

DESIGNAZIONE DI RESPONSABILE DEL TRATTAMENTO CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI E REGOLAMENTAZIONE CONTRATTUALE

(Art. 28 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016)

PREMESSO CHE

- a. Tra il Cliente ed il fornitore indicato nel contratto cui il presente documento si riferisce (di seguito FORNITORE) è in essere un contratto per l'erogazione di servizi informatici (di seguito SERVIZIO e/o SERVIZI), di cui la presente è parte integrante;
- b. nel presente contratto le parti concordano di definire
 - Con il termine "GDPR" 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
 - Con il termine "Normativa Privacy" le disposizioni del GDPR nonché tutte le altre disposizioni delle leggi dell'Unione o delle leggi degli Stati membri relative alla protezione dei dati personali e alla loro libera circolazione;
- c. nello svolgimento del SERVIZIO, il Titolare del trattamento dei dati personali, ai sensi e per gli effetti dell'Art. 4 comma 1 numero 7) del GDPR, è il CLIENTE e incombe sul CLIENTE il compimento di tutti gli atti previsti dalla Normativa Privacy per il trattamento dei dati personali, vale a dire l'informativa, la raccolta del consenso, l'adozione di tutte le misure autorizzative, di incarico e di conservazione e di altro tipo anche per realizzare il Sistema sicurezza ivi comprese le relative misure;

Ciò premesso, tra le PARTI,

SI CONVIENE E SI STIPULA

quanto di seguito riportato.

Art. 1. Designazione di Responsabile del trattamento

1. Per i compiti che in base al CONTRATTO per il SERVIZIO, restano affidati al FORNITORE, quest'ultimo ai sensi dell'Art.4 c.1 n.8) del GDPR è designato *Responsabile del trattamento*.
2. Il *Responsabile del trattamento* precisa di essere in grado di offrire garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti GDPR e garantisca la tutela dei diritti degli interessati.

Art.2. Oggetto della presente regolamentazione

1. Oggetto delle presenti condizioni è definire le modalità e le condizioni contrattuali nelle quali il *Responsabile del trattamento* si impegna ad effettuare, per conto del *Titolare del trattamento* le operazioni di trattamento dei dati personali.
2. Nel quadro delle loro relazioni contrattuali, le parti si impegnano a rispettare la regolamentazione in vigore applicabile al trattamento dei dati a carattere personale (dati personali) e, in particolare, il "GDPR" e la "Normativa Privacy".

Art.3. Durata del contratto

1. Il presente allegato avrà la durata del contratto a cui si riferisce.

Art.4. Descrizione delle prestazioni del Responsabile del trattamento

1. Il responsabile del trattamento è autorizzato a trattare, per conto del Titolare del trattamento, dati a carattere personale necessari per fornire il servizio/i quali previsti dal contratto. I dati che il Titolare del trattamento ha già fornito e che fornirà avranno già acquisito il consenso degli interessati al loro

trattamento ai sensi dell'Art. 6 comma 1 lett. A) del GDPR, salvi i casi indicati nel predetto art. 6 di trattamento consentito anche in assenza di consenso.

Il Titolare del trattamento garantisce il Responsabile del trattamento di disporre legittimamente di tutte le informazioni (testi, dati, notizie, segni, immagini, suoni e quant'altro) che affiderà al Responsabile del trattamento per il loro trattamento, assicurando altresì che dette informazioni non violano in alcun modo diritti di terzi.

Il Titolare del trattamento mantiene la titolarità delle informazioni che saranno comunicate al Responsabile del trattamento per il SERVIZIO ed assume espressamente ogni più ampia responsabilità in ordine al contenuto dei relativi dati personali e manleva il Responsabile del trattamento da ogni obbligo e/o onere di accertamento e/o di controllo diretto e indiretto al riguardo.

2. La natura delle operazioni realizzate sui dati è la messa in esercizio, manutenzione e aggiornamento del sistema informativo acquistato e/o utilizzato dal Titolare.
3. La finalità del trattamento è di fornire un servizio di manutenzione ed assistenza al Titolare. Il Titolare del trattamento dichiara che il trattamento è affidato al Responsabile del trattamento per lo svolgimento del SERVIZIO come meglio descritto nel CONTRATTO.

Per quanto di sua competenza il Responsabile del trattamento, nel trattare i dati per l'erogazione del SERVIZIO, effettuerà il trattamento in osservanza dell'Art.5 del GDPR relativo ai "Principi applicabili al trattamento dei dati personali".

4. La natura dei dati trattati dal Responsabile del trattamento varia in funzione del servizio acquistato dal Titolare. Il trattamento potrebbe estendersi anche ai dati particolari di cui all'Art.9 del GDPR per i quali il *Titolare del trattamento* e il *Responsabile del trattamento* rilasceranno ai propri Addetti l'autorizzazione.
5. Le categorie di persone interessate sono essenzialmente clienti del Titolare del trattamento, utenti che autorizzati dal Titolare trattano i dati del servizio informativo acquistato, e in relazione all'ambito del servizio dipendenti, collaboratori, fornitori.
6. Per l'esecuzione dell'incarico oggetto del presente contratto, il *Titolare del trattamento* mette a disposizione del *Responsabile del trattamento* le informazioni necessarie all'esecuzione delle attività di assistenza e manutenzione e indirizzate all'utilizzo appropriato del sistema informativo.
7. Gli ADDETTI al trattamento del FORNITORE ricopriranno la figura di Addetti al trattamento designati dal Responsabile del trattamento ai sensi dell'art. 28 comma 3 lett. B del GDPR.

Poiché il trattamento dei dati è fatto anche direttamente dal CLIENTE, Titolare del trattamento, questi, per il trattamento diretto, provvederà a designare tali Addetti con l'osservanza di tutti gli obblighi della Normativa Privacy e con esonero del Responsabile del trattamento, in relazione a ciò, da ogni sorta di responsabilità. Gli addetti al trattamento per il Titolare quindi saranno designati dal Titolare del trattamento e gli addetti al trattamento per il Responsabile del trattamento saranno designati dal Responsabile del trattamento in ottemperanza ed osservanza delle disposizioni in merito dettate dal GDPR.

Le operazioni di trattamento quindi saranno effettuate per il fornitore da Addetti che opereranno sotto la diretta autorità del Responsabile del trattamento, attenendosi alle istruzioni da questi impartite. La designazione sarà effettuata per iscritto e individuerà puntualmente l'ambito del trattamento consentito ed autorizzato. Si considererà tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito ed autorizzato agli addetti all'unità medesima.

Il *Responsabile del trattamento* si dichiara edotto che chiunque agisca sotto la sua autorità e abbia accesso a dati personali, non può trattare tali dati se non è stato istruito in tal senso.

Art. 5. Obblighi del Responsabile del trattamento di fronte al Titolare del trattamento

Perché sia garantito un adeguato trattamento dei dati il *Responsabile del trattamento*, al quale è affidato il trattamento per lo svolgimento del SERVIZIO, assume specificamente i seguenti impegni.

Il *Responsabile del trattamento*, nello svolgimento delle sue funzioni, si impegna ad assolvere ed osservare i seguenti obblighi.

a) Osservanza, nel trattamento dei dati personali, delle istruzioni date dal Titolare

1. Il *Responsabile del trattamento* dovrà trattare i dati solo per le finalità sopra specificate e per l'esecuzione delle prestazioni contrattuali.
2. Il *Responsabile del trattamento* dovrà trattare i dati in conformità a quanto previsto nel Registro dei trattamenti per il Servizio ed il Titolare ritiene adeguate le misure di sicurezza ivi previste;
3. I dati saranno trattati dal Responsabile del trattamento su territorio Italiano. Qualora in futuro il trattamento dovesse essere eseguito anche all'estero sia in paesi UE che Extra UE, il Responsabile ne darà immediata comunicazione al Titolare per convenire le garanzie che lo stesso richiederà in funzione del luogo in cui il trattamento sarà svolto.
4. Se il *Responsabile del trattamento* sarà tenuto ad effettuare un trasferimento dei dati verso un paese terzo o un'organizzazione internazionale, in virtù delle leggi dell'Unione o delle leggi dello stato membro al quale è sottoposto, deve informare il *Titolare del trattamento* circa tale obbligo giuridico prima del trasferimento al fine di ottenere autorizzazione, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b. Garantire la riservatezza

1. Il *Responsabile del trattamento* garantisce l'osservanza della **riservatezza** dei dati a carattere personale (dati personali) trattati nell'ambito del presente contratto.
2. Il *Responsabile del trattamento* garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza e che esse ricevano e che venga loro data la formazione necessaria in materia di trattamenti dei dati personali e di protezione dei dati a carattere personale.

c. Adozione delle misure di sicurezza del trattamento

1. Il *Responsabile del trattamento* deve procedere al trattamento dei dati personali in presenza delle misure richieste ai sensi dell'articolo 32 (Sicurezza del trattamento) del *GDPR*. Le misure di sicurezza adottate sono quelle dichiarate nel Registro dei trattamenti relative al servizio. Il Titolare prende atto che in alcuni casi il Responsabile del trattamento, procederà al trattamento attraverso gli strumenti predisposti e configurati dallo stesso e pertanto dovrà adottare ogni cautela necessaria solo qualora il trattamento sia effettuato fuori dal controllo dello strumento impostato e configurato dal Titolare.
2. Se il *Responsabile del trattamento* ha aderito ad un codice di comportamento, o ha esibito una certificazione, deve operare in presenza delle misure di sicurezza previste dal codice di comportamento o dai protocolli di cui alla certificazione. In questo caso il Titolare accetterà la certificazione come prova del fatto che il Responsabile del trattamento ha adottato misure adeguate rispetto al trattamento effettuato. In questo caso il Titolare rinuncia ad effettuare attività di audit sui sistemi e sulle procedure del Fornitore

d. Nomina di altro Responsabile da parte del Responsabile del trattamento

1. La Società può affidare il servizio di gestione dei Servizi a terzi responsabili del trattamento in qualsiasi momento, previa comunicazione scritta al Cliente, il quale potrà opporsi entro 15 giorni dal ricevimento di tale comunicazione. In tale caso, essendo la scelta di affidare il servizio strategica per il business del fornitore, il cliente potrà scegliere se dare disdetta al contratto o modificare l'erogazione del servizio in modalità on premise.

La Società dichiara e garantisce che tali ulteriori responsabili presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative idonee a garantire il rispetto delle disposizioni della vigente Normativa sulla Privacy e si impegna a vincolare contrattualmente gli ulteriori responsabili al rispetto degli stessi obblighi in materia di protezione dei dati personali assunti dalla Società nei confronti del Cliente.

Il Titolare del trattamento, considerata la complessità delle operazioni tecniche di trattamento elettronico dei dati per il SERVIZIO e l'eventuale esigenza del Responsabile del trattamento di avvalersi di personale specializzato o di apparati a elevata connotazione tecnologica che, eventualmente, comprensibilmente, non fossero disponibili presso le strutture degli stessi, autorizza il Responsabile del trattamento ad affidare, sotto la propria responsabilità, l'esecuzione di operazioni di trattamento informatico a società del settore che per

esperienza, capacità e affidabilità forniscano idonea garanzia del pieno rispetto della legge, con particolare riguardo alla *Normativa Privacy* compresa la Sicurezza.

2. Spetta al *Responsabile del trattamento* iniziale assicurare che l'ulteriore *Responsabile del trattamento* presenti le stesse garanzie sufficienti alla messa in opera di misure tecniche ed organizzative appropriate di modo che il trattamento risponda alle esigenze del regolamento europeo sulla protezione dei dati.

3. Qualora l'ulteriore *Responsabile del trattamento* ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale conserva, nei confronti del *Titolare del trattamento*, l'intera responsabilità dell'adempimento degli obblighi dell'ulteriore Responsabile.

e) Assistenza al Titolare per l'esercizio dei diritti degli interessati

1. Per quanto possibile, il *Responsabile del trattamento*, tenendo conto della natura del trattamento, deve assistere il *Titolare del trattamento* al fine dell'adempimento dell'obbligo del *Titolare del trattamento* di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al *Capo III (Diritti dell'interessato)*: di far seguito alle domande di esercizio dei diritti di accesso, di rettifica, di cancellazione e di opposizione, alla limitazione del trattamento, a trasportare i dati, di non essere oggetto di una decisione individuale automatizzata (compreso il profilo).

Il *Responsabile del trattamento*, nella misura in cui ciò sia possibile, assisterà il *Titolare* con misure tecniche e organizzative adeguate.

2. In relazione al diritto di informazione degli interessati, Spetta al *Titolare del trattamento* fornire l'informativa di cui agli art. 13-14 alle persone interessate per le operazioni del trattamento al momento della raccolta dei dati.

f) Assistenza al Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR

1. Il *Responsabile del trattamento*, tenendo conto della natura del trattamento e delle informazioni a disposizione del *Responsabile del trattamento* deve assistere il *Titolare del trattamento* nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del *GDPR* vale a dire:

- l'articolo 32. *Sicurezza del trattamento*;
- l'articolo 33. *Notifica di una violazione dei dati personali all'autorità di controllo*;
- l'articolo 34. *Comunicazione di una violazione dei dati personali all'interessato*;
- l'articolo 35. *Valutazione d'impatto sulla protezione dei dati*;
- l'articolo 36. *Consultazione preventiva*.

2. Assistenza per la "Sicurezza del trattamento" - Il *Responsabile del trattamento* ha l'obbligo di assistere il *Titolare del trattamento* nella realizzazione della *Sicurezza del trattamento*, conformemente all'articolo 32 del *GDPR*.

Il *RESPONSABILE del trattamento*, in caso di situazioni anomale o di emergenze, provvederà a relazionare periodicamente sulle misure di sicurezza adottate – anche mediante eventuali questionari e liste di controllo – ed ad informare immediatamente il titolare del trattamento.

3. Particolari misure di sicurezza del Responsabile del trattamento già in atto - Prende atto il *Titolare del trattamento* che, per il SERVIZIO, il Responsabile del trattamento ha in essere misure di sicurezza adeguate in osservanza del *GDPR*.

Per i dati personali trattati nell'infrastruttura informatica del Responsabile del trattamento rimane comunque l'obbligo, per lo stesso, di caratterizzare il sistema di trattamento dati in conformità ai requisiti di sicurezza e, su richiesta del *Titolare del trattamento*, a servizio cessato, di cancellare i dati comunicati dal *Titolare del trattamento* per lo svolgimento del SERVIZIO; nel qual caso, il Responsabile del trattamento, provvederà a cancellarli quando non siano più necessari per lo svolgimento del SERVIZIO o per gli atti conseguenti.

Amministratori di sistema. In relazione alle attività svolte dal Responsabile del trattamento riferite alla conservazione dei dati personali e alle attività sistemistiche dirette alla manutenzione della rete e all'aggiornamento dei relativi data base e sistemi operativi, gli operatori del Responsabile del trattamento avranno la funzione di Amministratori di sistema.

Gli adempimenti previsti dal Garante per la privacy nel provvedimento del 27 novembre 2008 saranno gestiti dal Responsabile del trattamento; in particolare sarà il Responsabile del trattamento a valutare le caratteristiche soggettive degli amministratori di sistema, ad effettuare le designazioni individuali, a verificare

le attività dagli stessi svolte ed a provvedere alla registrazione dei relativi accessi. In relazione a quanto previsto dal provvedimento stesso il Responsabile del trattamento si obbliga a comunicare al Titolare del trattamento l'elenco aggiornato degli Amministratori di sistema; la comunicazione di tali dati potrà avvenire in formato elettronico o cartaceo ed il Titolare del trattamento considera evaso tale adempimento anche con la semplice messa a disposizione dell'elenco aggiornato dei nominativi degli stessi Amministratori di sistema in un'area internet a ciò dedicata.

4. Assistenza per l'obbligo di "Notifica di una violazione dei dati personali all'autorità di controllo" - Il Responsabile del trattamento ha l'obbligo di assistere il Titolare del trattamento nell'adempimento degli obblighi di "Notifica di una violazione dei dati personali all'autorità di controllo", conformemente all'articolo 33 del GDPR. Il Responsabile del trattamento notifica al Titolare del trattamento ogni violazione di dati a carattere personale nel tempo massimo di 24 ore dopo esserne venuto a conoscenza tramite PEC. Tale notifica è accompagnata da quanto espressamente indicato nel 3° comma dell'articolo 33, utile per permettere al Titolare del trattamento, se necessario, di notificare questa violazione all'autorità di controllo competente.

5. Assistenza per l'obbligo di "Comunicazione di una violazione dei dati personali all'interessato" - Il Responsabile del trattamento ha l'obbligo di assistere il Titolare del trattamento nell'adempimento degli obblighi di "Comunicazione di una violazione dei dati personali all'interessato", conformemente all'articolo 34 del GDPR; tale comunicazione andrà comunque sempre fatta da parte del Titolare del trattamento.

g) Assistenza, del Responsabile del trattamento, nell'adempimento dell'obbligo del Titolare del trattamento della "Valutazione d'impatto sulla protezione dei dati"

1. Il Responsabile del trattamento assisterà il Titolare del trattamento nell'adempimento degli obblighi della "Valutazione d'impatto sulla protezione dei dati", conformemente all'articolo 35 del GDPR, fornendo al titolare ogni informazione utile in suo possesso.

h) Assistenza del Responsabile del trattamento nell'adempimento dell'obbligo del Titolare del trattamento della "Consultazione preventiva"

1. Il Responsabile del trattamento assiste il Titolare del trattamento nella consultazione preventiva dell'autorità di controllo, prevista dall'articolo 36 del GDPR, fornendo al titolare ogni informazione utile in suo possesso.

i) Restituzione di tutti i dati personali al termine dell'incarico

1. Dopo che è terminata la prestazione dei servizi relativi al trattamento il Responsabile del trattamento, su scelta del Titolare del trattamento, dovrà restituire o cancellare tutti i dati personali e cancellare le copie esistenti.

I dati in possesso del Responsabile del trattamento dovranno essere restituiti al Titolare del trattamento attraverso la consegna del backup del data base o dei files su cui risiedono i dati personali; entro 90 gg dalla data di risoluzione del contratto o dell'incarico, dovranno essere distrutti.

Eventuali ulteriori copie dei dati stessi di backup, salvo diversi accordi che potranno intervenire, tra il Titolare e il Responsabile [alla cessazione del rapporto] dovranno essere distrutte dal Responsabile del trattamento entro tempi compatibili con le ulteriori necessità che possono prospettarsi anche alla cessazione del SERVIZIO e comunque per un tempo non superiore a 12 mesi decorsi i 90 gg dalla data di cessazione suddetta e nel periodo intermedio tra la fine del rapporto e detto termine i dati saranno conservati dal Responsabile del trattamento per fini esclusivamente di sicurezza e non destinati alla comunicazione e alla diffusione

2. In deroga a quanto indicato ai punti precedenti il Responsabile del trattamento, dovrà conservare detti dati, nel caso in cui il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati e dovrà conservarli fino al termine imposto da detta normativa o da detti provvedimenti.

l) Messa a disposizione del Titolare del trattamento di tutte le informazioni necessarie per dimostrare il rispetto degli obblighi

1. Il Responsabile del trattamento metterà a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 del GDPR e deve consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato o dalle autorità. Qualora tali attività comportino un costo per il Responsabile del trattamento, tali attività andranno valutate a livello progettuale con la definizione di una valutazione economica.

m) Caso in cui un'istruzione al Responsabile del trattamento sia ritenuta in violazione del GDPR

1. Qualora, il *Responsabile del trattamento*, a suo parere ritenga che, un'istruzione del *Titolare del trattamento* violi il GDPR o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati dovrà informare immediatamente il *Titolare del trattamento*.

n) osservanza dei principi di “privacy by design” e di “privacy by default”

1. Il *Responsabile del trattamento* nello svolgimento dell'incarico, dovrà operare in osservanza dei principi di protezione dei dati a partire da quando questi vengono progettati (privacy by design) e della protezione dei dati di default. La definizione dei requisiti di base dei sistemi e del rispetto di questi principi sarà definito su base progettuale in fase di start up del servizio.

o) i compiti per il SERVIZIO

1. I compiti del *Responsabile del trattamento* sono quelli indicati nel CONTRATTO, in precedenza indicato, che regola il SERVIZIO e qualificati quali obblighi o attività dovute dal FORNITORE.

Art. 6. Obblighi del Titolare del trattamento di fronte al *Responsabile del trattamento*

Il Titolare del trattamento deve:

- a. fornire al Responsabile del trattamento i dati previsti all'art. 4 delle presenti clausole;
- b. documentare per iscritto tutte le istruzioni riguardanti il trattamento dei dati da parte del Responsabile del trattamento;
- c. vigilare, in anticipo e durante la durata di tutto il trattamento, sul rispetto degli obblighi previsti dal regolamento europeo sulla protezione dei dati da parte del Responsabile del trattamento;
- d. supervisionare il trattamento, effettuando audit e ispezioni.

Art. 7 Luoghi ove sono e saranno custoditi i dati

Per i SERVIZI comportanti il trattamento dei dati in BANCHE DATI create dal Responsabile del trattamento per il SERVIZIO i dati personali saranno custoditi presso la sede del FORNITORE e nel luogo o nei luoghi indicati nel CONTRATTO regolante il SERVIZIO e saranno ivi trattati e conservati. I servizi saranno erogati dall'Italia. Qualora ci fosse la necessità di erogare i servizi da territori Ue o Extra UE ne sarà data immediata notizia al Titolare che deciderà se continuare o risolvere il contratto.

Art. 8 Controlli

Il Titolare del trattamento, si riserva, anche tramite verifiche periodiche, di vigilare sulla puntuale osservanza delle disposizioni di legge sul trattamento dei dati stessi e sul rispetto delle proprie istruzioni indicate nel presente documento. Il Responsabile del trattamento dovrà consentire al Titolare del trattamento, dandogli piena collaborazione, periodiche verifiche circa l'adeguatezza delle misure di sicurezza adottate e il rispetto della Normativa Privacy e delle disposizioni del Titolare del trattamento stesso.

Ogni attività di audit da parte del Titolare dovrà essere convenuta con il Responsabile del trattamento. Qualora tali attività comportino oneri e spese non previste dal presente contratto tutte le richieste del Titolare dovranno essere gestite a livello progettuale con una stima dei costi necessari per la loro attuazione (siano esse attività di penetration test, vulnerability assessment, altro).