MANUALE DI ADEGUAMENTO AL REG.UE 679/2016

«Manelli Impresa S.p.A.»

STUDIO CONSULENZA BARBONE

WWW.STUDIOCONSULENZABARBONE.IT

Manuale Privacy

redatto conformemente al DPMS 44001:2016
(Codice di condotta di proprietà della UNIQUALITY)

«Manelli Impresa S.p.A.»
«Via Clemente Cancelli, 11, 70043 Monopoli (BA)»
P.IVA «06746680724»
e-mail «frontoffice@manelli.eu» PEC «manelli@legalmail.it»

☒ **COPIA SOGGETTA A REV. N° «0» Ed. «2022»** Distribuita a [(1)]: il:«Data_Docs»	☐ **COPIA NON SOGGETTA A REV. N° «Revisione» Ed. «Edizione»** Distribuita a: il:«Data_Docs»

[(1)] Il destinatario è pregato di firmare digitalmente il presente manuale e metterlo in conservazione.

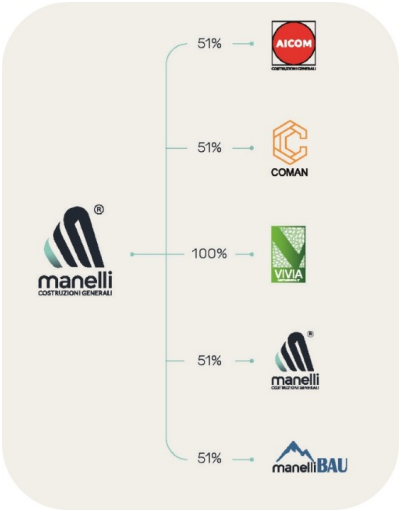
0.1 STATO DI REVISIONE DEL MANUALE

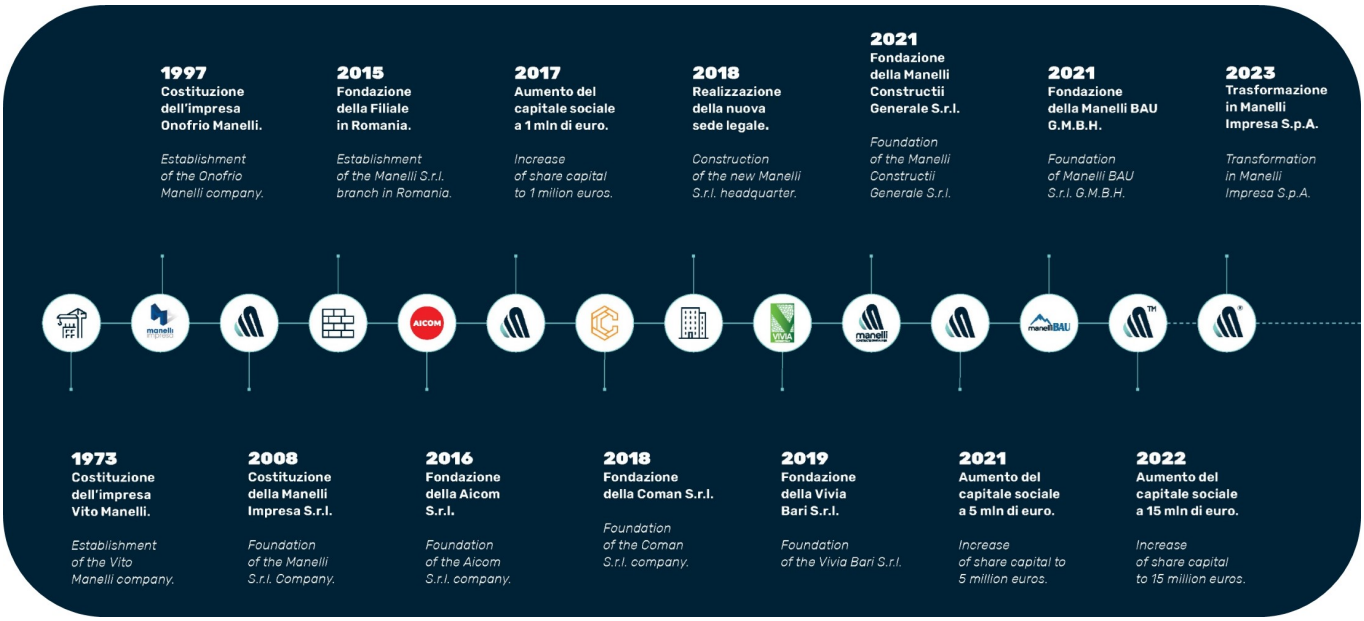
Revisione	Sezioni Modificate	Descrizione delle modifiche	Natura delle modifiche
«0»	0	PRIMA EMISSIONE	IMPLEMENTAZIONE DEL SISTEMA DI GESTIONE PER LA PRIVACY

0.2 DESCRIZIONE DELLA SOCIETÀ

0.2.1 Presentazione azienda

Con oltre 40 anni di esperienza, la **Manelli Impresa S.p.A.** emerge nel panorama nazionale e internazionale tra le più importanti aziende nel settore delle infrastrutture e delle costruzioni civili e industriali.
La società si basa su una economia aziendale equilibrata, su rapporti di correttezza e fiducia nei confronti dei clienti e sulla valorizzazione del lavoro e dei risultati raggiunti dai suoi dipendenti. L'arte della motivazione si basa sulla capacità di formulare strategie chiare, di garantire il flusso delle informazioni e di rendere più partecipi i dipendenti nelle sfide decisive. Sicurezza, affidabilità e crescita tecnologica, sono i nostri strumenti per soddisfare le richieste dei clienti e garantire loro i migliori risultati.
La **Manelli Impresa S.p.A.** crede nelle persone e nel loro ruolo all'interno della propria struttura organizzativa e si fonda sul rispetto etico e morale di chi, ogni giorno, lavora e collabora con la società, motivando lo spirito di squadra e un costante miglioramento individuale.
L'Impresa è dotata di un sistema di gestione integrato, sottoposto ad approfonditi audit periodici e certificato negli ambiti della qualità, dell'ambiente, della sicurezza e della responsabilità sociale d'impresa.





0.2.2 Descrizione delle attività svolte

«Manelli Impresa S.p.A.» si occupa di **"Progettazione, costruzione, manutenzione e ristrutturazione di edifici civili, opere infrastrutturali (opere ferroviarie); progettazione ed installazione di impianti tecnologici (elettrici, trasmissione dati, termofluidici caldo e freddo e idrico-sanitario)"**

0.3.3 Dati istituzionali e collocazione logistica

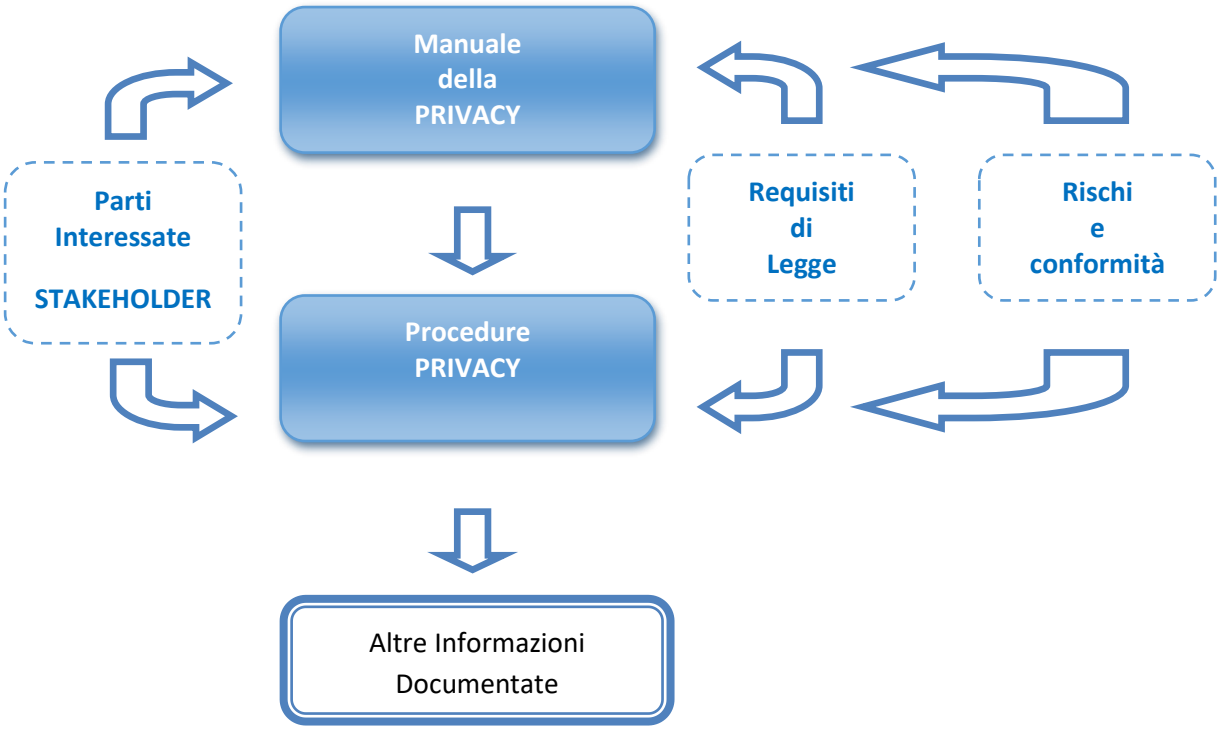
Ragione sociale	«Manelli Impresa S.p.A.»
Sede amministrativa	«Via Clemente Cancelli, 11, 70043 Monopoli»
Sede estera	«B-dul Regina Maria, Nr.1, Bloc P5B, Sc.1, Et.7, ap nr. 20/21 Sector 4, 040121 Bucuresti, Romania»
C.A.P.	«70043 »
città	«Monopoli»
Provincia	«BA»
P.IVA	«06746680724 »
Numero telefono	«080 747826»
Numero fax	«080 744379»
e-mail	«frontoffice@manelli.eu»
PEC	«manelli@legalmail.it»
Numero responsabili	
Numero operatori	510
Direzione generale	
Titolare del trattamento dei dati	«Onofrio Manelli»
Referente del trattamento dati	Dott. Ernesto Barbone

L1 SCOPO

Scopo di questo documento è mettere a disposizione uno strumento di analisi per poter delineare il quadro delle misure di sicurezza da dover applicare per garantire la sicurezza applicata alla gestione dei dati personali ed è stato redatto sulla base del disposto del regolamento UE 2016/679 allo scopo di:
<<PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI, NONCHÉ NORME RELATIVE ALLA LIBERA CIRCOLAZIONE DI TALI DATI. (art. 1 Reg. UE 2016/679)>>.
La società « Manelli Impresa S.p.A.» ha predisposto un Sistema di Gestione per la PRIVACY adatto alla propria organizzazione, alle attività svolte ed alle proprie specializzazioni, con l'intento di attuare e mantenere una efficace gestione dei dati nei propri processi, come stabilito dalla Politica per la PRIVACY e quanto previsto dal DPMS 44001:2016 (Codice di condotta di proprietà della UNIQUALITY) a cui la « Manelli Impresa S.p.A.» fa riferimento.
Il Sistema di Gestione per la PRIVACY viene definito nel presente Manuale della PRIVACY ed in Procedure ed Istruzioni ad esso correlate che insieme descrivono le prescrizioni e le modalità per il trattamento, il controllo obbligatorio del rispetto delle norme (requisiti) del DPMS 44001:2016 ed il monitoraggio dei dati attraverso un meccanismo che consente all'organismo di certificazione di verificarne la conformità, fatti salvi i compiti e poteri delle autorità di controllo competente.

L1.1 Architettura del Sistema di Gestione

L'architettura della documentazione del Sistema è presentata con lo schema che segue.



L.2 CAMPO DI APPLICAZIONE

Il Sistema di Gestione per la PRIVACY si applica a quelle attività che hanno influenza diretta o indiretta sui dati in ambito ai settori di intervento ed alle specializzazioni della Società.

Nello specifico il campo di applicazione è relativo a:

“Progettazione, costruzione, manutenzione e ristrutturazione di edifici civili, opere infrastrutturali (opere ferroviarie); progettazione ed installazione di impianti tecnologici (elettrici, trasmissione dati, termofluidici caldo e freddo e idrico-sanitario)”

Nel presente Manuale della PRIVACY vengono pertanto definiti o richiamati:

- La Politica per la PRIVACY della Società;
- La verifica della congruità al Reg. Eu 679:2016 ed al DPMS 44001:2016
- L’organizzazione gerarchica e funzionale della Società;
- Il campo di applicazione del Sistema di Gestione per la PRIVACY;
- La struttura documentale del Sistema di Gestione per la PRIVACY della Società ed in particolare le procedure predisposte per l’attuazione ed il funzionamento della stessa;
- I diversi processi che costituiscono il Sistema di Gestione per la PRIVACY della Società e le interazioni fra gli stessi;

- I compiti, le responsabilità e l'autorità attribuite alle diverse funzioni interne inserite nell'organigramma, nonché le interfacce fra le funzioni stesse e con le organizzazioni esterne coinvolte e interessate dal Sistema di Gestione per la PRIVACY della Società;
- I criteri ed i requisiti applicabili per le attività di controllo, assicurazione e gestione per la PRIVACY e per la pianificazione ed attuazione del miglioramento continuo del Sistema e dell'organizzazione della Società.

Il Manuale, unitamente alle procedure ed alle istruzioni ad esso correlate, alle attività di coinvolgimento, informazione, formazione e addestramento del personale, veicola ai Responsabili di Funzione della Società la volontà del titolare del trattamento dei dati di adottare, ottimizzare e migliorare continuamente il Sistema di Gestione per la PRIVACY.
La diffusione della Politica per la PRIVACY, a tutto il personale dipendente della società, rientra fra le competenze prioritarie dei Responsabili del trattamento ed avviene mediante la divulgazione ed il sostenimento dell'attuazione dei criteri e delle prescrizioni definite nel presente Manuale e nelle procedure ed Istruzioni ad esso correlate ed attraverso la trasposizione costante delle informazioni necessarie a fornire, ai diversi livelli dell'organizzazione della Società, la consapevolezza dell'importanza del rispetto dei requisiti specificati nel reg. Eu. 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

L.3 Principi applicabili al trattamento di dati personali

I dati personali devono essere:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato «liceità, correttezza e trasparenza»;

b) raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali («limitazione della finalità»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; (i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal regolamento 679/2016 a tutela dei diritti e delle libertà dell'interessato («limitazione della

conservazione»));

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

L.3.1 RIFERIMENTO DI CONFORMITÀ

Il Sistema di Gestione per la PRIVACY della società, come descritto nel presente Manuale, soddisfa i requisiti della seguente norma:

- DPMS 44001:2016 codice di condotta rev.00 del 25 maggio 2016 – Requisiti".
- Reg. Eu. 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

L.4 RIFERIMENTI PER LA REALIZZAZIONE

Costituiscono riferimento per il Sistema di Gestione per la PRIVACY descritto nel presente Manuale le seguenti norme:

- REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- Trattato sul funzionamento dell'Unione Europea (TFEU) introdotto dal trattato di Lisbona;
- Decisione quadro 2008/977/GAI;
- Carta dei diritti fondamentali dell'Unione Europea;
- La norma UNI CEI EN ISO/IEC 17065:2012 - Valutazione della conformità. Requisiti per organismi che certificano prodotti, processi e servizi;
- UNI CEI EN ISO/IEC 17021:2011 "Valutazione della conformità - Requisiti per gli organismi che forniscono audit e certificazione di sistemi di gestione";
- ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems – Requirements;
- Codice di condotta di proprietà della Uniquality rev. 00 del 25.05.2016.

L.5 TERMINI E DEFINIZIONI

Per quanto concerne i termini e le definizioni adottate nel presente Manuale della PRIVACY, si fa riferimento a:

DOCUMENTO COGENTE DI RIFERIMENTO:
REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

DATI PERSONALI: qualunque informazione relativa a persona fisica identificata o identificabile persona giuridica, ente od associazione, identificati o identificabili (interessato); anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

DATI SENSIBILI: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale degli eventuali altri diritti fondamentali garantiti dalla costituzione europea.

DATI GIUDIZIARI: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, 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 ai sensi degli articoli 60 e 61 del codice di procedura penale.

TRATTAMENTO: qualsiasi operazione o insieme di operazioni con o senza l'ausilio di processi automatizzati è applicata a dati personali o insiemi di dati personali come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento con la modifica, l'estrazione, la consultazione, l'uso della comunicazione mediante trasmissione diffusione o qualsiasi altra forma di messa a disposizione il raffronto o l'interconnessione la limitazione la cancellazione o la distruzione.

LIMITAZIONE DI TRATTAMENTO: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.

PROFILAZIONE: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relative alla 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 oggi spostamenti detta persona fisica.

PSEUDONIMIZZAZIONE: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

ARCHIVIO: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati indipendentemente dal fatto che per insieme sia centralizzato decentralizzato ho ripartito in modo funzionale e geografico.

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 dei 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.

RESPONSABILE TRATTAMENTO: la persona fisica o giuridica l'autorità pubblica il servizio o altro organismo tratta Dati personali per conto del titolare del trattamento.

RESPONSABILE DELLA PROTEZIONE DEI DATI "DATA PROTECTION OFFICER" (DPO): la persona fisica, designata dal titolare del trattamento e dal responsabile del trattamento, incaricata di informare e fornire consulenza al titolare e al responsabile nonché ai dipendenti. Ha la funzione di sorvegliare l'osservanza della normativa vigente e del codice di condotta, in ambito della protezione dati personali; fornire pareri sulla valutazione di impatto; cooperare; fungere da punto di contatto con l'autorità di controllo per tutte le questioni inerenti la protezione dei dati personali.

INTERESSATO: la persona fisica cui si riferiscono i dati personali.

DESTINATARIO: la persona fisica o giuridica l'autorità pubblica il servizio ho un altro organismo che riceve comunicazione di dati personali che si tratti o meno di terzi.

TERZO: la persona fisica o giuridica autorità pubblica il servizio o un altro organismo che non sia 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.

CONSENSO: la libera manifestazione di volontà dell'interessato con cui questi accetta espressamente un determinato trattamento dei suoi dati personali, del quale è stato preventivamente informato da chi ha un potere decisionale sul trattamento (vedi titolare). È sufficiente che il consenso sia "documentato" in forma scritta (ossia annotato, trascritto, riportato dal titolare o dal responsabile o da un incaricato del trattamento su un registro o un atto o un verbale), a meno che il trattamento riguardi dati "sensibili"; in questo caso occorre il consenso rilasciato per iscritto dall'interessato (ad es., con la sua sottoscrizione).

VIOLAZIONE DEI DATI PERSONALI (DATA BREACH): si intende la divulgazione (intenzionale o non), la distruzione, la perdita, la modifica o l'accesso non autorizzato ai dati trattati da aziende o pubbliche amministrazioni.

DATI RELATIVI ALLA SALUTE: i dati attinenti alla salute fisica o mentale di una persona, compreso la prestazione di servizi d'assistenza sanitaria che rivelano informazioni relative al suo stato di salute.

DATI GENETICI: 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 perché risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

DATI BIOMETRICI: Dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche fisiologiche o comportamentali della persona fisica che ne consentono confermano l'identificazione univoca quale immagine facciale o i dati dattiloscopici.

STABILIMENTO PRINCIPALE:

a) per quanto riguarda il 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 mezzi del trattamento dei dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'unione perché 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 responsabile del trattamento con stabilimenti in più di uno Stato membro il luogo in cui ha sede la sua amministrazione centrale nell'unione ho sei il responsabile del trattamento non ha un'amministrazione centrale dell'unione lo stabilimento del responsabile del trattamento nell'unione in cui sono condotte le principali attività di trattamento nel contesto delle attività dello stabilimento del responsabile del trattamento nella misura in cui tale responsabile È soggetto a obblighi specifici ai sensi del presente regolamento.

RAPPRESENTANTE: la persona fisica o giuridica stabilità dell'unione che desidero del titolare o dal Responsabile il trattamento dei dati per iscritto li rappresenta per quanto riguarda gli obblighi rispettivi a norma del documento cogente di riferimento.

IMPRESA: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica.

GRUPPO IMPRENDITORIALE: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate.

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.

AUTORITÀ DI CONTROLLO: l'autorità pubblica indipendente istituita da uno Stato membro.

AUTORITÀ DI CONTROLLO INTERESSATA: un'autorità di controllo interessato al trattamento di dati personali in quanto ha:

a) il titolare del trattamento poi responsabile del trattamento stabilito sul territorio dello Stato membro vitale autorità di controllo;
b) interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento;
c) un reclamo è stato proposto a tale autorità di controllo.

TRATTAMENTO TRANSFRONTALIERO:

a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure
b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro.

OBIEZIONE PERTINENTE E MOTIVATA: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione.

SERVIZIO DELLA SOCIETÀ DELL'INFORMAZIONE: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio (1).

ORGANIZZAZIONE INTERNAZIONALE: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più stati.

POLITICA PER LA PRIVACY: Obbiettivi ed indirizzi generali di un'organizzazione, relativi alla PRIVACY, espressi in modo formale dall'alta direzione.

ORGANIZZAZIONE: Insieme di persone e di mezzi, con definite responsabilità, autorità ed interrelazioni.

NON CONFORMITÀ: Mancato soddisfacimento di un requisito**.**

CORREZIONE: Azione per eliminare una non conformità rilevata**.**

AZIONE CORRETTIVA: Azione per eliminare la causa di una non conformità rilevata, o altre situazioni indesiderabili rilevate**.**

AZIONE PREVENTIVA: Azione per eliminare la causa di una non conformità potenziale o di altre situazioni potenziali indesiderabili**.**

PROCEDURA: Modo specifico per svolgere un'attività o un processo**.**

DOCUMENTO: Informazioni con il loro mezzo di supporto**.**

SPECIFICA: Documento che stabilisce i requisiti**.**

REGISTRAZIONE: Documento che riporta i risultati o fornisce evidenza delle attività svolte**.**

EVIDENZA OGGETTIVA: Dati che supportano l'esistenza o la veridicità di qualcosa.

ISPEZIONE, CONTROLLO E COLLAUDO: Valutazione della conformità mediante osservazioni e giudizi associati, quando opportuno, a misurazioni, prove e verifiche.

VERIFICA: Conferma, sostenuta da evidenza oggettive, del soddisfacimento di requisiti specificati.

RIESAME: Attività effettuata per riscontrare l'idoneità, l'adeguatezza e l'efficacia di qualcosa a conseguire gli obbiettivi stabiliti**.**

AUDIT: processo tematico indipendente È documentato vero che nell'evidenza dell'audit E valutarle con obiettività affidabilità quali misure dell'audit sono stati soddisfatti.

L.6 ABBREVIAZIONI E SIGLE

ORGANIGRAMMA	
RL	Rappresentante legale
TTD	Titolare trattamento Dati
RTD	Responsabile trattamento dati
DPO	Data Protection Officer
RP	Responsabile Privacy

TERMINOLOGIA	
MP	Manuale PRIVACY
NC	Non Conformità
AC	Azioni correttive
AP	Azioni preventive

Qualsiasi altro/a termine/abbreviazione, definizione o sigla particolare, riportata nel contesto del presente Manuale della PRIVACY, per cliente si renda necessaria una spiegazione, al fine di permetterne la comprensione del significato, viene definita e descritta direttamente nella sezione o nel capitolo di competenza.

P6 AMBIENTE IN CUI OPERA L'ENTITA'

P6.1 L'AMBIENTE IN CUI SI SVOLGE L'ATTIVITA' PER LA PROTEZIONE DEI DATI

Ambiente in cui opera

I trattamenti connessi ai servizi offerti hanno luogo presso la predetta sede e sono curati solo da personale tecnico incaricato del trattamento, oppure da eventuali incaricati di occasionali operazioni di manutenzione adeguatamente formati sulla tutela della riservatezza.
La società analizza l'ambiente in cui opera e individua i fattori che possono influenzare la propria capacità di mettere in atto un'adeguata politica per la protezione dei dati personali.
La società opera nel settore edile.

I trattamenti di dati personali che vengono effettuati sono i seguenti:

□ raccolta
□ registrazione
□ organizzazione
□ conservazione
□ consultazione
□ elaborazione
□ modificazione
□ selezione
□ estrazione
□ raffronto
□ utilizzo
□ interconnessione
□ blocco
□ comunicazione
□ diffusione
□ cancellazione
□ distruzione

L'analisi della struttura della società e delle relative aree di trattamento è fondamentale per poter individuare il flusso dei dati elaborati e definire i soggetti coinvolti nel trattamento.
Le operazioni di trattamento dei dati personali gestiti dalla società sono svolte dal responsabile del trattamento indipendentemente dal fatto che le lavorazioni di trattamento in tutto in parte viene effettuato o meno in uno degli stati membri dell'unione.
Idealmente le attività di gestione dei dati possono essere suddivise in tre macro- aree, in funzione del fatto che il loro fine sia il reperimento delle informazioni, il trattamento interno delle informazioni o il loro uso nei rapporti con l'esterno.

1. <u>Il Reperimento delle informazioni</u>
   La raccolta dei dati avviene principalmente tramite colloqui diretti con gli interessati. I clienti (o i dipendenti) che si rivolgono alla società mettono a disposizione tutta la relativa documentazione per rendere possibile l'esecuzione di quanto previsto in contratto.

2. <u>Il Trattamento Interno delle Informazioni</u>
   Si raggruppano in tale macro-tipologia le varie operazioni poste in essere durante la raccolta delle informazioni, per organizzarle e renderle agevolmente usufruibili per gli utilizzatori autorizzati. Esse sono:

   - La registrazione dei dati, cioè il loro inserimento in supporti informatici e/o cartacei al fine di renderli disponibili per i successivi trattamenti;
   - L'organizzazione dei dati in senso stretto, cioè operazioni che ne favoriscono la fruibilità attraverso l'aggregazione o la disaggregazione, l'accorpamento, la catalogazione, ecc.;
   - La elaborazione ed in particolare la selezione, l'estrazione ed il raffronto, vale a dire quelle operazioni che attribuiscono significatività ai dati in relazione allo scopo per il quale essi sono stati raccolti;
   - La modificazione dei dati registrati, in relazione a variazioni o a nuove acquisizioni;
   - La conservazione dei dati per tutto il tempo necessario per gli scopi per i quali sono stati raccolti o successivamente trattati;

3. L'uso Delle Informazioni Nei Rapporti Con L'esterno
   L'utilizzo delle informazioni avviene instaurando un rapporto o un contatto con la persona fisica o giuridica sul conto della quale si sono raccolte le informazioni.

4. Finalità Del Trattamento
   I dati personali potranno essere trattati per le seguenti finalità ovvero nell'ambito dei processi di vendita dei servizi/prodotti e nelle attività sottoindicate.
   Elenco non esaustivo dei possibili servizi:
   - Informazione scritta;
   - Richiesta Preventivo;
   - Accettazione preventivo;
   - Reclamo;
   - Rettifica fattura;
   - Servizi indicati all'interno dei contratti di servizio con i committenti;
   - Consulenza commerciale;
   - Commercializzazione all'ingrosso di materiali, macchine, pezzi di ricambio, attrezzature;
   - Attività connesse alla gestione delle Risorse Umane della società.

In tali processi/servizi vengono raccolti i dati personali (come ad esempio, dati anagrafici, indirizzo di posta elettronica, indirizzo postale, carta di credito e coordinate bancarie, numero di telefono, codici fiscali, numero identificativi univoci legati alla fornitura dei servizi) per l'espletamento delle attività necessarie o comunque connesse alla conclusione, gestione ed esecuzione delle attività, o per l'esecuzione degli obblighi previsti dalla legge, da un regolamento o dalla normativa, nazionale e/o comunitaria, nonché da disposizioni impartite da autorità a ciò legittimate dalla legge o da organi di vigilanza e controllo.
La società per la tipologia di servizi svolti ha determinato quali sono le parti interessate (stakeholders) importanti per le attività di trattamento dei dati e precisamente:

- Associazione dei consumatori;
- Associazioni di categoria.

Influenze esterne e interne

La società comunica parte dei dati trattati ad alcuni soggetti interni ed esterni con i quali collabora stabilmente ai fini dell'erogazione dei propri servizi:

- Clienti;
- Fornitori di Beni e Servizi;
- Consulenti Fiscali;
- Personale Interno (Dipendenti, Collaboratori, Apprendisti);
- Collaboratori Esterni;
- Consulenti diversi;
- Istituti Bancari e Assicurativi.

I dati sono trattati dal titolare del trattamento e dal responsabile del trattamento. Gli incarichi sono attribuiti in modo formale utilizzando appositi incarichi o contratti a cui si fa riferimento all'informativa ed al consenso secondo quanto previsto dal reg. Eu 679/2016.

I dati possono essere soggetti a influenze interne o esterne e molto diversificati fra loro:

- **Fattori esterni:** possono essere di natura legale, tecnologica, concorrenziale, di mercato, culturale o socio-economica ed essere a livello internazionale, nazionale, regionale o locale.

- **Fattori interni:** possono riferirsi a valori, cultura, conoscenza e performance proprie dell'organizzazione.

P6.2 COSA INTERESSA AGLI STAKEHOLDERS

Esigenze ed aspettative delle parti interessate

La società determina quali sono i suoi stakeholder importanti per le attività di trattamento dei dati e le esigenze specifiche.

Associazioni, consumatori, organismi rappresentanti le categorie di titolari del trattamento o dei responsabili, associazioni professionali dei DPO, associazioni professionali degli Auditor Privacy, altro.

Pertanto, **Manelli Impresa S.p.A.** ha:

- identificato le parti interessate rilevanti per il sistema gestione per la PRIVACY:
  - clienti;
  - dipendenti;
  - collaboratori;
  - fornitori.
- i requisiti di tali parti interessate che sono rilevanti per il sistema gestione PRIVACY:
  - dipendenti (assunzione; idoneità; busta paga; ecc…);
  - clienti (contratti; comunicazioni; promozioni; fatturazione; ecc..);
  - fornitori (contratti; ordini; fatturazione; comunicazioni; ecc..).
- quali di queste esigenze e aspettative diventano suoi obblighi di conformità:
  - dipendenti (dati anagrafici; dati sanitari per idoneità;
  - clienti (dati anagrafici per fini fiscali);
  - l'organizzazione monitora e riesamina le informazioni che riguardano tali parti interessate e i loro requisiti rilevanti.

P6.3 IL PERIMETRO DEL SISTEMA GESTIONE DELLA PROTEZIONE DATI

Di seguito vengono elencati gli ambienti (ciò che influenza esternamente e interamente il trattamento) gestiti all'interno del sistema di gestione per la PRIVACY, cosa interessa agli Stakholders, i prodotti e attività e servizi realizzati e le interfacce interne ed esterne.

Stakholders sono considerati tutte le figure che hanno fornito i propri dati per le finalità scopo della società e tutte le figure professionali coinvolte nella gestione degli stessi per fini amministrativi, legali e commerciali.

Ambiente	Attività	Primario o di Supporto	Interno o Esterno	Interfacce interne ed esterne
Pc	Gestione Clienti	P	I	Gestione fornitori / Sviluppo attrezzature / Manutenzione/ commercialista
Server	Gestione Fornitori	P	I	Lavorazioni esterne / Produzione / Gestione magazzino/ commercialista
Archivio cartaceo	Lavorazioni esterne	P	E	Gestione magazzino / Gestione Fornitori/ commercialista
Portatili	Sviluppo	P	I	Gestione Clienti / Produzione/
Archivio cloud	Produzione	P	I	Gestione Clienti / Gestione magazzino/ enti pubblici
PC esterni	Manutenzione	S	I	Produzione
	Gestione magazzino	P	I	Gestione Fornitori / Produzione / Lavorazioni esterne
	Gestione personale	S	I	Tutti
	Amministrazione	S	I/E	Tutti
	Gestione Sistema PRIVACY	S	I	Tutti
	Sistema Informatico	S	I	Tutti

Sulla base di tale analisi si definisce il perimetro.

P6.4 IL SISTEMA DI GESTIONE DELLA PROTEZIONE DEI DATI

Scopo del presente manuale e quello di descrivere la conformità ai requisiti previsti dal DPMS 44001:2016 (Codice di condotta di proprietà della UNIQUALITY)

La Società:

1) mantiene informazioni documentate per il supporto ed il funzionamento dei propri processi sui dati personali;
2) conserva le informazioni documentate affinché si possa avere fiducia nel fatto che i processi siano condotti come pianificati;
3) aggiorna il suo profilo di rischio rispetto ai dati personali trattati.

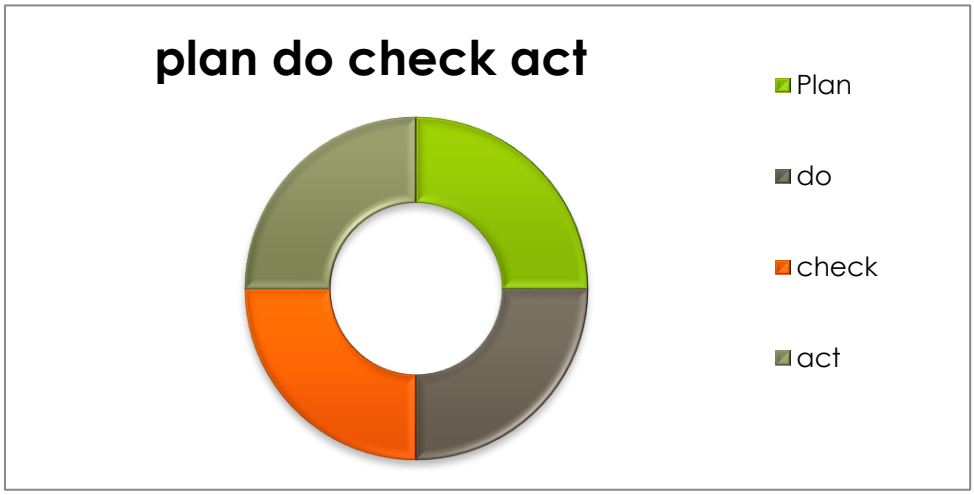
Il presente manuale si basa sulla metodologia del **PCDA** Plan-do-check-act (pianificare, attuare, verificare, agire):

Plan: Stabilire target e sequenze di attività per fornire risultati conformi alla politica per la produzione di dati dell'entità.

Do: Attuare le attività per la protezione dei dati.

Check: Controllare le attività per la protezione dei dati rispetto alle politiche della protezione dei dati ai target ai requisiti cogenti riportando opportune informazioni documentate su quanto ottenuto.

Act: Attività e azioni a seguire il progresso continuo del modello DPMS.



P7 IL TITOLARE DEL TRATTAMENTO

P7.1 IL DOVERE DEL TITOLARE DEL TRATTAMENTO DEI DATI

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al reg. Eu. 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali. Dette misure sono riesaminate e aggiornate annualmente.

Il Sig. Onofrio Manelli, titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita dei sistemi, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza il consenso della persona fisica interessata.

La Società:

a. Assicura che la politica della società verso la protezione dei dati sia definita e congruente con la

linea strategica della società, con l'ambiente in cui opera e con il profilo di rischio dell'entità stessa;

b. Mette a disposizione risorse umane, tecniche e finanziarie necessarie al sistema di gestione della protezione dei dati personali per operare in modo efficace;

c. Adotta misure appropriate per fornire all'interessato tutte le informazioni qualora i dati personali siano raccolti presso l'interessato e qualora i dati personali siano stati ottenuti presso terzi;

d. Effettua le comunicazioni relative al diritto di accesso dell'interessato, alla rettifica e cancellazione, al diritto di opposizione ed al processo decisionale automatizzato relativo alle persone fisiche comprese le informazioni relative all'attività di profilazione e la comunicazione di una violazione dei dati personali all'interessato. Dette informazioni sono documentate nelle informative;

e. Agevola l'esercizio dei diritti dell'interessato, alla rettifica e cancellazione, al diritto di opposizione ed al processo decisionale automatizzato relativo alle persone fisiche;

f. Fornisce all'interessato le informazioni relative all'azione intrapresa riguardo una richiesta riferita al diritto di accesso dell'interessato, alla rettifica, cancellazione, al diritto di opposizione ed al processo decisionale automatizzato relativo alle persone fisiche, senza ingiustificato ritardo e, comunque al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi se necessario tenuto conto della complessità del numero delle richieste. Il titolare del trattamento in forma all'interessato di tale proroga e dei motivi del ritardo entro un mese dal ricevimento della richiesta se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite ove possibile con mezzi elettronici salvo diversa indicazione dell'interessato.

P7.2 POLITICA PER LA PROTEZIONE DEI DATI

La Direzione Aziendale ha definito la Politica della PRIVACY attraverso il documento denominato "POLITICA PER LA PRIVACY" ed assicura che tale Politica sia adeguata all'ambiente ed alla finalità del trattamento e comunicata e compresa all'interno della Società attraverso le seguenti azioni:

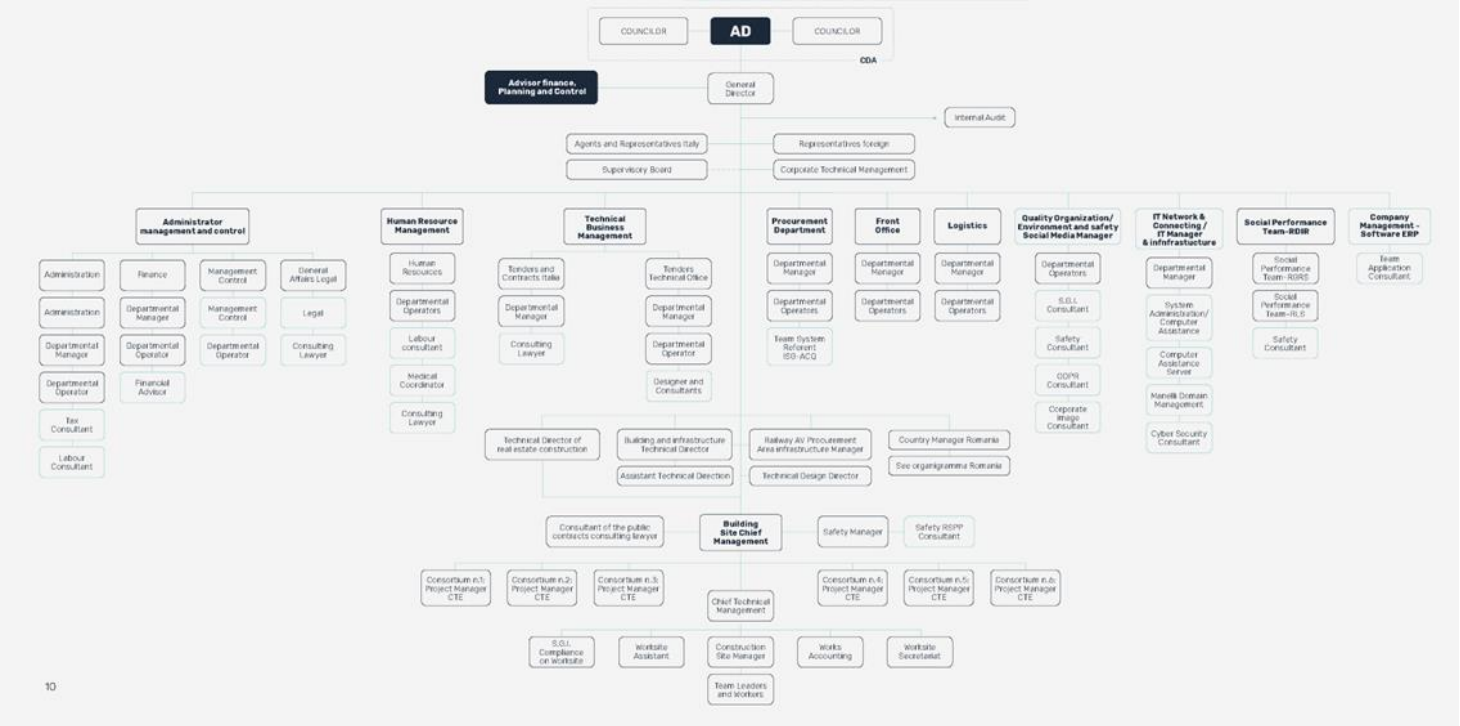
- Formazione diretta in fase di consegna del consenso;
- Riunione annuale con tutto il personale per illustrare la Politica della PRIVACY;
- Esposizione della Politica della PRIVACY in punti visibili della società;
- Comunicata agli stakeholders ritenuti importanti per il trattamento dei dati.

La Politica della PRIVACY definita viene costantemente aggiornata in relazione ai mutamenti dell'ambiente e riesaminata ogni anno, in occasione delle attività di Riesame del Sistema di Gestione per la PRIVACY, al fine di verificarne l'adeguatezza.

P7.3 Organizzazione

Organizzazione societaria

La struttura organizzativa della Società è rappresentata dall'Organigramma funzionale riportato di seguito nel presente Manuale. I requisiti minimi, le principali mansioni e le responsabilità delle Funzioni che dirigono, eseguono e controllano le diverse attività in ambito ai processi del Sistema di Gestione per la PRIVACY della società in relazione ai corrispondenti requisiti applicabili della norma di riferimento sono definiti di seguito:



Responsabilità ed autorità delle funzioni interne

I compiti, le responsabilità e l'autorità delle diverse funzioni inserite nella struttura organizzativa della società sono stati assegnati dal titolare del trattamento a mezzo di adeguate deleghe.

Organigramma nominativo della società

L'Organigramma nominativo della società, necessario ad identificare le persone a cui sono state attribuite le funzioni indicate nei paragrafi precedenti, viene riportato in un documento, separato dal presente Manuale, emesso e mantenuto costantemente aggiornato dal Responsabile PRIVACY ed approvato dal titolare del trattamento dati. Tale documento viene distribuito in copia a tutti i responsabili di funzione della società e l'originale viene archiviato e conservato, evidenza dell'avvenuta distribuzione è la firma dello stesso da tutti gli addetti.

Contitolari del trattamento

Quando due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di acceso ai dati personali. Tale accordo deve essere messo a disposizione per gli interessati. Indipendentemente dalle disposizioni dell'accordo, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento.

Responsabili del trattamento

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

Autorizzazione scritta

Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

Contratto o atto giuridico

I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale,

salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure richieste ai sensi dell'articolo 32;

d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;

e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;

f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;

h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato (es Auditor Privacy).

Il Responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

P.8 PLAN

P8.1 RISK MANAGEMENT

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire ed essere in grado di mostrare, che il trattamento è effettuato conformemente al documento cogente di riferimento tenuto conto della natura del perimetro dell'ambiente E delle finalità del trattamento nonché dei rischi aventi probabilità e gravità diverse per diritti e le libertà delle persone fisiche fornendo assicurazione che il sistema di gestione della protezione dei dati sia efficace nel conseguire risultati attesi prevedendo o riducendo gli effetti indesiderati. La società deve pianificare azioni adeguate per affrontare i rischi per definire criteri di accettazione e le modalità di trattamento e per valutare l'efficacia.

La società mantiene informazioni documentate sull'analisi di rischio. Detta analisi viene revisionata periodicamente e mantenuta aggiornata a seguito di modifiche del trattamento.

La stima del rischio complessivo, che grava su un determinato trattamento di dati, è il risultato della combinazione di due tipi di rischi:

- quelli insiti nella tipologia dei dati trattati, che dipendono dalla loro appetibilità per i soggetti interni ed esterni all'organizzazione, nonché dalla loro pericolosità per la privacy dei soggetti cui essi si riferiscono;
- quelli legati alle caratteristiche degli strumenti utilizzati per procedere al trattamento dei dati.

Nelle tabelle sottostanti si procede alla stima del rischio, che dipende dalla Tipologia dei dati trattati dal Titolare combinando il fattore della loro appetibilità per i terzi, con quello che esprime la loro pericolosità per la privacy del soggetto cui i dati si riferiscono:

1 - Bassa	È applicabile ad almeno uno dei seguenti: ▪ la minaccia si può verificare con frequenza inferiore rispetto a quanto riportato dalle ricerche più note; ▪ in caso di attacco deliberato, i dati sono poco appetibili e l'immagine aziendale non è compromessa e pertanto i tentativi di attacco o non sono iniziati o sono condotti da malintenzionati scarsamente preparati da un punto di vista tecnico e con scarse risorse a disposizione; ▪ in caso di attacco non deliberato, l'ambito è poco complesso e quindi è difficile commettere errori; ▪ in caso di eventi naturali, gli studi dimostrano che la minaccia può verificarsi molto raramente.
2 - Media	È applicabile ad almeno uno dei seguenti: ▪ la minaccia si può verificare più frequentemente rispetto a quanto riportato dalle ricerche più note; ▪ in caso di attacco deliberato, i dati sono poco appetibili e l'immagine aziendale non è compromessa e quindi può essere condotto da malintenzionati non particolarmente motivati, mediamente preparati da un punto di vista tecnico e con scarse risorse a disposizione; o in alternativa, gli studi confermano che tentativi di attacco sono comunque rari; ▪ in caso di attacco non deliberato, l'ambito è mediamente complesso e quindi possono essere commessi errori; ▪ in caso di eventi naturali, gli studi dimostrano che la minaccia può verificarsi nella media dei casi studiati.

3 - Alta	È applicabile ad almeno uno dei seguenti: la minaccia si può verificare più frequentemente rispetto a quanto riportato dalle ricerche più note; ▪ in caso di attacco deliberato, i dati sono appetibili o l'immagine aziendale è compromessa, e quindi può essere condotto da malintenzionati molto motivati, tecnicamente preparati e con ingenti risorse a disposizione; o in alternativa, gli studi confermano che tentativi di attacco sono comunque portati molto di frequente; ▪ in caso di attacco non deliberato, l'ambito è di elevata complessità (per esempio per molteplicità di sedi, tipologie di sistemi informatici, utenti interni e/o esterni) e quindi è facile siano commessi errori; ▪ in caso di eventi naturali, gli studi dimostrano che la minaccia si verifica quasi certamente.

La valutazione complessiva del livello di rischio prende in considerazione anche eventuali accadimenti potenzialmente occorsi in periodi precedenti nonché

Possibilità: è la natura stessa dell'evento se contemplabile nella mia organizzazione o meno il parametro è si / no;

Probabilità: siamo nell'ambito della valutazione del valore di accadimento dell'evento, la casistica statistica di accadimento;

Accaduto in passato: elemento di indicazione di gravità dell'evento in quanto già in precedenza verificatosi.

L'analisi dei dati per la valutazione del rischio potrà fornire la seguente espressione dei dati:

Livello di rischio
Basso < 19
20 < Medio < 40
Alto > 40

Dato rilevato come valore in uscita dall'analisi del rischio effettuata sulla società è pari a:

BASSO

Misure tecniche e organizzative

Il titolare il trattamento ed il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza commisurato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudomizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi del trattamento;
c) la capacità di ripristinare la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Il tutto valutato con spiccata valorizzazione della riservatezza, integrità e disponibilità del dato, compreso il piano di valutazione e controllo attuato ad ogni audit della privacy o alla verifica annuale dell'analisi del rischio.

Nel valutare l'adeguato livello di sicurezza si è tenuto conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione dalla perdita dalla modifica dalla divulgazione non autorizzata o dall'accesso in modo accidentale o illegale ai dati personali trasmessi, conservati o comunque trattati.

Per la società «**Manelli Impresa S.p.A.**», "Risk-based thinking" significa considerare il rischio qualitativamente e dipendente dal contesto, dall'ambiente, dal perimetro e dalle finalità dal trattamento dei dati della società.

Valutazione d'impatto sulla protezione dei dati

Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.
Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.
La valutazione d'impatto sulla protezione dei dati è richiesta in particolare nei casi seguenti:

1. una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
2. il trattamento, su larga scala, di categorie particolari di dati personali che rilevino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o fisiologiche o l'appartenenza sindacale, nonché trattare dati genetici, biometrici, intesi a identificare in modo univoco una persona fisica dati relativi a condanne penali o reati;
3. la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

La valutazione d'impatto sulla protezione dei dati contiene una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità, una valutazione dei rischi per i diritti e le libertà degli interessati.
Le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al documento cogente di riferimento tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.
L'identificazione del responsabile del trattamento se esplicitamente delegato dal titolare del trattamento.

Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento

Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.

P8.2 TARGETS PER LA PROTEZIONE DEI DATI

L' azienda ha stabilito i targets per la protezione dei dati con la politica in materia di protezione dei dati quantificabili, pertinenti ai trattamenti relativi alle attività ed ai trattamenti della società.
Detti targets sono comunicati e compresi all'interno della società e rivisti periodicamente quando necessario.

P8.3 CAMBIAMENTI

Se la società determina la necessità di cambiamento delle attività e/o dei trattamenti e le conseguenti variazioni al sistema di gestione della protezione dei dati adottato deve riesaminare l'analisi dei rischi valutare l'integrità del sistema di gestione, la disponibilità di risorse in termini economici, finanziari e del personale e valutare un eventuale ridistribuzione delle responsabilità.

D.9 SOSTEGNO ALL'OPERATIVITA'

D9.1 RISORSE E MEZZI PER LA PROTEZIONE DEI DATI

Il titolare del trattamento stabilisce e fornisce risorse umane, tecniche e finanziarie, nonché i locali e le infrastrutture necessari per l'effettivo adempimento dei suoi compiti e per l'esercizio dei propri poteri.

Per garantire che siano rispettate le prescrizioni del regolamento 679/2016 e del DPMS 44001/2016, riguardo al trattamento che il responsabile del trattamento deve eseguire per conto del titolare del trattamento, quando affida delle attività di trattamento a un responsabile del trattamento il titolare del trattamento dovrebbe ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto

misure tecniche e organizzative che soddisfino i requisiti del documento cogente, anche per la sicurezza del trattamento.

Il titolare del trattamento che designi sia per autonoma scelta che per obbligo normativo un DPO deve mettere a disposizione di queste risorse necessarie per assolvere ai compiti previsti dal documento cogente di riferimento.

D9.2 COMPETENZA NELLA MANSIONE PER IL TRATTAMENTO DEI DATI

Il titolare del trattamento determina le competenze nella mansione necessarie all'efficace gestione del sistema per la protezione dei dati, e deve assicurarsi che le risorse umane coinvolte nella gestione dei dati siano competenti nella mansione.
La competenza viene resa disponibile e documentata sulla base di un apprendimento formale (es. Titolo di studio), apprendimento non formale (corsi di formazione) apprendimento informale (esperienza lavorativa).

Il DPO è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti.

Il titolare del trattamento e il responsabile del trattamento sostengono il DPO nell'esecuzione dei suoi compiti fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base ad un contratto di servizi.

D9.3 COGNIZIONE SUL TRATTAMENTO DEI DATI

l titolare del trattamento anche attraverso le attività del DPO quando presente promuove la cognizione sul corretto trattamento dei dati ai responsabili del trattamento ed a tutto il personale della società riguardo agli obblighi imposti loro dal reg. eu 679/2016. In particolare, le persone della società devono aver cognizione della Politica sulla Privacy di come per le loro attività contribuiscano al corretto trattamento dei dati e di cosa accadrebbe nel caso di violazione dei requisiti indicati nel reg.eu 679/2016

Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.
Azioni: implementato sistema di alert che preveda l'invio di e-mail al titolare e responsabile alla variazione dei dati presenti nel sistema.

D9.4 COMUNICAZIONI ESTERNE ED INTERNE PER LA PROTEZIONE DEI DATI

Il titolare del trattamento determina quali comunicazioni siano pertinenti per il corretto funzionamento del sistema di gestione per la protezione dei dati.
Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni e le

comunicazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.
Una comunicazione efficace è essenziale per il presente sistema di gestione, il titolare «Onofrio Manelli» garantisce che siano presenti meccanismi che la facilitino.

Le modifiche del sistema di gestione per la PRIVACY vengono comunicati alle parti interessate:

- Interne: divulgazione attraverso comunicazioni esposte in bacheca aziendale;
- Esterne: divulgazione attraverso comunicazioni scritte tramite posta elettronica solo nel caso di variazioni significative per la parte interessata.

Azioni: implementato sistema di alert che preveda l'invio di e-mail al titolare e responsabile alla variazione dei dati presenti nel sistema.

D9.5 INFORMAZIONI DOCUMENTATE PER LA PROTEZIONE DEI DATI

La documentazione del Sistema di Gestione per la PRIVACY costituisce lo strumento attivo che ne formalizza la struttura, attraverso la raccolta organizzata ed aggiornata dei Documenti che ne regolano la gestione ed il funzionamento, includendo anche i Documenti relativi ai rapporti con i Fornitori e i Clienti in materia di Gestione per la PRIVACY.
La documentazione del Sistema di Gestione per la PRIVACY include:

Documenti di origine interna:

- Il documento relativo alla Politica e gli Obiettivi della PRIVACY stabiliti dalla Direzione Aziendale ed il RQ;
- Il Manuale della PRIVACY;
- Le Procedure, quelle aggiuntive che il Responsabile del trattamento ha ritenuto utile predisporre per definire le modalità di gestione dei processi del Sistema di Gestione per la PRIVACY, nonché tutti gli altri documenti necessari per garantirne un controllo sui dati;
- Istruzioni;
- Registrazioni (informativa, report di audit, consenso, nomine, deleghe, elenco documenti, registro dei trattamenti, registro azioni di miglioramento, riesame annuale, comunicazioni, comunicazione data breach,..).

Documenti di origine esterna:

- Leggi, decreti e regolamenti applicabili;
- Norme tecniche e di sistema;
- Documentazione tecnica fornita dai clienti.

Pensare ad una comunicazione periodica con le informazioni sulla privacy in termini di modifiche e aggiornamenti legislativi.

9.5.2 Creazione e aggiornamento delle informazioni documentate

La Società ha predisposto una procedura documentata al fine di stabilire modalità e responsabilità per la gestione dei documenti del Sistema di Gestione per la PRIVACY, incluse le informazioni documentate della PRIVACY.
La procedura documentata definisce:

- le funzioni responsabili, in fase di prima emissione, di redigere, verificare, ed approvare i documenti;
- il contenuto e le modalità per l'identificazione di ogni documento del SG Privacy;
- le modalità per revisionare/modificare i documenti (funzioni responsabili di aggiornare, verificare ed approvare i documenti revisionati e modalità per identificare le modifiche e lo stato di revisione dei documenti);
- le modalità di distribuzione, archiviazione e conservazione.

9.5. 3 Controllo delle informazioni documentate

Le informazioni documentate della PRIVACY sono conservate dalla società per dimostrare il conseguimento dei livelli di PRIVACY previsti e l'efficacia del Sistema attuato.
I documenti di registrazione della PRIVACY costituiscono un'importante fonte d'informazione per il titolare Privacy nella valutazione dell'andamento della PRIVACY e per la Direzione, allo scopo di poter verificare il livello di conformità delle attività e di attuazione delle politiche.
Tutte le informazioni documentate sono sempre leggibili, facilmente identificabili e rintracciabili.

D.10 ESECUZIONE E CONTROLLI PER LA PROTEZIONE DEI DATI

In ambito alla pianificazione del Sistema di Gestione per la PRIVACY sono stati definiti i processi correlati alla realizzazione dei prodotti ed all'erogazione delle prestazioni da parte della società e predisposta la documentazione necessaria ad assicurarne l'attuazione, il monitoraggio e la registrazione nel rispetto della Politica e degli Obiettivi per la PRIVACY stabiliti.

Registri delle attività di trattamento

Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;

b) le finalità del trattamento;

c) una descrizione delle categorie di interessati e delle categorie di dati personale;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Registri delle categorie attività di trattamento

Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;

b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

I registri sono tenuti in forma scritta, anche in formato elettronico.

Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

La tenuta dei registri non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati o i dati personali relativi a condanne penali e a reati.

Il titolare del trattamento e responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguata al rischio, che comprendono, tra le altre, se del caso:

e) la pseudomizzazione e la cifratura dei dati personali;

f) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi del trattamento;

g) la capacità di ripristinare la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

h) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

C11 ANALISI E CONTROLLO PER LA PROTEZIONE DI DATI

C11.1 METODI E STRUMENTI DI CONTROLLO

Il titolare del trattamento dopo l'analisi dei rischi ed in riferimento ai processi identificati per la protezione dei dati, individua i metodi e gli strumenti necessari a garantire che il trattamento dei dati personali sia conforme ai requisiti del documento cogente di riferimento e indicare le persone o le funzioni interne che hanno il compito di effettuare i controlli, i monitoraggi, le misure e i test, le tempistiche della loro effettuazione e le modalità di analisi dei risultati. Devono essere conservate informazioni documentate relativamente ai controlli, monitoraggi, misure, test, metodi ed analisi. I metodi scelti devono essere in accordo con la linea strategica del titolare del trattamento e proporzionali al rischio sulla protezione dati e coerenti con il rischio d'impresa.

C11.2 SELF AUDIT

In ambito alla Società vengono eseguite periodicamente verifiche ispettive Interne (Audit) per stabilire se le attività del Sistema di Gestione per la PRIVACY ed i relativi risultati soddisfano le disposizioni pianificate, i requisiti della norma di riferimento ed i requisiti interni definiti e valutare se il Sistema è stato efficacemente attuato e mantenuto aggiornato.

In particolare, attraverso gli Audit interni la società si propone di:

- valutare il livello di applicazione delle procedure gestionali e dei documenti in base ai quali la funzione verificata deve operare, valutando altresì la competenza e la consapevolezza maturata dal personale della funzione stessa in merito ai criteri ed alle prescrizioni riportate nella suddetta documentazione e per la sua applicazione;
- valutare le modalità operative, le interfacce, le prescrizioni e le responsabilità stabilite nella documentazione del Sistema di Gestione per la PRIVACY e di conseguenza stabilirne l'efficacia, considerando le difficoltà e le problematiche riscontrate dal personale nell'attuazione.

La conduzione delle verifiche ispettive interne è affidata a personale che risponde ai seguenti requisiti:

- possiede solida conoscenza delle attività svolte dalla Società;
- è indipendente da chi ha diretta responsabilità per le attività sottoposte ad audit;
- assicura l'obbiettività e l'imparzialità del processo di verifica ispettiva;
- è stato preventivamente qualificato ed abilitato all'esercizio di tale funzione.

L'attribuzione e la notifica dell'abilitazione avvengono a cura del Titolare del trattamento dati attraverso una dichiarazione scritta riportante gli estremi ed i riferimenti della qualifica.

La pianificazione degli Audit Interni è attuata dal responsabile del trattamento dei dati secondo criteri che tengono conto dell'importanza e criticità delle aree oggetto di verifica e dei risultati di precedenti verifiche. Gli Audit Interni avvengono sulla base di apposite liste di riscontro e le registrazioni degli esiti sono documentate, sottoposti all'attenzione dei responsabili coinvolti e conservati da RQ.
Le responsabilità, le modalità ed i requisiti per la conduzione delle verifiche ispettive sono definiti nella procedura.

C11.3 ANALISI DEL TITOLARE DEL TRATTAMENTO

Il titolare del trattamento deve sottoporre ad analisi l'intero sistema di gestione per la protezione dei dati per acquisire contezza della sua continua adeguatezza, implementazione, idoneità ed efficacia. I risultati dell'analisi devono essere conservati come informazioni documentate.

A12 AZIONI E PROGRESSI SUL SISTEMA PER LA PROTEZIONE DEI DATI

Nel caso in cui, durante lo svolgimento delle attività si verifichi una non conformità, il titolare del trattamento o il responsabile deve reagire con immediatezza alla non conformità, attraverso un trattamento e l'avvio di un'azione correttiva che ha lo scopo di eliminare la causa della non conformità. Se si avvia un'azione correttiva, deve esserne verificata l'efficacia. Le non conformità e le azioni correttive devono essere conservate come informazioni documentate per un tempo definito. In caso di violazione dei dati personali, il titolare del trattamento, emette una non conformità, e notifica la violazione all'autorità di controllo competente senza ingiustificato ritardo e entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica non sia effettuata entro 72 ore, deve essere corredata dai motivi del ritardo. Con gli output dell'analisi del titolare del trattamento, l'entità attraverso l'adeguata prevenzione o riduzione degli effetti indesiderati sul trattamento dei dati, deve fornire evidenza del progresso continuo del sistema di gestione per la protezione dei dati messo in atto.