INDICE

Ed.	Rev.	Data	Descrizione Modifica	Emissione RSQ	Verifica RSQ	Approvazione DIR
				Nome	Nome	Nome
1	0	30/09/2018	Nuova emissione – adeguamento GDPR	Data Firma	Data Firma	Data Firma

Lista di Distribuzione

Copia N°	Destinatario	Copia Controllata	Copia Non Controllata	Modalità di distribuzione	
1		☐	☐	Cartacea ☐	Elettronica ☐
2		☐	☐	Cartacea ☐	Elettronica ☐
3		☐	☐	Cartacea ☐	Elettronica ☐

1 CAMPO DI APPLICAZIONE

Lo scopo del presente documento è definire chiaramente gli obiettivi del progetto di implementazione del Regolamento Generale Europeo sulla Protezione dei Dati (GDPR – Regolamento UE 679/2016), i documenti che devono essere scritti, le scadenze, i ruoli e le responsabilità all'interno del processo.
Il documento si applica a tutte le attività svolte nel progetto di sviluppo, implementazione e mantenimento dei requisiti del GDPR.
I destinatari di questo documento sono i membri dell'Alta direzione e i membri del gruppo di progetto individuati per lo sviluppo dello stesso.

Il processo si applica a tutta la struttura.
Il contenuto deve essere divulgato e spiegato a tutti gli autorizzati (dipendenti, collaboratori e terze parti che operano per conto di FURFARO).
La parte che riguarda i dipendenti deve essere divulgata e spiegata a cura dei diretti responsabili.
Eventuali situazioni di deviazione accertate rispetto a quanto precisato nel presente documento dovranno essere rimosse nel più breve tempo possibile.

2 OBIETTIVO

Obiettivo del processo, infatti, è quello di implementare il Sistema di Gestione del GDPR in conformità al Regolamento Generale sulla Protezione dei Dati.

3 GENERALITÀ

L'approccio con il quale questo documento è stato redatto si ispira al principio della Privacy by design che prevede di gestire la privacy a partire dalla progettazione di un processo aziendale e tenendo conto delle componenti informatiche di supporto.
Pertanto il sistema di gestione per la qualità adottato dalla società FURFARO ha lo scopo di migliorare l'affidabilità della propria organizzazione e, di conseguenza, garantire la soddisfazione dei clienti, della proprietà, dei dipendenti, dei fornitori e il sistema per la gestione e la protezione dei dati personali trattati.

Il documento è predisposto e tenuto aggiornato anche per definire, sulla base delle analisi dei rischi, della distribuzione dei compiti e delle responsabilità, nell'ambito delle strutture preposte al trattamento dei dati:
- i criteri tecnici e organizzativi per la protezione dei dispositivi, delle aree e dei locali interessati dalle misure di sicurezza, nonché tutte le procedure per controllare l'accesso delle persone autorizzate agli stessi
- i criteri e le procedure per assicurare l'integrità dei dati
- i criteri e le procedure per la sicurezza delle trasmissioni dei dati
- l'elaborazione di un piano di formazione verso tutti gli i referenti dell'organigramma della Privacy, al fine di renderli edotti dei rischi individuati e dei modi per prevenire danni.

La compliance al Regolamento Generale Europeo sulla Protezione dei Dati (GDPR – Regolamento UE 679/2016) si traduce con lo sviluppo di idonee informazioni documentate in funzione del proprio grado di complessità, costituita da documenti operativi e da registrazioni.

Il sistema di gestione privacy (SGP) prevede l'implementazione dei seguenti documenti (e lo scopo), ove applicabili, alcuni dei quali possono essere accorpati e/o contenere allegati che non sono espressamente riportati nel seguente elenco:
- Politica sulla Protezione dei Dati Personali – una politica intesa a stabilire i principi generali della protezione dei dati oltre a dimostrare l'impegno dell'azienda nei confronti di tali principi;
- Politica di Protezione dei Dati dei Dipendenti – una politica per stabilire le condizioni in cui l'azienda gestisce i dati personali dei propri dipendenti;
- Informativa sulla Privacy - una comunicazione per stabilire le condizioni in base alle quali l'azienda gestisce i dati personali dei propri clienti / visitatori del sito;
- Registro delle Comunicazioni sulla Privacy - un documento in cui è necessario elencare tutti gli avvisi pubblicati;
- Politica di Conservazione dei Dati - una politica per definire il periodo in cui i dati personali possono essere conservati dall'azienda;
- Descrizione del Lavoro del Responsabile della Protezione dei Dati (DPO): un documento che descrive le responsabilità del Responsabile della Protezione dei Dati;

- Linee guida per l'Elenco dei Dati e la Mappatura delle Attività di Trattamento - un documento che spiega come elencare tutte le attività relative al trattamento dei dati;
- Elenco delle Attività di Trattamento dei Dati - un documento destinato ad essere utilizzato dall'azienda per dimostrare la conformità ai requisiti dell'art. 30 del GDPR dell'UE;
- Modulo di Consenso dell'Interessato - un documento utilizzato dall'Azienda per ottenere il consenso degli interessati al trattamento dei dati personali per uno scopo specifico;
- Modulo di Recesso da parte dell'Interessato - un documento utilizzato dagli interessati per ritirare il proprio consenso;
- Modulo di Consenso del Titolare della Responsabilità Genitoriale - un documento utilizzato dall'Azienda per ottenere il consenso del genitore / tutore legale / rappresentante di minore per trattarne i dati personali per uno scopo specifico;
- Modulo di Recesso del Titolare della Responsabilità Genitoriale - un documento utilizzato dal genitore / tutore legale / rappresentante di minore per ritirare il consenso al trattamento dei dati personali per uno scopo specifico;
- Procedura di Richiesta di Accesso ai Dati da parte dell'Interessato: un documento per impostare il processo attraverso il quale l'azienda risponde alle richieste dei soggetti interessati;
- Metodologia di Valutazione d'impatto sulla Protezione dei Dati - un documento che descrive come valutare la necessità e la proporzionalità di una determinata attività di trattamento e come fornire misure per mitigare i rischi potenziali ai diritti e alle libertà degli interessati;
- Registro della Valutazione d'impatto sulla Protezione dei Dati - un documento utilizzato dall'azienda per documentare il processo di Valutazione d'impatto sulla Protezione dei Dati.;
- Procedura di Trasferimento Transfrontaliero di Dati Peronali - un documento per stabilire le condizioni alle quali può essere eseguito un flusso transfrontaliero di dati;
- Clausole Contrattuali Tipo - clausole tipo emesse dalla Commissione dell'UE per fornire adeguate garanzie in materia di tutela della vita privata e dei diritti e delle libertà fondamentali degli individui e per quanto riguarda l'esercizio dei relativi diritti.
- Questionario di Conformità al GDPR del Responsabile esterno del trattamento dati un questionario inteso a valutare la conformità dei fornitori con il GDPR dell'UE;
- Accordo con i Fornitori di Trattamento dei Dati - un documento contrattuale inteso a stabilire i limiti e le condizioni in base al quale un fornitore (processore) può elaborare dati personali per conto della società (controllore);
- Politica di Sicurezza IT - descrive le regole fondamentali di sicurezza per tutti i dipendenti;
- Politica di Controllo dell'Accesso - definisce come la direzione approvi i diritti di accesso a particolari utenti dei sistemi informativi;
- Procedure di sicurezza per il Dipartimento di Informatica - descrive le regole di sicurezza che devono essere utilizzate per le infrastrutture informatiche;
- Politica Bring Your Own Device (BYOD) - descrive le regole per l'utilizzo di dispositivi mobili e di altri dispositivi non aziendali per scopi aziendali;
- Politica per Dispositivi Mobili e Telelavoro - descrive le regole di sicurezza per l'utilizzo di computer portatili, telefoni cellulari e altri dispositivi al di fuori dei locali aziendali;
- Politica di Clear Desk e Clear Screen - definisce come proteggere le informazioni che si trovano sul posto di lavoro e sugli schermi del computer;
- Politica di Classificazione delle Informazioni - definisce come classificare i dati in base alla riservatezza e come proteggere i dati di conseguenza;
- Politica di Anonimizzazione e Pseudonimizzazione - definisce come utilizzare queste tecniche per proteggere l'elaborazione dei dati personali;
- Politica sull'Uso della Cifratura - definisce come utilizzare i controlli e le chiavi crittografiche per proteggere la riservatezza e l'integrità dei dati;
- Piano di Disaster Recovery - definisce come recuperare le infrastrutture e i dati dopo un incidente;
- Procedura di Audit Interno - definisce come verificare, stimare e valutare le garanzie organizzative e tecniche all'interno di un'azienda;
- Procedura di Risposta e Comunicazione di una Violazione dei Dati - una procedura che stabilisce gli obblighi dell'azienda in caso di violazione di dati personali;
- Registro delle Violazioni - Registro interno aziendale sulle violazioni dei dati;
- Modulo di Comunicazione di una Violazione all'Autorità di Controllo - documento da utilizzare in caso di violazione di dati
- Modulo di Comunicazione di una Violazione agli Interessati - documento da utilizzare in caso di violazione di dati;

4 PROCEDURA

4.1 DATI TRATTATI

Rif. Articoli 4, 9, 10, 11 del Regolamento (UE) n. 679/2016 (GDPR - General Data Protection Regulation)

FURFARO srl tratta i dati in modo esclusivamente elettronico con un limitato archivio cartaceo in parte relativo ai documenti amministrativi che per legge devono essere conservati in questa modalità.
L'azienda tratta i seguenti tipi di dati.

- Dati Comuni (informazioni non riguardanti una persona fisica identificata o identificabile)
- Dati Personali (informazioni riguardanti una persona fisica identificata o identificabile)
- Dati Personali particolari (informazioni idonee a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona).

L'azienda non tratta dati personali relativi a condanne penali e reati.

4.2 FUNZIONAMENTO E CONTROLLO DEI PROCESSI

Rif. Articolo 4 del Regolamento (UE) n. 679/2016 (GDPR - General Data Protection Regulation)

Come indicato FURFARO srl ha integrato la gestione dei processi aziendali secondo la normativa UNI EN ISO 9001:2015 e il trattamento dei dati personali svolto dall'azienda secondo il Decreto legislativo 30/06/2003, n. 196 "Codice in materia di protezione dei dati personali" e il Regolamento (UE) 27/04/2016, n. 679, General Data Protection Regulation (GDPR).
Questa integrazione è stata recepita all'interno del sistema aziendale cartaceo / informativo in cui i processi, le informazioni e i documenti sono gestiti.
Gli archivi del sistema informativo aziendale sono conservati in una base di dati, secondo quanto descritto nell'istruzione privacy e definito dall'Amministrazione di sistema.
Il sistema informativo aziendale garantisce inoltre la tenuta sotto controllo delle registrazioni, assicurando il rispetto dei requisiti di cui ai punti 7.5.2 e 7.5.3 della norma UNI EN ISO 9001:2015.

4.2.1 SITO INTERNET

Le informazioni del Sistema Gestione Privacy sono gestite e mantenute, in parte, sul sito Internet dell'azienda.

4.2.2 REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Rif. Articoli 30 e 32 del Regolamento (UE) n. 679/2016 (GDPR - General Data Protection Regulation)

Ai sensi dell'articolo 30 del Regolamento (UE) n. 679/2016 il titolare del trattamento ha adottato per ogni processo aziendale un registro delle attività di trattamento effettuate. Per semplificare la cooperazione con l'autorità di controllo e l'accesso alle informazioni, il registro è gestito in modo elettronico classificando ogni processo sulla base di:

- finalità del trattamento
- categorie di interessati
- categorie di dati trattati
- categorie di dati interessati
- settore aziendale
- categorie di destinatari
- trasferimenti paese terzo o organizzazione internazionale
- termini di cancellazione previsti
- misure di sicurezza tecniche e organizzative
- modalità di trattamento
- strumenti utilizzati

All'interno dell'organigramma dell'azienda rispetto all'applicazione della normativa sulla privacy con l'individuazione del titolare del trattamento, del responsabile del trattamento, dell'incaricato e dell'amministratore di sistema.

4.3 INFORMATIVE

Rif. Articoli 6, 7, 12, 13, 14 del Regolamento (UE) n. 679/2016 (GDPR - General Data Protection Regulation)

Prima di effettuare il trattamento di dati personali, l'azienda fornisce all'interessato le informazioni necessarie per metterlo nelle condizioni di esercitare i propri diritti.
In ogni documento del SGQ o interfaccia del sito Internet che prevedano l'acquisizione e il trattamento di dati personali è indicata la presenza dell'informativa al link del sito web aziendale e l'espressa indicazione che, con l'approvazione del documento o con la trasmissione di informazioni online, gli interessati dichiarano anche di aver letto le informazioni pubblicate ed esprimono il consenso al trattamento dei dati personali nelle modalità indicate.

4.4 INDIVIDUAZIONE RISORSE DA PROTEGGERE

Rif. Articolo 4 del Regolamento (UE) n. 679/2016 (GDPR - General Data Protection Regulation)

Il sistema di gestione privacy è costituito da una serie di documenti nei quali sono descritti gli archivi e i luoghi fisici dove vengono gestiti e conservati i dati, gli strumenti informatici utilizzati, l'infrastruttura tecnologica aziendale (hardware, software di base e connettività) le policy applicate dall'amministratore di sistema.

4.5 LEADERSHIP

Rif. articoli 24, 25, 26, 27, 28, 29, 40 del Regolamento (UE) n. 679/2016 (GDPR - General Data Protection Regulation)

4.5.1 LEADERSHIP

La direzione di FURFARO srl mette in campo la leadership e l'impegno necessari per gestire il SGP oltre il SGQ:

- assumendosi la responsabilità dell'efficacia dei sistemi di gestione privacy
- assicurando l'integrazione dei requisiti del sistema di gestione della Privacy nei processi di business dell'organizzazione
- assicurando la disponibilità delle risorse necessarie al funzionamento del sistema di gestione della Privacy
- comunicando l'importanza della conformità ai requisiti del sistema di gestione della Privacy
- assicurando che il sistema di gestione della Privacy consegua i risultati attesi
- facendo partecipare attivamente, guidando e sostenendo le persone affinché contribuiscano all'efficacia del sistema di gestione della Privacy

4.5.2 RUOLI, RESPONSABILITÀ E AUTORITÀ

La direzione aziendale assicura che le responsabilità e le autorità per i ruoli pertinenti siano assegnate, comunicate e comprese all'interno dell'organizzazione.
La direzione assegna le responsabilità e le autorità per:

- assicurare che il SGP sia conforme ai requisiti espressi dalla normativa di riferimento
- riferire sulle prestazioni del sistema di gestione privacy
- assicurare la promozione della focalizzazione sul cliente nell'ambito dell'intera organizzazione
- assicurare che l'integrità del sistema di gestione privacy sia mantenuta, quando vengono pianificate e attuate modifiche al sistema stesso.

Per quanto riguarda il sistema di gestione della privacy sono stati individuati i seguenti ruoli:

- Titolare trattamento, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
- Responsabile trattamento, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- Amministratore di sistema, cui compete la gestione e la manutenzione di un impianto di elaborazione o di sue componenti. Amministratori di reti, di basi di dati; di apparati di sicurezza. Compiti specifici realizzazione di copie di sicurezza (operazioni di backup e recovery dei dati) alla custodia delle credenziali alla gestione dei sistemi di autenticazione e di autorizzazione;
- Incaricato gestione dati, chiunque agisca sotto l'autorità del responsabile del trattamento o sotto quella del titolare del trattamento, che abbia accesso a dati personali.

L'organigramma aziendale del SGQ e SGP è disponibile e gestito nell'ambito della procedura di gestione delle risorse umane.
I Ruoli, responsabilità e autorità sono formalizzati e trasmessi a tutto il personale aziendale come lettera di nomina.

4.5.2.1 Data Privacy Officer (DPO) / Responsabile della Protezione dei Dati

Ai sensi dell'articolo 37 del Regolamento (UE) 27/04/2016, n. 679, l'azienda non è tenuta alla nomina del responsabile della protezione dei dati (DPO – Data Protection Officer).

4.5.3 POLITICA PRIVACY

FURFARO Srl intende proteggere le informazioni e i dati gestiti nell'ambito delle proprie attività da tutte le minacce interne o esterne, intenzionali o accidentali, secondo le disposizioni previste dal Regolamento (UE) n. 679/2016.
La politica della privacy si applica a tutte le funzioni e i livelli dell'azienda. La sua attuazione è obbligatoria per tutto il personale ed è essere inserita nella regolamentazione degli accordi con qualsiasi soggetto esterno coinvolto con il trattamento di informazioni che rientrano nel campo del SGP.
FURFARO Srl consente la comunicazione e la diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività aziendali che avvengono nel rispetto delle regole e delle norme vigenti.

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni trattate, incluse quelle contenenti dati personali, assicurandone l'accesso solo a chi è autorizzato, l'integrità, la riservatezza, la disponibilità e la protezione.
La mancanza di adeguati livelli di sicurezza (fisica, logica, delle informazioni) può infatti comportare il danneggiamento dell'immagine aziendale, la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle leggi vigenti nonché danni di natura economica e finanziaria.
L'azienda identifica tutte le esigenze di sicurezza tramite la valutazione del rischio sulla protezione dei dati che permette di valutare le potenziali conseguenze e i danni che possono derivare dalla mancata applicazione di misure di sicurezza al sistema informativo e quale sia la realistica probabilità di attuazione delle minacce identificate, consentendo di acquisire consapevolezza sul livello di esposizione a minacce dei propri sistemi di gestione dei dati. I risultati di questa valutazione determinano le azioni necessarie per individuare le corrette e adeguate misure di sicurezza e i meccanismi per garantire la protezione dei dati personali.

L'osservanza e l'attuazione della politica sono responsabilità di:
- tutto il personale che, a qualsiasi titolo, collabora con l'azienda ed è in qualche modo coinvolto con il trattamento di dati e informazioni
- tutti i soggetti esterni che intrattengono rapporti e collaborano con l'azienda

La Direzione sostiene attivamente le attività inerenti la gestione della privacy aziendale tramite un chiaro indirizzo, un impegno evidente, degli incarichi espliciti e il riconoscimento delle responsabilità relative alla sicurezza delle informazioni.
Pertanto, FURFARO Srl riconosce la propria responsabilità e si impegna a proteggere i dati personali che gli utenti affidano all'azienda da perdita, uso improprio o accesso non autorizzato. Per la protezione dei dati personali degli utenti, l'azienda si avvale di una serie di tecnologie e procedure aziendali di protezione.

4.6 PIANIFICAZIONE

Rif. articoli 30, 32, 35 del Regolamento (UE) n. 679/2016 (GDPR - General Data Protection Regulation)

4.6.1 RISCHI SUI DATI TRATTATI

L'analisi dei rischi è gestita attraverso il riesame della direzione, basata sullo standard normativo della serie ISO 27001 (Sicurezza delle informazioni) il cui risultato è analizzato sempre all'interno del riesame della direzione, nel quale sono almeno indicati:

- la tipologia di rischio
- i rischi che possono incorrere sui dati
- le probabilità che l'evento si verifichi
- il danno sulla sicurezza dei dati
- le opzioni di trattamento
- i criteri di intervento.

Durante il riesame del SGQ (e del SGP), oppure a seguito di non conformità che si siano verificate l'analisi dei rischi sui dati trattati è soggetta a verifica.

4.6.2 MISURE MINIME DI SICUREZZA

Le misure minime di sicurezza sono gestite considerando almeno:
- il codice della misura minima

- i trattamenti interessati
- la struttura o le persone addette all'adozione della misura
- lo stato di attuazione della misura

Durante il riesame del SGQ (e del SGP), oppure a seguito di non conformità che si siano verificate le misure minime di sicurezza sono soggette a verifica.

4.6.3 VALUTAZIONE DI IMPATTO

La valutazione di impatto è necessaria quando i rischi sugli effetti dell'interessato al trattamento sono alti, oppure quando si ricade nell'ambito di applicazione obbligatoria di impatto (caso in cui l'azienda non ricade poiché in generale non si rileva un rischio elevato per i diritti e le libertà delle persone fisiche).
La valutazione di impatto non è applicabile alla società perché non ricorrono rischi elevati per gli interessati in relazione ai trattamenti effettuati e perché non si ricade nel campo di applicazione espresso dall'art. 35 del regolamento e dai documenti dei gruppi di lavoro specifici.
Infatti la società non gestisce:

- la 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
- il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 101
- la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Durante il riesame del SGQ (e del SGP), oppure a seguito di non conformità che si siano verificate la valutazione di impatto sui dati trattati è soggetta a verifica di applicabilità.

4.6.4 PIANIFICAZIONE DELLE MODIFICHE

Quando l'organizzazione determina l'esigenza di modifiche al sistema di gestione della Privacy, queste sono effettuate in modo pianificato.

4.7 SUPPORTO

Rif. articoli 4, 30 e 32 de Regolamento (UE) n. 679/2016 (GDPR - General Data Protection Regulation)

4.7.1 RISORSE

L'organizzazione determina e fornisce le risorse (personale interno, fornitori, informazioni, infrastrutture, budget, etc.) necessarie per l'istituzione, l'attuazione, il mantenimento e il miglioramento continuo del SGP.
L'adeguatezza e la disponibilità delle risorse umane e strumentali necessarie per l'esecuzione delle attività sono verificate da DIR a livello generale in fase di riesame del SGP (con il riesame del SGQ).

Le risorse umane (interne ed esterne che collaborano o operano per conto di FURFARO Srl) che trattano i dati personali sono autorizzate con lettera di nomina.

Le informazioni concernenti la dotazione hardware e software, le relative manutenzioni e la rete informatica aziendale sono ottenibili dalla istruzione privacy e di competenze dell'Amministrazione di sistema.

4.7.2 COMPETENZE

La Direzione assicura che il personale aziendale sia competente, al fine del corretto svolgimento dei ruoli assegnati in ambito privacy, sulla base di un adeguato grado di formazione e addestramento ed esperienza.

4.7.3 CONSAPEVOLEZZA

L'organizzazione stabilisce percorsi formativi interni affinché il personale sia sempre aggiornato sulle modalità di funzionamento del SGP.

4.7.4 COMUNICAZIONE

FURFARO srl mantiene un canale continuo di diffusione delle informazioni sia interne che esterne pertinenti ai SGQ e SGP.

4.7.5 INFORMAZIONI DOCUMENTATE

FURFARO srl mantiene informazioni documentate del SGQ e del SGP e delle stesse ne attua la tenuta sotto controllo in riferimento alla procedura interna di gestione delle informazioni documentate, che assicura il rispetto dei requisiti di cui ai punti 7.5.2 e 7.5.3 della norma ISO 9001:2015.

4.8 ATTIVITÀ OPERATIVE

Rif. articolo 4 del Regolamento (UE) n. 679/2016 (GDPR - General Data Protection Regulation)

4.8.1 PROCESSI RELATIVI AI CLIENTI

In fase precontrattuale e contrattuale sono implementate le attività di protezione dei dati personali attraverso le informative e documenti correlati.

4.8.2 PROCESSI RELATIVI AI FORNITORI

In fase precontrattuale e contrattuale sono implementate le attività di protezione dei dati personali attraverso le informative e documenti correlati.

4.8.3 PROCESSI RELATIVI AL PERSONALE INTERNO E COLLABORATORI

In fase di selezione, assunzione / contratto di collaborazione e durante il rapporto di lavoro / collaborazione il personale è informato del trattamento che il Titolare del trattamento effettua sui dati raccolti / gestiti, fornendo la necessaria documentazione (informativa, consenso, diritti, ecc.).

4.8.4 IDENTIFICAZIONE E RINTRACCIABILITÀ

L'identificazione delle banche dati è prevista per quelle di proprietà.
Eventuali banche dati di proprietà del cliente devono essere rimosse dai sistemi della FURFARO Srl o rese anonimizzate all'atto di eventuali prove e collaudi che prevedano l'uso dei dati in esse contenuti.

4.8.5 PROPRIETÀ DEL CLIENTE

Il trattamento dei dati eventualmente consegnati dal cliente, avvengono nel rispetto di quanto previsto dalle normative sulla privacy e sulla tutela dei diritti d'autore.

4.8.6 CONSERVAZIONE DEL PRODOTTO

Riguardano elaborati cartacei contenenti dati personali, banche dati, applicazioni software di gestione dati personali.
Il ciclo di vita di tutti questi "prodotti" prevede la corretta esecuzione dell'istruzione Privacy con il supporto dell'Amministrazione di sistema al fine di assicurare il rispetto dei requisiti normativi del GDPR.

4.8.7 TRATTAMENTO DEI DATI PERSONALI

Il controllo sul trattamento dei dati personali è effettuato dal titolare del trattamento.
L'identificazione e la rintracciabilità dell'operato degli amministratori di sistema avviene sulla base della corretta esecuzione dell'istruzione Privacy.

4.9 VALUTAZIONE DELLE PRESTAZIONI

Rif. articolo 4 del Regolamento (UE) n. 679/2016 (GDPR - General Data Protection Regulation)

FURFARO Srl ha pianificato e attua idonei processi di monitoraggio e misurazione del SGP.
La Direzione promuove il SGP e si impegna a fornire all'organizzazione tutte le risorse necessarie alla sua attuazione.

Gli audit interni sono effettuati per monitorare il SGQ e il SGP e assicurare che siano sempre conformi alle normative vigenti e alle politiche aziendali. Attraverso la procedura di riferimento è pianificato e condotto l'audit.

Il riesame del SGQ e SGP effettuato per assicurarsi della continua idoneità, adeguatezza ed efficacia del SGP (oltre che SGQ), fornisce informazioni necessarie affinché sia valutata la necessità di revisione generale del sistema di gestione della privacy o specifica di determinate informazioni documentate.

4.10 MIGLIORAMENTO

Rif. articoli 4, 15, 16, 17, 18, 20, 21, 22 del Regolamento (UE) n. 679/2016 (GDPR - General Data Protection Regulation)

4.10.1 OUTPUT NON CONFORMI

FURFARO Srl applica la procedura di gestione delle Non conformità nella quale sono descritte le responsabilità e le modalità di trattamento degli output non conformi riferiti al SGP (intese quali non conformità riscontrate nel trattamento dei dati personali rispetto alle disposizioni contenute nel SGP, oppure a seguito di segnalazioni dell'interessato) o al mancato rispetto di regolamenti aziendali (es. accessi non autorizzati, trattamenti non autorizzati, ecc.).

4.10.2 AZIONI DI MIGLIORAMENTO E CORRETTIVE

È il processo all'interno del quale sono gestite le cause delle non conformità per evitare che quest'ultime possano ripetersi.
Quando si verifica una non conformità l'azienda è organizzata per reagire, valutare l'esigenza di azioni per eliminare la causa, attuare ogni azione necessaria, riesaminare l'efficacia di ogni azione correttiva intrapresa, effettuare, se necessario, modifiche al sistema di gestione della privacy.

4.10.3 EVASIONE RICHIESTE DEGLI INTERESSATI

FURFARO Srl prende in carico tutte le richieste degli interessati e le processa nel rispetto delle tempistiche previste dal Regolamento (UE) n. 679/2016.
Tutte le comunicazioni in ingresso e in uscita relative a richieste degli interessati sono protocollate all'interno del "Sistema gestione privacy". Questo consente di tenere traccia di tutte le richieste pervenute dando luogo al registro di gestione ed evasione delle richieste degli interessati.

5 ALLEGATI

PRIVACY					
CODIFICA E REV.	DESCRIZIONE	UTILIZZATO DA	ARCHIVIATO DA	MODALITÀ DI ARCHIVIAZIONE	TEMPI DI ARCHIVIAZIONE
SGP GDPR	SISTEMA DI GESTIONE PRIVACY				

6 RIFERIMENTI

NORMA UNI EN ISO 9001 7 Supporto

La normativa di riferimento Privacy, non esaustiva, è costituita da:

- Regolamento (UE) 27/04/2016, n. 679, General Data Protection Regulation (GDPR)
- Deliberazione del Garante per la protezione dei dati personali deliberazione 23/11/2006, n. 53 “Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati”
- Linee guida del Garante per la protezione dei dati personali 10/03/2007 “Posta elettronica e internet”
- Deliberazione del Garante per la protezione dei dati personali 14/06/2007, n. 23 “Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico”
- Documento del Garante per la protezione dei dati personali 27/11/2008 “Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”
- Provvedimento del Garante per la protezione dei dati personali 08/04/2010 “Videosorveglianza”
- Linee Guida del Garante per la protezione dei dati personali 04/07/2013 “Attività promozionale e contrasto allo spam”
- Documento del Garante per la protezione dei dati personali 08/05/2014 “Individuazione delle modalità semplificate per l’informativa e l’acquisizione del consenso per l’uso dei cookie”
- Documento del Garante per la protezione dei dati personali 05/06/2015 “Chiarimenti in merito all’attuazione della normativa in materia di cookie”
- Campagna informativa del Garante per la protezione dei dati personali 24/05/2016 “Violazioni di dati personali (data breach): gli adempimenti previsti”
- Documento del Garante per la protezione dei dati personali 16/02/2017 “Verifica preliminare. Sistema di controllo accessi biometrico facciale”

7 DIAGRAMMA DI FLUSSO

N.A.