Teknos S.p.A.
SEDE LEGALE: VIA SANTELLA PARCO LA PERLA – 81055 S. MARIA C.V. (CE)
UFFICI: VIA NAZIONALE APPIA KM 196 – 81050 VITULAZIO (CE)

MANUALE GDPR
Adottato ai sensi dell'art.24 del Regolamento Europeo UE 2016/679 Dlgs 101/2018
101/2018 – d. lgs. N.101/2018

1	17/02/2025	Prima emissione	Avv. L. Laurenza	CDA
Rev.	**Data**	**Descrizione Modifica**	**Preparata da**	**Verificata ed Approvata da**

Sommario

1. SCOPO DEL MANUALE GDPR

Teknos S.p.A. (di seguito "società"), al fine di rispondere alle prescrizioni indicate dal Regolamento UE 2016/679 (General Data Protection Regulation - di seguito per brevità "GDPR"), in merito al trattamento dei dati personali ha predisposto il presente documento denominato "Manuale GDPR".

Il presente manuale sostituisce il "Documento Programmatico sulla Sicurezza" (per brevità DPS) e rappresenta lo strumento operativo e gestionale per programmare e verificare l'adozione delle misure tecniche e organizzative adeguate, secondo quanto previsto dagli articoli 24 e 32 del GDPR.

Questo documento è stato emesso, approvato ed aggiornato dalla direzione.

Il Manuale GDPR, costituisce un valido strumento per:

- definire compiti, istruzioni e responsabilità dei soggetti, che a vario titolo sono preposti al trattamento dei dati personali e all'adozione delle misure tecniche ed organizzative di sicurezza e di protezione;
- descrivere le politiche aziendali, nonché le azioni e gli adempimenti adottati per garantire un livello di sicurezza adeguato;
- individuare indirizzi e misure per consentire la gestione delle emergenze e garantire la continuità operativa ed il ripristino degli strumenti e dei dati;
- indicare azioni per consentire il controllo del sistema di sicurezza.

Il presente manuale è strutturato in paragrafi e allegati:

- i paragrafi recano la descrizione delle azioni da adottare e delle regole generali da rispettare, per cui sono conoscibili da tutti;
- gli allegati contengono le indicazioni operative e la descrizione delle misure tecniche ed organizzative adottate dalla società (per cui di norma non sono pubblici, in quanto aventi natura riservata e riferita a processi critici).

2. PROFILI SOGGETTIVI - CHI

2.1 Titolare e responsabili del trattamento

La disciplina europea in tema di protezione dei dati personali (GDPR), in continuità rispetto al codice della privacy italiano, individua due figure soggettive particolari, aventi una responsabilità specifica per quanto concerne il trattamento dei dati personali:

a) il **titolare del trattamento**: è TEKNOS SpA (di seguito per brevità "società"), come entità considerata nel suo complesso, rappresentata dall'amministratore pro-tempore;

b) il **responsabile del trattamento** (art. 28 GDPR): è la persona fisica o la persona giuridica che presenta garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento e garantisca la tutela dei diritti dell'interessato.

I responsabili del trattamento possono essere individuati:

- all'interno dell'organizzazione aziendale (quindi, nella figura di un dipendente della società), che ha il compito di coordinare la gestione dei documenti e di tutti gli aspetti relativi agli adempimenti legati al GDPR
- all'esterno, nelle figure che, in base ad un contratto o ad un atto, prestano servizi per conto della società e quindi sono preposte a svolgere operazioni di trattamento in nome e nell'interesse della stessa.

A tal fine, la società valuta i fornitori, consulenti e collaboratori esterni, ai quali sono affidati attività e compiti che comportano la necessità di accedere ai dati personali e/o agli strumenti elettronici aziendali, per cui occorre formalizzare la designazione in qualità di responsabile del trattamento, predisponendo apposito documento di nomina (**PRI_C.1**).

2.2 Autorizzati al trattamento dei dati personali (alias incaricati del trattamento)

Il titolare o il responsabile del trattamento svolge le operazioni di trattamento mediante la preposizione e l'ausilio di persone fisiche: si tratta dei soggetti autorizzati al trattamento (ai sensi dell'art. 29 GDPR), che, in continuità rispetto al codice della privacy, possono continuare ad essere chiamati incaricati del trattamento.

Secondo la definizione riportata nel GDPR si tratta di "chiunque agisca sotto l'autorità del titolare o del responsabile del trattamento, dovendo essere istruito con un atto scritto".

La designazione degli autorizzati al trattamento (*alias* incaricati del trattamento) è effettuata dal responsabile del trattamento ed avviene mediante una apposita lettera (**PRI_C.4**); è inoltre presente un documento di nomina dei soggetti interni designati all'amministrazione dei sistemi informatici (**PRI_C.3**).

2.3 Responsabile della Protezione dei Dati Personali (RPD)

Ai soggetti indicati nei due paragrafi precedenti, con l'adozione del GDPR si aggiunge il Responsabile della protezione dei dati (RPD), che è figura obbligatoria quando il trattamento dei dati è effettuato da un'autorità pubblica ovvero nelle ipotesi previste dall'art. 37 del Regolamento UE 2016/679.

La società ha scelto di non procedere alla nomina di un RPD, in quanto non necessaria.

3. ELENCO DEI TRATTAMENTI - COSA

Il Regolamento UE 2016/679 (GDPR) ha ad oggetto la disciplina dell'attività di trattamento dei dati personali e si applica solo ed esclusivamente ai trattamenti di dati personali riferiti a persone fisiche, mentre sono escluse dall'ambito di applicazione del regolamento le informazioni relative alle persone giuridiche.

In particolare:

- per **trattamento** si intende "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, con 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";

- per **dato personale** si intende "**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".

Sono due le categorie fondamentali di dati personali:

1) **dati comuni:** le informazioni riferite a persone fisiche identificate o comunque identificabili, che non siano idonee a rivelare gli stati, i fatti e le qualità, di cui all'art. 9 del GDPR;
2) **dati particolari:** si intendono i dati che "rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici, dati relativi alla salute o

alla vita sessuale o all'orientamento sessuale della persona"; per tali dati è vietato il trattamento, salvo che non ricorrano i presupposti di liceità e di legittimazione, previsti dal comma 2 dell'articolo GDPR.

4. ISTRUZIONI PER IL TRATTAMENTO DEI DATI PERSONALI E PROTEZIONE DEI DAI PERSONALI - COME

4.1 Principi ed obiettivi in materia di sicurezza e della determinazione delle modalità di trattamento dei dati personali

Gli obiettivi di sicurezza, che la società si pone con la redazione e l'aggiornamento del presente manuale, sono:

1. dimostrare che sono adottate le misure tecniche ed organizzative adeguate, secondo quanto previsto dall'art. 24 del GDPR;
2. garantire il rispetto del principio della *privacy by design*, ai sensi dell'art. 25, comma 1 del GDPR;
3. mettere in atto le misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento (*privacy by default*), ai sensi dell'art. 25, comma 2 del GDPR;
4. ridurre, a livelli accettabili e gestibili, i principali rischi di sicurezza, a cui il sistema informativo aziendale può essere sottoposto;
5. mantenere, compatibilmente con i vincoli di sicurezza previsti dal GDPR e dalle eventuali indicazioni dell'Autorità Nazionale di Controllo, il massimo livello di usabilità del sistema.

La determinazione dei compiti e delle istruzioni da impartire al personale è riportata in apposito allegato (**PRI_C.5**).

Le regole per la protezione dei dati personali presenti su supporto informatico sono riportate nella procedura interna del sistema Qualità **P4201** "Gestione della documentazione".

4.2 Attività e azioni del titolare del trattamento per la garanzia della conformità dei trattamenti di dati al GDPR

La società, in qualità di titolare del trattamento, provvede a determinare le finalità e le modalità dei trattamenti.

Pertanto, al fine di garantire la conformità delle attività di trattamento dei dati al GDPR, la società procede a:

a) nominare fornitori e soggetti esterni all'organizzazione aziendale in qualità di responsabili esterni del trattamento, utilizzando il modello di atto di nomina, rif. **PRI_C.1**;

b) designare in qualità di autorizzati al trattamento (ossia incaricati al trattamento dei dati) le persone fisiche preposte allo svolgimento delle operazioni di trattamento, utilizzando l'apposita lettera (**PRI_C.4**);

c) consegnare a ciascuna persona (sia dipendente, sia collaboratore strutturato) le istruzioni scritte per il trattamento dei dati e le misure di sicurezza adottate da CONTEK, riportate nell'allegato **PRI_C.5**;

d) vigilare sul rispetto da parte degli incaricati e dei soggetti nominati in qualità di responsabili esterni delle istruzioni relative alle misure di sicurezza previste dalla società, adottando le misure correttive e integrative necessarie;

e) collaborare, con i soggetti preposti alla gestione e alla amministrazione dei sistemi, alla definizione del profilo di autorizzazione da associare alle credenziali di autenticazione assegnate a ciascun incaricato del trattamento dei dati. Per profilo di autorizzazione si intende
"l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti"; il "sistema di autorizzazione" è costituito dall'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente;

f) provvedere a richiedere la disattivazione, ovvero la variazione del profilo di autorizzazione associato a ciascun incaricato, nel caso in cui la persona fisica cessi di operare all'interno della struttura di propria competenza ovvero, per qualsiasi motivo, fosse stato modificato il suo
profilo professionale;

g) vigilare sull'attività svolta dagli incaricati del trattamento, verificando il rispetto delle procedure operative e delle istruzioni impartite dall'azienda, anche in materia di misure di sicurezza.

La società, inoltre, per quanto riguarda la gestione e la manutenzione degli strumenti elettronici, si avvale sia di personale interno, sia di soggetti esterni, che sono nominati amministratori di sistema, in conformità alle indicazioni fornite dal Garante per la protezione dei dati personali nel provvedimento generale del 27 novembre 2008, così come modificato ed integrato con deliberazione del 25 giugno 2009.

La designazione delle persone fisiche in qualità di amministratore di sistema avviene mediante l'utilizzo del modello di lettera di nomina, doc. rif. **PRI_C.3**.

4.3 Liceità del trattamento e obblighi di informazione

Il trattamento dei dati personali deve essere svolto in modo lecito, corretto e trasparente, secondo quanto previsto dall'art. 5 del GDPR.

Inoltre, la raccolta dei dati deve avvenire per finalità determinate, esplicite e legittime e i dati possono essere trattati in modo che l'attività da svolgere non sia incompatibile con tali finalità.

Pertanto, all'interessato o alla persona che fornisce i dati, al momento della raccolta degli stessi, deve essere fornita una idonea informativa, secondo quanto previsto e nelle forme di cui agli articoli 12 – 13 – 14 del GDPR. Al fine di

ottemperare a quanto sopra, TEKNOS ha predisposto:

- **per i dipendenti**, i cui dati vengono raccolti all'atto dell'assunzione e che necessitano di consenso, il documento PRI_A.1, nel rispetto delle regole di legittimazione, previste dagli articoli 6 e 9 del GDPR, rispettivamente per la raccolta ed il trattamento dei dati comuni e dei dati particolari;
- **per clienti e fornitori**, con i quali la società intrattiene rapporti, il documento PRI_C.6. Per quanto concerne i trattamenti di dati personali di cui è titolare la società di norma non occorre

  l'acquisizione del consenso dell'interessato, considerato che le finalità del trattamento medesimo sono connesse all'adempimento o l'esecuzione di prestazioni di un contratto di cui è parte l'interessato medesimo ovvero per adempiere un obbligo legale

5. SICUREZZA DEI DATI PERSONALI – PERCHE'

5.1 Analisi e valutazione dei rischi e piano di sicurezza

Il GDPR è finalizzato, ai sensi dell'art. 32, a favorire e a garantire che il titolare del trattamento e il responsabile del trattamento mettano in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

La sicurezza può essere definita come "l'insieme delle misure atte a garantire la disponibilità, l'integrità e la riservatezza delle informazioni gestite" e dunque "l'insieme di tutte le misure atte a difendere il sistema informativo dalle possibili minacce d'attacco".

I rischi di perdita dei dati, anche accidentale, di accesso abusivo e di trattamento illecito o non consentito dei dati possono essere causati (a titolo meramente esemplificativo) da:

- malfunzionamenti di sistemi hardware e software, applicativi software e servizi;
- persone esterne all'organizzazione (hacker, spie, terroristi, vandali, ecc.);
- eventi naturali (inondazioni, incendi, terremoti, tempeste, ecc.);
- persone interne all'organizzazione; e possono essere identificati come:
- accidentali,
- deliberati.

Principale obiettivo di un sistema di sicurezza è quindi la salvaguardia delle informazioni.

A tal fine, per ciascun sistema informativo automatizzato aziendale, per gli strumenti elettronici e per gli archivi e documenti cartacei deve essere fornita la cosiddetta **garanzia "R.I.D."**, ossia "**Riservatezza** – **Integrità** – **Disponibilità"**:

- **Riservatezza (o Confidenzialità):** solo gli utenti autorizzati possono accedere alle informazioni necessarie;
- **Integrità:** protezione contro alterazioni o danneggiamenti; tutela dell'accuratezza e completezza dei dati;
- **Disponibilità:** le informazioni sono rese disponibili quando occorre e nell'ambito di un contesto pertinente.

Fra le risorse (*asset*) da tutelare rientrano certamente:

- dati digitali;
- documenti cartacei;
- flussi informativi;

nonché componenti materiali come:

- server;
- computer;
- reti; ma anche:
- il personale;
- gli edifici;
- gli uffici.

L'approccio alla sicurezza deve avvenire in una logica di prevenzione piuttosto che in una logica di gestione delle emergenze o di semplice controllo / vigilanza.

L'architettura del sistema, al fine di garantire le esigenze di sicurezza di protezione degli strumenti e dei dati, si basa su 3 elementi fondamentali:

- le politiche aziendali di sicurezza;
- le soluzioni organizzative e tecnologiche;
- gli atteggiamenti individuali.

Le misure tecniche ed organizzative devono essere adottate mediante l'utilizzo di un **processo di autodeterminazione**, per cui occorre provvedere alla riduzione dei rischi, che possono interessare i dati personali oggetto di trattamento in seno all'azienda e che riguardano il sistema informativo nel suo complesso.

- Il sistema di protezione dei dati personali della società si basa sui seguenti principi generali:
- tutte le informazioni (dati, documenti, archivi, ...) devono essere protette e disponibili;
- al fine di garantire la riservatezza dei contenuti e delle informazioni, la sicurezza deve riguardare anche le reti di comunicazioni elettroniche dei dati;

- si deve procedere alla previsione di misure di sicurezza per la protezione delle aree e locali, in cui sono localizzati i server considerati "sensibili" per l'attività dell'azienda e gli archivi cartacei, monitorandone le caratteristiche tecniche e le misure di tutela dagli accessi non autorizzati;
- tutte le operazioni di trattamento dei dati, effettuate utilizzando strumenti connessi alla rete di comunicazione elettronica, devono essere oggetto di tracciabilità, garantendo il non ripudio delle operazioni svolte, dovendo utilizzare un sistema di autenticazione informatica, che consenta un controllo dell'identità di "chi sta facendo che cosa";
- devono essere predisposte misure tecniche ed organizzative di sicurezza per l'accesso ai locali, che ospitano i server e gli strumenti elettronici in dotazione alle postazioni di lavoro, favorendo possibilmente la localizzazione e l'ubicazione in unico luogo o in luoghi collegati, al fine di consentire una migliore gestione degli strumenti e della sicurezza attiva e passiva;
- ogni eventuale incidente o evento straordinario, che possa pregiudicare la sicurezza dei dati e dei sistemi, deve essere oggetto di analisi e di rapporto scritto;
- tutti i progetti per lo sviluppo di nuovi sistemi / servizi, aventi natura trasversale e che possano interessare il sistema informativo dell'azienda, devono essere comunque gestiti secondo quanto riportato nel presente manuale;
- al pari, tutte le modifiche eventualmente apportate ai processi organizzativi devono essere documentate nel presente manuale o nei documenti del sistema di qualità aziendale.

In particolare, l'analisi e la valutazione dei rischi sono effettuate utilizzando il documento di analisi rischi aziendale (inserito nel sistema di gestione qualità), al quale si rimanda e che viene aggiornato annualmente nell'abito delle attività di mantenimento dell'organizzazione.

All'esito dell'analisi e della valutazione dei rischi, si procede alla determinazione delle misure di tecniche ed organizzative di sicurezza, ai sensi dell'art. 32 del GDPR, elencate e descritte nel documento stesso e nei documenti correlati.

5.2 Gestione dell'emergenza e ripristino della disponibilità dei dati e degli strumenti

Al fine di garantire la continuità operativa dei sistemi e quindi dei trattamenti di dati personali nonché, allo scopo di fronteggiare eventi che possano causare il danneggiamento degli strumenti elettronici e la distruzione o perdita delle informazioni critiche, la norma prevede che si debbano intraprendere azioni efficaci per fronteggiare l'emergenza e le possibili interruzioni dei processi aziendali.

TEKNOS al fine di ottemperare a quanto sopra ha definito adottare una serie di misure tecniche e organizzative finalizzate a prevenire, contrastare e/o ridurre gli effetti relativi ad una specifica minaccia, oltre ad attuare una puntuale attività di verifica e controllo.

Di seguito si riepilogano le principali misure tecniche e organizzative adottate:

5.2.1 Continuità del servizio

PRECAUZIONI DI BASE

- **BACK-UP DEI DATI**

* Eseguire back-up periodici e frequenti dei dati, sia in formato cartaceo che elettronico (back- up incrementale su base periodica e completo a intervalli regolari su un periodo più lungo);

* Conservare i back-up su un sito esterno;

* Proteggere i dati di back-up con lo stesso livello di sicurezza dei dati memorizzati sul server in produzione;

- **GESTIONE DELLA CONTINUITÀ OPERATIVA**

* Creare un piano di gestione della continuità operativa dei servizi IT, anche breve, includendo l'elenco delle persone coinvolte;

* Identificare chiaramente modalità e destinatario della comunicazione di "incidente";

* testare periodicamente il ripristino dei back-up e l'applicazione del piano di gestione della continuità operativa;

- **ATTREZZATURE**

* Utilizzare un gruppo di continuità per proteggere l'utilizzo della infrastruttura;

* inserire la ridondanza dell'unità di memoria;

5.2.2 Sicurezza fisica

Rafforzare la sicurezza dei locali che ospitano le infrastrutture IT e le apparecchiature di rete, con accesso ai locali controllato.

PRECAUZIONI DI BASE

* installare sistemi di allarme antintrusione e controllarli periodicamente;

* installare rilevatori di fumo e anti-allagamento e ispezionarli periodicamente;

* garantire la sicurezza di chiavi e codici di allarme che concedono l'accesso ai locali;

* separare le aree dell'edificio in base ai rischi (mediante livelli di abilitazione del controllo accessi);

* gestire un elenco degli addetti e dei livelli di abilitazione della gestione accessi;

* gestire l'accesso dei visitatori, con accompagnamento al di fuori delle "aree di ricevimento pubbliche";

* proteggere fisicamente le apparecchiature IT da "eventi esterni imprevedibili" (ad es. allagamento, fulmini, mancanza di rete, ecc.) e condizionando i locali al fine di evitare il surriscaldamento delle apparecchiature

5.2.3 Sicurezza degli archivi storici

Assicurare l'archiviazione e salvataggio dei dati che non vengono più utilizzati fino al termine del periodo di trattamento.

Tali dati vengono protetti soprattutto quando questi sono considerati "dati sensibili".

PRECAUZIONI DI BASE

* definire una procedura di gestione degli archivi;

* garantire metodi e livelli di accesso con apposita abilitazione;

* utilizzare supporti fisici che garantiscano buoni livelli in termini di longevità.

6. SISTEMI DI VIDEOSORVEGLIANZA

L'attività di vigilanza effettuata tramite **telecamere** rientra tra i temi più importanti tra quelli relativi alla protezione dei dati personali. Vista la natura potenzialmente invasiva del mezzo, lo stesso Garante per la Privacy si è espresso più volte sull'argomento e ha emanato diversi provvedimenti e fornito indicazioni che puntano a regolarizzare la videosorveglianza.

6.1 Videosorveglianza privata e pubblica

In ambito privato l'installazione di impianti di videosorveglianza è completamente **libera** e non richiede alcuna autorizzazione anche ad esempio da parte degli altri condomini. L'unica condizione prevista è che le riprese non riguardino spazi collettivi o luoghi di passaggio pubblico: occorre fare attenzione ed evitare che le telecamere (compresi i videocitofoni) non inquadrino spazi pubblici esterni come la porta del vicino. Le riprese effettuate, infine, non potranno essere in alcun modo diffuse.

Nel caso in cui l'oggetto della videosorveglianza sia uno spazio pubblico o effettuata da un'azienda sopraggiunge invece l'**obbligo dell'informativa**, ovvero della necessità che gli interessati siano informati della presenza di una zona sorvegliata a mezzo video, anche nel caso di eventi pubblici, con cartelli espliciti, comprensibili e sempre visibili.

L'informativa può essere minima, ad esempio con un semplice cartello recante la dicitura "area videosorvegliata" con adeguata immagine esplicativa.

Per il testo completo si potrà, con un semplice rimando, fare riferimento all'informativa completa con adeguata rispondenza alla normativa GDPR 2016/679.

6.2 Adempimenti aziendali

Al fine di ottemperare a quanto prescritto dal Garante, relativamente al proprio impianto di videosorveglianza, TEKNOS ha provveduto a:

- ⇨ inoltrare all'Ispettorato Nazionale del lavoro di competenza apposita richiesta di "Autorizzazione per impianti di videosorveglianza" compilando il modulo INL 1.4 ed allegato tutta la relativa documentazione tecnica necessaria (**PRI_B.1 + allegati**);
- ⇨ apporre idonei cartelli segnalatori in corrispondenza delle telecamere (**PRI_B.2**);
- ⇨ predisporre apposita informativa (**PRI_B.3**) e consegnarla ai propri dipendenti, con controfirma per presa visione, oltre che esporla nella bacheca aziendale, ben visibile a tutti.

6.3 Informativa verso terzi

Al fine di informare i propri clienti, TEKNOS ha predisposto una Informativa sintetica (**PRI_D.0**) inerente i sistemi di videosorveglianza sui luoghi di lavoro per illustrare, anche se senza presunzione di esaustività, gli adempimenti formali cui ogni azienda con dipendenti deve ottemperare.

7. ELENCO ALLEGATI AL MANUALE GDPR

Documento	Descrizione	Ultima Revisione	Causali aggiornamento	Destinatari	Modalità distribuzione
PRI_A.1	Informativa sul trattamento dei dati personali dipendenti	13/02/25	Prima emissione	Dipendenti, collaboratori, lavoratori interinali, consulenti	Consegna copia cartacea controfirmata per presa visione
PRI_A.2	Informativa modalità di trattamento dati personali al medico del lavoro	13/02/25	Prima emissione	Medico del lavoro	Consegna mediante invio per PEC controfirmata per presa visione
PRI_B.1	Istanza di autorizzazione impianti videosorveglianza	13/02/25	Presentazione	Ispettorato Nazionale del Lavoro	Consegna telematica mediante PEC a INL e cartacea a mezzo raccomandata con R.R.
PRI_B.2	Cartello segnalatore	----	----	Dipendenti, consulenti, collaboratori e visitatori delle sede	Apposizione nelle aree interessate dalle riprese
PRI_B.3	Informativa videosorveglianza nei locali TEKNOS	13/02/25	Prima emissione	Dipendenti, consulenti, collaboratori e visitatori delle sede	Consegna copia cartacea controfirmata per presa visione e affissione in bacheca
PRI_C.1	Lettera designazione responsabile esterno del trattamento	13/02/25	Prima emissione	Fornitori, consulenti e collaboratori società	Designazione tramite invio della lettera per PEC all'indirizzo indicato nel portale www.inipec.gov.it
PRI_C.2	Registro dei trattamenti semplificato	13/02/25	Prima emissione	Documento riservato	Documento interno
PRI_C.3	Lettera di incarico di "Amministratore del sistema informatico aziendale""	13/02/25	Prima emissione	Amministratore del sistema informatico aziendale	Designazione tramite consegna cartacea controfirmata per accettazione
PRI_C.4	Lettera designazione autorizzati al trattamento	13/02/25	Prima emissione	Responsabili del trattamento Autorizzati al trattamento	Designazione tramite consegna cartacea controfirmata per accettazione
PRI_C.5	Istruzioni e misure di sicurezza in tema di trattamento dei dati	13/02/25	Prima emissione	Dipendenti, collaboratori, lavoratori interinali, consulenti	Consegna copia cartacea controfirmata per presa visione
PRI_C.6	Informativa sul trattamento dei dati personali clienti/fornitori	13/02/25	Prima emissione	Clienti, Fornitori, Collaboratori	Distribuzione mediante PEC a soggetti già trattati ed ai nuovi fornitori; ai nuovi clienti invio congiunto al modulo TD47 - richiesta dati anagrafici

Documento	Descrizione	Ultima Revisione	Causali aggiornamento	Destinatari	Modalità distribuzione
PRI_D.0	Informativa generale sistemi di videosorveglianza sui luoghi di lavoro	13/02/25	Prima emissione	Clienti	Consegna copia cartacea o invio a mezzo mail
MD-6101	Analisi e valutazione dei rischi	13/02/25	Prima emissione	Documento riservato	Documento interno
P-4201	Procedura di gestione della documentazione	13/02/25	Prima emissione	Documento riservato	Documento interno