MODELLO ORGANIZZATIVO PRIVACY

REGOLAMENTO EUROPEO 679/2016
E D.LGS 196/2003 e SMI

Ed.0 del 05.12.2019

PREMESSA

Il presente Modello raccoglie le *misure tecniche ed organizzative* che la UNINFORM attua per garantire - ed essere in grado di dimostrare - la conformità al Regolamento UE 2016/679 delle attività di trattamento dei dati personali delle persone fisiche, Cittadini Europei e residenti nell'Unione Europea, che la Società effettui direttamente o che soggetti terzi effettuino per suo conto.

L'adozione delle *misure tecniche ed organizzative adeguate* è imposta dagli artt. 24 e seguenti del GDPR, ai sensi dei quali le politiche interne e le misure da attuare per soddisfare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di *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 delle persone fisiche.

Infatti il GDPR è costituito da *tre principi ispiratori*, che permeano e sostengono l'*intero impianto normativo*:

1) ***accountability***, ossia il principio di responsabilizzazione. In pratica viene attribuito ai Titolari 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 Regolamento. Ciò impone un approccio integrato, che interessi tutte le aree aziendali, concreto e *risk-based* e 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.

Da detti principi discendono le seguenti regole *operative*:

a) l'istituzione del ***Registro delle attività di trattamento*** (art.30 e cons. 171) 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;

b) Il ***processo di data breach,*** (art. 33 e 34) ossia le regole per la notifica delle eventuali violazioni dei dati personali, che richiede un'attenta analisi e conoscenza delle informazioni gestite, ma soprattutto investimenti

tecnologici nelle modalità di monitoraggio, securizzazione e compartimentazione dei danni che ne possono derivare;

c) il trattamento dei dati personali 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:

- *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*".
- *adempimento di obblighi contrattuali*, ossia 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;
- *obblighi di legge cui è soggetto il titolare del trattamento,* nel qual caso la finalità è specificata per legge;
- *Interessi vitali della persona interessata o di terzi*: ossia 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;
- *legittimo interesse prevalente del titolare o di terzi cui i dati vengono comunicati,* ossia 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;
- *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.

*****

Al fine di rispettare le sopra menzionate regole, l'elaborazione del presente modello ha richiesto la preventiva esecuzione di una attenta e critica attività di *auditing*, che ha consentito l'esame della singola realtà aziendale e della valutazione dei trattamenti da questa posta in essere.
L'obiettivo del presente **Modello Organizzativo Privacy** è, pertanto, quello di garantire e dimostrare che il trattamento dei dati personali da parte di UNINFORM avviene in modo lecito, corretto e trasparente secondo la definizione sopra datane, attraverso una gestione interna ben strutturata che promuove 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, così da aumentare la propria affidabilità verso clienti, partners, consulenti e dipendenti.

1. DEFINIZIONI

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

- **dato personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»);
- **interessato**: persona fisica a cui si riferiscono i dati personali;
- **dati particolari**: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici, dati

relativi alla salute o alla vita e/o all'orientamento sessuale della persona, dati giudiziari;

- **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;
- **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;
- **dati giudiziari**: quelli idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative, dipendenti da reato e dei relativi carichi pendenti o la qualità di imputato o di indagato;

- **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;
- **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;
- **titolare del trattamento**: la persona fisica o giuridica, l'autorità pubblica, 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 in base alle indicazioni di quest'ultimo;
- **incaricato**: persona fisica autorizzata al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile;

- **destinatario**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali per un determinato scopo;
- **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;
- **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.

2. POLICY AZIENDALE

2.1. La UNINFROM ha per scopo la promozione della vita associativa e lo scambio di esperienze culturali, prevalentemente fra studenti universitari, neo laureati e giovani professionisti, finalizzati anche alla formazione e all'arricchimento delle conoscenza, sia nell'ambito tecnico che del mondo scientifico.

Per il perseguimento dello scopo sociale, l'Associazione si propone di svolgere le seguenti attività:

- istituzione di corsi di studio e organizzazioni dei relativi servizi;
- organizzazione di seminari di studio per studenti e studenti lavoratori;
- svolgimento di corsi di aggiornamento culturale e professionale;
- organizzazione di gruppi di lavoro per lo studio, a livello scientifico, delle tematiche interessanti l'evoluzione delle discipline universitarie;
- istituzione di centri di documentazione al servizio dei soci per attività di studio e di ricerca, per ricerche bibliografiche;
- acquisto e distribuzione di pubblicazioni a prevalente beneficio dei soci;
- indizione di manifestazioni, convegni, dibattiti;
- stipula di convenzioni con enti pubblici e privati per la gestione di corsi e seminari e la fornitura di servizi ai soci;
- redazione ed edizione di pubblicazioni periodiche, tesi, studi, elaborazioni monografiche, notiziari, indagini, ricerche;
- sviluppo di studi e ricerche in specifici settori, con conferimento di eventuali borse di studio.

L'Associazione avvia e instaura collaborazioni temporanee o stabili con persone fisiche o con enti pubblici e privati o associazioni, organismi e movimenti con i quali ritiene di condividere iniziative e attività comunque rientranti nelle proprie finalità statutarie.
Promuove, altresì, attraverso la collaborazione delle attività degli associati e la dazione di contributi, lo sviluppo in senso lato di associazioni nazionali ed internazionali che si propongono il migliorismo fisico e culturale dell'infanzia.
Per il perseguimento del proprio scopo, pertanto, la UNINFORM, svolge tutte le attività a ciò necessarie tra le quali – per quanto qui interessa:

- la gestione dei clienti e dei relativi contratti;
- la gestione del proprio personale;
- la gestione dei rapporti con i fornitori e dei professionisti;
- la gestione dei rapporti con i partner;
- l'approvvigionamento degli strumenti, dei materiali e dei servizi;
- la gestione dei contratti in generale.

2.2. Nello svolgimento di tali attività, la UNINFORM gestisce differenti **tipologie di dati personali**, ovvero:

- ***dati anagrafici in senso stretto*** riferibili ai dipendenti ed ai loro familiari, ai clienti, ai fornitori, nonché ai professionisti e consulenti esterni;
- ***dati giudiziari*** riferibili ai dipendenti e ai clienti;
- ***dati relativi alla salute*** dei dipendenti e dei clienti;
- ***dati atti a rivelare l'appartenenza sindacale*** *dei dipendenti*;
- ***dati bancari*** dei dipendenti, dei clienti, dei professionisti e dei consulenti in generale;
- ***dati biometrici***, quali le fotografie dei dipendenti, dei clienti, e dei professionisti in generale, eventualmente destinate ad essere pubblicate sul sito internet ufficiale di UNINFORM;
- ***dati di identificazione elettronica*** riferibili a soggetti terzi, acquisiti attraverso la navigazione del proprio sito web;
- ***dati inerenti le qualifiche professionali e la carriera*** dei dipendenti, nonché dei clienti;

2.3. La **base giuridica** del trattamento di tali dati da parte di UNINFORM è rappresentata da:

- il consenso dell'interessato
- l'adempimento degli obblighi contrattuali e pre-contrattuali di cui UNINFORM è parte;
- l'adempimento degli obblighi di Legge cui la stessa è tenuta;

- legittimo interesse del Titolare.

2.4. Ogni Funzione della UNINFORM tratta i dati personali sopra elencati limitatamente alla propria funzione, come definita dall'**organigramma aziendale** (Allegato **1**).

2.4.1. Quando gestiti in ***forma cartacea***, tutti i documenti sono custoditi in una stanza archivio chiusa a chiave e con accesso limitato. I documenti di comune e continuo utilizzo sono conservati nei rispettivi uffici e collocati dentro armadi o stanze con chiusura a chiave ad accesso consentito solo alle persone autorizzate. Sono impartite a tutti gli incaricati precise istruzioni sul trattamento dei dati e delle pratiche cartacee, in particolare la *duplicazione elettronica* mediante scansione dei documenti cartacei, onde prevenirne la distruzione totale accidentale e consentire la archiviazione segregata, con accesso riservato al solo personale autorizzato.

Regolarmente il Titolare del trattamento controlla che le regole di tenuta della documentazione cartacea siano osservate da tutti gli incaricati sottoposti.

2.4.2. Quando gestiti in ***forma elettronica***, i dati ed i relativi documenti vengono trattati mediante *personal computers*, fissi e portatili, nonché eventuali *smartphones* messi a disposizione del personale ed utilizzati in esclusiva da ciascun incaricato. I dispositivi informatici sono tutti protetti da *passwords*. La *passwords* è conoscibile esclusivamente dall'affidatario del dispositivo informatico, dall'Amministratore del sistema e dalla direzione.

2.5. La **rete informatica aziendale** è attualmente composta dalle seguenti attrezzature:

- 3 Pc fissi Lenovo tutti con Window 10, Office 2016 e Adobe
- 4 Pc portatili Acer tutti con Window 10, Office 2016 e Adobe
- 3 stampanti

2.5.1. L'accesso alla rete aziendale è consentito in modo selezionato.

2.5.2. Per le singole regole del trattamento cartaceo e informatico si rinvia al **regolamento interno** allegato (Allegato **2**).

2.6. I dati raccolti da UNINFORM non sono oggetto di **diffusione e/o di trasferimento all'estero**, né all'interno né all'esterno dell'Unione Europea, ad eccezione delle foto pubblicate sui social media previo consenso, per cui il trattamento sarà regolato in conformità a quanto previsto dal capo V del GDPR UE 679/2016 e autorizzato in base a specifiche decisioni dell'Unione Europea. Saranno quindi adottate tutte le cautele necessarie al fine di garantire la più totale protezione dei dati personali basando tale trasferimento: a) su decisioni di adeguatezza dei paesi terzi destinatari espressi dalla Commissione Europea; b) su garanzie adeguate espresse dal

soggetto terzo destinatario ai sensi dell'art. 46 del Regolamento; c) sull'adozione di norme vincolanti d'impresa.

2.7. 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.

3. AREE E LOCALI

3.1. Il trattamento dei dati avviene, con le modalità di seguito riportate, presso la sede legale e operativa, situata in Roma Corso Trieste, 155, come da **piantina** allegata (Allegato **3**).

3.2. L'**accesso all'edificio** di Corso Trieste, 155 è consentito anche al pubblico ed avviene da un'unica entrata, situata nella medesima via.

3.3. Gli **uffici** sono protetti da porta blindata e sistema di allarme.

3.4 La **sala di attesa** è separata dall'area uffici, e l'Ufficio Segreteria è sempre presente durante orario ufficio.

3.5. L' Archivio cartaceo è posto all'interno di una **stanza archivio** chiusa a chiave e ad accesso ristretto

4. TITOLARI, RESPONSABILI E INCARICATI

Le figure e le funzioni coinvolte nella UNINFORM nelle attività di protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale sono:

4.1. *TITOLARE DEL TRATTAMENTO*: è la stessa UNINFORM, in persona del legale rappresentante pro tempore, sul quale, conseguentemente, incombono tutti gli obblighi e le responsabilità che la legge, italiana ed europea, gli 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 e al D. Lgs. n. 196/2003, come modificato dal D. Lgs. N. 101/2018.

4.2. In un ambito specifico UNINFORM risulta essere *CONTITOLARE DEL TRATTAMENTO* ai sensi dell'art. 26 del GDPR, e precisamente in relazione ai dati dei clienti che la UNINFORM trasmette ai partners, relativamente ai quali la UNINFORM procede al trattamento con le medesime modalità

utilizzate per i dati dei propri clienti, chiedendo altresì ai partners di adeguarsi a dette modalità di trattamento.

4.3. *RESPONSABILI DEL TRATTAMENTO*.

4.3.1. INTERNI: la UNINFORM non ha nominato responsabili interni, per cui la gestione dei dati fa capo al titolare del trattamento.

4.3.2. ESTERNI: Qualora sia necessario o strumentale per l'esecuzione delle specifiche finalità, i dati personali, oltre che al personale interno di UNINFORM sono comunicati a destinatari nominati ai sensi dell'art. 28 del GDPR, che li trattano in qualità di Responsabili che agiscono sotto l'autorità del Titolare al fine di ottemperare ad obblighi di legge, a contratti o alle finalità connesse.

Precisamente, i dati possono essere comunicati a destinatari appartenenti alle seguenti categorie:

- Docenti dei corsi
- Avvocati;
- Consulente del Lavoro;
- Consulenti Assicurativi;
- Consulenti informatici;
- Istituti di Credito;
- Società di Revisione;
- Altri Consulenti esterni che gestiscono dati personali;
- Società Partners.

Rispetto a detto elenco, ovviamente, di volta in volta, potranno essere nominati altre categorie di Responsabili, Consulenti o Società esterne che trattano dati personali di cui UNINFORM sia titolare.

L'elenco nominativo dei Responsabili del trattamento designati è costantemente aggiornato e disponibile presso la sede di UNINFORM.

La UNINFORM ha predisposto una specifica **lettera di incarico** (Allegato **4**) per la nomina e le direttive dei responsabili esterni ai fini di una corretta gestione da parte di quest'ultimi dei dati di cui vengono a conoscenza in conseguenza dell'affidamento da parte dell'associazione di specifiche attività, quali a titolo esemplificativo e non esaustivo: docenza, consulenza legale, consulenza in materia di lavoro, redazione buste paga, ecc.

4.4. *INCARICATI DEL TRATTAMENTO:* la persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile.

Gli incaricati del trattamento di UNINFORM sono coloro i quali, facenti parte dell'organico di UNINFORM, provvedono materialmente al trattamento dei dati personali.

UNINFORM cura l'aggiornamento costante dei propri incaricati mediante corsi di formazione ed aggiornamento (vedi cap. 10).

5. PORTABILITA' E CANCELLAZIONE

5.1. Portabilità: Ai sensi dell'Art. 20 del GDPR UE 679/2016, la UNINFORM si impegna a fornire, qualora venga richiesto dall'interessato, i dati personali dello stesso in un formato strutturato, di uso comune e leggibile da dispositivo automatico, senza ingiustificato ritardo e, comunque, entro un mese dalla richiesta (Art. 12 GDPR UE 679/2016).

5.2. Cancellazione (Diritto all'Obblio): L'interessato ha il diritto di chiedere, in qualsiasi momento, la cancellazione dei dati personali che lo riguardano e la UNINFORM si obbliga a cancellare senza ingiustificato ritardo i dati personali, come disposto dall'Art. 17 del GDPR UE 679/2016, nonché a comunicare detta richiesta a tutti gli altri soggetti a cui ha trasmesso detti dati.

6. REGISTRO DEI TRATTAMENTI – RISK ASSESSMENT – MISURE DI SICUREZZA E GAP ANALYSIS

6.1. Nel rispetto dell'art.30 del regolamento Europeo la UNINFORM ha redatto il **Registro dei Trattamenti** nel quale è stata svolta una attenta analisi circa i dati trattati, le finalità, le modalità, la base giuridica, il luogo e tempo di conservazione, la categoria degli interessati e quella dei destinatari, così evidenziando i controlli ed i processi che consentono di soddisfare l'*accountability* del sistema privacy (Allegato **5**).

6.2 Al fine di implementare le azioni volte all'adeguamento al Regolamento UE 679/2016 in materia di dati personali, è stata effettuata inizialmente una analisi dell'attuale organizzazione e della documentazione vigente in materia di privacy e misure tecniche utilizzate.

In particolare, si è proceduto, con l'ausilio di consulenti esterni, con l'esame della principale documentazione organizzativa e procedurale; alla luce di tale analisi, è stato predisposto uno specifico questionario finalizzato all'identificazione dei principali rischi di non conformità al Regolamento UE 679/2016.

Sulla base delle informazioni raccolte è stata sviluppato un processo strutturato di analisi del rischio: per ogni gruppo/categoria di dati trattati sono state individuate tutte le minacce di violazione ed è stata effettuata una valutazione del livello di **probabilità** e di **severità** del rischio, utilizzando la **Matrice dei Rischi**.

La matrice di valutazione del rischio mostra un valore compreso tra 1 e 5 (a-e) per tutte le minacce individuate in base alla gravità delle conseguenze e la probabilità di accadimento. Le 5 categorie che descrivono la gravità di un potenziale scenario e la probabilità di occorrenza sono di seguito indicate:

Severità della violazione	Descrizione
Catastrofico **a**	Impatto catastrofico sui diritti e le libertà degli interessati, ad esempio attacco di un virus/malware informatico oppure sabotaggio dei sistemi informatici.
Pericoloso **b**	La violazione rappresenta un serio pericolo per i diritti e le libertà degli interessati, per esempio furto di dati cartacei o informatici o furto di apparecchiature informatiche.
Maggiore **c**	Impatto maggiore sui diritti e le libertà degli interessati, ad esempio rottura hardware o perdita/smarrimento di un dispositivo di archiviazione dati (PC portatile, chiavetta USB).
Minore **d**	Impatto maggiore sui diritti e le libertà degli interessati, per esempio un black-out elettrico.
Trascurabile **e**	Nessuna conseguenza sui diritti e le libertà degli interessati.

Probabilità di accadimento	Descrizione
Frequente **5**	Probabile che si verifichi molte volte (si è verificato frequentemente)
Occasionale **4**	Probabile che si verifichi qualche volta (si è verificato raramente)
Remoto **3**	Improbabile ma possibile che si verifichi (si è verificato raramente)
Improbabile **2**	Molto improbabile che si verifichi (non si è mai verificato)
Estremamente improbabile **1**	Quasi inconcepibile che l'evento possa verificarsi

Dopo aver individuato un valore per la gravità e la probabilità di un evento, si moltiplicano i due valori. Il risultato è l'indicatore di rischio per la specifica violazione. Basandosi su questo indicatore, il rischio è stato classificato come accettabile, tollerabile o inaccettabile sulla base della seguente matrice:

		Severità				
		Catastrofico A	Pericoloso B	Maggiore C	Minore D	Trascurabile E
Probabilità	Frequente 5	inaccettabile	inaccettabile	inaccettabile	tollerabile	tollerabile
	Occasionale 4	inaccettabile	inaccettabile	tollerabile	tollerabile	tollerabile
	Remoto 3	inaccettabile	tollerabile	tollerabile	tollerabile	accettabile
	Improbabile 2	tollerabile	tollerabile	tollerabile	accettabile	accettabile
	Estremamente improbabile 1	accettabile	accettabile	accettabile	accettabile	accettabile

Il livello di rischio ottenuto rappresenta una indicazione iniziale, cioè prima della applicazione delle misure di sicurezza.
In base alle misure di sicurezza applicate e ai controlli eseguiti nel trattamento, si riduce la probabilità/frequenza di accadimento e/o l'impatto per le varie tipologie di rischio analizzate. Con la stessa matrice sopra indicata si è calcolato quindi il **rischio residuale** (cioè ridotto dalle contromisure di sicurezza applicate).
La riduzione del livello di rischio, dal rischio iniziale al rischio residuale, rappresenta l'efficacia delle misure di sicurezza applicate e evidenzia gli interventi/investimenti fatti per assicurare la "sicurezza".

Rating per la classificazione del livello di rischio
Quando la valutazione del "rischio residuale" nella matrice è:
verde = livello di rischio considerato accettabile;
giallo = necessario pianificare interventi di mitigazione;
rosso = indispensabile attivare rapidamente contromisure di adeguamento.

Le misure tecniche ed organizzative individuate sono state confrontate con quelle già esistenti per sviluppare una **gap analisysis** e stabilire un **piano di adeguamento**, definendo i tempi di attuazione.
Annualmente o per ogni scadenza delle attività a piano, vengono verificati gli interventi eseguiti e eventualmente aggiornata l'analisi dei rischi.
Tutte le informazioni relative alla analisi del rischio e alle misure di sicurezza sono dettagliate negli allegati "Analisi del rischio" e "Gap analisys" (Allegato 6).

7. Registro delle Violazioni e DATA BREACH

7.1. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio, in apposito registro denominato **Registro delle Violazioni** (Allegato **7**).
7.2. Fermo restando l'obbligo dell'annotazione di tutte le violazioni sul registro, Il GDPR disciplina il ***data breach*** prevedendo espressamente un obbligo di notifica e comunicazione in capo al titolare, in presenza di violazioni di dati personali che possano compromettere le libertà e i diritti dei soggetti interessati.
Il criterio dirimente per valutare la necessità di avviare una procedura di notifica è la probabilità che la violazione possa porre a rischio (per la notifica all'autorità) o ad elevato rischio (per la comunicazione agli interessati) le libertà e i diritti degli individui.
7.2.1. Gestione Data Breach Interno: Ogni operatore aziendale autorizzato a trattare dati, qualora venga a conoscenza di un potenziale caso di data breach, avvisa tempestivamente il Titolare del Trattamento. La segnalazione perviene al Titolare del Trattamento tramite le consuete modalità di gestione dei flussi documentali già in uso in azienda. Il Titolare del Trattamento effettua una valutazione dell'evento avvalendosi, nel caso, di professionalità necessarie per la corretta analisi della situazione. Ai fini di una corretta classificazione dell'episodio, il Titolare del Trattamento utilizzerà lo schema delle violazione contenuto nel risk assessment (vd allegato 6). Sulla scorta delle determinazioni raggiunte, il Titolare del Trattamento predispone l'eventuale comunicazione all'Autorità Garante, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui il titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza del verificarsi di un incidente di sicurezza che riguardi dati personali. Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo. E' comunque fatta salva la possibilità di

fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow-up (c.d. notifica in fasi).
La notifica deve almeno: a)descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione; 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; c) descrivere le probabili conseguenze della violazione dei dati personali; d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
La notifica deve essere effettuata, utilizzando il fac simile scaricabile dal sito del Garante Privacy, a mezzo pec all'indirizzo:

protocollo@pec.gpdp.it

La scelta e le motivazioni che hanno portato a non notificare l'evento deve essere documentata a cura del Titolare del Trattamento, nel Registro delle Violazioni.
7.2.2. Gestione Data Breach Esterno: Ogni responsabile del trattamento, qualora venga a conoscenza di un potenziale data breach che riguardi dati di cui l'azienda sia titolare, ne dà avviso senza ingiustificato ritardo al Titolare del Trattamento. Per "ingiustificato ritardo" si considera la notizia pervenuta al titolare al più tardi entro 12 ore dalla presa di conoscenza iniziale da parte del responsabile. Il Titolare del Trattamento effettua una valutazione dell'evento avvalendosi, nel caso, di professionalità necessarie per la corretta analisi della situazione. Ai fini di una corretta classificazione dell'episodio, il Titolare del Trattamento utilizzerà lo schema delle violazione contenuto nel risk assessment (vd allegato 6). Pertanto, sulla scorta delle determinazioni raggiunte, il Titolare del Trattamento predispone l'eventuale comunicazione all'Autorità Garante, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui il titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali. Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo. E' comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla

violazione di cui il titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow-up (c.d. notifica in fasi).
Per la modalità e contenuto della notifica si rinvia al precedente paragrafo 7.2.1. Anche in questo caso, la scelta e le motivazioni che hanno portato a non notificare l'evento deve essere documentata a cura del Titolare del Trattamento.
7.2.3. Modalità di comunicazione agli interessati: Nel caso in cui dal data breach possa derivare un rischio elevato per i diritti e le libertà delle persone, anche queste devono essere informate senza ingiustificato ritardo, al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione. Il Titolare del Trattamento predispone l'eventuale comunicazione all'interessato/agli interessati, da inviarsi nei tempi e nei modi che lo stesso, anche attraverso eventuale richiesta di consulenza individuerà come più opportuna come specificato nell'art. 34 del GDPR e tenendo conto di eventuali indicazioni fornite dall'Autorità Garante.

8. INFORMATIVE:

8.1. La UNINFORM ha predisposto tre specifiche informative, una rivolta ai dipendenti e più in generale alle persone valutate ai fini di un inserimento di lavoro, l'altra rivolta a fornitori, professionisti, clienti e terzi in genere ed infine, una per i partecipanti ai master.
8.2. La UNINFORM ha altresì predisposto le informative di privacy policy e cookie policy, pubblicate sul proprio sito internet.
8.3. La UNINFORM ha anche predisposto una informativa di avviso che deve essere messa a corredo della mail aziendale e dunque essere riportata in ogni mail in uscita dalla UNINFORM stessa.
Tutte le suddette **informative** sonno accluse al presente manuale (Allegato **8**)

9. DIVIETI E SISTEMA DISCIPLINARE

9.1. Ogni Utente è responsabile dei dati e delle informazioni delle quali entra in possesso per lo svolgimento della sua attività lavorativa. Deve quindi trattare i dati e le informazioni adottando ogni idonea misura di sicurezza al fine di tutelarne la riservatezza, la sicurezza, l'integrità ed il corretto utilizzo.
I dati e le informazioni potranno essere comunicate a terze parti esclusivamente nell'ambito della propria funzione e secondo le finalità connesse alla propria attività lavorativa.

9.2. Di seguito sono riportati specifici **divieti per gli Utenti**, da intendersi tutti preceduti dalla locuzione “è Vietato”:

- Il trattamento dei dati senza prima aver fornito l’informativa all’interessato ed averne acquisito il consenso;
- lasciare incustoditi documenti contenenti dati personali;
- l’utilizzo di dati personali per motivi illeciti e/o comunque diversi rispetto alla finalità per cui gli stessi sono stati forniti;
- l’accesso e la utilizzazione di documenti per i quali non si dispone di autorizzazione;
- la comunicazione di dati e informazioni verso terzi che possano arrecare danno all’immagine, alla reputazione, alla produttività, alla proprietà intellettuale e del know-how ed alla redditività aziendale o che possano violare i vincoli contrattuali e di legge connessi al rapporto di lavoro.
- la divulgazione a terzi di informazioni riservate, confidenziali o comunque di proprietà del Titolare.
- alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e /o cancellare dati e/o informazioni;
- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico o di soggetti concorrenti, pubblici o privati al fine di acquisire informazioni riservate;
- svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l’interruzione, totale o parziale, o l’alterazione del suo funzionamento;
- svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni;
- svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
- svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;

- distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità;
- caricare programmi non provenienti da una fonte certa e autorizzata dalla Società;
- utilizzare illegalmente password di computer, codici di accesso o informazioni simili per compiere una delle condotte sopra indicate;
- utilizzare strumenti o apparecchiature, inclusi programmi informatici, per decriptare software o altri dati informatici;
- distribuire il software aziendale a soggetti terzi;
- accedere illegalmente e duplicare banche dati.

9.3. Gli Utenti, inoltre, devono seguire le seguenti **regole di navigazione** della rete Internet:

- è tassativamente vietato scaricare materiale e programmi in violazione della legislazione sui diritti di autore, che siano essi appartenenti a persone o aziende, coperti da copyright, brevetto o proprietà intellettuale, ivi compresa l'installazione o la distribuzione di software che non sia specificatamente licenziato per essere utilizzato all'interno di UNINFORM;
- è tassativamente vietato navigare siti e scaricare materiale pericolosi/vietati o aventi contenuti illegali (contenuto offensivo, molesto, volgare, blasfemo, xenofobo, razziale, pornografico, pedopornografico, terrorismo o comunque inappropriato o illegale), salvo specifiche esigenze di lavoro;
- è vietato effettuare copia non autorizzata di materiale coperto da copyright compreso ma non limitato a digitalizzazione e distribuzione di foto da riviste, libri o altre fonti, musica o materiale video;
- è vietato utilizzare l'infrastruttura tecnologica di UNINFORM per procurarsi e diffondere materiale in violazione con le normative vigenti;
- è vietato effettuare attività che possano generare dei problemi di sicurezza o danneggiare le comunicazioni sulla rete;
- è vietato eseguire qualsiasi forma di monitoraggio della rete che permetta di catturare dati non espressamente inviati all'host dell'Utente (sniffing) a meno che questa attività non faccia parte dei compiti dell'Utente e quindi formalmente autorizzata dagli amministratori di sistema;
- è vietato aggirare le procedure di autenticazione o la sicurezza di qualunque host, rete, account.

9.4. Data Breach: Ogni utente è tenuto a comunicare al Titolare del Trattamento immediatamente e comunque non oltre le 24 ore eventuali violazioni di dati personali compiuti direttamente o delle quali è venuto a conoscenza nello svolgimento delle proprie funzioni.
9.5. La violazione dei suddetti divieti e obblighi è sanzionata secondo il **sistema disciplinare** accluso al presente manuale (Allegato **9**).

10. FORMAZIONE

10.1. In osservanza alle disposizioni dell'art. 28 e art. 32 comma 4 del Reg. EU 679/16, tutti i soggetti addetti al trattamento dei dati personali devono essere in grado di fornire al Titolare garanzie professionali sufficienti che soddisfino i requisiti di formazione e competenza richiesti dalla natura dell'incarico.
10.2. A tal proposito, almeno una volta l'anno, la UNINFORM organizza degli **interventi formativi** rivolti agli incaricati dei trattamenti che hanno la finalità di rendere loro edotti:

- sulla segretezza della componente riservata delle credenziali di accesso agli strumenti informatici e sulla diligente custodia dei dispositivi in possesso ed uso esclusivo dell'addetto;
- sulla custodia e l'accessibilità dello strumento informatico durante una sessione di trattamento;
- sul controllo e sulla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali;
- sulle procedure aziendali da applicare per la sicurezza e la protezione dei dati, quali ad esempio il cambio delle password, il salvataggio dei dati, aggiornamenti di antivirus e tutto quanto necessario a far si che le misure di sicurezza stabilite dall'azienda vengano a tutti gli effetti messe in pratica;
- sui profili di autorizzazione e gli ambiti di applicazione degli stessi riferiti per classi omogenee di addetti;
- sulle Policy aziendali in riferimento all'utilizzo della posta elettronica e di internet;
- sui diritti dell'interessato ex artt. dal 15 al 22.

10.3. Il piano formativo del personale tiene conto dei seguenti criteri:

a) aggiornamento/modifica delle istruzioni agli addetti;
b) aggiornamento/modifica delle misure di sicurezza adottate.
c) modifiche organizzative
d) modifiche della normativa di riferimento.

11. VADEMECUM

Vedi Prospetto delle Attività (Allegato **10**)

12. ALLEGATI:

Allegato **1.** Organigramma
Allegato **2.** Regolamento Interno Privacy
Allegato **3.** Piantina edificio sede
Allegato **4.** Lettera incarico Responsabili Esterni
Allegato **5.** Registro delle Attività di Trattamento
Allegato **6.** Analisi dei Rischi - Gap Analysis – Misure di Sicurezza
Allegato **7.** Registro delle Violazioni
Allegato **8.** Informative
Allegato **9.** Sistema Disciplinare
Allegato **10.** Prospetto delle Attività