Regolamento per l'adeguamento al GDPR (Reg. UE 2016/679) e per l'impostazione di un Sistema per la Gestione della Sicurezza delle Informazioni

Data creazione: 21/6/2018

Data aggiornamento: 10/07/2018

Il presente documento si compone di n. 16 pagine (inclusa la presente)

INDICE

1. Premessa

Dal 25 maggio 2018 è divenuto operativo il *"Regolamento (UE) 2016/679"* del Parlamento europeo e del Consiglio 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) rendendo più trasparente il comportamento degli Enti verso le informazioni riguardante una persona fisica identificata o identificabile (interessato).

I destinatari del Regolamento sono tutti i soggetti (organizzazioni) che, nell'esercizio della loro attività lavorativa, utilizzano (trattano) dati personali di individui. Tali organizzazioni, che determinano per il loro funzionamento le finalità e i mezzi del trattamento, sono definiti Titolari del Trattamento dei dati personali. Qualora un'organizzazione operi trattamenti per conto di titolari si parla invece di Responsabili del Trattamento.

Il presente documento è stato elaborato in conformità con il Regolamento UE 2016/679 relativo alla protezione dei dati personali (a seguire solo *GDPR)*, anche alla luce delle Linee Guida, dei Provvedimenti e delle altre indicazioni pubblicate sul sito dell'Autorità Garante per la Protezione dei Dati Personali (a seguire solo *Garante*).

2. Obiettivo del presente Regolamento

Il presente regolamento permette di raggiungere i seguenti obiettivi:

 implementare il principio fondamentale di responsabilizzazione ("accountability") introdotto dal GDPR, in base al quale il titolare deve non solo essere conforme alle prescrizioni del GDPR, ma deve anche essere in grado di dimostrare la conformità raggiunta;

 indicare metodologie e prassi operative specifiche per l'adeguamento alle prescrizioni del GDPR, tenendo conto del contesto specifico dell'Ente;

 in particolare, per quanto riguarda la sicurezza, individuare precisamente una procedura per testare, verificare periodicamente e valutare regolarmente l'efficacia delle misure tecniche ed organizzative da mettere in atto per assicurare un adeguato livello di sicurezza e di protezione dei dati;

 impostare un SGSI – Sistema di Gestione della Sicurezza delle Informazioni - che permetta di dimostrare che l'Istituto è conforme ai requisiti di sicurezza previsti dall'art. 32 del GDPR e conforme a riconosciuti *standard* di sicurezza a livello internazionale.

3. "Concetti chiave" GDPR (art. 4 RGPD)

- *Dato personale*: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»);
- *dato particolare (già definito "dato sensibile")*: qualsiasi dato personale idoneo a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché il dato personale idoneo a rivelare lo stato di salute e la vita sessuale dell'interessato;
- *dato giudiziario* qualsiasi dato personale idoneo a rivelare procedimenti o provvedimenti di natura giudiziaria;
- *trattamento*: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a 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;

- *profilazione*: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- *pseudonimizzazione*: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- *archivio*: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato o decentralizzato;
- *titolare del trattamento*: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
- *responsabile del trattamento*: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- *consenso dell'interessato*: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso a che i dati personali che lo riguardano siano oggetto di trattamento;
- *violazione dei dati personali*: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- *autorità di controllo*: organismo volto al controllo del rispetto della normativa sulla protezione dei dati personali, istituito in ogni Stato membro.

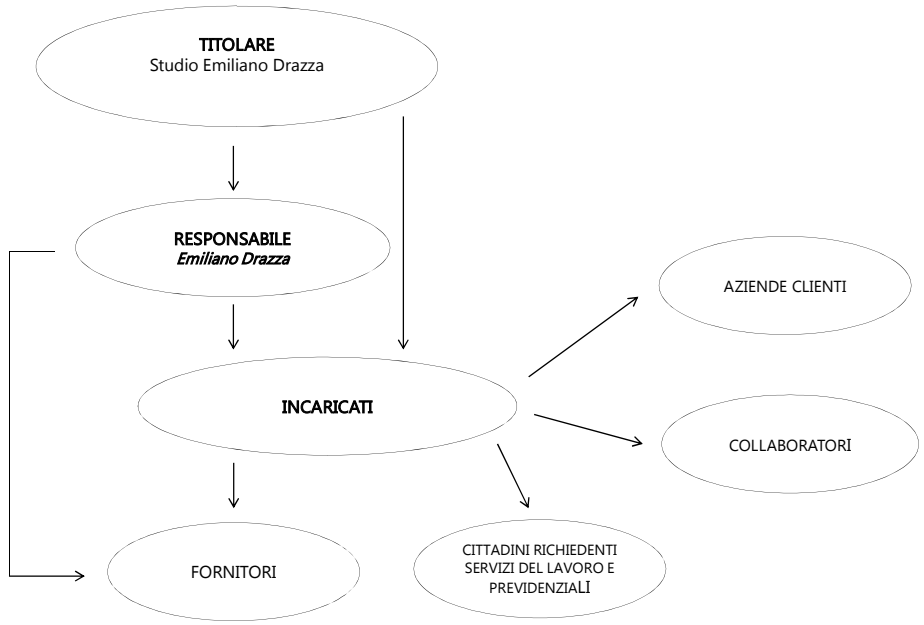
4. "Policy" dello Studio sulla protezione dei dati personali

Lo Studio professionale pone alla base del proprio sistema di gestione per la Privacy i seguenti strumenti:
→ individuare al proprio interno le figure coinvolte nel Trattamento dei dati e fornire loro adeguata formazione, supporto tecnico e sufficienti risorse;
→ trattare tutti i dati personali in modo lecito, corretto e trasparente nei confronti dell'interessato e solo in presenza delle condizioni di liceità previste dal GDPR, e nello specifico:
a) consenso dell'interessato al Trattamento dei propri dati personali per una o più specifiche finalità;
b) il Trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte;
c) il Trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del Trattamento;
d) il Trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il Trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del Trattamento;
f) il Trattamento è necessario per il perseguimento del legittimo interesse del Titolare del Trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.
→ raccogliere dati solo per finalità determinate, esplicite e legittime;
→ trattare i dati in possesso dell'ente in modo compatibile con le finalità per le quali sono raccolti;
→ astenersi di regola dal trattare senza il consenso esplicito dell'interessato i suoi dati particolari;
→ applicare il principio della *"minimizzazione dei dati"*, in base al quale il Trattamento dei dati viene limitato allo stretto indispensabile in relazione alle finalità per le quali i dati sono raccolti;

→ raccogliere i dati in modo esatto, correggere tempestivamente i dati non esatti ed aggiornarli ogni volta che sia necessario;
→ conservare i dati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
→ trattare i dati personali secondo i principi di integrità e riservatezza, quindi in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;
→ svolgere periodicamente *audit* interni sul sistema Privacy;
→ predisporre, per i dati sensibili dell'attività legale nel'ambito dei diritto di famiglia e della tutela sanitaria, e conservare un Registro di tutti i trattamenti effettuati, comprensivo della valutazione del rischio per ciascun Trattamento;
→ adottare adeguati provvedimenti disciplinari nei confronti degli addetti dell'ente che non osservano le disposizioni aziendali sulla Privacy;
→ garantire ad ogni interessato i diritti di accesso, rettifica e cancellazione dei dati che lo riguardano.

5. Organigramma

ORGANIGRAMMA PRIVACY
STUDIO EMILIANO DRAZZA



Elenco interessati al trattamento dei dati personali:

1) *aziende clienti e dipendenti delle stesse*
2) *cittadini richiedenti servizi di previdenza e consulenza del lavoro*
3) *Fornitori*

4) Collaboratori

Individuazione responsabili e/o incaricati al trattamento dei dati

Interessati	responsabile e/o Incaricato	compiti
1) Aziende clienti e dipendenti delle stesse	*Emanuela Scarozza*	*incaricato consulenza e servizi lavoro e previdenza*
	Davide Drazza	*incaricato consulenza e servizi lavoro e previdenza*
	Alfredo Bruno	*incaricato consulenza e servizi lavoro e previdenza*
	Emiliano Drazza	*responsabile consulenza e servizi lavoro e previdenza*
	Nicola Rucci	*responsabile esterno servizi informatici lavoro*
2) Cittadini richiedenti servizi di previdenza e consulenza	*Emiliano Drazza*	*responsabile consulenza e servizi lavoro e previdenza*
	Emanuela Scarozza	*incaricato consulenza e servizi lavoro e previdenza*
	Davide Drazza	*incaricato consulenza e servizi lavoro e previdenza*
	Alfredo Bruno	*incaricato consulenza e servizi lavoro e previdenza*
3) Fornitori	*Davide Drazza*	*incaricato monitoraggio e gestione contratti*
	Emiliano Drazza	*responsabile monitoraggio e acquisizione contratti*
4) Collaboratori	*Davide Drazza*	*incaricato monitoraggio e gestione contratti*
	Emiliano Drazza	*responsabile monitoraggio e gestione contratti*

Ogni Responsabile e/o Incaricato dovrà essere nominato dal Titolare con atto scritto contenente l'indicazione specifica dei compiti affidatigli relativamente al trattamento dei dati cui è preposto; le lettere di incarico dovranno essere custodite all'interno dell'Ente e poste a disposizione dell'Autorità di controllo.

5.1. Titolare del Trattamento

Il Titolare del trattamento (*data controller*) è *"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le **finalità** e i **mezzi** del trattamento di dati personali"* (art. 4. par. 1, n. 7 GDPR). In sostanza il titolare è colui che tratta i dati senza ricevere istruzioni da altri, colui che decide "perché" e "come" devono essere trattati i dati.
Pertanto, il Titolare del Trattamento è il Dr. Emiliano Drazza quale titolare dello studio omonimo

5.2. Responsabile Protezione Dati (DPO)

Ai sensi degli articoli 37, 38 e 39 del GDPR il Titolare del Trattamento può designare un responsabile della protezione dei dati che nella fattispecie non si intende designare.

5.3. Responsabile esterno

Per tutte le attività che l'Ente intenda esternalizzare è obbligatoria la nomina di un Responsabile Esterno del Trattamento ai sensi dell'art. 28 Regolamento UE n. 2016/679 (a seguire GDPR); ciò in relazione ai seguenti settori di attività, oggetto della collaborazione professionale:

- ☐ Elaborazione contabile, amministrativa e fiscale
- ☐ Elaborazione contributiva e in materia di consulenza del lavoro
- ☐ Consulenza Legale
- ☐ Consulenza Sicurezza del lavoro
- ☐ Medico del Lavoro
- ☐ Consulenza Tecnica di progettazione
- ☐ Consulenza sulla Privacy
- ☐ Altro: _____

Segue modello di nomina di Responsabile esterno.

CARTA INTESTATA

Spett.le…….

Lo studio Emiliano Drazza, con sede legale in Roma alla via Federico Delpino 7, C. F. DRZMLN56R22H501A. , in qualità di "Titolare" del trattamento dei dati personali, ai sensi e per gli effetti del GDPR 2016/679

premesso che

- ai sensi dell'art. 4 del GDPR 2016/679 per trattamento dai dati personali si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a 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;
- tenuto conto dei requisiti di esperienza, di capacità e di affidabilità **(indicazione del Responsabile)** è stato incaricato del trattamento dei dati relativi a…**(indicazione della tipologia di interessati al trattamento dei dati ossia Utenti/Fornitori/Personale dipendente/ Collaboratori)** ;
- che, pertanto, risulta opportuno nominare, **(indicazione del Responsabile)** quale Responsabile del Trattamento dei dati personali concernenti i …**(indicazione della tipologia di interessati al trattamento dei dati ossia Utenti/Fornitori/Personale dipendente/ Collaboratori)** dello Studio Drazza il cui trattamento si renda necessario per l'espletamento dell'incarico conferito con **(separato contratto e/o con il presente contratto)**

Tutto ciò premesso, con la presente

nomina

(indicazione del Responsabile) *responsabile esterno del trattamento dei dati personali*

1) Ai fini dell'esecuzione dell'accordo, il Responsabile effettua il trattamento dei seguenti dati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati:
…**(indicazione della tipologia di interessati al trattamento dei dati ossia Utenti/Fornitori/Personale dipendente/ Collaboratori e della relativa attività in concreto posta in essere dal responsabile).**
2) Il Responsabile esterno del trattamento dei dati ha il potere e il dovere di provvedere affinché tutte le operazioni di trattamento informatico e manuale dei dati personali, nei limiti delle proprie competenze e attribuzioni, siano effettuate nel rispetto della normativa vigente e dei regolamenti aziendali in materia di tutela dei dati personali.

3) Il Responsabile, sebbene non in via esaustiva, avrà i compiti e le attribuzioni di seguito elencate e dunque dovrà:
a. garantire che il trattamento dei dati personali di cui è Titolare lo Studio Drazza e di cui venga a conoscenza con l'attività svolta in conformità a quanto previsto dalla vigente normativa e dalle presenti istruzioni;
b. aggiornare periodicamente l'elenco dei trattamenti dei dati personali e le relative banche dati da esso Responsabile gestite;
c. tenere, ove obbligatorio, il Registro dei trattamenti, come previsto da art. 30 del GDPR, in formato elettronico, di tutte le categorie di attività relative al trattamento svolte per conto della Pontificia Facoltà;
d. nominare per iscritto gli "Incaricati del trattamento" attribuendo i livelli di autorizzazione all'accesso ai dati. Il Responsabile del trattamento, quindi:
-provvederà a impartire agli Incaricati idonee istruzioni per iscritto circa le modalità di esecuzione delle attività demandate e a vigilare sul rispetto delle istruzioni impartite;
-aggiornerà con cadenza almeno annuale l'individuazione dell'ambito di trattamento consentito ai singoli incaricati e provvederà a mantenere un elenco aggiornato degli incaricati;
-garantirà che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
-programmare e attuare idonee azioni di informazione e formazione degli incaricati nominati;
e. verificare periodicamente la corretta applicazione della normativa vigente in materia di privacy nonché l'adozione di tutte le misure necessarie a garantire un livello di sicurezza adeguato ai sensi dell'art.32 del GDPR;
f. provvedere affinché vengano rigorosamente adottate tutte le misure idonee a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati trattati con l'Attività, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità per le quali i dati sono stati raccolti;
g. garantire la portabilità dei dati personali trattati in esecuzione del Contratto, ai sensi dell'art. 20 del GDPR, assicurando che gli stessi possano essere trasmessi in un formato strutturato, di uso comune e leggibile da qualsiasi dispositivo automatico;
h. assistere il Titolare del Trattamento per quanto concerne gli obblighi di notifica e ogni altra comunicazione verso il Garante, ove dovute;
i. tenendo conto della natura del trattamento, assistere il Titolare del Trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del Trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del Regolamento Europeo 2016/679;
l. mettere a disposizione del Titolare del Trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dalla normativa vigente;
m. comunicare al Titolare del Trattamento qualsiasi variazione della situazione oggettiva o delle sue proprie caratteristiche soggettive, tali da compromettere il corretto espletamento dei compiti descritti nella presente;
n. informare il Titolare del Trattamento senza ingiustificato ritardo e comunque non oltre le 72 ore dal momento in cui ne è venuto a conoscenza di eventuali violazioni dei dati personali adottando, di concerto con lo stesso, nuove misure di sicurezza atte a circoscrivere gli effetti negativi dell'evento e a ripristinare la situazione precedente;
o. ottemperare tempestivamente alle eventuali richieste inoltrate dal Titolare del Trattamento al fine di rendere conforme il trattamento dei dati posto in essere in esecuzione del Contratto, agli eventuali provvedimenti emessi dal Garante Privacy in materia di trattamento di dati personali;
p. avvertire prontamente il Titolare, entro tre (3) giorni lavorativi, in merito alle eventuali richieste degli interessati che dovessero pervenire al Responsabile, inviando copia delle istanze ricevute all'indirizzo e-mail: **e-mail privacy** e collaborare al fine di garantire il pieno esercizio da parte degli interessati di tutti i diritti previsti Regolamento UE;
q. avvisare immediatamente, e comunque entro tre (3) giorni lavorativi, il Titolare del Trattamento di qualsiasi richiesta o comunicazione da parte dell'Autorità Garante o di quella Giudiziaria o di Pubblica Sicurezza

eventualmente ricevuta, inviando copia delle istanze all'indirizzo e-mail: **e-mail privacy** per concordare congiuntamente il riscontro.
4) Resta inteso che, in caso di cessazione del rapporto intercorrente con lo Studio Drazza per qualsivoglia motivo e/o ragione, cesserà automaticamente anche la presente nomina, con obbligo di restituzione della documentazione inerente l'Ente e/o eventuale sua distruzione a nostra richiesta (fatti salvi gli obblighi di conservazione imposti per Legge).

La presente nomina è consegnata al Responsabile esterno del trattamento dei dati in duplice copia.

Roma, lì ……

PER ACCETTAZIONE
Il Responsabile del Trattamento
(nominativo)
Timbro e Firma

5.4. Incaricati al trattamento

Il GDPR non prevede espressamente la figura dell'incaricato, ma non ne esclude la nomina, facendo riferimento a persone autorizzate al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile (art. 4, n. 10 GDPR).
Incaricato o autorizzato, di fatto è il soggetto, persona fisica, che effettua materialmente le operazioni di trattamento sui dati personali. L'autorizzato può operare alle dipendenze del titolare, ma anche del responsabile se nominato. Ovviamente gli autorizzati sono nominati con apposito incarico scritto nel quale verranno specificate sia la natura dei dati da trattare che la tipologia di trattamento consentita (raccolta, elaborazione, conservazione, consultazione etc…..).
E', altresì, necessario alla luce della nuova normativa che sia fornita loro la necessaria formazione. In caso contrario, infatti, anche in presenza di formali designazioni, queste sarebbero del tutto prive di valore.
Segue modello di lettera di conferimento di incarico al trattamento.

Il sottoscritto, Emiliano Drazza , in qualità di Titolare del Trattamento conferisce l'incarico al Trattamento dei dati, con le modalità a seguire definite.

Nome e cognome dell'incaricato:

Mansioni svolte:

Categoria soggetti interessati:

Dati che l'incaricato è autorizzato a trattare e tipologia del trattamento:

L'incaricato, nel firmare il presente incarico per accettazione, s'impegna a rispettare le regole di Policy interna impartite dal titolare del trattamento dei Dati Personali, relativamente alle clausole compatibili con le mansioni svolte ed i dati personali oggetto dell'incarico, consapevole che in caso di violazione potrà incorrere in provvedimenti sanzionatori.

data firma del Titolare firma dell'Incaricato per accettazione

6. Formazione ed aggiornamento in materia di Privacy

Il Titolare del Trattamento, con l'assistenza del DPO se nominato, organizza la formazione e l'aggiornamento periodico di tutto il personale dell'ente in materia di Privacy.
Per la formazione sulla Privacy sono previsti i seguenti contenuti minimi:
a. formazione iniziale di almeno 2 ore per i collaboratori sul GDPR e sul presente Regolamento;
b. formazione continua di almeno 1 ore per ogni anno di contratto ai collaboratori dello Studio sugli aggiornamenti al presente Regolamento, sulle novità normative e sui risultati dell'attività di audit sulla Privacy nel periodo di riferimento.
I contenuti delle attività formative e la partecipazione dei soggetti sopra indicati saranno registrati attraverso idonee procedure; è auspicabile la consegna di materiale relativo agli argomenti trattati durante gli incontri formativi.

7. Consenso al Trattamento dei dati e informativa (art. 7 GDPR)

L'articolo 7 del GDPR prevede l'atto di consenso dell'interessato al Trattamento dei dati personali presenti le caratteristiche:
"1. Qualora il Trattamento sia basato sul consenso, il Titolare del Trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al Trattamento dei propri dati personali.
2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.
3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del Trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.
4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al Trattamento di dati personali non necessario all'esecuzione di tale contratto".
Rilevante a tale scopo è anche il Considerando 32 del GDPR, in base al quale *Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il Trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il Trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di Trattamento svolte per la stessa o le stesse finalità. Qualora il Trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso.*

Ci impegniamo, pertanto, a raccogliere il consenso al Trattamento dei dati degli interessati utenti, fornitori, dipendenti, collaboratori nel rispetto dei criteri sopra riportati ed a tal fine fornisce il seguente modello di informativa.

INFORMATIVA AI SENSI DELL' ART. 13 GDPR - REGOLAMENTO 2016/679

Lo Studio Drazza Emiliano , con sede legale in Roma alla Federico Delpino 7, C.A.P. 00171, CF drzmln56r22h501a, (in seguito, "**Titolare**"), in qualità di titolare del trattamento, La informa, ai sensi dell'art. 13 del Regolamento UE n. 2016/679 (in seguito, "**GDPR**"), che i Suoi dati saranno trattati con le modalità e per le finalità seguenti.

1. Oggetto del Trattamento

Il Titolare tratta i dati personali, identificativi (ad esempio, nome, cognome, ragione sociale, indirizzo, telefono, *e-mail*, riferimenti bancari e di pagamento) – in seguito, "**dati personali**" o anche "**dati**", da Lei comunicati a codesto Studio in ragione del rapporto giuridico con essa instaurato.

2. Finalità del trattamento

I Suoi dati personali sono trattati:

a) senza il suo consenso espresso ai sensi dell'art. 9 GDPR (c.d. finalità di servizio), per:

- finalità connesse e strumentali alla gestione del rapporto di lavoro dei suoi dipendenti;
- finalità connesse e strumentali alla gestione del rapporto con i professionisti incaricati di ricoprire i ruoli tecnico-professionali all'interno dell'azienda ;
- finalità di tipo amministrativo e/o contabile;
- finalità relative al controllo di adempimento o assolvimento di obblighi derivanti da leggi, regolamenti, statuti, ordine dell'Autorità, e rilevamento dati statistici ad uso interno e, su richiesta, dall'I.S.T.A.T.;
- finalità relative all'esercizio di diritti del Titolare (ad esempio il diritto di difesa in giudizio);
- *b) solo previo Suo specifico e distinto consenso (art. 7 GDPR),* per le seguenti finalità di *marketing*:
- inviarLe via *e-mail*, posta e/o *sms* e/o contatti telefonici, *newsletter,* comunicazioni commerciali e/o materiale pubblicitario su prodotti o servizi offerti dal Titolare e rilevazione del grado di soddisfazione sulla qualità dei servizi.

3. Modalità di trattamento

Il trattamento dei Suoi dati personali è realizzato per mezzo delle operazioni indicate all'art. 4 n. 2) GDPR e precisamente: raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, cancellazione e distruzione dei dati. I Suoi dati personali sono sottoposti a trattamento sia cartaceo che elettronico e/o automatizzato.

Il Titolare tratterà i dati personali per il tempo necessario per adempiere alle finalità di cui sopra e, comunque, per non oltre 10 anni dalla cessazione del rapporto per le finalità di servizio e per non oltre 2 anni dalla raccolta dei dati per le finalità di *marketing*.

4. Accesso ai dati

I Suoi dati potranno essere resi accessibili per le finalità di cui all'art. 2.a) e 2.b):

- a dipendenti e collaboratori del Titolare o delle società o aziende individuali e in qualità di incaricati e/o responsabili interni del trattamento e/o amministratori di sistema;
- a società terze o altri soggetti (a titolo indicativo, istituti di credito, studi professionali, consulenti, società di assicurazione per la prestazione di servizi assicurativi, etc.) che svolgono attività in *outsourcing* per conto del Titolare, nella loro qualità di responsabili esterni del trattamento.

Il trattamento dei dati personali sarà improntato ai principi di correttezza, liceità e trasparenza e di tutela della Sua riservatezza e dei Suoi diritti.

5. Comunicazione dei dati

Posto che i Suoi dati personali non saranno diffusi La informiamo che, per le finalità di cui all'art. 2.a), senza la necessità di un espresso consenso, il Titolare potrà comunicarli a Organismi di vigilanza (quali IVASS), Autorità

giudiziarie, a società di assicurazione per la prestazione di servizi assicurativi, nonché a quei soggetti ai quali la comunicazione sia obbligatoria per legge per l'espletamento delle dette finalità.
I soggetti di cui sopra tratteranno i dati nella loro qualità di autonomi titolari del trattamento.

6. Trasferimento dati

I dati personali sono conservati su *server* ubicati all'interno dello studio.. Resta in ogni caso inteso che il Titolare, ove si rendesse necessario, potrà spostare i *server* anche in territorio extra-UE. In tal caso, il Titolare assicura sin d'ora che il trasferimento dei dati al di fuori dell'Unione europea avverrà in conformità alle disposizioni di legge applicabili, previa stipula delle clausole contrattuali *standard* previste dalla Commissione Europea.

7. Natura del conferimento dei dati e conseguenze del rifiuto di rispondere

Il conferimento dei dati per le finalità di cui all'art. 2.a) è obbligatorio per la attività connesse e derivanti dal rapporto giuridico con Lei instaurato. In mancanza non potranno esserLe garantiti i servizi di cui sopra.
Il conferimento dei dati per le finalità di cui all'art. 2.b) è, invece, facoltativo. Può, quindi, decidere di non conferire alcun dato o di negare successivamente la possibilità di trattare dati già forniti: in tal caso, non potrà ricevere *newsletter*, comunicazioni commerciali e materiale pubblicitario inerenti ai servizi offerti dal Titolare. Continuerà, comunque, ad avere diritto ai servizi di cui all'art. 2.a).

8. Diritti dell'interessato

In ogni momento potrà esercitare i suoi diritti nei confronti del titolare del trattamento, ai sensi degli articoli 15 (diritto di accesso ai dati) - 16 (diritto di rettifica) – 17 (diritto all'oblio) – 18 (diritto di limitazione di trattamento)– 19 (obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento) – 20 (diritto alla portabilità dei dati)– 21 (diritto di opposizione) GDPR - Regolamento 2016/679, nonché il diritto di reclamo all'Autorità Garante.

9. Modalità di esercizio dei diritti

Potrà in qualsiasi momento esercitare i diritti previsti dagli artt. da 15 a 22 del Regolamento Europeo 2016/679 inviando una raccomandata a.r. allo Studio Drazza con sede in Roma alla via Federico Delpino 7, C.A.P. 00171.

10 . Titolare, responsabile e incaricati

Il Titolare del trattamento è il Dr. Emiliano Drazza con sede legale in Roma alla via Fderico Delpino 7, C.A.P.00171.
L'elenco aggiornato dei responsabili e degli incaricati al trattamento è custodito presso la sede legale del Titolare del trattamento.

MODULO DI CONSENSO

Il/la sottoscritto/a , in qualità di:

□ azienda

□ dipendente di azienda cliente del Titolare

□ collaboratore

□ cittadino richiedente servizio lavoro/previdenziale

acquisite le informazioni fornite dal titolare del trattamento ai sensi dell'articolo 13 del Regolamento europeo 2016/679:

- presta il suo consenso al trattamento dei dati personali per i fini indicati nella suddetta informativa di cui al punto 2a):
□ SI □ NO

- presta il suo consenso al trattamento dei dati personali per i fini indicati nella suddetta informativa di cui al punto 2b) (facoltativo):
□ SI □ NO

Roma, lì ……
Firma
……

8. Misure di sicurezza

Obiettivo precipuo del presente Regolamento è quello di garantire un sistema di prevenzione contro le possibili violazioni di dati personali dei quale l'Ente venga in possesso in ragione delle finalità perseguite: da qui, la necessità di dotarsi di un adeguato sistema di sicurezza.
Il raggiungimento del detto fine richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche l'efficienza degli opportuni meccanismi organizzativi; ed invero, le misure tecniche per quanto possano essere sofisticate non saranno mai efficienti se non debitamente e correttamente usate. *Ad esempio:* anche il più sofisticato sistema tecnologico a nulla varrà se le varie postazioni non sono dotate di adeguate password di accesso o ancora se la documentazione conservata su supporti cartacei venga custodita in luoghi accessibili a tutti.
Ne consegue che coloro i quali, per il ruolo ricoperto all'interno della Facoltà - siano dipendenti, collaboratori, volontari - vengano a contatto e trattino dati personali sono tenuti all'osservanza dei generali principi di *"riservatezza", "diligenza", "integrità"* oltre che delle seguenti specifiche norme di comportamento e principi di sicurezza:
1) ogni utilizzo dei dati personali diverso da finalità strettamente professionali è espressamente vietato;
2) rispettare i principi generali del GDPR, con particolare riferimento alla liceità e correttezza del proprio agire;
3) utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni rispettando l'obbligo di riservatezza e segretezza; rispettare le misure di sicurezza idonee adottate dalla società, atte a salvaguardare la riservatezza e l'integrità dei dati;
4) in caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;
5) svolgere le attività previste dai trattamenti secondo le direttive del responsabile del Trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del Trattamento dei dati;
6) informare il Titolare e/o il DPO (se nominato) in caso di incidente di sicurezza che coinvolga dati particolari e non;
7) raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
8) i locali, in cui sono custoditi i dati personali (ed in particolare quelli di natura particolare), devono essere soggetti a controllo e a verifica, al fine di evitare che durante l'orario di lavoro possano essere accessibili da parte di soggetti non autorizzati. (Si raccomanda, in caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, di adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'organizzazione di appartenenza);
9) ciascun incaricato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card). Si devono adottare le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei all'organizzazione o non specificamente autorizzati. A tal fine si rende necessario mantenere riservate le proprie credenziali di autenticazione;

10) per la gestione della sessione di lavoro sul pc (fisso e portatile), si applicano le seguenti regole:
- dotare il P.C. di diverse password, ognuna con il proprio ruolo preciso:
  a. Password di accesso al computer
  b. Password di accesso alla rete
  c. Password di specifici programmi
  d. Password del salvaschermo
- per la corretta gestione della password è necessario:
  - cambiare la password obbligatoriamente ogni 6 mesi
  - la password deve contenere almeno 8 caratteri di cui 2 numerici e 1 speciale
  - ogni password ricevuta va modificata al primo utilizzo
  - la password deve essere conservata in un luogo sicuro
  - non rivelare o condividere la password con i colleghi di lavoro, famigliari e amici, soprattutto attraverso il telefono
  - non utilizzare la funzione, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni
- se l'incaricato si assenta momentaneamente dalla propria postazione deve accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone; pertanto, deve chiudere la sessione di lavoro sul PC facendo *Logout*, oppure in alternativa deve avere attivo un salvaschermo *(screen-saver)* protetto dalle credenziali di autenticazione
- le periferiche esterne *(Hard Disk, Pen Drive, CD, ecc.)* devono essere custodite in luoghi non accessibili a terzi
- eseguire periodicamente salvataggi dei dati custodendoli in luoghi sicuri
- non installare programmi, anche in versione demo. In particolare, è vietata l'installazione di giochi, programmi in prova *(shareware),* programmi gratuiti *(freeware)*, programmi "pirata", e in generale tutti i software non autorizzati dal Servizio Informatico
- non modificare i parametri di configurazione del proprio PC senza espressa autorizzazione e senza il supporto di personale tecnico qualificato;

11) nell'uso della posta elettronica occorre rispettare le seguenti regole di comportamento:
- se si ricevono *e-mail* da destinatari sconosciuti contenenti *file* di qualsiasi tipo, procedere alla loro immediata eliminazione
- è fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione
- la casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione
- nell'ipotesi in cui l'*e-mail* debba essere utilizzata per la trasmissione di dati particolari (ex dati sensibili), si raccomanda di prestare attenzione a che:
  - l'indirizzo del destinatario sia stato correttamente digitato
  - l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile
  - nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio;

12) per prevenire eventuali danneggiamenti al *software* causati dalla presenza o dall'azione di programmi virus informatici, su ogni elaboratore dell'ente è stato installato un *software antivirus* aziendale che si aggiorna automaticamente all'ultima versione disponibile; l'antivirus aziendale non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito; nel caso il programma antivirus installato sul proprio PC riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus è necessario darne immediatamente segnalazione al responsabile del Servizio Informatico;

13) in merito alla gestione degli strumenti "non elettronici" (vale a dire sia documenti cartacei sia documenti di altro tipo) i documenti contenenti dati particolari o giudiziari devono essere protetti in appositi armadi dotati di

chiavi; tutti i documenti contenenti dati particolari o giudiziari, che si ritiene debbano essere eliminati, devono essere distrutti e non gettati nei cestini; per proteggere i dati personali, soprattutto i dati particolari (ex dati sensibili) è necessario evitare il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici (corridoi o sale riunioni), come pure l'abbandono in vista sulle scrivanie quando ci si debba assentare dal proprio posto di lavoro; quando si esegue la stampa di un documento contenente dati personali, in particolare su una stampante condivisa, occorre ritirare tempestivamente i documenti stampati per evitare l'accesso a soggetti non abilitati al Trattamento;
14) in merito alla distruzione delle copie cartacee, coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzando strumenti per la riproduzione cartacea di documenti digitali, sono tenuti a procedere alla relativa distruzione del supporto, qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli, salva l'ipotesi di uso esclusivamente personale per eventuali appunti o brutte copie, da distruggere immediatamente quando non più necessarie;
15) il Trattamento sicuro di documenti contenenti dati personali richiede la presenza di misure di sicurezza con le quali l'incaricato possa interagire ed una serie di accorgimenti direttamente gestibili dall'Incaricato stesso. In particolare, si richiede:
• la presenza e l'uso tassativo di armadi e cassetti dotati di chiusura adeguata
• la presenza e l'uso tassativo, ove si richieda la distruzione di documenti contenenti dati particolari (ex dati sensibili) e giudiziari, di un trita documenti
• la presenza e l'uso tassativo nell'ambiente fisico di ricovero dei dati di opportuni accorgimenti strutturali per impedire l'accesso per scopo di furto (porta blindata all'accesso principale, luoghi destinati ad archivio provvisti di porte con opportuni sistemi di chiusura);

Per la sicurezza informatica , lo Studio ha analizzato le specifiche tecniche utilizzate , che sono state riassunte e delineate nell'allegato B.

9. Obbligo di notificazione immediata di una violazione dei dati e registro delle violazioni
Nel caso si verifichi un qualsiasi tipo di violazione dei dati, o se ne abbia anche solamente il sospetto, ne deve essere data immediata comunicazione al Titolare e/o al Responsabile della protezione dei dati, il quale si attiverà immediatamente per valutare se vi sia stata effettivamente una violazione, la portata e le conseguenze, e valutare se sussistano i presupposti per effettuare la notificazione entro 72 ore all'Autorità di controllo.
Coerentemente con quanto previsto dall'art. 33 comma 5, deve essere in ogni caso tenuto un registro di tutte le violazioni di dati verificatesi, a prescindere dal fatto che siano state notificate all'autorità di controllo. Il suddetto registro deve contenere come minimo le seguenti informazioni:
- data della violazione
- descrizione delle circostanze e dell'evento
- tipologia e quantità di interessati impattati
- conseguenze della violazione
- data di comunicazione della violazione al Garante per la protezione dei dati (se la comunicazione è stata effettuata).

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, ai sensi dell'art. 34 GDPR il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo. La comunicazione all'interessato deve descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d), ossia comunicare il nome e i dati di contatto del responsabile della protezione dei dati, descrivere le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione verificatasi. La suddetta comunicazione all'interessato non è richiesta se è soddisfatta una delle seguenti condizioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.
La comunicazione all'organo di controllo deve contenere le seguenti informazioni:

a) dati del titolare
b) natura della comunicazione (se nuova oppure se segue una precedente comunicazione)
c) breve descrizione della violazione verificatasi
d) indicazione temporale [specificare la data se certa o indicare il periodo non determinato *(tra il e il)* o la possibilità che sia ancora in corso]
e) indicazione del luogo (specificare se all'interno o fuori dalla sede dell'Ente, ad esempio a seguito di smarrimento di un dispositivo o di un supporto portatile)
f) tipologia di violazione (specificare se trattasi di lettura, copia, furto, cancellazione di dati personali…etc)
g) dispositivo oggetto della violazione (computer, strumenti backup, documento cartaceo, rete)
h) descrizione delle misure di sicurezza adottate dall'Ente in relazione a quella specifica violazione
i) interessati al trattamento coinvolti (numero esatto, "circa" o sconosciuto)
j) tipologia dei dati violati (ad es: dati anagrafici, indirizzo, numero di telefono fisso o mobile, posta elettronica ….)
k) livello di gravità della violazione (basso, medio, alto)
l) indicare se è stata data o meno comunicazione all'interessato, ai sensi dell'art. 34 GDPR, dell'avvenuta violazione
m) eventuali strumenti posti in essere per contenere la violazione e/o prevenire violazioni future.

10. Registro dei trattamenti
L'articolo 30 del GDPR prevede che ogni Titolare del Trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di Trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:
- il nome e i dati di contatto del Titolare del Trattamento e, ove applicabile, del contitolare del Trattamento, del rappresentante del Titolare del Trattamento e del responsabile della protezione dei dati;
- le finalità del Trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati
- i termini ultimi previsti per la cancellazione delle diverse categorie di dati
- una descrizione generale delle misure di sicurezza tecniche e organizzative adottate dall'ente.

Lo stesso Regolamento prevede che tale obbligo non si applica di regola alle imprese o organizzazioni con meno di 250 dipendenti, ma lo studio intende istituirlo per i dati previdenziali e assistenziali contenuti nelle richieste di servizi avanzate da singoli cittadini in proprio e non in quanto dipendenti delle aziende clienti..
La bozza dell'adottando Registro dei Trattamenti è separatamente custodita.

F.TO **EMILIANO DRAZZA**

ALL.B AL REGOLAMENTO DI SICUREZZA DATI

DOCUMENTO ILLUSTRATIVO DELLE MISURE DI SICUREZZA STUDIO DRAZZA

APPLICATO NELLA GESTIONE DEI DATI INFORMATICI IN CONFORMITÀ DEI TRATTAMENTI DEI DATI PERSONALI

REGOLAMENTO EUROPEO 679/2016 - GDPR

Lo Studio Drazza ha da sempre curato l'innovazione tecnologica, ha sempre visto nella figura del suo fondatore, Drazza Emiliano, uno strenue sostenitore dello sviluppo di sistemi gestionali nuovi, atti a semplificare i processi lavorativi, a ridurre al minimo gli errori ed a massimizzare l'efficienza.

Questo è stato possibile con la presenza e la collaborazione continuativa di un programmatore-sistemista che ha dapprima realizzato buona parte dei tool utilizzati e contestualmente si è sempre occupato della sicurezza informatica, anche prima del 2003 con l'introduzione del D.l. 196 del 30 giugno 2003.

Con l'arrivo del GDPR, entrato in vigore il 25 maggio 2018 lo Studio ha adeguato le misure di sicurezza a quanto richiesto dalla nuova normativa garantendo così la riservatezza dei dati informatici e la loro protezione contro gli accessi indesiderati.

Il GDPR prevede che il titolare del trattamento si assicuri che "nessuno", se non autorizzato ed incaricato al trattamento, possa avvicinarsi fisicamente ai server per compromettere, anche involontariamente, i dati in esso contenuti collegando chiavette usb, hard disk esterni, ecc. La prima precauzione presa è stata quella di isolare in una stanza climatizzata, con inferriate alla finestra, i pc che fungono da server, **con porta chiusa a chiave** e custodita dal titolare in luogo sicuro. Lo studio non è aperto al pubblico, gli ospiti sono sempre accompagnati dai collaboratori e l'accesso allo studio è protetto da porta blindata.

Il solo locale dei server è poi **monitorato da una telecamera IP** che collegata alla rete invia degli alert in caso di rilevazione movimento. Tutti i dispositivi server sono protetti da interruzioni di alimentazione con un **gruppo di continuità** della APC che ne garantisce il funzionamento per circa 20 minuti. Se l'interruzione si protrae, vengono in automatico avviate le procedure di spegnimento automatico di tutti i pc quando la carica delle batterie scende sotto una certa soglia.

Lo Studio si avvale attualmente dei seguenti dispositivi:

1- **Server DELL** Poweredge T110 II con licenza Windows Server 2012 Foundation con:
   - **HD da 1 TB Raid 0** (su cui ci sono i dati del gestionale Team System Paghe e tutti i file pdf)
   - HD da 1 TB per copie di backup interne giornaliere.
   - HD da 1 TB per memorizzare dati non rilevanti.

- **Ruoli e servizi installati:** Controller di dominio, Active Directory, Server DNS, Condivisione file, Network Policy Server, Remote Desktop Service.

2- **PC MAIN** con licenza Windows 10 Pro con:
   - HD SSD da 64 GB.
   - HD sata da 300 GB RAID 0 (*db gestionale presenze Keros di Cronos (Postgre DB), db gestionale presenze Presegest (MsSQL server)*
   - VMWeb – **Macchina virtuale** con IIS7 che funge da **server web** per l'applicazione Presegest
3- ***NAS Qnap TS-231*** con 2 HD Western Digital Purple per NAS da 1 TB ciascuno, configurati in RAID 0.
4- *Pc **portatile DELL** – con licenza windows 10 Pro (stazione di lavoro) con 2° monitor samsung 24".*
5- *PC **portatile HP** con licenza windows 10 Home (utilizzo saltuario).*
6- *Numero **4** (quattro) **PC Fissi** con licenza Windows 10 Pro, monitor 21"o 24" (stazione di lavoro).*
7- *N° 1 switch ethernet 24 porte non managed.*
8- *N° 1 switch ethernet 10 porte gigalan non managed.*
9- *N° 2 router (1 Fastweb con fibra FTTS (principale), l'altro Telecom Italia sempre in tecnologia fibra FTTS (backup)). Entrambi i router sono configurati con **firewall attivo,** adottato per il port mapping dei soli servizi essenziali come di seguito descritto.*
10- ***2 IPhone** su cui viene controllata la posta elettronica.*

Nello specifico il server è configurato come "controller di dominio", "server di active directory" e "server di licenze RDP". Tutti i computer contrassegnati come "Stazione di lavoro" sono pc associati al dominio, pertanto l'autenticazione dell'utente all'avvio è gestita in maniera centralizzata. La gestione delle password degli utenti è effettuata centralmente secondo le "Best practise policies" suggerite da Microsoft.

Tutti i collaboratori di Studio, sebbene le loro postazioni siano localmente collegate con il server, effettuano l'accesso a quest'ultimo tramite **desktop remoto, consentito solo tramite autenticazione a livello di rete,** dove si concentra e realizza tutto il loro lavoro.

Gli accessi degli utenti vengono registrati in un appposito log e conservato per 6 mesi.

Il gestionale paghe utilizzato per la gestione dei dati delle Aziende e dei loro dipendenti è "**Suite Paghe Evolution**" della società *Team System*. Dal 25 maggio 2018 questa ha reso disponibile ed operativo il modulo per l'autenticazione degli accessi e la tracciabilità delle operazioni fatte dagli utenti secondo quanto previsto dal GDPR. Il software, i suoi dati ed i documenti prodotti (cedolini, F24, ecc.) sono tutti memorizzati nel server su **dischi ridondanti** (RAID 0) che garantiscono la protezione dei dati in caso di rottura accidentale di uno dei dischi. Inoltre i dati sono memorizzati con struttura "azienda per azienda, matricola per matricola, tipo di

documento per tipo si documento" per poter far fronte a correzioni, cancellazioni di dati "mirate" se richieste dagli interessati, oppure a scadenza degli obblighi di legge per rispettare i principi di limitazione della conservazione, di minimizzazione dei dati, di correttezza e di integrità.

Ad intervalli regolari (120 minuti) i dati del gestionale sono copiati su altri dischi, interni al server, non ridondanti, per una ulteriore copia (ne vengono conservate 6, per un totale di 12 ore). Alle ore 13 ed alle ore 19 di tutti i giorni lavorativi, i dati del gestionale vengono copiati tramite "Volume Shadow Copy" (meccanismo che consente la copia di un file anche se questo è in uso), compressi, criptati con password, e trasmessi al NAS in rete LAN tramite protocollo FTPS (TLS) (comunicazione criptata).

Il NAS non ha abilitato altri servizi di rete se non la connessione sicura FTP con TLS. Questo garantisce che il trasferimento dei backup è sicuro in rete, che nessuna infezione da virus Criptolocker possa manomettere le copie di sicurezza, ne tantomeno lo possano i collaboratori di studio perché non in possesso delle credenziali.

Alle ore 20 di tutti i giorni lavorativi il NAS locale trasmette tramite il protocollo RTRR (Real Time Remote Replication) su connessione SSL le copie contenute in se stesso su uno spazio acquistato su Server Aruba, che garantisce, a sua volta, la regolarità della conservazione dei dati secondo le regole del GDPR.

Si sottolinea il fatto che ciò che finisce su Aruba è comunque un file criptato, che non può essere decifrato senza la chiave utilizzata in fase di crittazione.

L'utilizzo esclusivo di sessioni terminal su server da parte di tutti gli utenti fa si che i dati non vengono mai spostati sulle workstation, la posta elettronica viene monitorata da un aggiornato antivirus e ad intervalli di 15 giorni sul NAS vengono fatte le copie degli ambienti di lavoro di tutti gli utenti, comprese le mail ricevute, inviate ed archiviate. Per completezza si precisa anche che gli utenti hanno **profili "standard"** sul server, non hanno diritti amministrativi e questo impedisce loro l'esecuzione di file dannosi per il sistema.

I dati del pc MAIN, dati delle presenze, sono copiati quotidianamente alle ore 13 su NAS sempre in modalità sicura. Il server web è ospitato da una macchina virtuale, poiché è ciò che è più esposto ad internet . La macchina è isolata dal resto della rete, pertanto se ci fosse un problema sul server web da questo non sarebbe possibile accedere ad altri dati.

Il presente documento di rilevazione sul trattamento e sicurezza del "dato" è stato redatto dallo Studio Drazza,ed costituisce la versione 2018.07.10 ; potrà subire variazioni senza preavviso dal momento che l'intento è quello di migliorare continuamente la gestione dei dati ed il loro trattamento; ciò comporterà inevitabilmente adeguamenti della struttura e dei processi utilizzati.

E' possibile contattarci in merito scrivendo a gdpr@consulenzaelavoro.it

Roma, 21/6/2018

Il titolare del trattamento

f.to *Dr. Drazza Emiliano*