

**Organizzazione e criteri per la gestione dei dati
in conformità con le norme che regolano la Privacy:
d. lgs. 196/2003 “Codice Privacy” e Regolamento UE 679/2016 “GDPR”**

Declaratoria sulla Policy

Nel regolare svolgimento delle attività, MASTER MANAGEMENT STUDI E RICERCHE (in seguito MASTER) raccoglie Dati Personali da clienti, fornitori, dipendenti, candidati a posizioni lavorative, appaltatori, azionisti, partner, utenti del sito web e altre terze Parti.

L’entrata in vigore di norme più restrittive e la digitalizzazione dei servizi sono un’opportunità per assicurare la nostra integrità in una delle aree più importanti della vita moderna - la protezione dei Dati Personali - e per questo abbiamo definito la nostra Data Privacy Policy, organizzata attorno a tre impegni di base:

- **Raccolta** e trattamento dei Dati Personali corretti e leciti.
- **Rispetto** dei diritti e delle scelte dei proprietari dei Dati.
- **Gestione** responsabile dei Dati Personali.

MASTER riconosce la necessità di trattare i Dati Personali con cautela e tutti - in azienda e nei luoghi in cui operiamo - siamo impegnati nel condurre le nostre attività in conformità a tutte le applicabili leggi sulla Privacy, e in linea con i più elevati standard di condotta etica.

Per domande o commenti su questa Policy è possibile inviare una e-mail all’indirizzo f.marinangeli@mastersicurezza.it. Saremo lieti e disponibili nel fornire ogni risposta o documentazione richiesta.

Federico Marinangeli

Legale Rappresentante



Roma, 14 maggio 2019

Indice

1. CRITERI GENERALI E AMBITO DI APPLICAZIONE
2. DEFINIZIONE DI “DATI PERSONALI”
3. RACCOLTA E TRATTAMENTO DEI DATI PERSONALI CORRETTI E LECITI
4. USO DEI DATI PERSONALI SOLO PER SCOPI LEGITTIMI E SPECIFICI
5. CONSERVAZIONE
6. ADOZIONE DI APPROPRIATE MISURE DI SICUREZZA
7. ADEGUATA PROTEZIONE AI TRASFERIMENTI, ANCHE INTERNAZIONALI

ALLEGATI

Allegato 1 - Procedura IT per il trattamento dei dati

Allegato 2 - Informativa per la formazione: Regolamento Europeo per la tutela dei Dati e i rapporti di collaborazione e Accordo con la Master Data Privacy Policy

Allegato 3 - Nomina Responsabile e/o SUB Responsabile del Trattamento

Allegato 4 - Nomina Responsabile del trattamento in qualità di Amministratore di Sistema

1. CRITERI GENERALI E AMBITO DI APPLICAZIONE

In questo documento viene descritto come sono gestiti i dati sensibili nelle attività quotidiane della MASTER, che è Titolare del trattamento degli stessi. I criteri di questa gestione si basano sulle norme che regolano la materia privacy (d. lgs. 196/2003 “Codice Privacy” e Regolamento UE 679/2016 “GDPR”) e, più in generale, sui nostri principi di trasparenza, riservatezza e correttezza.

La nostra Data Privacy Policy definisce l’organizzazione della MASTER per il trattamento dei dati e la condotta attesa da ogni dipendente e collaboratore quando raccoglie, gestisce e usa dati personali di clienti, fornitori, partner, appaltatori e altre Terze Parti. Le persone che lavorano in MASTER hanno accesso ai dati e lavorano seguendo gli stessi principi di riservatezza e sicurezza.

2. DEFINIZIONE DI “DATI PERSONALI”

La definizione di Dati Personali si riferisce a qualsiasi informazione relativa a un individuo e può includere tra gli altri:

- **informazioni di contatto** (nome, indirizzo abitativo e professionale, telefono, indirizzi e-mail);
- **informazioni personali** (data di nascita, cittadinanza, fotografie, dati identificativi elettronici quali cookie, indirizzi IP e password);
- **informazioni professionali e d’impiego** (istruzione e formazione);
- **dettagli finanziari** (dati identificativi fiscali e numero di conto corrente bancario).

Per operare in conformità a questa Data Privacy Policy, sono fornite regole d’implementazione interna, linee guida e formazione, con tutta la necessaria documentazione di supporto.

3. RACCOLTA E TRATTAMENTO DEI DATI PERSONALI CORRETTI E LECITI

Quando raccoglie Dati Personali, MASTER informa gli interessati in modo chiaro, onesto e trasparente sulla natura dei Dati Personali che raccoglie e su cosa intende fare con essi. Non è autorizzato l’uso dei Dati per scopi diversi da quelli inizialmente comunicati, a meno che non siano fornite adeguate informazioni agli individui interessati e, ove applicabile, venga dato a MASTER il consenso per l’uso previsto. In generale, siamo autorizzati a usare i Dati Personali per scopi secondari quando attuiamo i controlli e audit interni, nel rispetto degli obblighi legali e regolatori in materia di Privacy.

4. USO DEI DATI PERSONALI SOLO PER SCOPI LEGITTIMI E SPECIFICI

MASTER raccoglie e tratta Dati Personali solo nella misura in cui sia stato fornito un consenso valido e informato o ciò sia richiesto da legittimi interessi imprenditoriali, come: stipulare o eseguire un contratto, effettuare e ricevere pagamenti, eseguire obblighi contrattuali e conformarsi agli impegni legali o regolatori.

Qualsiasi consenso dato alla raccolta e all’uso dei Dati Personali deve essere prestato liberamente e in risposta a una chiara informativa di MASTER sull’uso che s’intende farne. Tale consenso è

revocabile in qualsiasi momento, senza indebite complicazioni. La data, il contenuto e la validità di tale consenso vanno sempre documentati.

Aderiamo alle istruzioni fornite dai Titolari del Trattamento dei Dati e permettiamo che il consenso prestato sia successivamente revocato. Durante il trattamento di Dati Personali per conto di un cliente o un'altra terza parte (Titolare del Trattamento dei Dati), MASTER si conformerà alle linee guida e istruzioni di questa Policy.

5. CONSERVAZIONE

Conserviamo i Dati Personali solo per il periodo di tempo richiesto dalle loro previste finalità. Rispondiamo a qualsiasi richiesta o reclamo presentato in connessione ai Dati Personali in nostro possesso e riconosciamo i diritti a:

- Richiedere l'accesso ai propri Dati Personali raccolti da MASTER e la ragione per cui li possediamo.
- Ottenere una copia dei propri Dati Personali in MASTER.
- Richiedere la rettifica o cancellazione di Dati Personali inesatti o incompleti.
- Revocare in qualsiasi momento il consenso prestato per la raccolta dei propri Dati Personali, compreso il diritto di recedere dall'iscrizione nel data base.

MASTER risponde alle richieste presentate dagli individui esercitanti i loro diritti entro un ragionevole periodo di tempo dopo la richiesta della persona, o qualsiasi periodo specifico che potrebbe essere richiesto dalle norme applicabili.

In caso di reclami, li gestisce, analizza e risponde tempestivamente in merito a qualsiasi violazione delle suddette regole o delle leggi sulla privacy dei dati.

6. ADOZIONE DI APPROPRIATE MISURE DI SICUREZZA

MASTER si attiene ad appropriate misure di sicurezza tecniche e organizzative per proteggere i Dati Personali ed ha implementato la procedura in **Allegato 1 Procedura IT per il trattamento dei dati**.

Le misure di sicurezza comprendono attività coerenti al tipo di trattamento e alla natura dei dati da proteggere; sono attuate prontamente per informare e tutelare le persone su qualsiasi violazione della privacy che abbia compromesso i loro Dati e notifica tale incidente alle autorità pertinenti, come richiesto dalle leggi applicabili.

7. ADEGUATA PROTEZIONE AI TRASFERIMENTI, ANCHE INTERNAZIONALI

MASTER trasferisce Dati Personali oltre i confini nazionali solo quando ciò sia giustificato per fini commerciali ed esistano garanzie per assicurare che i Dati Personali continuino a essere tutelati, almeno allo stesso livello di protezione richiesto dalla giurisdizione di origine.

Quando i Dati Personali sono trasferiti, ci assicuriamo di avere preso le misure necessarie per proteggerli prima del trasferimento stesso.

ALLEGATO 1 - PROCEDURA IT PER IL TRATTAMENTO DEI DATI

INFRASTRUTTURA IN GENERALE

L'infrastruttura IT della Master Management Studi e Ricerche è basata su una rete Lan di tipo esemplificato con un centro stella rappresentato da uno Switch 48 porte e altri 3 switch di servizio gestiti e con protocollo VLAN configurato per separare i protocolli VOIP da quelli Dati LAN. È stata configurata altresì una rete WLAN con accesspoint Ubiquiti e server di gestione UNIFI, il tutto protetto da protocollo WPA2 e regole di scheduling pre-programmate. La rete fisica è rappresentata da cavi rame in cat 5E e ogni device è connesso attraverso opportuna presa.

STOCCAGGIO DATI E PROCEDURE DI BACKUP

I dati di lavoro sono conservati in una unità NAS (Synology Diskstation) parallelamente ad altri file che sono memorizzati in Microsoft One Drive for Business. L'accesso all'unità NAS è protetto fisicamente da:

- 1) Porta di ingresso alla stanza chiusa con chiave custodita da personale demandato
- 2) Porta armadio rack contenente l'unità chiusa a chiave e custodita da personale demandato
- 3) Sistema di allarme/videosorveglianza gestito da personale interno

L'unità è provvista di sistema RAID per la salvaguardia dell'operatività e provvede a replicare i propri dati sia su unità esterna che su apposita sede remota (per alcuni file e cartelle). In caso di guasto dell'unità è possibile ripristinare il funzionamento inserendo i dischi in altra unità oppure qualora vi sia guasto sui dischi è possibile o sostituire gli stessi oppure ricorrere al ripristino del backup. Il Backup viene eseguito ogni 3 ore e la retention copre 6 mesi di tempo. L'accesso in rete all'unità è regolato attraverso apposita ACL in accordo con diritti d'accesso dei singoli utenti.

POSTA ELETTRONICA E CLOUD

La posta elettronica della Master Management risiede presso Microsoft Corporation attraverso il servizio Office 365, per le politiche di conservazione è stato configurato il servizio di archiviazione. Riguardo le procedure si rimanda al contratto di servizi della Società stessa.

BLOCCO DEI DATI E CONSERVAZIONE

Qualora sia segnalato un uso inappropriato dei dati, l'account viene bloccato ed impedito l'accesso sia a file che ai servizi. Nel momento in cui una risorsa cessa il rapporto di collaborazione con MASTER, i suoi dati sono conservati per 30 giorni dopodiché vengono eliminati sia dal cloud che on premise.

RETE WAN E SICUREZZA

La connettività internet è fornita dal gestore attraverso il proprio hardware al quale è stato affiancato un firewall hardware ed un sistema di filtri/antivirus in cloud. Il firewall è configurato per bloccare attacchi di tipo DDOS e tentativi di intrusione. L'antivirus è aggiornato continuamente ogni ora e provvede ad una scansione giornaliera con reporting in tempo reale. Sono stati imposti dei blocchi a pagine con contenuto non adatto e con probabile codice modificato.

PC IN RETE E ACCESSO

L'uso dei Computer in rete è regolato da apposite utenze protette da password che scadono ogni 6 mesi.

Le password sono compliant ai requisiti di complessità e lunghezza.

Ogni utente non ha i diritti di amministrazione sul PC e solo il Network Admin può eseguire operazioni di installazione/disinstallazione.

ALLEGATO 2 - INFORMATIVA PER LA FORMAZIONE: REGOLAMENTO EUROPEO PER LA TUTELA DEI DATI E I RAPPORTI DI COLLABORAZIONE E ACCORDO CON LA MASTER DATA PRIVACY POLICY

Questo Allegato, è utilizzato in MASTER per formare e informare dipendenti, consulenti, professionisti, clienti, fornitori e collaboratori esterni sul **Regolamento Europeo n.679 del 27 aprile 2016**. È riferito a tutto quel che prevede il trattamento dei dati personali per la tutela delle persone fisiche, con riguardo al trattamento dei dati personali. È propedeutico alla registrazione del **consenso/non consenso** all'accordo con la Master Data Privacy Policy e al trattamento e trasferimento dei dati personali.

Premesse

Formalizzazione: Nonostante il nostro rapporto si basi sulla fiducia, il GDPR ci obbliga a formalizzare il tuo impegno quando tratti dati che sono del cliente finale.

Qualità del servizio: Sappiamo anche che il GDPR è un'opportunità per continuare a migliorare la qualità del nostro servizio; dimostrare la nostra professionalità; continuare a coltivare la fiducia dei nostri clienti attraverso i nostri comportamenti, le nostre capacità, il nostro lavoro e la nostra attitudine positiva.

Differenziazione: Non vogliamo essere guidati dalla preoccupazione di commettere errori nel rispettare il GDPR, bensì dall'opportunità di differenziarci, attraverso un trattamento sicuro e rispettoso dei dati personali.

Valori: Noi, come te, abbiamo una ferma volontà di rispettare i diritti fondamentali delle persone, non solo perché è legalmente nostro obbligo, ma perché tale atteggiamento è parte dei nostri valori. Senza dimenticare che la nostra professione è in stretta connessione con l'essere umano e con il miglioramento delle sue capacità e sviluppo e, quindi, abbiamo una responsabilità aggiuntiva quando si tratta di trattare dati personali perché il diritto alla protezione dei dati è un diritto fondamentale. Sono molte, quindi, le ragioni per prestare particolare attenzione a questo regolamento: legali, professionali, valoriali, di reputazione, commerciali.

Atteggiamento proattivo e responsabile: Sappiamo che durante la prestazione di un servizio dobbiamo trattare i dati personali del cliente. Sono dati di cui MASTER non sempre è il titolare del trattamento, ma il responsabile. Abbiamo, per questo, una responsabilità nel prenderci cura dei dati personali e conservarli correttamente. Perdere i dati o trattarli in modo errato non solo può danneggiare l'interessato stesso, ma anche la società per la quale prestiamo il servizio. E noi, non vogliamo causare danni a nessuno.

Professionalità: Contiamo di concordare sul fatto che la cura dei dati con un atteggiamento proattivo e responsabile è, oggi, una risorsa preziosa che rende un professionista migliore. Ci impegniamo a fornire un servizio eccellente e questo ci spinge a prendere in considerazione le normative sulla protezione dei dati.

Fiducia: Inoltre, sappiamo entrambi che è una questione di fiducia. La fiducia che il cliente ripone in noi come azienda lo porta a comunicare determinati dati personali per l'esecuzione di un servizio. A nostra volta, confidiamo in te, come professionista, affinché, quando fornisci un servizio per conto di MASTER, ti prenda cura di questi dati come stabilito dalle normative. È una catena di fiducia che non vogliamo rompere, ma rafforzare. E, per questo, tu sei un "anello" essenziale.

CLAUSOLE

Abbiamo scelto di chiarire le clausole richieste dal Regolamento sulla Privacy in modalità FAQ. In questo modo le risposte - che leggi di seguito - sono utili per formarti e orientarti nella conoscenza delle norme che ispirano questo accordo: d. lgs. 196/2003 "Codice Privacy" e Regolamento UE 679/2016 "GDPR".

PRIMA - In quali casi si applica la tua condizione di sub responsabile del trattamento?

Scopo e Ruoli: Si applica ai servizi a cui partecipi. Ad esempio, se domani MASTER (responsabile esterno del trattamento) firma un contratto con un cliente (titolare del trattamento) per un servizio di prevenzione e sicurezza nei luoghi di lavoro o una formazione (senza limitarci a questi casi), dove tratteremo dati personali, e tu partecipi come consulente esterno nell'erogazione del servizio, in quel momento, **automaticamente, sei sub-responsabile del trattamento dei dati personali** che MASTER tratterà per conto del Titolare (il cliente).

SECONDA - Prima di firmare il contratto devi fare un controllo preventivo?

Fai un check: Ci fidiamo di te e siamo sicuri che potrai svolgere questo ruolo senza problemi, grazie al tuo comportamento, alle tue capacità/skills e al tuo impegno che ci hai dimostrato durante il periodo in cui abbiamo collaborato insieme. D'altra parte, è importante che tu sia consapevole di quali sono i tuoi obblighi e pertanto, questo documento è accompagnato dall'Allegato 2 che ti chiediamo di leggere attentamente.

TERZA - Hai l'obbligo di accettare questo incarico come sub responsabile del trattamento?

MASTER ha l'obbligo di chiederti di assumere determinate misure di sicurezza per il trattamento dei dati, così come di poter verificare e monitorare che tu le rispetti. Per questo è **necessario che il consulente esterno assuma il ruolo** di sub responsabile del trattamento laddove richiesto legalmente o contrattualmente dal cliente.

QUARTA - Cosa devi fare come sub responsabile del trattamento?

Compiti: Tutto ciò che devi fare è rispettare le misure organizzative e di sicurezza che ti trasmettiamo nell'allegato sopra menzionato. Ma non preoccuparti perché è semplice! L'importante è essere consapevoli delle misure e applicarle correttamente. MASTER sarà sempre al tuo fianco per supportarti nel caso di dubbi o domande.

QUINTA - Le condizioni stabilite negli allegati possono modificarsi?

Cambiamenti: Sì, potrebbero essere modificate per eventuali aggiornamenti normativi o perché il nostro cliente potrebbe chiederci in un contratto specifico delle misure aggiuntive o complementari, che riteniamo ragionevoli rispettare, per la tipologia di dati da trattare o rischi potenziali per i diritti e le libertà dell'interessato.

SESTA - Che impatto avrebbero questi cambiamenti?

Gestione del Cambiamento: Prima di dover attuare qualsiasi nuova misura invieremo un'e-mail all'indirizzo che ci hai indicato e attraverso il quale comunichiamo abitualmente con te. Ti spiegheremo le variazioni e ti chiederemo di accettarle, se sei d'accordo. In caso affermativo, ti chiederemo una risposta via e-mail e/o con qualsiasi altra modalità che considereremo appropriata, al fine di creare un rapporto trasparente e chiaro con te.

SETTIMA - Altri obblighi

Obblighi legali: Accetti di rispettare tutti gli obblighi che possano derivare dalla tua condizione di sub responsabile o responsabile del trattamento che, anche se non sono citati in questo accordo, esistono espressamente nelle attuali normative sulla protezione dei dati, così come i processi, le politiche o le regole che, in relazione a questo argomento, possa creare e comunicare MASTER.

OTTAVA - Formazione

Apprendimento: Firmando questo documento, riconosci che hai già partecipato ad almeno una formazione sul GDPR organizzate da MASTER e accetti di frequentare nuovi corsi di formazione che potremmo organizzare sulle norme di protezione dei dati relative ai tuoi obblighi professionali.

NONA - Durata

Tempo: Il presente Accordo decorre dalla data della sua sottoscrizione e rimarrà in vigore fin tanto che il sub responsabile o responsabile del trattamento effettuerà il trattamento dei Dati Personali di cui MASTER è Responsabile del trattamento e/o Titolare del Trattamento.

DECIMA - Diritto di audit e di verifica periodica

Audit: MASTER si riserva il diritto di compiere attività di audit e, in particolare, avrà facoltà di verificare, con un preavviso di almeno 7 (sette) giorni lavorativi, anche presso la sede del sub responsabile e/o responsabile del trattamento, la conformità delle procedure adottate da quest'ultimo rispetto a quanto indicato nel presente Accordo o richiesto dalla normativa.

UNDICI - Clausole finali

Il presente Accordo sostituisce ogni precedente intesa, anche verbale, fra le parti e costituisce l'unico esistente in relazione alle materie in esso trattate. L'eventuale tolleranza di una parte all'inadempimento dell'altra non potrà in alcun modo essere considerata come rinuncia ai diritti derivanti dal presente Accordo. Qualsiasi notifica, lettera o altra comunicazione prevista dal presente Accordo è comunicata per iscritto tramite email e/o lettera agli indirizzi di seguito indicati: amministrazione@mastersicurezza.it e f.marinangeli@mastersicurezza.it

ALLEGATO 3 - NOMINA RESPONSABILE E/O SUB RESPONSABILE DEL TRATTAMENTO

Gentile (*inserire nome e cognome*)

nonostante il nostro rapporto si basi sulla fiducia, il GDPR ci obbliga a formalizzare il tuo impegno quando tratti dati che sono del cliente finale. Così come il cliente disciplina il servizio con MASTER attraverso un contratto in cui può nominarci responsabili del Trattamento dei Dati, a nostra volta noi **nominiamo te**, formalmente, **sub responsabile del trattamento**. Questo ruolo è regolato dalle normative applicabili in materia di protezione dei dati e delle disposizioni contrattuali, attraverso il seguente

ACCORDO TRA

MASTER MANAGEMENT STUDI E RICERCHE srl (di seguito MASTER) con sede in Via Sallustiana, 15 - 00183 Roma - P.IVA 01549771002.

E

Nome e Cognome Consulente/Collaboratore _____
residente in _____ CAP _____
città _____ Codice Fiscale - P.IVA _____ e-mail _____
in seguito indicate come "le Parti".

Ai sensi dell'art. 13 del Regolamento Europeo (EU) 679/2016 relativo alla protezione dei dati personali (di seguito il "GDPR") e della normativa nazionale, compresi i singoli provvedimenti dell'Autorità di controllo, Garante per la protezione dei dati personali, ove applicabile, le comunichiamo che, nella sua qualità di Consulente, Professionista e/o Collaboratore esterno, MASTER potrà raccogliere i suoi dati, qualificati come personali dal predetto Regolamento. Pertanto, MASTER è tenuta, in qualità di Titolare del trattamento, a fornirle alcune informazioni riguardanti il trattamento degli stessi.

Specifichiamo che per "trattamento" di dati personali, ai sensi del GDPR, si intende qualsiasi operazione o insieme di operazioni, compiute da MASTER con o senza l'ausilio di processi automatizzati e applicate ai suoi dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione. Il trattamento dei dati riguarda solamente dati "comuni" (esempio: nome/cognome/indirizzo/telefono/email/codice fiscale/dati bancari) ovvero informazioni che non comprendono dati particolari ai sensi dell'articolo 9 del GDPR.

1. Identificazione del Titolare del Trattamento

Il Titolare del trattamento dei dati personali è MASTER MANAGEMENT STUDI E RICERCHE srl con sede in Via Sallustiana, 15 - 00183 Roma - P.IVA 01549771002.

2. Finalità del Trattamento

Il trattamento dei dati personali degli interessati, persegue la finalità di:

- stipulare e dare esecuzione ai rapporti contrattuali e servizi professionali (di seguito il "Contratto") con i consulenti, professionisti e/o collaboratori autonomi di MASTER;
- rispondere a specifiche richieste provenienti dall'interessato (consulenti, professionisti e/o collaboratori autonomi) ai fini di una successiva relazione contrattuale;

- adempiere agli obblighi previsti dalla legge, da un regolamento o dalla normativa comunitaria;
- gestire di eventuali reclami, contenziosi. Ad esempio, per far valere o difendere nelle sedi competenti (giudiziarie, arbitrali, amministrative, ecc.) diritti del titolare del trattamento;
- attuare comunicazioni relative allo svolgimento del rapporto contrattuale.

3. Modalità del Trattamento e Comunicazione dei Dati

In relazione alle finalità sovraesposte i dati sono oggetto di trattamento informatico e cartaceo.

Comunicazione dei Dati. Il titolare del trattamento potrà comunicare i dati degli interessati a terzi, quali autonomi titolari, ovvero responsabili al trattamento, che prestano al Titolare servizi accessori all'esecuzione del Contratto. I dati potranno essere comunicati a tutte quelle persone fisiche e/o giuridiche, pubbliche e/o private quando la comunicazione risulti necessaria o funzionale alla costituzione del rapporto di collaborazione, nei modi e per le finalità sopra illustrate, in particolare (a mero titolo esemplificativo):

- ai soci dei Titolari per l'esercizio dei loro diritti di controllo;
- ai nostri collaboratori, dipendenti, nell'ambito delle relative mansioni incaricati di trattare i dati;
- a Società del settore bancario e creditizio che forniscono servizi per la gestione delle transazioni finanziarie connesse ai pagamenti degli interessati;
- a fornitori del comparto dei servizi IT per servizi di installazione, assistenza e manutenzione di impianti e sistemi informatici e telematici e di tutti i servizi funzionalmente connessi e necessari per l'adempimento delle prestazioni oggetto del Contratto;
- a persone, società o studi professionali, che prestano attività di assistenza, consulenza o collaborazione al Titolare in materia contabile, amministrativa, legale, tributaria e finanziaria relativamente al Contratto;
- a piattaforme tecnologiche o strumenti tecnologici (ad esempio, Drive o Google Docs) che, se si trovano fuori dall'unione europea, hanno aderito all'Accordo denominato "EU-U.S. Privacy Shield", accordo che, secondo la decisione della Commissione Europea del 12 luglio 2016 n. 2016/1250, garantisce un livello adeguato di protezione dei dati personali trasferiti dall'Unione europea ad organizzazioni aventi sede negli Stati Uniti d'America;
- a tutti i soggetti cui la facoltà di accesso a tali dati è riconosciuta in forza di provvedimenti normativi.

In tutti i casi sopra illustrati, la base giuridica - a seconda dei casi - saranno il Contratto di servizi, l'obbligo di adempiere a norme di legge, l'interesse legittimo e - quando nessuna delle anteriori basi giuridiche sia di applicazione - sarà il consenso dell'interessato.

4. Trasferimento dei dati all'estero

MASTER trasferisce Dati Personali oltre i confini nazionali solo quando ciò sia giustificato per fini commerciali ed esistano garanzie per assicurare che i Dati Personali continuino a essere tutelati, almeno allo stesso livello di protezione richiesto dalla giurisdizione di origine. Quando i Dati Personali sono trasferiti, ci assicuriamo di avere preso le misure necessarie per proteggerli prima del trasferimento stesso.

5. Periodo di conservazione dei dati

I dati forniti verranno conservati per tutta la durata del rapporto di collaborazione e per un periodo successivo fino a 30 giorni, dopodiché vengono eliminati sia dal cloud che on premise.

6. I suoi Diritti

Lei potrà esercitare, in relazione al trattamento dei dati ivi descritto, i diritti previsti dal Regolamento (art.15-21): ricevere conferma dell'esistenza dei suoi dati personali e accedere al loro contenuto (**diritti di accesso**); aggiornare, modificare e/o correggere i suoi dati personali (**diritto di rettifica**); chiederne la cancellazione o la limitazione del

trattamento dei dati trattati in violazione di legge compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o altrimenti trattati (**diritto all'oblio e diritto alla limitazione**); opporsi al trattamento (**diritto di opposizione**) in qualsiasi momento; revocare il consenso, ove prestato, senza pregiudizio per la liceità del trattamento basata sul consenso prestato prima della revoca; proporre reclamo all'Autorità di controllo in caso di violazione della normativa in materia di protezione dei dati personali; ricevere copia dei dati in formato elettronico che lo riguardano e chiedere che tali dati siano trasmessi ad un altro titolare del trattamento (**diritto alla portabilità dei dati**).

7. Revoca del consenso al trattamento.

Si ricorda che, ai sensi dell'art. 7 del Regolamento, è riconosciuta la facoltà di revocare per iscritto il consenso al trattamento dei dati personali. Per esercitare tali diritti Lei potrà inviare una richiesta scritta all'indirizzo postale della sede legale (Via Sallustiana 15 – 00187 Roma) o all' indirizzo info@mastersicurezza.it.

DICHIARAZIONE DI PRESA VISIONE DELL'INFORMAZIONE (art. 13 GDPR)

Il/La sottoscritto/a..... dichiara di aver ricevuto le informazioni di cui all'art. 13 del Regolamento UE 2016/679, in particolare sui diritti riconosciuti dallo stesso, e di acconsentire ai sensi e per effetto dell'articolo 7 e s.s. del Regolamento UE 2016/679 al trattamento dei suoi dati personali con le modalità e per le finalità indicate nell'informativa stessa, comunque strettamente connesse e strumentali alla gestione del rapporto di collaborazione.

Dichiaro di fornire il consenso al trasferimento dei dati personali per le finalità sopra indicate:

Sì No

Roma

Firma.....

ALLEGATO 4 - NOMINA RESPONSABILE DEL TRATTAMENTO IN QUALITÀ DI AMMINISTRATORE DI SISTEMA

Provvedimento Generale del Garante per la Protezione dei Dati Personali del 27 novembre 2008

Il sottoscritto FEDERICO MARINANGELI, Legale Rappresentante di MASTER MANAGEMENT STUDI E RICERCHE SRL sita in via Sallustiana 15 00187 Roma, in qualità di Titolare del trattamento di dati personali operati nell'ambito della propria attività professionale, con il presente atto designa:

il Signor (*nome e cognome*)

P.IVA

INDIRIZZO

Responsabile del trattamento in qualità di Amministratore di Sistema

Ai sensi e per gli effetti degli articoli da 31 a 36 del D.Lgs. 30 giugno 2003 n. 196 nonché in osservanza del Disciplinare Tecnico in materia di misure minime di sicurezza di cui all'allegato B) del medesimo Codice.

L'Amministratore di Sistema (System Administrator) viene designato quale figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati (Database Administrator), i sistemi software complessi quali i sistemi ERP (Enterprise Resource Planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, i sistemi hardware e software che consentono di utilizzare la rete internet e il servizio di posta elettronica (Network Administrator) nella misura in cui consentano di intervenire sui dati personali.

Il Signor (*nome e cognome*) nella qualità di Amministratore di Sistema ha il potere e il dovere di compiere tutto quanto si renderà necessario ai fini del rispetto e della corretta applicazione del D.Lgs. 30 giugno 2003 n. 196, con particolare riferimento al profilo relativo alla sicurezza nella custodia e nel trattamento dei dati personali.

La designazione del Signor (*nome e cognome*) avviene in ragione del possesso in capo a quest'ultimo/a dei requisiti di capacità tecniche, professionali e di condotta.

Specificatamente, l'Amministratore di Sistema sarà tenuto a:

job description - elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato e alle dimensioni dell'azienda/studio professionale

1 - classificare analiticamente le banche dati ed impostare/organizzare un sistema complessivo di trattamento dei dati personali comuni e sensibili che riguardi tutte le operazioni richiamate dall'art. 4, comma 1, lett. a) nessuna esclusa, predisponendo e curando ogni relativa fase applicativa nel rispetto della normativa vigente in materia di protezione dei dati personali;

2 - individuare per iscritto il/i soggetto/i incaricato della custodia delle parole chiave per l'accesso al sistema informativo e vigilare sulla sua attività;

3 - individuare per iscritto gli altri soggetti, diversi dal/dagli incaricato/i della custodia delle parole chiave, che possono avere accesso ad informazioni che concernono le medesime;

- 4 – impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici, conforme a quanto previsto dai punti da 1 a 10 del Disciplinare Tecnico, allegato B) al D.Lgs. 196/2003;
- 5 – impostare e gestire un sistema di autorizzazione per gli incaricati dei trattamenti di dati personali effettuati con strumenti elettronici, conforme a quanto previsto dai punti da 12 a 14 del Disciplinare Tecnico, allegato B) del D.Lgs. 196/2003;
- 6 - adottare un sistema idoneo alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici; le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste; tali registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi;
- 7 - assicurare e gestire sistemi di salvataggio e di ripristino dei dati (backup/recovery), anche automatici nonché approntare adeguate misure e/o sistemi software di salvaguardia per la protezione dei dati personali (antivirus, firewall, IDS);
- 8 – impartire a tutti gli incaricati istruzioni organizzative e tecniche che prevedano le modalità di utilizzo dei sistemi di salvataggio dei dati con frequenza almeno settimanale;
- 9 – adottare procedure per la custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi;
- 10 - organizzare i flussi di rete, la gestione dei supporti di memorizzazione, la manutenzione hardware, la verifica di eventuali tentativi di accessi non autorizzati al sistema provenienti da soggetti terzi quali accesso abusivo al sistema informatico o telematico (articolo 615 ter), frode informatica (articolo 640 ter), danneggiamento di informazioni, dati e programmi informatici (articoli 635 bis e ter), danneggiamento di sistemi informatici e telematici (articoli 635 quater e quinquies);
- 11 – predisporre, anche in contraddittorio con il Titolare dei trattamenti, un piano di controlli periodici, da eseguirsi con cadenza almeno semestrale, atti a verificare l'efficacia delle misure di sicurezza adottate in azienda/studio professionale;
- 12 – coadiuvare, se richiesto, il Titolare del trattamento nella predisposizione e/o aggiornamento e/o integrazione del Documento Programmatico sulla Sicurezza (D.P.S.) previsto dal punto 19 del Disciplinare Tecnico, allegato B) del D.Lgs. 196/2003 nonché alla stesura del documento denominato "Disciplinare in Materia di Utilizzo di Strumenti Informatici".

È compito dell'Amministratore di Sistema monitorare costantemente lo stato di sicurezza di tutti i processi di elaborazione dati di cui sopra, mantenendo aggiornati tutti i supporti hardware e software e, se del caso, comunicando al Titolare tutte le attività da porre in essere al fine di garantire un adeguato livello di sicurezza in proporzione alla tipologia e quantità dei dati personali trattati.

L'operato dell'Amministratore di Sistema sarà oggetto, con cadenza annuale, ad una attività di verifica da parte del Titolare del trattamento, tesa a controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previsti dalle norme vigenti.

Roma, li Il Titolare

L'Amministratore di Sistema

La preghiamo di restituirci copia della presente, firmata per accettazione.