

MODELLO ORGANIZZATIVO SULLA PROTEZIONE DEI DATI PERSONALI

Sommario

B)4.1 Responsabilità dei Designati al trattamento.....	11
C)4.2 Divieti.....	12
D)4.3 Procedure di sicurezza.....	13
E)4.3.1 Gestione delle credenziali di accesso alle Postazioni Informatiche.....	13
F)4.3.2 Controllo degli accessi agli archivi elettronici e protezione degli stessi.....	14
G)4.3.3 Connessione alla rete Internet.....	15
H)4.3.4 Posta elettronica e instant messaging.....	15
I)4.3.5 Controllo degli accessi agli uffici e protezione dei locali dove vengono custoditi gli archivi.....	15
J)4.3.6 Gestione dei fascicoli cartacei.....	16
K)4.3.7 Siti web e social network.....	17

1. PREMESSA

Il presente Modello Organizzativo sulla Protezione dei Dati Personali (di seguito per brevità semplicemente “MODELLO”) raccoglie le misure tecniche ed organizzative che IN CAMMINO CON ROBERTO STRACCIA ODV (di seguito anche semplicemente “ORGANIZZAZIONE”) attua per garantire la conformità al Regolamento UE 2016/679 (di seguito per brevità semplicemente “GDPR”) delle attività di trattamento dei dati personali delle persone fisiche che l’Organizzazione effettua direttamente o che soggetti terzi effettuano per suo conto.

L’adozione delle misure tecniche ed organizzative adeguate è introdotta dagli artt. 24 e seguenti del GDPR, ai sensi dei quali le politiche interne e le misure da attuare per soddisfare i principi della c.d. *privacy by design* e *privacy by default*, devono tener conto, in concreto, della natura, dell’ambito di applicazione, del contesto e delle finalità di trattamento nonché del rischio per i diritti e le libertà fondamentali delle persone fisiche.

Al fine di rispettare tali requisiti, pertanto, l’elaborazione del presente modello ha richiesto la preventiva esecuzione di un’analisi dei rischi connessi al trattamento dei dati personali.

Il GDPR è costituito da tre principi ispiratori che permeano e sostengono l’intero impianto normativo, e più precisamente dai principi di:

- 1) **accountability**, ovvero il principio di responsabilizzazione: il GDPR non effettua una tipizzazione puntuale delle misure tecniche e organizzative, esprimendosi unicamente in termini di loro adeguatezza al rischio *“tenendo conto dello stato dell’arte e dei costi di attuazione, nonché della natura, dell’oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche”* (art. 32 GDPR). Si tratta di una innovazione profonda in quanto viene attribuito a chi gestisce dati personali di terzi il compito di decidere autonomamente le modalità, le garanzie ed i limiti del trattamento dei dati personali nel rispetto delle disposizioni normative ed alla luce di alcuni criteri specifici indicati nel GDPR. Ciò impone un approccio orientato al rischio (risk-based) che dia luogo a comportamenti proattivi;
- 2) **privacy by design**, che impone l’adozione di misure di protezione fin dalla fase di progettazione del trattamento;
- 3) **privacy by default**, che prescrive un utilizzo che si limiti, per impostazione predefinita, ai soli dati necessari a rispondere alle finalità specifiche della gestione dei dati.

Tali principi ispiratori si riflettono sui cosiddetti “pilastri” del GDPR, ossia sulle principali novità operative quali:

- a) la designazione, in determinati casi, del Responsabile della Protezione dei Dati (Data Protection Officer, artt. 37-39 GDPR) intesa come figura di garanzia che deve raccogliere in sé competenze normative, tecniche, comunicative e di conoscenza profonda della struttura e dell’organizzazione aziendale;
- b) l’istituzione del Registro delle attività di trattamento (art. 30 e cons. 171 GDPR) che costituisce il punto di partenza per la predisposizione dell’intero impianto documentale,

deputato a raccogliere le evidenze, i controlli ed i processi che consentono di soddisfare l'accountability del sistema privacy;

- c) il processo di data breach, (art. 33 e 34 GDPR) ossia la notifica delle eventuali violazioni dei dati personali, che richiede un'attenta analisi e conoscenza delle informazioni gestite.

Diretto corollario dei sopra riferiti principi generali di *accountability*, *privacy by design* e *privacy by default*, è che la piena *compliance* al GDPR impone che il trattamento dei dati personali avvenga secondo i principi di liceità, correttezza e trasparenza.

Come nella precedente normativa, il trattamento è lecito allorché trovi fondamento in una base giuridica che, fermo restando in ogni caso l'obbligo di informativa a carico del Titolare del trattamento, può consistere in quanto segue:

- 1) **consenso dell'interessato** che deve essere libero, specifico, informato ed inequivocabile, non essendo ammesso il consenso tacito o presunto: deve, in altri termini, essere manifestato attraverso una "dichiarazione o azione positiva inequivocabile". Inoltre, per i dati "sensibili" di cui all'art. 9 GDPR, esso deve essere anche "esplicito", non necessariamente "documentato per iscritto" né da prestare in "forma scritta", sebbene tale modalità sia quella maggiormente idonea a dimostrare la sua prestazione, la sua inequivocabilità ed il suo essere "esplicito";
- 2) **adempimento di obblighi contrattuali**, ovvero sia il trattamento è lecito se è necessario all'esecuzione di un contratto di cui l'interessato è parte od all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- 3) **obblighi di legge** cui è soggetto il titolare del trattamento, nel qual caso la finalità è specificata per legge;
- 4) **interessi vitali** della persona interessata o di terzi: ovvero sia se è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; utilizzabile però come base giuridica solo se nessuna delle altre condizioni di liceità può trovare concreta applicazione;
- 5) **legittimo interesse** prevalente del titolare o di terzi cui i dati vengono comunicati, ovvero sia quando il trattamento è necessario per il perseguimento dei legittimi interessi 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;
- 6) **interesse pubblico o esercizio di pubblici poteri**, ovvero 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 (tramite legge statale o dell'Unione) ed anche in tal caso la finalità deve essere specificata per legge.

Il trattamento dei dati personali è corretto se trasparente nei confronti degli interessati, ossia i dati personali devono essere trattati per scopi determinati, espliciti e legittimi, e senza scorrettezze o raggiri nei confronti degli interessati (essendo dunque vietata un'informazione confusa o parziale). Quello della trasparenza non è solo un principio fondamentale del

trattamento, ma anche un vero e proprio diritto dell'interessato: devono cioè essere trasparenti e corrette le modalità di raccolta dei dati e di utilizzo degli stessi.

Gli interessati devono essere informati in merito alle finalità del trattamento, alle modalità del trattamento e all'indirizzo del titolare del trattamento, prima che si avvii il trattamento stesso. Le modalità del trattamento devono essere esplicitate in maniera comprensibile in modo che gli interessati siano in grado di capire cosa accadrà ai loro dati.

L'interessato deve avere a disposizione una procedura efficace e accessibile per consentirgli di ottenere l'accesso ai suoi dati in un tempo ragionevole, e quindi di conoscere se e quali dati sono detenuti dal titolare.

Qualsiasi trattamento occulto o segreto deve, quindi, ritenersi illecito. I titolari e i responsabili devono garantire agli interessati che i dati saranno trattati secondo liceità e correttezza e in modo da conformarsi, per quanto possibile, alla volontà degli stessi interessati.

2. DEFINIZIONI

Ai fini del GDPR ed in relazione ai concetti specificamente coinvolti dalle attività di trattamento effettuate direttamente ed indirettamente dall'Organizzazione, ai sensi dell'art. 4 del GDPR si intendono per:

- 1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- 2) «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;
- 3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- 4) «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;
- 5) «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;

- 6) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- 7) «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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- 8) «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;
- 9) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
- 10) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- 11) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- 12) «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;
- 13) «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- 14) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

- 15) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- 16) «stabilimento principale»:
- a. per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
 - b. con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;
- 17) «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;
- 18) «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le Organizzazioni di persone o le associazioni che esercitano regolarmente un'attività economica;
- 19) «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
- 20) «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;
- 21) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;
- 22) «autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:
- a. il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;

- b. gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
- c. un reclamo è stato proposto a tale autorità di controllo.

3. OBIETTIVO E STRUTTURA DEL MODELLO ORGANIZZATIVO

L'obiettivo del presente Modello è di garantire e dimostrare che il trattamento dei dati personali da parte di IN CAMMINO CON ROBERTO STRACCIA ODV avviene in modo lecito, corretto e trasparente secondo la definizione di cui sopra, da raggiungere attraverso la realizzazione di una gestione interna che promuova la cultura della privacy e della sicurezza dei dati personali, consolidando i principi comportamentali idonei a garantire la trasparenza, la sicurezza e la correttezza dei trattamenti, aumentando la propria affidabilità verso i propri clienti, partners, consulenti e dipendenti.

Con l'ulteriore conseguenza di evitare la possibile erogazione delle sanzioni amministrative pecuniarie di cui all'art. 83 GDPR nonché di quelle penali di cui alla normativa nazionale per quanto ancora in vigore, potendo, con la sua adozione, dimostrare l'attuazione concreta, efficiente ed efficace delle misure tecniche ed organizzative adeguate alla protezione dei dati personali da essa trattati, direttamente o tramite soggetti terzi che li effettuano per suo conto.

Il presente Modello fornisce una panoramica sul sistema complessivo delle misure tecniche e organizzative che, sulla base delle concrete esigenze sistematiche ed operative della Organizzazione e all'esito dell'analisi dei rischi, si ritengono adeguate, contenendo i principi, le regole organizzative e gli strumenti di controllo per garantire il trattamento lecito, corretto e trasparente dei dati personali.

4. TITOLARI, RESPONSABILI E DESIGNATI

IN CAMMINO CON ROBERTO STRACCIA ODV ha ritenuto di non nominare un Data Protection Officer ai sensi dell'art. 37 GDPR, non sussistendone i requisiti di legge e non ritenendosi detta figura necessaria in ragione della natura dei dati trattati e dei rischi per i diritti e le libertà fondamentali degli interessati. Pertanto, le figure e le funzioni coinvolte nell'Organizzazione nelle attività di protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale sono:

A) Titolare del Trattamento

È la stessa IN CAMMINO CON ROBERTO STRACCIA ODV che riveste tale funzione e sulla quale, conseguentemente, incombono tutti gli obblighi e le responsabilità che la legge, italiana ed europea, le impone. Primo fra tutti, l'obbligo di mettere in atto, riesaminare ed aggiornare le misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è da essa effettuato conformemente al GDPR.

Quanto al regime di responsabilità, IN CAMMINO CON ROBERTO STRACCIA ODV risponde quale Titolare, in via esclusiva, e quale Contitolare, in via solidale per l'intero ammontare, del danno materiale o immateriale cagionato a qualunque interessato da una violazione del GDPR, salvo che dimostri che l'evento dannoso non gli è in alcun modo imputabile.

B) Responsabile del Trattamento

Il GDPR definisce all'art. 28 il Responsabile del trattamento come il soggetto che effettua trattamenti di dati personali per conto del Titolare, presentando garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che i trattamenti stessi soddisfino i requisiti del GDPR e garantiscano la tutela dei diritti dell'interessato.

È opinione diffusa tra gli interpreti che la figura ora delineata sia riferita al Responsabile del trattamento "esterno" rispetto alla struttura aziendale del Titolare del trattamento e che, pertanto, non sia espressamente disciplinata la figura del Responsabile del trattamento "interno".

IN CAMMINO CON ROBERTO STRACCIA ODV si può avvalere di Responsabili del Trattamento attraverso specifici atti di designazione o attraverso contratti di servizio. I Responsabili del trattamento, ove esistenti, sono individuati nell'Organigramma Privacy qui allegato (**All. n. 1**).

Quanto al regime di responsabilità, i Responsabili del trattamento rispondono per il danno causato dal trattamento solo se non hanno adempiuto gli obblighi del GDPR specificatamente loro diretti o se hanno agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare del trattamento.

C) Designati al trattamento

La figura del Designato al trattamento è definibile come la persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile.

Anche se nella traduzione italiana del GDPR non compare mai il termine "designato al trattamento" e pur non essendo espressamente prevista dal GDPR questa figura come funzione giuridicamente autonoma, il Garante italiano, nella guida all'applicazione del Regolamento, giustifica e considera non incompatibile con il regolamento la figura del Designato. Anzi, tale modalità operativa è considerata una buona prassi volta a poter ulteriormente comprovare la *compliance* al GDPR.

I Designati del trattamento di IN CAMMINO CON ROBERTO STRACCIA ODV sono coloro i quali provvedono materialmente al trattamento dei dati personali sotto la supervisione del Titolare del trattamento.

IN CAMMINO CON ROBERTO STRACCIA ODV cura l'aggiornamento costante dei propri Designati mediante corsi di formazione e aggiornamento.

5. POLICY DELL'ORGANIZZAZIONE

IN CAMMINO CON ROBERTO STRACCIA ODV è una Organizzazione che opera nel campo del VOLONTARIATO Per il perseguimento del proprio scopo, pertanto, l'Organizzazione svolge tutte le attività a ciò necessarie tra le quali, per quanto qui interessa:

- gestione del sito web www.robetostraccia.it
- gestione dell'attività associativa consistente in database soci per campagna associazioni

Nello svolgimento di tali attività, IN CAMMINO CON ROBERTO STRACCIA ODV gestisce differenti tipologie di dati personali, e più precisamente:

- 1) dati anagrafici dei soci e associati;
- 2) dati anagrafici dei volontari;

Le basi giuridiche del trattamento di tali dati da parte di IN CAMMINO CON ROBERTO STRACCIA ODV sono indicate nelle rispettive informative rilasciate agli interessati e possono di seguito riepilogarsi:

- esecuzione di contratti o di accordi precontrattuali;
- consenso dell'Interessato;
- obblighi di legge.

I dati suddetti possono essere trattati attraverso strumenti cartacei ed elettronici, sia presso la sede operativa, che attraverso la Rete Internet.

Nel trattamento dei dati personali, l'Organizzazione osserva le regole che seguono.

A) 4.1 Responsabilità dei Designati al trattamento

Le autorizzazioni ai designati al trattamento (di seguito semplicemente "Designati") sono concesse dal Titolare del Trattamento mediante nomina scritta nella quale si individua ambito e profilo di autorizzazione.

Il Titolare del Trattamento rilascia ai Designati le credenziali di accesso (username e password) ai sistemi informatici dell'Organizzazione. La password è strettamente personale e non deve essere comunicata e/o condivisa con nessun'altra persona all'interno dell'Organizzazione. Ogni Designato è responsabile di tutte le azioni e le funzioni svolte tramite le sue credenziali.

Il Designato deve attenersi scrupolosamente alle procedure operative indicate dal Titolare del Trattamento nelle rispettive nomine e/o comunicate durante le sessioni formative o nel corso del rapporto di collaborazione.

I Designati hanno l'obbligo di segnalare immediatamente al Titolare del Trattamento qualsiasi evento o situazione di rischio della sicurezza dei sistemi informatici o delle informazioni al fine di tutelare i diritti e le libertà degli interessati e il patrimonio informativo dell'Organizzazione oltre che garantire la necessaria continuità operativa.

Ciascun Designato deve:

- rispettare i principi generali del Regolamento (Ue) 2016/679 (GDPR) e della normativa nazionale in vigore, con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi;
- rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;
- utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti dell'Organizzazione;
- rispettare le misure di sicurezza idonee adottate dall'Organizzazione, atte a salvaguardare la riservatezza e l'integrità dei dati;
- segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;
- accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze;
- in caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- mantenere riservate le proprie credenziali di autenticazione;
- non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del Titolare o del Responsabile del trattamento dei dati, ove nominato;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il Titolare in caso di incidente di sicurezza che coinvolga i dati;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli dell'Organizzazione e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.

B) 4.2 Divieti

L'uso di tutti i dispositivi hardware dell'Organizzazione è autorizzato per le sole finalità lavorative e professionali, nell'ambito della mansione e del profilo di autorizzazione previsto per l'utilizzatore. Qualsiasi altro utilizzo è vietato.

È vietato modificare la posizione, la configurazione hardware e software, la modalità di collegamento alla rete dell'Organizzazione e all'alimentazione elettrica, da parte del Designato, senza specifica autorizzazione del Titolare del Trattamento.

Non è consentito l'uso di software applicativi diversi da quelli installati nelle Postazioni Informatiche.

È tassativamente vietato rivelare la propria password di accesso alla rete dell'Organizzazione, agli applicativi o ai servizi disponibili. Qualsiasi azione effettuata utilizzando la coppia "nome utente e password" sarà attribuita in termini di responsabilità al Designato registrato, a meno di comprovato illecito da parte di terzi.

È vietato conservare nei sistemi e unità di memorizzazione assegnati, file, documenti, mail, immagini, video non legati alle finalità lavorative e professionali, in particolar modo di contenuto osceno o violento, offensivo alla morale o alla pubblica decenza, oltraggioso e/o discriminatorio.

È tassativamente vietata la navigazione in siti Internet non legati alle finalità lavorative e professionali, alla ricerca, allo studio e formazione. È vietato effettuare navigazione in siti web di contenuto osceno o violento, offensivo alla morale o alla pubblica decenza, oltraggioso, che incitano all'odio o alla discriminazione.

È tassativamente vietata la navigazione in siti Internet che consentano o siano a rischio di diffusione di virus, cavalli di troia o di altri programmi il cui obiettivo sia la distruzione, alterazione, sabotaggio, intercettazione, hacking o pirateria informatica a danno dei computer di altri Designati interni o esterni al perimetro dell'Organizzazione.

È vietato l'utilizzo dei social media, forum, chat-line, instant messaging, Voice over IP o video chat per finalità diverse da quelle dell'Organizzazione o di formazione.

È vietato l'invio di dati tramite posta elettronica al di fuori dell'Organizzazione senza il preventivo consenso scritto del Titolare del Trattamento.

Il trasporto al di fuori dall'ufficio di dispositivi di memorizzazione e/o di materiale cartaceo contenente dati dell'Organizzazione è assolutamente vietato.

Eventuali repliche o copie di sicurezza delle informazioni dell'Organizzazione devono essere autorizzate dal Titolare del Trattamento e opportunamente tracciate.

Il mancato rispetto o la violazione delle regole contenute nel presente Modello è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite dalla Legge.

C) 4.3 Procedure di sicurezza

D) 4.3.1 Gestione delle credenziali di accesso alle Postazioni Informatiche

I Designati si impegnano a rispettare i criteri di creazione, conservazione e gestione delle credenziali di accesso di seguito indicati.

1) obbligo di cambiare la password al primo accesso rispettando i criteri di seguito descritti, evitando combinazioni facili da identificare. Devono scegliere password univoche, che abbiano un senso solo per il Designato che le sceglie, evitando di usare la stessa password per altre utenze:

- deve essere di lunghezza non inferiore ad 8 caratteri;
- deve essere cambiata almeno ogni 6 (sei) mesi;
- deve contenere almeno 3 caratteri tra numeri, caratteri alfabetici in maiuscolo e minuscolo, e caratteri speciali;
- deve essere sempre diversa da quelle precedentemente utilizzate;
- deve essere nota esclusivamente all'utilizzatore e non può essere assegnata e/o comunicata ad altri;
- non deve contenere riferimenti agevolmente riconducibili all'Incaricato (es. data di nascita);

2) la password è strettamente personale e non deve essere comunicata e/o condivisa con nessun'altra persona all'interno dell'Organizzazione;

3) I Designati non devono mai fornire le proprie credenziali di accesso rispondendo ad e-mail, WhatsApp o altra chat al fine di contrastare possibili frodi informatiche;

4) qualora vi sia la ragionevole certezza che le credenziali assegnate siano state utilizzate da terzi, il Designato dovrà cambiare immediatamente la password;

5) è tassativamente vietato memorizzarle le credenziali su fogli di carta, documenti cartacei e file non criptati.

E) *4.3.2 Controllo degli accessi agli archivi elettronici e protezione degli stessi*

Al fine di proteggere i dati personali contenuti negli archivi elettronici dell'Organizzazione, sono state adottate le seguenti misure:

- 1) l'accesso alla rete informatica e agli archivi elettronici dei dati è consentito solo ai computer autorizzati e previa autenticazione tramite uno username e una password;
- 2) quotidianamente viene effettuato il backup automatico di tutti gli archivi elettronici su hard-disk esterno a cura del Titolare del Trattamento o di soggetto da esso incaricato;
- 3) parte degli archivi elettronici potrebbe essere sincronizzata su server esterni, situati sul territorio dell'Unione Europea o negli USA, mediante servizi di cloud computing che offrono garanzie adeguate di sicurezza;
- 4) è fatto divieto a chiunque di effettuare copie non autorizzate dei dati contenuti negli archivi elettronici.

F) *4.3.3 Connessione alla rete Internet*

- 1) il collegamento ad Internet avviene esclusivamente tramite un router interno;

- 2) ciascun computer è protetto anche da un software anti-virus e anti-malware aggiornato automaticamente. È obbligo di ciascun Designato verificare che gli aggiornamenti automatici vengano regolarmente effettuati;
- 3) è vietato l'uso dei social network al di fuori delle mansioni e delle finalità eventualmente previste dall'Organizzazione.

G) *4.3.4 Posta elettronica e instant messaging*

- 1) È fatto divieto aprire allegati di posta elettronica non richiesti senza il preventivo consenso del Titolare del Trattamento e/o del Responsabile del Trattamento, ove nominato.
- 2) È fatto divieto aprire allegati di posta elettronica nei formati sospetti (es. .ZIP, .ISO, .MSI, .CAB). Avvisare Titolare e/o Responsabile del Trattamento, ove nominato;
- 3) È fatto divieto aprire messaggi di posta elettronica da mittenti sospetti;
- 4) In caso di apertura di un messaggio e-mail e/o dell'allegato proveniente da indirizzo sospetto, staccare immediatamente il cavo di rete, spegnere il computer, segnalare immediatamente l'accaduto al Titolare e/o al Responsabile del Trattamento, ove nominato;

H) *4.3.5 Controllo degli accessi agli uffici e protezione dei locali dove vengono custoditi gli archivi*

I locali ove sono custoditi i dati personali devono essere soggetti a controllo e a verifica da parte di ciascun Designato, al fine di evitare che durante l'orario di lavoro possano essere conosciuti o 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. Laddove si esegue il trattamento di dati personali, deve essere possibile ricoverare in luogo sicuro i documenti cartacei ed i supporti rimovibili contenenti tali dati. Al termine dell'orario lavorativo, ove la dinamica delle attività ed il numero di occupanti lo consentano, è necessario chiudere sempre a chiave gli uffici nei quali vengono svolti trattamenti di dati personali.

Inoltre:

- 1) L'accesso agli uffici è consentito solamente al personale autorizzato per iscritto dal Titolare del Trattamento;
- 2) collaboratori e clienti possono accedere solamente negli orari di apertura dell'ufficio e solo in presenza di personale autorizzato;
- 3) tutti i locali nei quali vengono custoditi gli archivi, sia elettronici che cartacei, sono protetti da porte dotate di serratura e munite di estintori costantemente oggetto di manutenzione

- 4) l'impianto elettrico è dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi.

I) *4.3.6 Gestione dei fascicoli cartacei*

- 1) È tassativamente vietato ai Designati accedere ai fascicoli cartacei per finalità diverse da quelle necessarie per la lavorazione della pratica;
- 2) i Designati autorizzati ad accedere ai fascicoli cartacei sono obbligati a riporre ciascun fascicolo all'interno del relativo archivio al termine della giornata lavorativa;
- 3) è tassativamente vietato a chiunque portare fuori dall'ufficio i fascicoli cartacei;
- 4) l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;
- 5) in caso di interruzione anche temporanea del lavoro, ogni Designato è obbligato a verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- 6) ogni Designato non può lasciare incustodito il proprio posto lavoro prima di aver provveduto alla messa in sicurezza dei dati;
- 7) è fatto divieto di lasciare incustoditi e accessibili a terzi gli strumenti elettronici con i quali il Designato effettua il trattamento dei dati;
- 8) gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati dai Designati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di collaborazione;
- 9) distruzione delle copie cartacee: si deve procedere alla distruzione del supporto qualora si verificano errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli.

J) *4.3.7 Siti web e social network*

IN CAMMINO CON ROBERTO STRACCIA ODV si avvale di un proprio sito web ufficiale, www.robustostraccia.it nell'ambito del quale i dati comunicati dall'utenza o comunque raccolti nel corso della navigazione non sono accompagnati da alcuna informazione personale aggiuntiva rispetto agli usuali dati la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet (quali ad esempio nomi di dominio, indirizzi IP, sistema operativo utilizzato, tipo di device e di browser utilizzati per la connessione) e vengono trattati per gestire esigenze di controllo delle modalità di utilizzo dello stesso, accertare responsabilità in caso di ipotetici reati informatici e ricavare informazioni statistiche anonime sull'uso del sito.

IN CAMMINO CON ROBERTO STRACCIA ODV si avvale anche di social network per scopi divulgativi e informativi.

Qualora sia necessario o strumentale per l'esecuzione delle specifiche finalità, i dati personali, oltre che dal personale interno di IN CAMMINO CON ROBERTO STRACCIA ODV sono comunicati a destinatari nominati ai sensi dell'art. 28 del GDPR, che li trattano in qualità di Responsabili del Trattamento al fine di ottemperare ad obblighi di legge, a contratti o alle finalità connesse. Precisamente, i dati potrebbero essere comunicati a destinatari appartenenti alle seguenti categorie:

- commercialista;
- consulente del lavoro;
- Istituti di Credito;
- Compagnie Assicurative;

In nessun caso i dati raccolti dall'Organizzazione saranno oggetto di diffusione.

Nel rispetto di quanto previsto dall'art. 5, comma 1, lett. e) del GDPR, i dati personali vengono conservati in una forma che consenta l'identificazione dell'Interessato per un arco di tempo non superiore al conseguimento delle finalità per le quali i dati stessi sono trattati o in base alle scadenze previste dalle norme di legge. La verifica sulla obsolescenza dei dati conservati in relazione alle finalità per cui sono stati raccolti viene effettuata periodicamente.

6. RISK ASSESSMENT

Al fine di implementare le azioni volte all'adeguamento al GDPR, è stata effettuata una ricognizione dell'attuale organizzazione e della documentazione vigente in materia di privacy e delle misure tecniche utilizzate.

In particolare, si è proceduto ad un'analisi dei rischi inerenti il trattamento dei dati, che si allega al presente Modello (**All. n. 2**).

All'esito di detta analisi dei rischi è stato individuato sia il livello di impatto del trattamento dei dati sui diritti e le libertà degli interessati, sia il livello di rischio, e sono state individuate le misure tecniche e organizzative idonee a mitigare i rischi inerenti.

7. GESTIONE DEL DATA BREACH

L'art. 33 GDPR impone al Titolare del Trattamento di notificare all'autorità di controllo l'eventuale violazione di dati personali entro 72 ore dal momento in cui ne viene a conoscenza.

L'obbligo di notifica scatta se la violazione comporta un rischio per i diritti e le libertà delle persone fisiche; qualora, poi, il rischio sia elevato, oltre alla notifica il Titolare è tenuto a darne comunicazione all'Interessato.

Nel caso in cui l'Incaricato e/o un Responsabile del Trattamento, ove nominato, abbiano notizia di una o più delle violazioni sottoindicate, avrà l'obbligo di darne immediata comunicazione al Titolare del Trattamento inviandogli un'e-mail all'indirizzo di posta elettronica omar.moretti@tiscali.it

1. violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
2. violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
3. violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

La comunicazione di violazione dovrà contenere tutti i dettagli della violazione, compresa la descrizione dell'accaduto, la quantità e la tipologia di dati personali coinvolti.

L'obbligo di notifica e quello aggiuntivo di comunicazione verranno valutati caso per caso dal Titolare del Trattamento in relazione alla tipologia di violazione e al suo impatto sui diritti e libertà degli Interessati. Per comprendere quando notificare la violazione è opportuno effettuare una valutazione dell'entità dei rischi:

- **Rischio assente:** la notifica al Garante non è obbligatoria
- **Rischio presente:** è necessaria la notifica al Garante
- **Rischio elevato:** In presenza di rischi "elevati", è necessaria la comunicazione agli interessati. Nel momento in cui il titolare del trattamento adotta sistemi di crittografia dei dati, e la violazione non comporta l'acquisizione della chiave di decrittografia, la comunicazione ai soggetti interessati non sarà obbligatoria.

I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (es. dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (es. rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (es. pazienti, minori, soggetti indagati).

Per la notifica della violazione e la comunicazione al Garante occorre compilare gli appositi moduli messi a disposizione dal Garante stesso e reperibili su www.garanteprivacy.it

Di seguito gli schemi da seguire per la compilazione della notifica ai sensi dell'art. 33 terzo comma GDPR e della comunicazione ai sensi dell'art. 34 secondo comma GDPR:

Notifica	Comunicazione
a) Descrivere la natura della violazione dei dati personali compresi, ove possibile, le	a) Descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati


<p>categorie e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione.</p> <p>b) Comunicare il nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni.</p> <p>c) Descrivere le probabili conseguenze della violazione dei dati personali.</p> <p>d) Descrivere le misure adottate o di cui si propone l'adozione da parte del titolare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.</p>	<p>personali.</p> <p>b) Comunicare il nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni.</p> <p>c) Descrivere le probabili conseguenze della violazione dei dati personali.</p> <p>d) Descrivere le misure adottate o di cui si propone l'adozione da parte del titolare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.</p>
--	--

Il Titolare del Trattamento, ove necessario in funzione della gravità della violazione, metterà in atto le misure tecniche e organizzative più adeguate per scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli Interessati, tenendone traccia scritta, tra le quali:

- a) contenimento della violazione e ripristino dei dati;
- b) valutazione del *data breach* e adozione delle misure atte a scongiurare il ripetersi in futuro della violazione.

* * *

Il presente Modello Organizzativo è soggetto a verifica periodica, almeno annuale, ed eventuale aggiornamento.

Luogo Moresco data 14/03/2021	Firma del Titolare del Trattamento 
-------------------------------	--

Allegati:

- 1) Organigramma privacy;
- 2) Documento di analisi dei rischi.