione, in qualità di Amministratore di Sistema testé nominato, dichiara di essere a conoscenza e di rispettare quanto stabilito dal Regolamento Europeo 679/2016 e successive modifiche e integrazioni e, in particolare, dichiara di:

1. conoscere e impegnarsi a rispettare, sotto la propria responsabilità, nell'ambito delle materie oggetto del presente incarico e nell'ambito di operatività di cui alla presente designazione, quanto indicato dalle *“Misure tecniche e organizzative*” che le fornisce il titolare;
2. conoscere e impegnarsi a rispettare, sotto la propria responsabilità, nell'ambito delle materie oggetto del presente incarico e nell'ambito di operatività di cui alla presente designazione, le prescrizioni di cui alle lettere c) e f) del punto 2 del Provvedimento;
3. attenersi agli obblighi di assoluta riservatezza connessi al suo incarico e alla designazione;
4. trattare dati personali solo se indispensabile in relazione all'assolvimento degli incarichi a Lei assegnati e, comunque, urgenti;
5. rispettare le prescrizioni impartite dal Titolare, tra cui il divieto assoluto di comunicare e/o diffondere a terzi non autorizzati le informazioni e i dati personali di cui sia venuto a conoscenza, a qualsiasi titolo.

Le ricordiamo che il Provvedimento obbliga la nostra Società alla “verifica” almeno annuale delle attività svolte dall'Amministratore di Sistema, in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

È inoltre prevista, conformemente al Provvedimento, la predisposizione da parte della nostra Società di sistemi idonei alla registrazione degli accessi logici ("Autenticazione informatica") ai sistemi di elaborazione e agli archivi elettronici. Tali registrazioni ("Access log") avranno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

La informiamo, infine, che i suoi estremi identificativi saranno comunicati secondo quanto stabilito all'art. 4 comma 3 del Provvedimento.

luogo, data

|  |
| --- |
| Il Titolare del trattamento |
|  |
| L’incaricato |
| *per accettazione dell’incarico* |

# Nomina soggetto autorizzato

# Fac-simile

**NOMINA DI AUTORIZZATO AL TRATTAMENTO DI DATI PERSONALI**

(art. 29, 32 General Data Protection Regulation UE 679/16)

Il Titolare del trattamento dei dati è «DENOMINAZIONE» Sede legale «Sede\_Legale» P.IVA/Codice Fiscale «Partita\_IVA» email «email» pec «PEC»

PREMESSO CHE

Il Reg UE 679/16, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, fissa le modalità da adottare per detto trattamento e individua i soggetti che, in relazione all'attività svolta, sono tenuti agli adempimenti previsti dalla stessa legge; in particolare, gli artt. 29 ‘Trattamento sotto l’autorità del titolare del trattamento o del responsabile del trattamento’ e 32 ‘Sicurezza del trattamentoʼ del suddetto regolamento prevedono che ‘Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dellʼUnione o degli Stati membri’.

**NOMINA**

Il/La sig./sig.ra «NOMINATIVO\_ADDETTO\_»,

**nell’ambito di trattamento dati relativo a:**

«AREA\_ORGANIZZATIVA\_1»

«AREA\_ORGANIZZATIVA\_2»

«AREA\_ORGANIZZATIVA\_3»

«AREA\_ORGANIZZATIVA\_4»

**Soggetto Autorizzato al trattamento dei seguenti dati:**

«DATI\_AUTORIZZAZIONE\_1»

«DATI\_AUTORIZZAZIONE\_2»

«DATI\_AUTORIZZAZIONE\_3»

«DATI\_AUTORIZZAZIONE\_4»

**Istruzioni**

L'Autorizzato dovrà effettuare il trattamento dei dati nel rispetto della normativa vigente e delle misure di sicurezza indicate dal suddetto regolamento e individuate dal titolare del trattamento e quelle che successivamente verranno indicate in aggiornamento a quelle ivi previste. L'Autorizzato dovrà, inoltre, rispettare le istruzioni impartite dal Titolare sia con il presente atto di nomina sia in seguito. A titolo esemplificativo, l’Autorizzato dovrà:

* procedere alla raccolta di dati personali, anche mediante l'approvazione di appositi moduli di raccolta;
* consegnare agli interessati, al momento della raccolta dei dati, il modulo contenente l'informativa, salvo che l'informativa medesima sia stata fornita direttamente dal Titolare;
* raccogliere, sempre al momento della raccolta dei dati, il consenso espresso e in forma granulare, documentato per iscritto, degli interessati ai trattamenti previsti, salvo che a ciò abbia provveduto direttamente il Titolare e salvo i casi di esonero previsti dalla stessa legge;
* trattare i dati personali nella misura necessaria e sufficiente alle finalità proprie della banca dati nella quale vengono inseriti;
* adottare, nel trattamento dei dati, tutte le misure di sicurezza che siano indicate, oggi o in futuro, dal Titolare. In particolare, per le banche dati informatiche, l’Autorizzato dovrà utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali altrui e/o di lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
* trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare;
* conservare i supporti informatici e/o cartacei contenenti i dati personali in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
* con specifico riferimento agli atti e documenti cartacei contenenti dati personali e alle loro copie, restituire gli stessi al termine delle operazioni affidate;
* utilizzare i supporti di memorizzazione già usati in passato solamente qualora i dati in essi precedentemente contenuti non siano in alcun modo recuperabili, altrimenti etichettarli e riporli negli appositi contenitori. Copie di dati personali su supporti removibili sono permesse solo se parte del trattamento, copie di categorie particolari di dati devono essere espressamente autorizzate dal Titolare del trattamento. In ogni caso tali supporti devono avere un’etichetta che li identifichi e non devono mai essere lasciati incustoditi; in caso si constati o si sospetti un incidente di sicurezza deve essere data immediata comunicazione al Titolare del trattamento;
* segnalare al Titolare eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza, al fine di ridurre al minimo i rischi di distruzione o perdita anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
* effettuare la comunicazione dei dati esclusivamente ai soggetti indicati dal Titolare e secondo le modalità stabilite dal medesimo;
* mantenere, salvo quanto precisato al punto precedente, la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo e anche successivamente al termine di esso;
* svolgere, in ogni caso, il trattamento dei dati personali per le finalità e secondo le modalità stabilite, anche in futuro, dal Titolare e comunque in modo lecito e secondo correttezza;
* fornire al Titolare, a semplice richiesta e secondo le modalità indicate, tutte le informazioni relative all'attività svolta, al fine di consentire allo stesso di svolgere efficacemente la propria attività di controllo;
* in generale, prestare la più ampia e completa collaborazione al Titolare al fine di compiere tutto quanto sia necessario e opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente.

Il/La sottoscritta “autorizzato/a” prende atto di quanto previsto nella presente nomina e dalla normativa vigente e assume la qualifica di ‘Autorizzato al trattamento dati’.

Letto, approvato e sottoscritto in \_\_\_\_\_\_\_\_\_\_\_\_ il \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Per il Titolare del trattamento L’autorizzato al trattamento

«DENOMINAZIONE» *«NOMINATIVO\_ADDETTO\_»*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

# Fac-simile

**Atto di designazione del Responsabile della Protezione dei Dati personali (DPO) ai sensi dell’art. 37 del GDPR**

Premesso che:

* Il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 *«relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)»* (di seguito *GDPR*), in vigore dal 24 maggio 2016, e applicabile a partire dal 25 maggio 2018, introduce la figura del Responsabile della Protezione dei dati personali (DPO) (artt. 37-39);
* Le predette disposizioni prevedono che il DPO *«può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi»* (art. 37, paragrafo 6) e deve essere individuato *«in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all’articolo 39»* (art. 37, paragrafo 5) *e «il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile del trattamento»* (considerando n. 97 del GDPR);

Considerato che il Titolare del trattamento*:* XXXcon sede inVia XXXX nella persona del legale rappresentante XXXXX,

è tenuto alla designazione obbligatoria del DPO nei termini previsti, rientrando nella fattispecie prevista dall’art. 37, par. 1, del GDPR;

* a seguito di valutazioni effettuate ha ritenuto che il soggetto di seguito indicato sia in possesso del livello di conoscenza specialistica e delle competenze richieste dall’art. 37, par. 5, del GDPR, per la nomina a DPO, e non si trova in situazioni di conflitto di interesse con la posizione da ricoprire e i compiti e le funzioni da espletare;

DESIGNA

XXXXXX**,** come Responsabile della protezione dei dati personali (DPO)

Nel rispetto di quanto previsto dall’art. 39, par.1, del GDPR il DPO è incaricato di svolgere, in piena autonomia e indipendenza, i seguenti compiti e funzioni:

* 1. informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR, nonché da altre disposizioni nazionali o dell’Unione relative alla protezione dei dati;
  2. sorvegliare l’osservanza del GDPR, di altre disposizioni nazionali o dell’Unione relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l’attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
  3. fornire, se richiesto, un parere in merito alla valutazione d’impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell’articolo 35 del GDPR;
  4. cooperare con il Garante per la protezione dei dati personali;
  5. fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all’articolo 36 ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

I compiti del Responsabile della Protezione dei Dati personali attengono all’insieme dei trattamenti di dati effettuati dal Titolare del trattamento.

La XXX si impegna a:

* 1. mettere a disposizione del DPO adeguate risorse al fine di consentire l’ottimale svolgimento dei compiti e delle funzioni assegnate;
  2. non rimuovere o penalizzare il DPO in ragione dell’adempimento dei compiti affidati nell’esercizio delle sue funzioni;
  3. garantire che il DPO eserciti le proprie funzioni in autonomia e indipendenza e in particolare, non assegnando allo stesso attività o compiti che risultino in contrasto o conflitto di interesse.

Luogo e data \_\_\_\_\_\_\_\_\_\_\_\_\_

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Per accettazione

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Timbro e firma