ORDINE DEGLI INGEGNERI DI CUNEO
Via V.Allione, 4 - 12100 – Cuneo (CN)
Codice fiscale: 80019740044

DOSSIER PRIVACY

ai sensi del Regolamento UE n. 2016/679 - relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e del Principio di Accountability

Testo approvato dal PRESIDENTE DELL'ORDINE

Firma _____

Testo adottato dall'ORDINE DEGLI INGEGNERI

Firma _____

Data	Revisione	Descrizione
24/05/2019	00	Prima emissione

INDICE

1. Scopo del documento e riferimenti normativi

Alla luce dell'introduzione, ad opera del GDPR – *General Data Protection Regulation*, del nuovo concetto di "Accountability" (Principio di responsabilizzazione), il Titolare del trattamento dei dati personali con il presente Dossier intende dimostrare, dopo aver posto in essere un'attenta valutazione delle misure tecniche e organizzative ritenute adeguate in base alla propria realtà, che i trattamenti posti in essere sono effettuati in modo conforme al Regolamento Europeo n. 2016/679, in condizioni di sicurezza per i diritti delle persone fisiche ed in modo tale da tutelare i dati e ridurre al minimo i rischi di distruzione o perdita degli stessi, nonché i rischi di accesso non autorizzato e utilizzo non consentito o non conforme alle finalità di raccolta.

Il presente documento ha lo scopo di raccogliere e rendere esplicite tutte le regole comportamentali, l'attribuzione di incarichi e responsabilità sia verso persone interne alla struttura, sia strutture esterne e collaboratori, nonché elencare le misure minime e idonee di sicurezza adottate in base a quanto disposto dal Regolamento Eu 2016/679.

Le definizioni, le norme e le procedure descritte nel presente documento si applicano sia ai trattamenti effettuati in forma cartacea, sia a quelli automatizzati effettuati con l'ausilio di strumenti elettronici.

La prassi interna e l'applicazione nonché la verifica del rispetto di quanto descritto nel presente documento, viene affidata sia ai percorsi formativi ed informativi (individuati al punto 12), sia durante controlli ed auditing periodici a cura del Titolare del trattamento, e/o del Responsabile interno del trattamento.

Per elaborare il Dossier Privacy si è tenuto conto delle seguenti normative:

- Regolamento UE n. 2016/679 - relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati
- D.Lgs. 10 agosto 2018, n. 101
- D.Lgs. n. 196/2003 - Codice in materia di protezione dei dati personali (nelle parti non abrogate)
- Decisioni della Commissione UE
- Linee Guida e provvedimenti dei Garanti Europei (WP29, Comitato Europeo Protezione dati)
- Provvedimenti del Garante per la protezione dei dati personali.

2. Terminologia e definizioni

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.
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.
Dato particolare	Qualsiasi informazione riguardante una persona fisica che riveli l'origine raziale, etnica, le convinzioni religiose o filosofiche, le opinioni politiche o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
Dati giudiziari	I dati personali che rivelano l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (quali, ad es., i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione).
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.
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.
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.
Autorizzato al trattamento	La persona fisica, designata per iscritto dal Titolare del trattamento dei dati, che opera sotto la diretta autorità di questo, attenendosi alle istruzioni impartite, nell'ambito del trattamento dei dati personali.
Responsabile trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento.
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.
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.
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.
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.

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.
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.
Comunicazione	Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli autorizzati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Diffusione	Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Strumenti elettronici	Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.
Credenziali di autenticazione	I dati ed i dispositivi in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.
Rischio	Effetto dell'incertezza. Scostamento da quanto atteso – positivo o negativo.

3. Titolare del trattamento dei dati personali

Titolare del trattamento dei dati personali è: **ORDINE DEGLI INGEGNERI DI CUNEO**
Via V.Allione, 4 – 12100 Cuneo (CN)
Codice fiscale: 80019740044

3.1. Sedi di riferimento

Al Titolare del trattamento è affidato il compito di redigere ed aggiornare ad ogni variazione l'elenco delle sedi e degli uffici in cui viene effettuato il trattamento dei dati.

In particolare la struttura ha la seguente sede legale e la/le seguente/i sede/i operativa/e:

SEDI	INDIRIZZO
Sede legale	Via V.Allione, 4 – 12100 Cuneo (CN)
Sede operativa	Via V.Allione, 4 – 12100 Cuneo (CN)

3.2. Attività prevalenti ed accessorie esercitate dal titolare del trattamento

Istituzione di autogoverno della professione di ingegnere, avente il fine di garantire la qualità delle attività svolte dai professionisti.

Funzioni organizzative previste ai fini della protezione dei dati

Nella definizione del Piano Privacy sono stati adottati alcuni dei ruoli sotto definiti; la copia originale con le firme dei soggetti nominati è conservata unitamente al suddetto Dossier Privacy; per un elenco sintetico si rimanda al punto 5 del presente documento.

4. Funzioni organizzative previste ai fini della protezione dei dati

4.1. Titolare del trattamento dei dati (TTD)

Il titolare del trattamento è il soggetto individuato all' art. 4. par. 1, n. 7 GDPR 2016/679 cui spetta la massima responsabilità amministrativa e penale in campo privacy, dotato di massima autonomia nell'impostazione del piano privacy, nel nominare le altre figure citate oltre e nel prescrivere, verificare ed eventualmente adottare ogni misura di sicurezza e procedura ritenga adatta per adempiere alla Legge.

Ha il compito di:

- mettere in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento Europeo G.D.P.R. 2016/679;
- riesaminare ed aggiornare le misure suddette qualora necessario, ovvero nei casi in cui sussistano delle variazioni di input, output o nei processi stessi;
- decidere, qualora lo ritenga opportuno, di affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare.

4.2. Autorizzato al trattamento dei dati (ATD)

L'autorizzato al trattamento è il soggetto che viene incaricato al trattamento per iscritto dal Titolare del trattamento o dal Responsabile interno privacy (se individuato) ed è colui che effettua nella pratica il trattamento dei dati personali; il potere discrezionale dell'addetto è limitato a quanto previsto nella lettera di autorizzazione, cui dovrà attenersi nello svolgimento delle proprie mansioni.

Ha il compito di:

- attenersi alle istruzioni impartite dal TTD attraverso la lettera di autorizzazione al trattamento dei dati personali;
- trattare i dati personali solo in conformità alle finalità previste e dichiarate e prestando particolare attenzione all'esattezza degli stessi;
- segnalare e chiedere delucidazioni al TTD in tutti i casi in cui non sia chiaro come trattare un dato personale;
- osservare tutte le misure di protezione e sicurezza per evitare i rischi di distruzione, perdita, accesso non autorizzato, trattamento non consentito dei dati personali;
- non lasciare nessun documento incustodito o in vista presso la propria postazione di lavoro, quando questi non siano necessari allo svolgimento della mansione (adottare e rispettare la politica della "scrivania pulita");
- non lasciare incustodito o accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali;
- adottare le misure adeguate nella gestione delle credenziali di autenticazione
- ricevere apposita formazione e partecipare alle sessioni di aggiornamento in materia privacy previste dalla legge vigente e disposte dal TTD.

L' autorizzato al trattamento dei dati (ATD) dovrà essere autorizzato mediante ***"MOD_Lettera di autorizzazione al trattamento dei dati"***.

4.3. Responsabile del trattamento dei dati (RTD)

Il Responsabile del trattamento è un soggetto esterno a cui vengono comunicati dati personali per adempiere ad obblighi contrattuali o svolgere servizi necessari per il perseguimento delle finalità indicate nell'informativa (es. commercialista, consulente del lavoro, medico competente ecc.).

Ha il compito di:

- assistere il TTD effettuando un trattamento per conto di questi;
- attenersi alle istruzioni impartite dal TTD attraverso la lettera di nomina a responsabile del trattamento dei dai personali;
- mettere in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento Europeo n. 2016/679.

Il Responsabile del trattamento dei dati (RTD) dovrà essere autorizzato mediante ***"MOD_Atto di nomina_Responsabile esterno del trattamento"***.

4.4. Responsabile della sicurezza dei dati personali (DPO)

In base all'articolo 37 del Regolamento Europeo n. 2016/679 tale figura risulta essere obbligatoria nei seguenti casi specifici:

- il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico;
- le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Il DPO ricopre tanto il ruolo cruciale di supervisore interno, al fine di dimostrare la conformità dei trattamenti effettuati all'interno dell'Organizzazione al Regolamento Europeo n. 2016/679, quanto quello di facilitatore e comunicatore verso il vertice dell'Organizzazione e verso l'esterno, anche in caso di incidenti di sicurezza, essendo un punto di contatto con l'Autorità Garante.

Il Responsabile della sicurezza dei dati personali (DPO) dovrà essere designato mediante "***MOD_Atto di designazione_Responsabile della Protezione dei Dati personali"***.

Il Titolare del trattamento dei dati, in virtù di quanto disposto all'art. 37 del Regolamento UE n. 2016/679, ritiene che la propria Organizzazione non rientra in uno dei casi di designazione obbligatoria del Responsabile della Protezione dei Dati personali.

4.5. Amministratore di sistema (AS)

Seppur il Regolamento UE n. 2016/679 non preveda espressamente questa figura, è consigliato che il Titolare del trattamento provveda a designare la stessa, in presenza di sistemi software complessi e nell'evenienza in cui tale funzione eserciti il suo operato in un contesto che renda ad esso tecnicamente possibile l'accesso, anche fortuito a dati personali del Titolare stesso. L'attribuzione deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato.

Qualora l'attività dell'Amministratore di sistema riguardi anche indirettamente servizi o sistemi che permettano il trattamento di informazioni di carattere personale dei lavoratori, il Titolare del trattamento è tenuto a rendere nota o conoscibile l'identità dell'Amministratore di sistema nell'ambito della propria Organizzazione. Ciò può essere fatto avvalendosi dell'informativa resa agli interessati ai sensi dell'art. 13 del GDPR 2016/679 nell'ambito del rapporto di lavoro che li lega al Titolare, oppure utilizzando strumenti di comunicazione interna.

L'Amministratore di sistema ha il compito di:

- redigere e verificare, ad ogni variazione, l'elenco dei sistemi di elaborazione;
- adottare i sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici;
- gestire e procedere al mantenimento delle connessioni di rete proprie dell'Organizzazione, garantendone la funzionalità e la sicurezza.

5. Distruzione dei compiti e delle responsabilità: Organigramma

TITOLARE DEL TRATTAMENTO DEI DATI	
ORDINE DEGLI INGEGNERI DI CUNOE	
AUTORIZZATI AL TRATTAMENTO	
BERTACCINI CHIARA	IMPIEGATA
FERRARA PATRIZIA	IMPIEGATA
ALLOA CASALE ELENA	COMPONENTE DEL CONSIGLIO DELL'ORDINE
ALLORA ANDREA	COMPONENTE DEL CONSIGLIO DELL'ORDINE

COSTAMAGNA SABRINA	COMPONENTE DEL CONSIGLIO DELL'ORDINE
DE GIOVANNI PAOLO	COMPONENTE DEL CONSIGLIO DELL'ORDINE
DEGIOANNI DANILO	COMPONENTE DEL CONSIGLIO DELL'ORDINE
GALLI MASSIMILIANO	COMPONENTE DEL CONSIGLIO DELL'ORDINE
GERBOTTO ERICA	COMPONENTE DEL CONSIGLIO DELL'ORDINE
ISOARDI ELVIO	COMPONENTE DEL CONSIGLIO DELL'ORDINE
PAROLA MAURO GIOVANNI	COMPONENTE DEL CONSIGLIO DELL'ORDINE
RISSO GIOVANNI ANDREA	COMPONENTE DEL CONSIGLIO DELL'ORDINE
ROSSO CARLO	COMPONENTE DEL CONSIGLIO DELL'ORDINE
SAVORETTO CRISTIANO	COMPONENTE DEL CONSIGLIO DELL'ORDINE
TERZUOLO PIERLUIGI	COMPONENTE DEL CONSIGLIO DELL'ORDINE
ZACCARIA GIULIANO	COMPONENTE DEL CONSIGLIO DELL'ORDINE
SORDO SERGIO	PRESIDENTE DEL CONSIGLIO DELL'ORDINE
AIMASSO ROBERTO	COMPONTENTE DEL CONSIGLIO DI DISCIPLINA DELL'ORDINE
ARNAUDO MAURIZIO	COMPONTENTE DEL CONSIGLIO DI DISCIPLINA DELL'ORDINE
BREIDA ANGELO	COMPONTENTE DEL CONSIGLIO DI DISCIPLINA DELL'ORDINE
CASTELLETTO MASSIMILIANO	COMPONTENTE DEL CONSIGLIO DI DISCIPLINA DELL'ORDINE
FISSORE ANNA MARIA	COMPONTENTE DEL CONSIGLIO DI DISCIPLINA DELL'ORDINE
GREGORINI SANDRO	COMPONTENTE DEL CONSIGLIO DI DISCIPLINA DELL'ORDINE
LERDA LUIGI	COMPONTENTE DEL CONSIGLIO DI DISCIPLINA DELL'ORDINE
PELLEGRINO IVO	COMPONTENTE DEL CONSIGLIO DI DISCIPLINA DELL'ORDINE
QUARANTA FRANCESCO	COMPONTENTE DEL CONSIGLIO DI DISCIPLINA DELL'ORDINE
RUBERTO FRANCO	COMPONTENTE DEL CONSIGLIO DI DISCIPLINA DELL'ORDINE
SAGLIETTO FABRIZIO	COMPONTENTE DEL CONSIGLIO DI DISCIPLINA DELL'ORDINE
SPINA ROBERTO	COMPONTENTE DEL CONSIGLIO DI DISCIPLINA DELL'ORDINE
DE RENZIS ROBERTO	COMPONTENTE DEL CONSIGLIO DI DISCIPLINA DELL'ORDINE
GALLO FABRIZIO	COMPONTENTE DEL CONSIGLIO DI DISCIPLINA DELL'ORDINE
ROVERA ENNIO	COMPONTENTE DEL CONSIGLIO DI DISCIPLINA DELL'ORDINE

La nomina dei vari soggetti è a tempo indeterminato e decade per revoca/dimissioni o per decisione del Titolare del trattamento.

6. Trattamenti di dati affidati all'esterno – Responsabili del trattamento ex. Art. 28 Regolamento UE n. 2016/679

Il Titolare del trattamento ha deciso di affidare il trattamento di alcune classi di dati personali in tutto o in parte all'esterno della propria struttura, a società / studi / liberi professionisti appositamente nominati che hanno il compito di archiviarli, custodirli, utilizzarli nell'espletamento delle attività e dei servizi resi per conto dell'ORDINE DEGLI INGEGNERI. Queste sono tenute ad informare immediatamente il Titolare in caso di situazioni anomale o di emergenza.

I soggetti esterni, direttamente nominati responsabili del trattamento dei dati personali per conto del Titolare, risultano dalle copie allegate delle comunicazioni di designazione dei Responsabili esterni del trattamento.

Attività esternalizzata	Tipologia dati interessati	Soggetto esterno
Servizi di consulenza del lavoro ed elaborazione paghe	Dati personali e particolari di dipendenti	STUDIO ASS. DI CONSULENZA DEL LAVORO DI DE RENZIS ROBERTO E ABELLO ANNA MARIA
Servizi di consulenza amministrativa, gestione contabile e consulenza fiscale	Dati personali di clienti e fornitori	DOTT.ROVERA ENNIO
Consulenza GDPR 2016/679	Dati personali di dipendenti e fornitori	STUDIO QUALITY SRL
Medico competente	Dati personali e particolari dei dipendenti	DOTT.LUCIGNANI PAOLO
Gestione e manutenzione strumenti informatici	Tutti i dati personali su archivi elettronici	TECSIS S.R.L. BEGLIARDO ALBERTO TASK SERVIZI INFORMATICI DI TALLONE ALBERTO
DPO (Data Protection Officer)	Dati personali di dipendenti ed eventualmente di consiglieri	DOTT.GHIBAUDO SANDRO

7. Adempimenti nei confronti degli interessati

L'acquisizione dei dati personali degli interessati avviene previa consegna dell'informativa e, ove necessario, previa raccolta del consenso al trattamento dei dati personali ai sensi del Regolamento UE n. 2016/679.

Allegati:

- **MOD_INF_1 Informativa iscritti + consenso**
- **MOD_INF_2 Informativa fornitori – collaboratori**
- **MOD_INF_3 Informativa lavoratori**
- **MOD_INF_4 Informativa consiglieri + consenso**
- **MOD_INF_5 Informativa curriculum**
- **MOD_INF_6 Informativa sito**
- **MOD_INF 7_ Informativa per i destinatari dei messaggi di posta**

Elenco dei trattamenti effettuati dal Titolare

Rientrano nei trattamenti effettuati dal Titolare la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione dei dati.

I trattamenti saranno svolti in forma automatizzata e/o manuale, con modalità e strumenti volti a garantire la massima sicurezza e riservatezza, ad opera di soggetti di ciò appositamente autorizzati in ottemperanza a quanto previsto dall'art. 4 e dal principio di Accountability del G.D.P.R.

Tutti i dati personali in possesso del Titolare vengono trattati nel pieno rispetto dei principi normativi di necessità, stretta pertinenza, non eccedenza ed indispensabilità e possono essere riassunti come di seguito:

- Dati personali ed eventualmente particolari degli iscritti;
- dati personali del personale dipendente ovvero dei collaboratori, quali quelli necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi o richiesti ai fini fiscali e previdenziali o dati di natura bancaria;
- dati personali dei fornitori relativi alla reperibilità ed alla corrispondenza con gli stessi;
- dati personali di altri professionisti ai quali il Titolare affida incarichi o si rivolge per consulenze, quali quelli relativi alla reperibilità ed alla corrispondenza con gli stessi, nonché necessari per fini fiscali o di natura bancaria;
- dati particolari del personale dipendente, conseguenti all'instaurazione del rapporto di lavoro, ovvero inerenti i rapporti con gli enti previdenziali ed assistenziali, eventuali dati giudiziari.

I trattamenti effettuati avvengono nel rispetto dei diritti e delle libertà fondamentali delle persone, nonché della dignità dell'interessato e del principio di riservatezza. I dati sono trattati in modo lecito e secondo correttezza; vengono raccolti e registrati per scopi determinati, espliciti e legittimi ed

eventualmente comunicati ai soggetti autorizzati nella misura strettamente necessaria e non eccedente rispetto alle finalità per le quali sono stati raccolti.

Eventuali nuovi trattamenti di dati saranno analizzati e valutati prima del loro inizio, predisponendo le opportune misure di sicurezza per una corretta gestione.

Per delineare i trattamenti effettuati, internamente ed esternamente per conto del Titolare del trattamento, si fa esplicito rinvio al documento ***"MOD_Rev.00_Registro dei trattamenti"*** nel quale per ciascuna banca dati vengono riportate le seguenti indicazioni:

- Descrizione e finalità del trattamento
- Base giuridica del trattamento
- Categorie di interessati
- Natura dei dati
- Processo/unità organizzativa di riferimento
- Categorie di destinatari a cui i dati sono o possono essere comunicati/che concorrono al trattamento
- Paesi terzi o organizzazioni internazionali verso cui i dati possono essere trasferiti
- Garanzie adottate per il trasferimento internazionale
- Tempi di conservazione
- Modalità di conservazione
- Misure di sicurezza adottate
- Processi valutativi automatizzati e sistematici o profilazione.

7.1. Categorie di soggetti interessati al trattamento

I soggetti interessati dalle operazioni di trattamento poste in essere dal Titolare rientrano delle seguenti categorie:

- iscritti
- fornitori
- lavoratori
- collaboratori

8. Valutazione d'impatto sulla protezione dei dati personali

La valutazione d'impatto sulla protezione dei dati personali è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dai trattamenti di dati personali, valutando detti rischi e le misure di protezione e di sicurezza adottate per affrontarli. La valutazione d'impatto sulla protezione dei dati è uno strumento importante per la responsabilizzazione in quanto sostiene i titolari del trattamento non soltanto nel rispettare i requisiti del regolamento generale sulla protezione dei dati, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento. In altre parole, una valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità.

8.1. Modalità operative

Il rischio consiste nella probabilità che i dati personali oggetto del trattamento possano essere alterati (integrità), conosciuti da soggetti non legittimati (riservatezza), resi indisponibile a chi deve conoscerli (disponibilità), confutati nella sua validità formale (ripudio dell'origine o della ricezione) o smarriti. Ciascun trattamento deve essere esaminato alla luce della minaccia cui è soggetto e della vulnerabilità che ne può derivare. Per vulnerabilità di un trattamento si intende un elemento di debolezza dello stesso che rende possibile o persino probabile la minaccia.

L'attività di valutazione deve identificare:

- i trattamenti di dati personali effettuati dal Titolare del trattamento;
- le minacce insistenti su ciascun trattamento di dati personali, relative alla riservatezza, integrità e disponibilità degli stessi (es. furti, errori, intrusioni, ecc..);
- la gravità dei rischi in relazione alla rilevanza ed alla probabilità stimata dell'evento;
- le azioni adottate dall'Organizzazione;
- le azioni correttive da adottare per ridurre o eliminare i rischi.

8.2. Definizioni e terminologia

Vediamo di seguito le principali definizioni:

- rischio: combinazione della probabilità di un evento e della sua conseguenza;
- probabilità: frequenza teorica con la quale un evento si verifica;
- evento: verificarsi di un insieme di circostanze;
- conseguenza: esito di un evento;
- minaccia: possibile causa di evento indesiderato che può comportare danni ad un sistema o a una Organizzazione.

8.3. Calcolo dell'Indice di rischio

Le situazioni di pericolo identificate per la presente Organizzazione sono state riassunte in un foglio elettronico di calcolo denominato "***MOD_Rev.00_Valutazione d'impatto sulla protezione dei dati (DPIA – Data Protection Impact Assessment)***" (Figura 1)

TRATTAMENTO	FINALITÁ DEL TRATTAMENTO	NECESSITÁ - PROPORZIONALITÁ	RISCHIO	MINACCE	IMPATTO	MISURE PRESENTI IN AZIENDA	G	P	R	VALUTAZIONE	OPPORTUNITÁ DI MIGLIORAMENTO

Figura 1 – Esempio di schermata del MOD_Rev.00_Valutazione d'impatto sulla protezione dei dati (DPIA – Data Protection Impact Assessment)

Nel presente documento vengono riportati:

- **TIPOLOGIA DI TRATTAMENTO**
- **FINALITÁ DEL TRATTAMENTO**
- **VALUTAZIONE DELLA NECESSITÁ E PROPORZIONALITÁ DEL TRATTAMENTO**
- **RISCHIO POSSIBILE**
  - ACCESSO ILLEGITTIMO DI DATI
  - MODIFICA INDESIDERATA DI DATI
  - PERDITA DI DATI
- **MINACCE**
- **IMPATTO POSSIBILE SULLA PROTEZIONE DEI DATI**
  - ACCESSO ILLEGITTIMO DI DATI
  - MODIFICA INDESIDERATA DI DATI
  - PERDITA DI DATI
- **MISURE PRESENTI IN AZIENDA**
- **VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI**
  - PROBABILITA' DI ACCADIMENTO
  - GRAVITA' STIMATA
  - INDICE DI RISCHIO
- **OPPORTUNITÀ DI MIGLIORAMENTO**

L'analisi deve mettere in relazione i seguenti valori:

- **grado di probabilità di un danno** ovvero la probabilità che la protezione dei dati personali ha di subire un danno nel momento in cui la minaccia viene materialmente arrecata; esso è definito secondo i seguenti criteri:
  - è espresso tramite i valori "1", "2", "3" "4" (probabilità dell'effetto bassa, moderata, media e alta);
  - il grado di probabilità attribuito alle varie minacce tiene conto della presenza di misure di sicurezza già operanti.
- **grado di gravità della minaccia** ovvero l'entità del danno che verrebbe arrecato qualora la minaccia effettivamente si realizzasse; esso è definito secondo i seguenti criteri:
  - è espresso tramite i valori "1" conseguenze lievi (non pregiudicano la sicurezza dei dati personali in possesso), "2" conseguenze moderate (raramente possono pregiudicare la sicurezza dei dati personali in possesso), "3" conseguenze medie (possono pregiudicare il processo) "4" conseguenze elevate (pregiudicano la sicurezza dei dati personali in possesso);
  - il grado di gravità attribuito alle varie minacce tiene conto della presenza di misure di sicurezza già operanti.
- **indice di rischio-valore del danno** ovvero le possibili conseguenze negative dovute dal trattamento di dati personali. Tali conseguenze negative possono riguardare:
  - ACCESSO ILLEGITTIMO DI DATI
  - MODIFICA INDESIDERATA DI DATI
  - PERDITA DI DATI

Il calcolo dell'indice di rischio è effettuato per ogni minaccia individuata, moltiplicando il valore della gravità della minaccia stessa per l'indice di probabilità. Il valore massimo ottenibile è perciò 16, nella combinazione "peggiore" della terna. A fronte dell'indice di rischio calcolato per ciascuna minaccia, viene effettuata una valutazione delle più opportune contromisure adottabili.

R = G x P		
GRAVITA' (G)		
LIVELLO	**GIUDIZIO**	**DESCRIZIONE**
1	BASSO	Conseguenze lievi (non pregiudicano l'efficacia / l'efficienza del processo
2	MODERATO	Conseguenze Moderate (raramente possono pregiudicare il processo solo in alcuni casi.
3	MEDIO	Conseguenze moderate (possono pregiudicare il processo).
4	ALTO	Conseguenze elevate (pregiudicano l'efficacia / efficienza del processo).
PROBABILITA' (P)		
LIVELLO	**GIUDIZIO**	**DESCRIZIONE**
1	BASSO	Probabilità dell'effetto bassa.
2	MODERATO	Probabilità dell'effetto Moderata
3	MEDIO	Probabilità dell'effetto Media
4	ALTO	Probabilità dell'effetto Alta

MATRICE PER LA STIMA DEL RISCHIO

	Molto Improbabile (1)	Poco Probabile (2)	Probabile (3)	Molto Probabile (4)
Molto Grave (4)	Basso (4)	Medio (8)	Alto (12)	Alto (16)
Grave (3)	Basso (3)	Medio (6)	Medio (9)	Alto (12)
Moderato (2)	Basso (2)	Basso (4)	Medio (6)	Medio (8)
Lieve (1)	Basso (1)	Basso (2)	Basso (3)	Basso (4)

RISCHIO (R)		
LIVELLO	**GIUDIZIO**	**DESCRIZIONE**
1 - 4	BASSO	Non necessitano di controllo
5 - 9	MODERATO	Definire le azioni di controllo. Valutare un programma di miglioramento a breve termine (12 mesi)
10 - 16	ALTO	Occorre definire un progamma di miglioramento immediato oppure apportare variazioni al processo e ripetere valutazione

9. Procedure interne di sistema

Al fine di prevenire il verificarsi di eventuali minacce alla riservatezza, all'integrità e alla disponibilità dei dati personali posseduti, il Titolare del trattamento ha condotto un'analisi sulle misure di sicurezza richieste per il trattamento dei dati personali, adottando delle procedure interne e degli accorgimenti tecnico/organizzativi, cui i diversi autorizzati debbono attenersi nell'espletamento delle rispettive attività di trattamento, rispettando in modo preciso le indicazioni in esse impartite.

Le procedure interne adottate sono riportate nel ***"MOD_Rev.00_Procedure interne di sistema"*** e vengono di seguito sintetizzate:

- **PRO. 1.0.** ***Gestione strumenti elettronici di trattamento***
- **PRO. 2.0.** ***Gestione strumenti non elettronici di trattamento***
- **PRO. 3.0.** ***Istruzioni di Back up***
- **PRO. 4.0.** ***Gestione dei curricula***
- **PRO. 50.** ***Istruzioni operative in caso di violazione dei dati personali***
- **PRO. 6.0.** ***Esercizio dei diritti degli interessati***

10. Piano di formazione

Indicazione e gestione del piano di formazione degli autorizzati al trattamento dei dati personali

Il Titolare del trattamento ha previsto interventi di formazione del personale preposto alle operazioni di trattamento dei dati personali, sulla base dell'esperienza, delle conoscenze ed in funzione anche delle mansioni svolte secondo quanto disposto dall'art. 29 del Regolamento Europeo n. 2016/679.

L'attività di formazione è pianificata al momento dell'ingresso in servizio di nuovi autorizzati al trattamento, nonché in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

La formazione è necessaria per rendere edotti gli autorizzati al trattamento circa i seguenti aspetti:

- Introduzione generale sulle novità introdotte dal G.D.P.R.
- Principio di accountability o responsabilizzazione del Titolare del trattamento dei dati
- Differenza tra dati comuni e particolari
- I diritti degli interessati
- Organigramma privacy: le figure principali (Titolare del trattamento dei dati; incaricato al trattamento dei dati; responsabile esterno del trattamento)
- L'informativa
- Le misure di sicurezza adottate
- Aspetto sanzionatorio

I piani di formazione sono organizzati all'interno della struttura del Titolare, con presentazione a cura di società o di consulenti specializzati in materia.

Il Titolare del trattamento provvede a redigere il Piano di formazione del personale, come indicato nel ***"MOD_REGISTRO FORMAZIONE PRIVACY"***, ove viene data evidenza della partecipazione al percorso formativo.