SOMMARIO

REVISIONI				
N° REV.	DATA REV.	DESCRIZIONE	RIF. PARAGRAFO	RIF. PAGINA
00		Prima emissione	Tutte	Tutte

Verifica	Approvazione	Emissione
Firma Resp:	Firma Direzione:	Firma RQ: Data:

1. Scopo

Scopo della presente procedura è quello di definire le modalità operative da adottare per garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale ed al diritto di protezione dei dati personali, così come previsto dal Regolamento UE 679 del 2016
Questa procedura è applicata per il trattamento di tutti i dati personali effettuato dall'azienda, con le eventuali precisazioni, limitazioni, esclusioni definite nella procedura stessa.

2. Riferimenti

UNI EN ISO 9001:2015
REGOLAMENTO UE 679 DEL 2016

- modello di informativa per dipendenti
- modello di informativa per clienti
- modello di informativa per fornitori
- modello di nomina per responsabile protezione dati
- modello di nomina per responsabile interno
- elenco credenziali di autenticazione
- Modello di Registro attività di trattamento
- Checklist

3. Schema generale di riferimento

Lo schema generale di riferimento per la gestione degli adempimenti per la privacy prevede l'esecuzione delle seguenti attività:

1. Identificare gli interessati dal trattamento e fornirgli un'adeguata informativa;
2. raccogliere i relativi consensi (ad esclusione dei casi in cui ciò non è richiesto);
3. definire l'organizzazione per la privacy,
4. adozione delle misure minime di sicurezza previste,
5. adempimenti periodici
6. monitoraggio e miglioramento del sistema

4. Informativa e Consenso

Prima di ogni cosa è necessario identificare gli interessati dal trattamento dei dati personali .
Per **Interessati** si intendono:
"Sono le persone fisiche, le persone giuridiche, l'ente o l'associazione cui si riferiscono i dati personali".

Prerequisito fondamentale per poter legalmente detenere e trattare dati personali è che sia stata fornita una adeguata informativa **agli interessati.**.

Si deve pertanto procedere a fornire una informativa in materia di trattamento dei dati personali a tutti gli interessati ovvero, principalmente:

- ai Dipendenti/Collaboratori dell'Azienda;
- ai Clienti;
- ai Fornitori.

4.1. Informativa e consenso a Dipendenti e personale interno

Ai Dipendenti ed al personale interno viene fornita una informativa sulla privacy utilizzando il **modello di informativa per dipendenti e collaboratori** allegato alla presente procedura.

Tale modello prevede anche la registrazione del consenso espresso dagli interessati.

La distribuzione delle informative e la raccolta dei consensi deve essere effettuata:

- prima dell'avvio dei trattamenti dei dati;
- al momento dell'assunzione/inserimento;

Ne viene rilasciata copia agli interessati.

Le informative raccolte sono archiviate a cura di dei responsabili interni

4.2. Informativa e consenso a Clienti

4.2.1. Informativa

Generalmente la raccolta dati di un cliente/potenziale cliente è finalizzata alla gestione dei rapporti di natura commerciale (richieste di preventivi, ordini e contratti, informazioni sui prodotti, sui servizi aziendali etc..); alla gestione dei rapporti economici-amministrativi (fatturazione, pagamenti, insoluti…)e per la gestione di rapporti di altra natura (marketing, customer satisfaction..etc)

L'informativa ai Clienti in merito al trattamento dei dati personali deve essere resa al momento del primo contatto con un Cliente ovvero con un potenziale Cliente.

A seconda di quanto possibile/opportuno, l'informativa può essere resa:

- predisponendo una informativa da consegnare materialmente al Cliente/Potenziale Cliente al momento del primo contatto, ovvero al momento della raccolta dei dati personali;
- inserendola nei modelli di preventivo/copia commissione /ordine/contratto;
- rendendola disponibile nel sito web aziendale (ed inserendo in tutti i documenti commerciali/aziendali un rimando alla URL dove è visibile tale informativa)
- spedendola via fax (ed archiviando i fax spediti)
- spedendola via e-mail (ed archiviando le mail inviate)

4.2.2. Consenso

Il consenso del Cliente al trattamento dei suoi dati viene richiesto tramite apposito modulo che riporta tutte le informazioni utili all'interessato: Titolare del Trattamento dei Dati, Repsonsabile del Trattamento, riferimenti telefonici ed altro

4.3. Fornitori

Per i Fornitori valgono le stesse considerazioni espresse per i Clienti, sia per quanto riguarda l'informativa che per quanto riguarda il consenso.
L'informativa può essere formulata utilizzando come riferimento il **modello di informativa per fornitori.**

4.4. Altro

5.4.1 Sito Web .

Qualora nel sito aziendale siano previsti dei form con cui vengono raccolti dati personali degli utenti/navigatori, deve essere fornita una apposita informativa rispondente ai requisiti del Regolamento UE 679 del 2016

L'invio dei dati inseriti nel form da parte degli utenti/navigatori deve essere possibile solo se viene espresso il consenso al trattamento dei dati secondo le finalità espresse.

5. L'organizzazione per la Privacy

Dopo aver provveduto a fornire le informative necessarie e ad aver raccolto i relativi consensi (quando previsto), devono essere realizzate le condizioni che consentono una **gestione "sicura" dei dati raccolti**, ovvero che consentano di ridurre al minimo i rischi di perdita, danneggiamento, furto, accessi e trattamenti non autorizzati.

Pertanto il Titolare del trattamento dei dati deve provvedere a:

- definire e rendere operativa una adeguata **organizzazione per la privacy**;
- definire e rendere operative le **misure minime di sicurezza** previste dal Codice e dalla normativa applicabile.
- Monitorare e sorvegliare la gestione dei dati personali, **definendo opportune azioni di miglioramento (organizzativo e tecnologico)**.

6. I Ruoli e le Responsabilità

In base a quanto previsto dal Regolamento UE 679 del 2016, all'interno dell'organizzazione devono essere previste le seguenti figure, aventi ruoli e responsabilità specifiche per quanto riguarda la gestione e protezione dei dati personali:

- Titolare del trattamento dei dati;
- Responsabili del trattamento dei dati
- Responsabile protezione dati

6.1. Titolare del Trattamento

la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

Il Titolare del trattamento generalmente coincide con l'Organizzazione stessa (L'Azienda nel suo complesso) e tale designazione viene riportata in calce in ogni informativa rilasciata.
Può inoltre essere riportato:

- su un verbale del consiglio di amministrazione
- sul manuale qualità dell'azienda
- su eventuali comunicazioni/circolari interne
- sul sito aziendale
- su qualsiasi altro documento si ritenga necessario.

6.2. Responsabile del trattamento

la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
Possono essere nominati **Responsabili interno o esterni all'azienda.**

I **Responsabili interni**, se nominati, sono scelti tra quei dipendenti che, per ruolo, esperienza, affidabilità, possono cooperare attivamente con il Titolare del trattamento per una corretta ed efficiente gestione dei dati personali da parte di tutti gli interessati. Devono inoltre essere definiti analiticamente i compiti dei Responsabili.
Per le nomine dei Responsabili interni possono essere utilizzate i **modelli di lettera di incarico** allegati alla procedura che dovranno essere accettati e firmati per accettazione.
Per l'individuazione dell'ambito dell'incarico e dei compiti assegnati, possono essere usati i **modelli di mansionario** allegati alla procedura.
Possibili **Responsabili "esterni"** per i quali deve essere prevista una nomina documentata possono essere:

- Consulente del lavoro, Fiscalista, Commercialista

- Medico incaricato
- Azienda servizi assistenza tecnica hardware e software di sistema
- Impresa di pulizie, Impresa di vigilanza
- Consulenti aziendali, Agenti,

Per le relative nomine ed individuazione dell'ambito dell'incarico potranno essere utilizzate i **modelli di lettera di incarico** allegati alla procedura che dovranno essere accettati e firmati per accettazione.
Nella lettera di incarico devono essere specificati in modo analitico i compiti affidati al Responsabile e le istruzioni a cui attenersi.
Eventuali ulteriori modelli potranno essere definiti all'occorrenza, codificati secondo il criterio definito ed inseriti nella presente procedura.

6.3 Mansionari ed organigramma

I mansionari sono definiti in apposito documento

7. Adozione delle Misure minime di sicurezza nei trattamenti con strumenti elettronici

L'adozione delle misure minime di sicurezza nel trattamento dei dati con strumenti elettronici prevede la realizzazione delle seguenti attività:

- Utilizzo di un sistema di autenticazione informatica
- Sistema di autorizzazione
- Installazione ed aggiornamento periodico di programmi antivirus e firewall;
- back up periodici dei dati
- misure per dati sensibili e giudiziari

7.1. Autenticazione informatica

Gli incaricati che trattano dati personali con strumenti elettronici devono accedere a tali dati utilizzando delle **credenziali di autenticazione** ovvero tramite l'utilizzo di **Username** e **Password.**

- Lo **Username** identifica l'utente ed è generalmente di dominio pubblico.
- La **Password** è strettamente riservata, è di almeno 8 caratteri e non deve essere facilmente riconducibile all'interessato.

Nel "Manuale per la sicurezza dei dati personali" sono fornite istruzioni sulla tutela e salvaguardia delle credenziali di autenticazione ed alcune semplici regole per la generazione di password.
Ad ogni incaricato possono essere assegnate una o più credenziali di autenticazione.
Ogni incaricato deve modificare la propria password almeno **ogni sei mesi**. In caso di trattamento di dati sensibili o giudiziari va modificata **ogni tre mesi**.
Qualora l'accesso al PC sia possibile solo tramite uso di password riservate, copia delle password deve essere comunicata anche al Titolare il quale ha il compito di redigere un **elenco credenziali di autenticazione** e di custodirle in un luogo riservato, protetto e sicuro.
Qualora fosse necessario accedere ai dati in assenza del diretto interessato, il Titolare provvederà ad utilizzare la copia delle password in suo possesso, dandone comunicazione (via e-mail, biglietto scritto, telefono, etc) all'interessato.

7.2. Sistema di autorizzazione

Se ritenuto necessario, devono essere previsti dei **profili di autorizzazione** che consentano l'accesso differenziato, per incaricato o per classi omogenee di incaricati, ai soli dati necessari per effettuare le operazioni di trattamento per le quali sono stati incaricati.
La configurazione, aggiornamento e gestione dei profili di autorizzazione è di competenza della [società esterna incaricata della manutenzione hardware] oppure [del responsabile sistemi informatici]

Almeno annualmente deve essere verificata dal Titolare del trattamento la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

7.3. Antivirus e firewall

7.3.1. Antivirus

Ogni postazione di lavoro deve essere dotata di adeguato antivirus.
Gli antivirus installati dovrebbero essere aggiornati **almeno mensilmente.**
A tale proposito sono state definite delle "Linee guida per la prevenzione dei virus" all'interno del "**Raccolta Istruzioni per la sicurezza dei dati personali**" cui si fa riferimento.

7.3.2. Firewall

Nel caso in cui sia presente una rete interna con accesso ad Internet, deve essere prevista la possibilità di installare un firewall di protezione.

La configurazione, aggiornamento e gestione del firewall, antivirus e dell'intera rete è di competenza della [società esterna incaricata della manutenzione hardware] oppure [del responsabile sistemi informatici]

7.4. back-up periodici dei dati

Il Titolare del trattamento, con il supporto eventuale del responsabile e degli Incaricati, definisce gli archivi informatici da sottoporre a back-up periodico e le modalità operative definendo eventualmente specifiche istruzioni scritte. La frequenza minima con cui effettuare i back-up è **settimanale.** La frequenza ed i responsabili individuati per tale attività sono riportati sul DPS:

7.5. Misure per dati sensibili e giudiziari

Eventuali dati sensibili o giudiziari trattati con strumenti elettronici devono essere protetti in modo adeguato.
I supporti rimovibili su cui tali dati sono memorizzati devono essere protetti e custoditi in modo da evitare accessi non autorizzati. Inoltre si prevede che tali supporti, se non utilizzati, siano distrutti o comunque resi inutilizzabili.

8. Adozione delle Misure minime di sicurezza nei trattamenti senza strumenti elettronici

L'adozione delle misure minime di sicurezza nel trattamento dei dati senza strumenti elettronici prevede la realizzazione delle seguenti attività:

- Definizione di adeguate istruzioni scritte agli incaricati finalizzate al controllo ed alla custodia, dei documenti contenenti dati personali durante tutte le operazioni necessarie per i trattamenti da effettuare. Tali istruzioni sono state definite nel "**Raccolta istruzioni per la sicurezza dei dati personali**" allegato alla presente procedura .
- Nel caso in cui gli incaricati trattino documenti contenenti dati sensibili o giudiziari, è responsabilità specifica dell'Interessato controllarli e custodirli fino alla restituzione in modo che non siano accessibili a persone prive di autorizzazione;
- L'accesso ai dati sensibili o giudiziari deve essere controllato. Le persone ammesse a qualunque titolo dopo l'orario di chiusura devono essere identificate e registrate.

9. Scadenze

- **Mensili**: Esecuzione copie di salvataggio dei dati;
- **Semestrali**: Aggiornare gli strumenti elettronici utilizzati al fine di proteggere i dati dal rischio di intrusione e dal rischio derivante da virus informatici
- **Annuali**:
  - Aggiornare l'individuazione dell'ambito di trattamento consentito ai singoli incaricati,

ove variato, anche parzialmente; (revisione mansionari, lettere di nomina..)
- Entro il 31 marzo di ogni anno, redigere il DPS
- Fare menzione dell'avvenuta redazione del DPS e/o del suo aggiornamento annuale nella lettera accompagnatoria del bilancio di esercizio (se dovuta)
- Aggiornare (semestrale per il trattamento di dati sensibili) i software volti a prevenire la vulnerabilità di strumenti elettronici ed a prevenirne i difetti (art. 17, Allegato B)
- Programmare interventi di formazione per gli incaricati del trattamento;
- Effettuare una verifica ispettiva interna per verificare la corretta gestione dei dati

10. Monitoraggi e miglioramento

Annualmente devono essere condotte azioni di monitoraggio allo scopo di verificare se:
- gli adempimenti previsti dal D.lgs 196/2003 ed allegati sono applicati correttamente;
- si rilevano necessità di modificare le attività allo scopo di migliorare e rendere più efficiente la gestione , la sicurezza e la protezione dei dati personali.

Lo strumento utilizzato per il monitoraggio periodico è la conduzione di **verifiche ispettive interne**.
Ogni Verifica ispettiva viene effettuata da un Valutatore incaricato dal Titolare mediante interviste la personale, esami di documenti, osservazioni delle attività e delle condizioni nelle aree interessate, misure ecc.
Quando possibile le informazioni acquisite vengono verificate ricorrendo a fonti indipendenti quali osservazioni alternative, controlli incrociati, ulteriori registrazioni in modo da ottenere così l'evidenza oggettiva di quanto osservato.
Nella conduzione delle Verifiche ispettive, il Valutatore si avvale di una o più "**liste di riscontro"**
Sostanzialmente una lista di riscontro é costituita da un elenco di domande connesse con la documentazione relativa ai processi/funzioni/aree prese in esame.
A fianco delle singole domande vengono previsti degli spazi per segnalare, durante l'indagine,
- il punteggio da assegnare ad ogni domanda (vedi dopo)
- i documenti esaminati/le persone intervistate,
- le non conformità riscontrate
- i provvedimenti da adottare per la risoluzione delle non conformità evidenziate,
- i tempi e le responsabilità connesse con la risoluzione delle non conformità;
- la chiusura(esito dei provvedimenti adottati).

I risultati delle Verifiche Ispettive effettuate sono analizzati ed esaminati dal Titolare del trattamento per:
- valutare eventuali carenze nell'applicazione di quanto stabilito,
- valutare eventuali azioni correttive o preventive da intraprendere
- decidere in merito alla necessità di aggiornare/modificare i contenuti Registro attivita trattamento dati

11. Formazione

Apposita formazione in materia di privacy, gestione dati personali e sicurezza delle informazioni deve essere prevista per:
- i neo assunti
- i nuovi collaboratori
- almeno annualmente a tutto il personale.

La formazione effettuata viene registrata secondo quanto previsto dalle procedure aziendali