ORDINE ASSISTENTI SOCIALI
Consiglio Regionale della Liguria

ORDINE ASSISTENTI SOCIALI

CONSIGLIO REGIONALE DELLA LIGURIA

Via XXV Aprile 16/7 – 16123 Genova

MODELLO ORGANIZZATIVO PRIVACY

ai sensi del Regolamento UE 2016/679

Genova, lì 17/06/2019

Il Titolare del trattamento

……

Edizione	Data	Aggiornamenti	Autore
1.0	17/06/2019	Prima edizione del documento	Il Titolare

ORDINE ASSISTENTI SOCIALI
Consiglio Regionale della Liguria

Indice

1. **Titolarità del trattamento dati**

Il presente Documento è relativo al trattamento dei dati effettuati dal seguente Titolare:

ORDINE ASSISTENTI SOCIALI – CONSIGLIO REGIONALE DELLA LIGURIA

C.F: 95040780108
Sede legale: Via XXV Aprile 16/7 – 16123 Genova
Tel. +39 010 2758830
Email: info@oasliguria.net
PEC: oasliguria@pec.it

Ad esso ci si riferirà, in tutto il seguito del presente documento, come al Modello Organizzativo Privacy (MOP) del Titolare.

Tutte le informazioni qui riportate sono aggiornate a cura del Titolare del trattamento dei dati.

2. **Descrizione generale della struttura aziendale**

Ai fini del presente Modello Organizzativo Privacy (di seguito indicato MOP) la struttura aziendale del Titolare è così riassumibile:

Tipo	**Denominazione**	**Ubicazione**	**Attività svolta**
Sede Legale	**ORDINE ASSISTENTI SOCIALI – CONSIGLIO REGIONALE DELLA LIGURIA**	Via XXV Aprile 16/7 – 16123 Genova	Ordine assistenti sociali

3. **Soggetti preposti ai trattamenti**

3.1 - Uffici preposti ai trattamenti

Nella struttura aziendale si possono identificare le seguenti aree:

Denominazione
Segreteria
Consiglio di disciplina
Archivio
Presidenza

Si precisa che la sede dell'Ordine è chiusa a chiave e non è accessibile a soggetti non autorizzati.

3.3 – Incaricati assegnati ai vari uffici

L'elenco dei dipendenti e degli addetti al trattamento dei dati è disponibile presso l'Ufficio del Personale del Titolare.

Persona	**Qualifica/Soggetto**
Maria Cristina De Vita	Amministrazione
Claudia Pezzo	Amministrazione
Giovanni Cabona	Presidente. Consigliere CROAS
Paola Cermelli	Consigliere Vicepresidente
Daniela Roveda	Consigliere Tesoriere
Marika Massari	Consigliere Segretario

I **componenti del consiglio Regionale** sono soggetti iscritti all'ordine degli assistenti sociali, ai quali viene affidata questa ulteriore carica (per i Consiglieri regionali è elettiva). Hanno 4 cariche (Presidente; Vicepresidente; Segretario; Tesoriere).

Le funzioni che vengono svolte da questi soggetti sono: corretta tenuta dell'Albo; monitoraggio della formazione continua; predisposizione del piano formativo annuale; controllo dei requisiti degli iscritti e relativo invio al Consiglio Territoriale di Disciplina delle comunicazioni di illecito di tipo ordinistico (es. non avere maturato crediti formativi previsti; non avere la PEC; non essere assicurato per chi esercita la libera professione, e in generale la mancanza degli obblighi previsti per essere iscritti all'Ordine); funzione di promozione e tutela della professione.

Per queste finalità: viene tenuto un consiglio al mese; sono presenti 4 commissioni (accreditamento; formazione; etica: politiche sociali) che di norma si trovano una volta al mese in vista del consiglio relativamente alle tematiche di cui si discuterà.

I c**onsiglieri territoriali di disciplina** sono di nomina del Presidente del Tribunale su segnalazione del Consiglio Regionale. Le funzioni sono di tipo disciplinare. Sono formati in 3 collegi. È presente il Presidente e 1 collaboratore.

L'elenco aggiornato dei consiglieri è tenuto dal titolare del trattamento presso gli uffici (ed anche reso noto tramite pubblicazione sul sito).

3.4 – Responsabili esterni

I soggetti che collaborano a vario titolo con il titolare sono i seguenti:

Persona	**Qualifica/Soggetto**
Fondazione Nazionale degli Assistenti Sociali	Studio commercialista

Fondazione Nazionale degli Assistenti Sociali	Consulente del lavoro e Studio paghe
-	Medico Aziendale
-	RSPP - Sicurezza aziendale (L.81/2008) e corsi ai dipendenti
Siges srl	Consulenza privacy e DPO
Gava broker	Assicurazioni
Architetto Andrea Gamba	Tecnico informatico / Manutenzione Hw della rete aziendale (AdS)
Hochfeiler srl	Tecnico informatico (protocollo informatico; albo unico; formazione continua)
Fastweb	Manutenzione sistema Internet Wi-Fi (AdS)
Cooperativa Solidarietà e lavoro ONLUS	Impresa di pulizie

4. Responsabile della Protezione dei dati personali (DPO)

Ai sensi dell'art. 37 del Regolamento UE 2016/679, il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:

a) *il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;*

b) *le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;*

c) *le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.*

Il Titolare, per l'attività svolta rientra categoria indicata dalla lettera a) dell'art. 37 del Regolamento UE 2016/679 e, pertanto, è tenuto alla nomina di un Responsabile per la Protezione dei dati.

Il Responsabile per la protezione dei dati è **SIGES SRL**, P. IVA 01171870122, con sede in via G. Ferrari 21, 21047 Saronno (VA), in persona del Dottor Francesco Re.

Il contatto messo a disposizione dal DPO è telefono **02/9671818** – e-mail **dpo2@sigesgroup.it**

La nomina è stata comunicata all'Autorità Garante ed è stato assegnato il seguente numero di protocollo: **0055927.30/10/2018.**

Ulteriori dettagli sono contenuti nell'ALLEGATO C

5. **Strutture tecnologiche e dettaglio Hardware**

6.1 – Strutture tecnologiche

Il sistema informatico del Titolare è preposto alle seguenti finalità:

- Gestione dell'amministrazione, finanza, contabilità e controllo
- Gestione dei servizi rivolti agli associati
- Gestione documenti in formato elettronico
- Comunicazione e contatto con associati, utenti e altri soggetti

Nello specifico, il dettaglio dei servizi tecnologici disponibili è il seguente:

Servizio	**Sistema**
Sw per gestione accesso ad Internet Wi-Fi dei clienti	
Applicazioni office automation	Microsoft Office
Posta elettronica	Microsoft Office
Sito Internet assistenti sociali	Microsoft Outlook
Navigazione Internet	Chrome
Sistema Antivirus	
Sistema operativo	Windows 7 / 10

La relazione del 14.6.2019 del tecnico IT Architetto Gamba fornisce ulteriori informazioni sulle strutture informatiche. Nello specifico la rete locale è così strutturata:
3 PC con Windows 7 e 10
Attualmente la rete è orizzontale (non sono presenti server centralizzati attualmente)
Ogni client è provvisto di antivirus e firewall
Ogni client è protetto da nome utente e password
Back up automatico del client segreteria
Periodicamente vengono svolte le seguenti attività: aggiornamento sw antivirus; verifica del regolare funzionamento del back up; verifica dello stato del disco rigido
Collegamento LAN/WAN provvisto di firewall.

Il titolare sta comunque pianificando operazioni di implementazione delle misure di sicurezza presenti (in particolare è al vaglio l'utilizzo di file server dedicato su un NAS.

Ulteriori elementi distintivi relativi alla rete informatica, alla connessione ad Internet e ai Personal Computer presenti in azienda, sono disponibili presso l'azienda ed i fornitori dei servizi IT aziendali.

6. Amministratori di sistema

Ai sensi della disposizione del Garante per la Protezione dei Dati Personali riguardante le "misure e accorgimenti prescritti al titolare dei trattamenti con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", emanata il 27 Novembre 2008, si forniscono di seguito gli estremi degli amministratori di sistema designati dal Titolare e dal Responsabile del trattamento, nonché gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato ovvero l'elenco delle funzioni ad essi attribuite.

Elenco dei soggetti incaricati, delle funzioni attribuite (manutenzione interna, teleassistenza, outsourcing) e dei criteri di controllo adottati.

Descrizione	**Addetto**	**Funzioni attribuite**	**Criteri di controllo**
Supervisione del sistema informatico	Andrea Gamba	Controllo semestrale delle seguenti procedure o attività: * account di accesso e password * gestione del cambio delle password periodico * disattivazione account inutilizzati * cartelle e permission * backup	Verifica visiva sull'attività svolta. Lavora in remoto oppure direttamente in loco.
Manutenzione e gestione del data-base on line. Protocollo informatico; albo unico; formazione continua	Hochfeiler srl	Protocollo informatico; albo unico; formazione continua.	Verifica visiva sull'attività svolta. Lavora in remoto dagli uffici di Roma.
Manutenzione del sistema informatico, del firewall e gestione dei salvataggi remoti	Andrea Gamba	Manutenzione in loco sistema informatico, server. Aggiornamenti Sw applicativi e sistema operativo Controllo semestrale delle seguenti procedure o attività: * account di accesso e password * configurazione mail * disattivazione account inutilizzati * cartelle e permission * backup * antivirus * log degli accessi al server * password sul salvaschermo Collegamento in teleassistenza per manutenzione software	Verifica visiva sull'attività svolta. Lavora in remoto oppure direttamente in loco.

7. Azioni di carattere generale attuabili dal Titolare per la protezione dei dati

Vengono di seguito presentate le principali azioni adottabili in tutta la struttura, che prevedono il coinvolgimento non solo del Titolare, dei Responsabili del trattamento (GDPR art. 4.8) e dei responsabili di reparto ma anche dei singoli incaricati al trattamento dei dati, indipendentemente dal fatto che siano dipendenti piuttosto che collaboratori, consulenti, stagisti o dipendenti di aziende terze che collaborano con la struttura.

1) Rispetto ai documenti cartacei gestiti nell'ambito lavorativo e contenenti dati personali:
   a) È necessario verificare che in ogni ufficio non siano presenti documenti cartacei contenenti dati personali, a maggior ragione rispetto ai dati sensibili/particolari (art. 9) non più necessari.
   b) Deve essere quindi effettuata un'attenta analisi rispetto a quali documenti devono essere distrutti perché non più utili ai fini dell'attività lavorativa. Si ricorda che la presenza di ogni documento deve essere giustificata sia in termini di finalità del trattamento, sia in termini di durata di conservazione, da indicare nell'informativa da presentare all'interessato (GDPR art. 13). Si consiglia di mettere a disposizione in ogni ambiente lavorativo di una macchina distruggi-documenti.

2) Rispetto all'accesso ai locali e agli armadi contenenti documenti con dati personali:

a) Verificare che tutti i dati personali, siano sempre conservati in armadi o in uffici sotto chiave, accessibili ai soli addetti autorizzati. Ove questo non sia possibile per ragioni di spazio, tali uffici dovranno essere presidiati e mai lasciati incustoditi (almeno la presenza del portiere). In caso di accesso ai locali da parte di soggetti non autorizzati (es. per l'effettuazione delle pulizie) sarà necessario il controllo continuo da parte di un addetto autorizzato (il c.d. “accesso controllato”).
b) Definire quali soggetti sono autorizzati ad accedere ai dati personali e a quali in particolare, a quali soggetti poter fornire la chiave di accesso all'armadio o al locale, oppure quali soggetti autorizzare in altra modalità. Tale analisi va effettuata per ogni locale, armadio od archivio.
c) Istituire se ritenuto utile un registro per la consegna delle chiavi ai soggetti autorizzati, per poterne monitorare l'accesso a posteriori (GDPR art. 32).

3) Rispetto all'accesso ai personal computer:

a) L'accesso controllato alla rete, ai computer, ai programmi e alle cartelle condivise viene garantito a partire da una corretta politica di gestione delle password. In particolare è necessario verificare che ogni profilo sia associato ad ogni specifico utente (nome utente/login e password), per garantire sia l'accesso ai soli dati personali necessari al singolo utente, sia per monitorare ogni utente rispetto all'accesso al sistema in base ai ruoli stabiliti dal Titolare.

4) Rispetto alla pulizia dei locali:

a) Gli addetti alle pulizie non possono essere nominati incaricati al trattamento dei dati personali, a maggior ragione di quelli sensibili.
b) Le pulizie degli spazi aziendali vanno pianificate e rese possibili solo in almeno una delle seguenti condizioni:
   (1) in caso di accesso autonomo del personale di pulizia, il locale deve essere stato lasciato senza alcun dato personale accessibile, specie se sensibile, sia sulla scrivania o all'interno di armadi o cassetti non chiusi a chiave.
   (2) in caso di impossibilità di garantire il mancato accesso ai dati, perché nel locale non sono presenti armadi o cassetti con chiusura a chiave, è necessario garantire la vigilanza ai dati personali presenti da parte di addetti autorizzati (es. da parte dei fruitori del locale).
   (3) Vanno quindi definite opportune procedure e policy operative.

5) Rispetto ai tempi di conservazione dei dati personali:

a) Per ogni tipologia di dato (amministrativo, eventualmente sanitario, inerente clienti, dipendenti, fornitori) definire i tempi di conservazione, che possono essere già predefiniti da una normativa (dovremo indicarne i riferimenti esatti) oppure scelti dal Titolare.

6) **Rispetto all'attività HARDWARE E DI RETE**

a) Tutti i PC presenti nella rete aziendale devono essere dotati di sistema operativo conforme, ovvero supportato della casa madre rispetto agli aggiornamenti periodici necessari per garantire costante protezione ai fini della sicurezza informatica.

b) Per tutti i PC presenti negli uffici, anche non collegati alla rete aziendale, deve essere presente almeno una password di accesso. Più password (quindi più utenti) se l'accesso avviene da più operatori.

c) Creazione di cartelle condivise preferibilmente dotate di cifratura dei dati, almeno rispetto alla gestione dei dati sensibili.

d) Per garantire adeguata protezione agli attacchi di rete provenienti dall'esterno, è necessario attuare il costante aggiornamenti del software presente nel Firewall di rete.

e) Per quanto concerne il sw utilizzato per l'assistenza remota da parte degli addetti alla manutenzione ai programmi e alla rete, deve essere attivato l'accesso solo se controllato dall'incaricato aziendale, evitando ogni accesso libero.

7) **Rispetto all'attività SOFTWARE**

a) È necessario che il software gestionale presente in azienda risponda ai seguenti requisiti minimi, imposti dalla normativa:
   (1) Accessibilità ai dati solo attraverso credenziali profilate
   (2) Gestione dei profili di accesso così definita:
      - Modificabile e adattabile in base alle singole mansioni
      - Verificabile periodicamente rispetto ai diritti di accesso
      - Rapidamente modificabile in caso di violazioni della sicurezza
   (3) Tracciabilità degli accessi di ogni utente
   (4) Raccomandabile, la cifratura del dato personale, sia per i dati on-line che per i backup

8. **Pianificazione degli interventi formativi da parte del Titolare**

Gli interventi formativi sono svolti in modo continuo a cura del Titolare del trattamento dati. A tutti i dipendenti è consegnato, all'atto dell'entrata in servizio, copia delle norme scritte relative ai trattamenti dati e, più in generale, alla tutela della privacy. Queste norme sono soggette ad aggiornamento costante, sia in caso di modifiche che di mutamento negli incarichi del soggetto. Nel secondo caso è prevista l'eventuale integrazione delle disposizioni scritte già in possesso del dipendente con le ulteriori direttive che dovessero rendersi necessarie.

Corso di formazione	**Descrizione**	**Classi di incarico interessate**	**Numero incaricati coinvolti**	**Calendario**
INZ1	Formazione iniziale del dipendente; consegna delle disposizioni scritte di comportamento per la gestione della privacy	Tutte	Tutti	Permanente a cura del Titolare trattamento dati
INZ2	Formazione eventualmente effettuata mediante affiancamento dei nuovi dipendenti ai colleghi ormai esperti	Tutte	Tutti	Permanente a cura del Titolare trattamento dati
AGG	Aggiornamento delle direttive per cambio incarico o per estensione del precedente incarico; modifica delle direttive e comunicazione agli incaricati	Tutte	Tutti	All'assegnazione del nuovo incarico
PRO	Formazione o aggiornamento direttive a seguito dell'introduzione di nuovi programmi o sistemi informatici	Tutte	Tutti	In occasione dell'introduzione di nuovi programmi o sistemi informatici
CAR	Fornitura di linee guida riassuntive in formato cartaceo	Tutte	Tutti	In occasione della formalizzazione dell'incarico rispetto alla mansione del dipendente

Tali norme interne, individuate dal Titolare, sono raccolte nell'**ALLEGATO B.**

Si riporta di seguito il Registro Storico delle Attività di informazione e formazione in tema di protezione dei dati personali.
Nel registro devono essere annotate sia i corsi di formazione sia la consegna o la pubblicazione presso le bacheche aziendali di materiale informativo.

Titolare del trattamento: Ragione sociale: Sede:		**REGISTRO STORICO DELLE ATTIVITÀ INFORMATIVE E FORMATIVE IN TEMA DI PROTEZIONE DEI DATI PERSONALI**	
Data evento	Tipologia di evento	Soggetti destinatari	Soggetti procedenti
12.06.2019	Sopralluogo ai fini dell'adeguamento alla normativa privacy. Analisi della normativa e della struttura aziendale.	Presidente; Segretario Consigliere.	DPO Dottor Francesco Re; (Siges srl)

9. **Analisi dei rischi e Valutazione di impatto (DPIA)**

Il trattamento dei dati implica alcuni rischi per i diritti e le libertà delle persone fisiche.

L'Analisi dei Rischi è stata effettuata un'apposita relazione in un documento separato, a disposizione del Titolare.

Valutazione di impatto (DPIA).
L'art. 35 del Regolamento UE 2016/679 prevede inoltre che "*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*. […] *La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:*
a) 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;
b) 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 10; o
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico."

In considerazione della tipologia, della natura, dell'oggetto e della finalità del trattamento effettuato dal Titolare,
rilevato il mancato uso di tecnologie particolari per il trattamento di cui sopra,
non si ritiene necessaria alcuna valutazione di impatto privacy ai sensi dell'art. 35 del Regolamento UE 2016/679.

10. **REGISTRO DEI TRATTAMENTI**

Indice dei trattamenti

N. del trattamento	TRATTAMENTO		
	Interessati	**n.**	**Descrizione finalità**
001	Iscritti all'Ordine – eventualmente Consiglieri	001	Gestione della posizione dell'iscritto (iscrizione, cancellazione, trasferimento …)
		002	adempimento di obblighi di legge (ad esempio, adempimenti di natura fiscale, …)
		003	Gestione del servizio di consulenza legale agli iscritti
002	Utenti	001	Gestione richieste e segnalazioni dell'utente (possono essere anche minori o essere relativi a dati particolari)
		002	Adempimento di obblighi derivanti dalle segnalazioni dell'utente
003	Dipendenti e assimilati (Stagisti, Tirocinanti)	001	assolvimento a obblighi derivanti da contratto di lavoro
		002	assolvimento di obblighi legali
004	Fornitori e collaboratori	001	fornitori e collaboratori
		002	adempimenti amministrativi-contabili

GENERALI	**Identificativo trattamento**		**001**
	Categoria di interessati		**ISCRITTI ALL'ORDINE – eventualmente Consiglieri**
	Delegato dal titolare	**Ruolo**	-
		Nominativo	-
		Contatto	-
CONTITOLARI	**Denominazione/Nominativo**		**Assente**
RAPPRESENTANTI	**Denominazione/Nominativo**		**Assente**
001	**Finalità del trattamento**		**GESTIONE DELLA POSIZIONE DELL'ISCRITTO ALL'ORDINE** (gestione dell'iscrizione, cancellazione, trasferimento, variazione indirizzo, formazione continua, gestione albo e formazione continua, procedimenti disciplinari, ecc.)
	Tipologia di dati		Dati personali comuni (es. Nome e Cognome, Paese di provenienza, Email, Telefono, dati anagrafici, titolo di studio, possesso dell'abilitazione all'esercizio della professione di assistente sociale)
	Tipologia di dati Relativamente ai soli Consiglieri		Relativamente ai consiglieri, in aggiunta ai trattamenti effettuati (in quanto i consiglieri sono iscritti all'Ordine) si trattano dati fiscali per i rimborsi di presenza.
	Base giuridica del trattamento		Esecuzione di un contratto di cui l'interessato è parte o applicazione di misure precontrattuali adottate su richiesta dell'Interessato (art. 6, comma 1, lett. b del Regolamento UE 2016/679).
	Formato del dato		Cartaceo e elettronico
	Luogo di conservazione dei dati all'interno della struttura		Uffici della sede dell'ordine (segreteria, archivio)
	Personale addetto		Incaricati addetti agli uffici
	Responsabili del trattamento		Commercialista, tecnico informatico
	Destinatari esterni		Studio Legale in caso di controversie
	Trasferimenti extra UE		-
	Termine di conservazione		Modulistica: durata del rapporto con l'iscritto (i documenti vengono conservati per sempre) Documenti amministrativi/contabili: 10 anni ex art. 2220 c.c. In caso di controversia, per tutta la durata della stessa e per il successivo periodo, pari al termine di prescrizione/decadenza/termine per le impugnazioni.
	Misure di sicurezza tecniche e/o organizzative	**Dati in formato cartaceo**	Documenti raccolti in cartelle. I documenti vengono trasferiti in archivio e conservati per 10 anni.
		Dati in formato elettronico	Profili degli utenti con credenziali personalizzate Antivirus aggiornato Backup su NAS
		Generali	Uffici non accessibili al pubblico. Gli iscritti possono accedere agli uffici solo se autorizzati (citofonando) ed anche in quel caso l'accesso è limitato a locali in cui non avviene alcun trattamento di dati personali.

002	**Finalità del trattamento**		**ADEMPIMENTO DI OBBLIGHI DI LEGGE** (ad esempio, normativa derivante da DPR 137/2012 artt. 7, 8; adempimenti di natura fiscale, contabile-amministrativa, …)
	Tipologia di dati		Dati personali comuni (nome, cognome, data e luogo di nascita, codice fiscale, indirizzo di residenza, numero di carta di identità, …)
	Base giuridica del trattamento		Adempimento di un obbligo legale (Art. 6, comma 1, lettera c) del Regolamento UE 2016/679)
	Formato del dato		Cartaceo e elettronico
	Luogo di conservazione dei dati all'interno della struttura		Uffici della sede dell'Ordine (segreteria, ufficio del presidente, archivio)
	Personale addetto		Incaricati addetti agli uffici
	Responsabili del trattamento		Commercialista; Società manutenzione SW.
	Destinatari esterni		Agenzia delle Entrate, Enti e PP.AA. ai quali devono essere comunicati i dati
	Trasferimenti extra UE		-
	Termine di conservazione		Come richiesto dalla normativa di riferimento. In mancanza di termini stabiliti per legge, i dati verranno conservati per 10 anni o, in caso di controversia, per tutta la durata della stessa e per il successivo periodo, pari al termine di prescrizione/decadenza/termine per le impugnazioni.
	Misure di sicurezza tecniche e/o organizzative	**Dati in formato cartaceo**	documenti raccolti in cartelle. I documenti vengono trasferiti in archivio chiuso a chiave.
		Dati in formato elettronico	Profili degli utenti personalizzati Antivirus aggiornato Backup su NAS
		Generali	Uffici non accessibili al pubblico. Gli iscritti possono accedere agli uffici solo se autorizzati (citofonando) ed anche in quel caso l'accesso è limitato a locali in cui non avviene alcun trattamento di dati personali.
003	**Finalità del trattamento**		**GESTIONE DEL SERVIZIO DI CONSULENZA LEGALE AGLI ISCRITTI**
	Tipologia di dati		Dati personali comuni (nome, cognome, dati relativi al soggiorno o alla presenza in struttura), possibili dati particolari spontaneamente indicati dagli interessati.
	Base giuridica del trattamento		Consenso dell'Interessato (Art. 6, comma 1, lettera a) del Regolamento UE 2016/679)
	Formato del dato		Cartaceo e elettronico
	Luogo di conservazione dei dati		Segreteria, ufficio del Presidente
	Personale addetto		Presidente e personale addetto
	Responsabili del trattamento		Avvocato che presta servizio di consulenza legale

	Destinatari esterni		-
	Trasferimenti extra UE		-
	Termine di conservazione		Periodo necessario per la consulenza ed eventuali giudizi, oltre a termine legale di prescrizione.
	Misure di sicurezza tecniche e/o organizzative	**Dati in formato cartaceo**	documenti raccolti in cartelle. I documenti vengono trasferiti in archivio chiuso a chiave.
		Dati in formato elettronico	Profili degli utenti con credenziali personalizzate Antivirus aggiornato Backup su NAS
		Generali	Uffici non accessibili al pubblico. Gli iscritti possono accedere agli uffici solo se autorizzati (citofonando) ed anche in quel caso l'accesso è limitato a locali in cui non avviene alcun trattamento di dati personali.

GENERALI	**Identificativo trattamento**		**002**
	Categoria di interessati		**UTENTI**
	Delegato dal titolare	**Ruolo**	-
		Nominativo	-
		Contatto	-
CONTITOLARI	**Denominazione/Nominativo**		**Assente**
RAPPRESENTANTI	**Denominazione/Nominativo**		**Assente**
001	**Finalità del trattamento**		**GESTIONE RICHIESTE E SEGNALAZIONI DELL'UTENTE** (come: segnalazioni, richieste di informazioni, anche richieste al consiglio territoriale di disciplina e quello che ne consegue …)
	Tipologia di dati		Dati personali comuni (Nome, cognome, contatti, ecc.). Dati personali particolari solo se spontaneamente comunicati dall'interessato.
	Base giuridica del trattamento		Esecuzione di un contratto di cui l'interessato è parte (art. 6, comma 1, lett. b del Regolamento UE 2016/679).
	Formato del dato		Cartaceo ed elettronico su PC
	Luogo di conservazione dei dati all'interno della struttura		Ufficio del Presidente e segreteria
	Personale addetto		Direttore e personale autorizzato
	Responsabili del trattamento		Società manutenzione informatica
	Destinatari esterni		Soggetti destinatari di comunicazioni o Autorità Giudiziarie. Studio legale in caso di controversia

	Trasferimenti extra UE		-
	Termine di conservazione		Periodo necessario per evadere le richieste o termini di legge in caso di controversie. In caso di controversia, per tutta la durata della stessa e per il successivo periodo, pari al termine di prescrizione/decadenza/termine per le impugnazioni.
	Misure di sicurezza tecniche e/o organizzative	**Dati in formato cartaceo**	Documenti raccolti in cartelle. I documenti vengono trasferiti in archivio chiuso a chiave.
		Dati in formato elettronico	Profili degli utenti con credenziali personalizzate Antivirus aggiornato Backup su NAS
		Generali	Uffici non accessibili al pubblico. Gli iscritti possono accedere agli uffici solo se autorizzati (citofonando) ed anche in quel caso l'accesso è limitato a locali in cui non avviene alcun trattamento di dati personali.
002	**Finalità del trattamento**		**ADEMPIMENTO DI OBBLIGHI DERIVANTI DALLE SEGNALAZIONI DELL'UTENTE** Giunta una segnalazione da parte dell'utente, l'ordine la trasmette al Presidente del Consiglio Territoriale di Disciplina (senza entrare nel merito della questione). Una volta terminato il procedimento, l'Ordine pubblica l'esito se viene richiesto oppure prende atto dell'archiviazione. La segnalazione può anche non derivare da una segnalazione, ma di iniziativa dell'Ordine.
	Tipologia di dati		Dati personali comuni, dati personali particolari
	Base giuridica del trattamento		Per i dati comuni Adempimento di un obbligo legale al quale è soggetto il titolare del trattamento (art. 6, comma 1, lett. c del Regolamento UE 2016/679). Per i dati particolari: Assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato, nella misura in cui sia autorizzato dal diritto dell'unione Europea o del diritto Italiano o da un contratto collettivo ai sensi del diritto dell'Unione Europea o del diritto Italiano (art. 9, comma 1, lett. b del Regolamento UE 2016/679).
	Formato del dato		Cartaceo e elettronico su PC, Software gestionale e server
	Luogo di conservazione dei dati all'interno della struttura		Ufficio del Presidente, segreteria, archivio
	Personale addetto		Presidente e personale addetto
	Responsabili del trattamento		Società manutenzione software gestionale
	Destinatari esterni		destinatari di comunicazioni obbligatorie o Autorità Giudiziarie
	Trasferimenti extra UE		-
	Termine di conservazione		Come richiesto dalla normativa di riferimento. In caso di controversia, per tutta la durata della stessa e per il successivo periodo, pari al termine di prescrizione/decadenza/termine per le impugnazioni.
	Misure di sicurezza tecniche e/o organizzative	**Dati in formato cartaceo**	Documenti raccolti in cartelle. I documenti vengono trasferiti in archivio chiuso a chiave.
		Dati in formato elettronico	Profili degli utenti con credenziali personalizzate Antivirus aggiornato Backup su NAS

		generali	Uffici non accessibili al pubblico. Gli iscritti possono accedere agli uffici solo se autorizzati (citofonando) ed anche in quel caso l'accesso è limitato a locali in cui non avviene alcun trattamento di dati personali.

GENERALI	**Identificativo trattamento**		**003**
	Categoria di interessati		**DIPENDENTI E ASSIMILATI (stagisti, tirocinanti)**
	Delegato dal titolare	**Ruolo**	-
		Nominativo	-
		Contatto	-
CONTITOLARI	**Denominazione/Nominativo**		**Assente**
RAPPRESENTANTI	**Denominazione/Nominativo**		**Assente**
001	**Finalità del trattamento**		**GESTIONE RAPPORTO DI LAVORO** (come: selezione, assunzione, dimissioni, licenziamento, ferie, permessi, malattia, gestione presenze, comunicazioni aziendali, …)
	Tipologia di dati		Dati personali comuni (Nome, cognome, luogo e data di nascita, codice fiscale, residenza/domicilio, carta di identità, CV, contatti, dati bancari, ecc.). Dati personali particolari (come appartenenza a categorie protette, idoneità del lavoratore, iscrizione a sindacati, associazioni, ecc.).
	Base giuridica del trattamento		Esecuzione di un contratto di cui l'interessato è parte (art. 6, comma 1, lett. b del Regolamento UE 2016/679).
	Formato del dato		Cartaceo ed elettronico su PC
	Luogo di conservazione dei dati all'interno della struttura		Ufficio del Presidente, segreteria
	Personale addetto		Presidente e addetti autorizzati al trattamento
	Responsabili del trattamento		Società manutenzione informatica, Commercialista, Studio paghe e contributi, Settore Igiene e sicurezza del lavoro, Settore formazione del personale
	Destinatari esterni		Ministero del Lavoro - Ispettorato territoriale del lavoro - INPS – INAIL e altri destinatari di comunicazioni obbligatorie. Soggetti destinatari di comunicazioni da parte del datore di lavoro su richiesta del lavoratore o di Autorità Giudiziarie. Studio legale in caso di controversia
	Trasferimenti extra UE		-
	Termine di conservazione		Come richiesto dalla normativa di riferimento. In mancanza di termini stabiliti per legge, i dati verranno conservati per tutta la durata del rapporto di lavoro e per i 10 anni successivi. In caso di controversia, per tutta la durata della stessa e per il successivo periodo, pari al termine di prescrizione/decadenza/termine per le impugnazioni.
	Misure di sicurezza tecniche e/o organizzative	**Dati in formato cartaceo**	Documenti raccolti in cartelle. I documenti vengono trasferiti in archivio chiuso a chiave.
		Dati in formato elettronico	Profili degli utenti con credenziali personalizzate Antivirus aggiornato Backup su NAS

		Generali	Uffici non accessibili al pubblico. Gli iscritti possono accedere agli uffici solo se autorizzati (citofonando) ed anche in quel caso l'accesso è limitato a locali in cui non avviene alcun trattamento di dati personali.
002	**Finalità del trattamento**		**ASSOLVIMENTO DI OBBLIGHI LEGALI**
	Tipologia di dati		Dati personali comuni, dati personali particolari
	Base giuridica del trattamento		Per i dati comuni Adempimento di un obbligo legale al quale è soggetto il titolare del trattamento (art. 6, comma 1, lett. c del Regolamento UE 2016/679). Per i dati particolari: Assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia del diritto del lavoro e della sicurezza e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'unione Europea o del diritto Italiano o da un contratto collettivo ai sensi del diritto dell'Unione Europea o del diritto Italiano (art. 9, comma 1, lett. b del Regolamento UE 2016/679).
	Formato del dato		Cartaceo e elettronico su PC, Software gestionale e server
	Luogo di conservazione dei dati all'interno della struttura		Ufficio del Presidente, segreteria
	Personale addetto		Presidente e personale autorizzato
	Responsabili del trattamento		Società manutenzione informatica, Commercialista, Studio paghe e contributi, Settore Igiene e sicurezza del lavoro, Settore formazione del personale, Medico competente
	Destinatari esterni		Ministero del Lavoro - Ispettorato territoriale del lavoro - INPS – INAIL e altri destinatari di comunicazioni obbligatorie. Soggetti destinatari di comunicazioni da parte del datore di lavoro su richiesta del lavoratore o di Autorità Giudiziarie
	Trasferimenti extra UE		-
	Termine di conservazione		Come richiesto dalla normativa di riferimento. In mancanza di termini stabiliti per legge, i dati verranno conservati per tutta la durata del rapporto di lavoro e per i 10 anni successivi. In caso di controversia, per tutta la durata della stessa e per il successivo periodo, pari al termine di prescrizione/decadenza/termine per le impugnazioni.
	Misure di sicurezza tecniche e/o organizzative	**Dati in formato cartaceo**	Documenti raccolti in cartelle. I documenti vengono trasferiti in archivio chiuso a chiave.
		Dati in formato elettronico	Profili degli utenti con credenziali personalizzate Antivirus aggiornato Backup su NAS
		generali	Uffici non accessibili al pubblico. Gli iscritti possono accedere agli uffici solo se autorizzati (citofonando) ed anche in quel caso l'accesso è limitato a locali in cui non avviene alcun trattamento di dati personali.

GENERALI	**Identificativo trattamento**		**004**
	Categoria di interessati		**FORNITORI E COLLABORATORI**
	Delegato dal titolare	**Ruolo**	-
		Nominativo	-
		Contatto	-
CONTITOLARI	**Denominazione/Nominativo**		**Assente**
RAPPRESENTANTI	**Denominazione/Nominativo**		**Assente**
001	**Finalità del trattamento**		**GESTIONE DEL RAPPORTO CONTRATTUALE** (es: stipulazione del contratto, gestione ordini, resi, gestione pagamenti, ecc.)
	Tipologia di dati		Dati personali comuni: denominazione ditta individuale, partita IVA/codice fiscale, nome e cognome, dati di contatto, indirizzo. Dati comuni dei referenti dei fornitori.
	Base giuridica del trattamento		Esecuzione di un contratto di cui l'interessato è parte (art. 6, comma 1, lett. b del Regolamento UE 2016/679).
	Formato del dato		Cartaceo e elettronico su PC, Software gestionale e server
	Luogo di conservazione dei dati all'interno della struttura		Ufficio del Presidente, segreteria, archivio
	Personale addetto		Presidente, personale autorizzato
	Responsabili del trattamento		Commercialista; Società manutenzione SW.
	Destinatari esterni		Studio legale in caso di controversia
	Trasferimenti extra UE		-
	Termine di conservazione		Come richiesto dalla normativa di riferimento. In mancanza di termini stabiliti per legge, i dati verranno conservati per tutta la durata del rapporto contrattuale e per i 10 anni successivi. In caso di controversia, per tutta la durata della stessa e per il successivo periodo, pari al termine di prescrizione/decadenza/termine per le impugnazioni.
	Misure di sicurezza tecniche e/o organizzative	**Dati in formato cartaceo**	Documenti raccolti in cartelle. I documenti vengono trasferiti in archivio chiuso a chiave.
		Dati in formato elettronico	Profili degli utenti con credenziali personalizzate Antivirus aggiornato Backup su NAS
		generali	Uffici non accessibili al pubblico. Gli iscritti possono accedere agli uffici solo se autorizzati (citofonando) ed anche in quel caso l'accesso è limitato a locali in cui non avviene alcun trattamento di dati personali.
002	**Finalità del trattamento**		**ADEMPIMENTI OBBLIGHI DI LEGGE** (come obblighi amministrativi-contabili, fiscali, …)

	Tipologia di dati		Dati personali comuni: denominazione ditta individuale, partita IVA/codice fiscale, nome e cognome, dati di contatto, indirizzo. Dati comuni dei referenti dei fornitori.
	Base giuridica del trattamento		Adempimento di un obbligo legale al quale è soggetto il titolare del trattamento (art. 6, comma 1, lett. c del Regolamento UE 2016/679).
	Formato del dato		Cartaceo e elettronico su PC, Software gestionale e server
	Luogo di conservazione dei dati all'interno della struttura		Ufficio del Presidente, segreteria, archivio
	Personale addetto		Presidente, personale autorizzato
	Responsabili del trattamento		Commercialista; Società manutenzione SW.
	Destinatari esterni		Agenzia delle Entrate, Altri destinatari di comunicazioni obbligatorie per legge
	Trasferimenti extra UE		-
	Termine di conservazione		Come richiesto dalla normativa di riferimento. In mancanza di termini stabiliti per legge, i dati verranno conservati per tutta la durata del rapporto contrattuale e per i 10 anni successivi. In caso di controversia, per tutta la durata della stessa e per il successivo periodo, pari al termine di prescrizione/decadenza/termine per le impugnazioni.
	Misure di sicurezza tecniche e/o organizzative	**Dati in formato cartaceo**	Documenti raccolti in cartelle. I documenti vengono trasferiti in archivio chiuso a chiave.
		Dati in formato elettronico	Profili degli utenti con credenziali personalizzate Antivirus aggiornato Backup su NAS
		Generali	Uffici non accessibili al pubblico. Gli iscritti possono accedere agli uffici solo se autorizzati (citofonando) ed anche in quel caso l'accesso è limitato a locali in cui non avviene alcun trattamento di dati personali.

ORDINE ASSISTENTI SOCIALI
Consiglio Regionale della Liguria

ALLEGATO A: PROCEDURE INTERNE

Titolo	**Responsabile dell'applicazione**	**Data di consegna ai dipendenti**
Regole generiche/di base	Il Titolare	
Procedura in caso di Data Breach	Il Titolare	
Regolamento per il funzionamento del Consiglio regionale		Presente sul sito dell'Ordine
Regolamento di amministrazione contabile (RAC)		Presente sul sito dell'Ordine
Manuale delle procedure amministrative		Cartaceo. Disponibile presso gli uffici del Titolare.
Regolamento commissione consultiva per l'autorizzazione e formazione continua CROAS Emilia Romagna		Presente sul sito dell'Ordine.
Regolamento per il funzionamento del procedimento disciplinare locale		Cartaceo. Disponibile presso gli uffici del Titolare.
Regolamento dei compensi e dei rimborsi		Presente sul sito dell'Ordine.
Regolamento per la formazione continua ai sensi del d.p.r. 137/2012		

11. **Procedure interne: regole generiche/di base**

1) Disposizioni generali per la gestione delle password

Ovunque sia indispensabile l'utilizzo di password per l'autenticazione di accessi al sistema informatico o la protezione di file riservati, la gestione delle stesse dovrà avvenire nel rispetto di tutte le norme di legge e delle misure previste per la tutela della privacy e la sicurezza del sistema informativo aziendale. In particolare dovranno essere osservate con scrupolo le seguenti misure specifiche.

Tutte le password aziendali sono considerate informazioni altamente confidenziali che non possono essere comunicate ad alcun soggetto non autorizzato. Le password personali sono segrete e non devono essere comunicate ad alcun soggetto. Le password personali che vincolano l'utilizzo di una risorsa aziendale (es. password di bios,) oppure di un file od un archivio elettronico devono essere consegnate in busta chiusa al responsabile aziendale delle password affinché possa utilizzarle in caso di bisogno.

Ogni singolo soggetto è responsabile della tutela della segretezza delle password aziendali di cui ha conoscenza; la tutela della segretezza delle password personali è in carico esclusivamente al singolo utente. Le password personali non vanno scritte o annotate.

Le password devono essere lunghe **almeno otto caratteri** e non debbono contenere elementi facilmente riconducibili al singolo utente cui si riferiscono (es. nome, cognome, data nascita ecc.), né devono essere tratte da elementi troppo evidenti rispetto al contesto ambientale o aziendale. Ove non fosse possibile l'utilizzo di otto caratteri si dovrà utilizzare il numero massimo fra quelli disponibili.

Le password devono essere cambiate con una frequenza almeno semestrale. In caso di trattamenti di dati sensibili o giudiziari le password vanno cambiate con frequenza almeno trimestrale.

Le password già utilizzate non vanno più usate in successivi cambiamenti delle parole di accesso. Ad ogni rotazione le nuove password devono essere originali. Laddove è possibile le nuove password non devono essere frutto di elaborazioni basate sulle vecchie, né derivare da regole predefinite di composizione.

2) Norme generali sull'uso delle postazioni di lavoro

L'utilizzo abituale o saltuario delle postazioni di lavoro (pc, terminali, server ecc.) dovrà avvenire nel pieno rispetto di tutte le norme di legge e delle misure previste per la tutela della privacy e la sicurezza del sistema informatico aziendale. In particolare dovranno essere osservate con scrupolo le seguenti misure specifiche:

L'utilizzo delle postazioni di lavoro è riservato unicamente ai fini aziendali. Nessun uso privato è consentito, salvo che non venga esplicitamente autorizzato per iscritto dai responsabili aziendali. L'uso delle postazioni di lavoro per scopi privati avverrà in ogni caso nel rispetto delle stesse modalità e delle stesse procedure stabilite per l'uso aziendale. In particolare, nessuna deroga è ammessa per il rispetto delle norme di legge e per le misure finalizzate alla tutela della riservatezza, alla continuità ed alla sicurezza del sistema informatico aziendale.

L'accesso alle postazioni di lavoro dovrà essere svolto nel rispetto dei sistemi di autenticazione posti a protezione del sistema informatico. Ciascun utente è responsabile per la tutela delle proprie password di accesso e si impegna a non diffonderne la conoscenza ad alcun soggetto.

Le password vincolanti per l'uso di una postazione o di un software dovranno essere consegnate in busta chiusa al responsabile delle password. Per ogni altra direttiva qui non specificata in merito alle password si dovrà fare riferimento alle norme generali per la loro gestione (vedasi relativo documento).

La postazione di lavoro è conservata dagli utenti nelle medesime condizioni in cui essa è consegnata ad inizio del turno di lavoro o all'atto della presa in carico. Ogni utente è responsabile della manutenzione ordinaria (es. pulizia video, tastiera o mouse, accensione e spegnimento corretti, scansione antivirus periodica ecc.) della postazione a lui assegnata o di cui usufruisce temporaneamente. Particolare cura dovrà essere adottata nella gestione di apparecchiature portatili quali notebook, palmari o simili. Nessuna manomissione è possibile sulla postazione, ivi compresa l'installazione di apparecchiature o altro hardware non autorizzato. Per qualsiasi necessità occorrerà fare riferimento al responsabile del sistema informatico.

Sulle postazioni di lavoro dovranno essere installati programmi (antivirus, firewall ecc.) posti a protezione delle postazioni stesse e, più in generale, del sistema informatico. Essi non dovranno mai essere disinstallati e dovranno essere soggetti ad aggiornamento costante. Per le postazioni che non dispongano di accessi alla rete Internet

e per le postazioni stand-alone dovranno essere esse in atto opportune soluzioni per consentire anche a queste di ricevere gli aggiornamenti necessari (uso di cartelle in rete, aggiornamento manuale, uso di supporti).

In caso di abbandono temporaneo della postazione di lavoro si dovranno abilitare quei sistemi necessari per ad impedirne l'uso da parte di terzi non autorizzati (es. salvaschermo con password). In mancanza di tali sistemi si dovrà terminare ogni sessione di lavoro prima di abbandonare la postazione e, nei casi estremi, procedere al suo spegnimento. La postazione va resa inaccessibile o spenta anche al termine dell'orario di lavoro o in caso di assenza prolungata.

Nessun programma o pacchetto d'installazione va inserito, scaricato o installato sulle postazioni di lavoro se non autorizzato. L'installazione di programmi è riservata al responsabile del sistema informatico. Ad esso ci si dovrà rivolgere per la manutenzione dei programmi di ciascuna postazione.

L'uso di supporti di memorizzazione removibili, in lettura o in scrittura, è limitato agli scopi aziendali. In particolare, il salvataggio di dati al di fuori delle procedure di back-up aziendali deve essere autorizzato. La conservazione di tali supporti, laddove possibile, dovrà avvenire negli stessi spazi dedicati al back-up aziendale o, in alternativa, in apposito luogo indicato dal responsabile della privacy e della sicurezza sui dati. Nessun altro utilizzo è possibile per tali supporti e dei dati ivi contenuti al di fuori del ripristino dei dati stessi in caso di bisogno.

3) Norme generali sull'uso della posta elettronica

L'utilizzo abituale o saltuario della posta elettronica come strumento di comunicazione dovrà avvenire nel pieno rispetto di tutte le norme di legge e delle misure previste per la tutela della privacy e la sicurezza del sistema informatico aziendale. In particolare dovranno essere osservate con scrupolo le seguenti misure specifiche:

L'utilizzo della posta elettronica è riservato unicamente ai fini aziendali. Nessun uso privato è consentito, salvo che non venga esplicitamente autorizzato per iscritto dai responsabili aziendali. Garantire il rispetto delle norme di legge e per le misure finalizzate alla tutela della riservatezza e della sicurezza del sistema informatico aziendale.

Laddove possibile si dovrà procedere all'archiviazione dei file contenenti i messaggi.

L'archiviazione dei file di posta dovrà avvenire non sulla postazione di lavoro personale ma in apposita cartella riservata sul server gestionale o documentale, ai fini del salvataggio di back-up. L'archiviazione della posta elettronica dovrà essere impostata su cadenza giornaliera.

L'accesso alle cartelle personali ed aziendali dovrà avvenire laddove possibile solo con l'uso di una password. La password per gli archivi di posta elettronica dovrà essere indicata in una busta chiusa consegnata al responsabile delle password. Il cambio della password di posta dovrà avvenire almeno semestralmente o trimestralmente se le mail possono contenere dati di tipo sensibile. La password dovrà essere di almeno otto caratteri alfanumerici e non dovrà contenere elementi facilmente riferibile all'utente come nome, cognome, data di nascita ecc. Per ogni altra direttiva qui non specificata in merito alle password si dovrà fare riferimento alle norme generali per la loro gestione (vedasi relativo documento).

La spedizione di messaggi di posta potrà avvenire solo a condizione che venga inserito in coda allo stesso il seguente messaggio, se necessario anche in lingua inglese per eventuali destinatari stranieri:

> *Le informazioni trasmesse in questa mail sono da considerarsi dati riservati destinati esclusivamente alla persona e/o alla società a cui sono indirizzati. Qualsiasi modifica, inoltro, diffusione o altro utilizzo delle informazioni qui trasmesse da parte di persone e/o società diverse dai destinatari indicati è proibito ai sensi del Regolamento UE 2016/679 e della legge 196/2003. Se Lei ha ricevuto questa mail per errore, per favore contatti il mittente e cancelli queste informazioni da ogni computer.*
>
> *This e-mail contains confidential information. Please do not read it if you are not the intended recipient(s). Any use, distribution, reproduction or disclosure by any other person is strictly prohibited in accordance to the REGULATION (EU) 2016/679 and the Italian Legislative Decree 196/2003. If you have received this e-mail in error, please notify the sender and destroy the original transmission and its attachments without reading or saving it in any manner.*

La spedizione di messaggi di posta elettronica a più soggetti destinatari non direttamente collegati tra loro dovrà avvenire avendo cura di inserire tali indirizzi plurimi nell'area di destinazione riservata (Ccn), così da tutelare i diritti dei singoli alla riservatezza sui propri indirizzi mail.

I messaggi di posta contenenti dati personali, in particolare dati sensibili, dovranno essere soggetti a criptazione. Qualora non si disponga di un sistema di criptazione valida, tali dati non dovranno essere inseriti in chiaro nel messaggio ma allegati in apposito file. Il file allegato dovrà essere esso stesso criptato o protetto da password per l'accesso oppure, in alternativa, dovrà contenere dati privi di qualsiasi elemento anagrafico in grado di identificare, direttamente o indirettamente, il soggetto cui le informazioni si riferiscono. Gli elementi anagrafici necessari all'interpretazione dei file allegati, se possibile, dovranno essere inviati per vie diverse al destinatario o, quantomeno, in mail separate, possibilmente dirette a due indirizzi diversi riferiti al destinatario. La trasmissione delle password di apertura degli allegati ai destinatari dovrà avvenire con una procedura ad hoc, se possibile non con l'uso della posta elettronica. Per clienti, fornitori ed altri soggetti con i quali l'azienda possa entrare in contatto l'elenco delle password per gli allegati sarà fornito dal responsabile delle password.

La ricezione, l'apertura, la lettura, il salvataggio, la copia o l'inoltro di messaggi o allegati dovrà avvenire solo a condizione di essere i destinatari della comunicazione. Nel caso di errori di spedizione si dovrà provvedere all'eliminazione completa dalla propria postazione del messaggio e degli eventuali allegati, segnalando laddove possibile l'errore al mittente. In caso di ricevimento di posta indesiderata si dovrà procedere alla segnalazione del fatto al mittente e alla richiesta di eliminazione del proprio indirizzo dalla sua mailing-list. Laddove necessario si dovrà provvedere a comunicare l'indirizzo del mittente al responsabile del sistema informatico, affinché egli possa provvedere ad impostare l'eventuale filtro anti-spamming sul sistema di firewall aziendale. In mancanza si dovrà provvedere quanto meno all'impostazione del filtro sulla postazione di lavoro personale.

4) Norme generali per l'uso degli archivi aziendali elettronici

L'utilizzo, abituale o saltuario degli archivi aziendali elettronici, in special modo quelli contenenti dati personali e sensibili, dovrà avvenire nel pieno rispetto di tutte le norme di legge e delle misure previste per la tutela della privacy e la sicurezza del sistema informativo aziendale. In particolare dovranno essere osservate con scrupolo le seguenti misure specifiche:

L'utilizzo dei file o degli archivi aziendali è riservato unicamente ai fini aziendali. Nessun altro uso è consentito.

L'accesso agli archivi dovrà essere svolto nel rispetto dei sistemi di autenticazione posti a protezione del sistema informatico. Ciascun utente è responsabile per la tutela delle proprie password d'accesso e s'impegna a non diffonderne la conoscenza ad alcun soggetto. Le password vincolanti per l'uso di una postazione o di un software dovranno essere consegnate in busta chiusa al responsabile delle password. Per ogni altra direttiva qui non specificata in merito alle password si dovrà fare riferimento alle norme generali per la loro gestione (vedasi relativo documento).

Ogni utente è autorizzato al trattamento di file e archivi aziendali solo nei limiti della propria lettera d'incarico al trattamento dati e delle proprie mansioni. Nessun altro trattamento è autorizzato al di fuori di quelli previsti per ogni utente. Grande attenzione dovrà essere posta alla prevenzione dei rischi generali e di quelli specifici evidenziati nelle lettere d'incarico di ciascun utente, avendo cura di rispettare scrupolosamente le misure di tutela indicate.

All'infuori delle procedure previste per il back-up dei dati, nessuna copia di file o archivio può essere creata se essa non è strettamente indispensabile allo svolgimento dell'attività aziendale, a condizione che ciò rientri nelle normali mansioni svolte dall'utente. Se l'originale di un file od un archivio è eliminato anche tutte le copie esistenti in azienda dovranno subire ugual sorte.

Nessuna comunicazione, trasmissione, diffusione o altro trattamento destinato a terzi di file o archivi aziendali, o di parti di essi, è autorizzata se i terzi non rientrano fra i soggetti incaricati o responsabili del trattamento dei dati trasmessi. In particolare, nel caso di dati sensibili o di particolare rilevanza per la sicurezza, i diritti e la dignità dell'interessato, nessuno dei trattamenti sopra citati è possibile se non in presenza di un'autorizzazione legale o del consenso scritto dell'interessato. Ciascun incaricato è tenuto ad accertarsi dell'esistenza di tale autorizzazione o consenso prima di eseguire il trattamento dati. In caso di dubbi o problemi, occorre fare riferimento ai propri responsabili gerarchici e/o al responsabile per la sicurezza e la privacy.

Qualsiasi trattamento dati che comporti la comunicazione, la trasmissione o l'accesso a file o archivi aziendali che contengano dati di un soggetto è sempre possibile, limitatamente alle informazioni di sua pertinenza, se è effettuato dal soggetto stesso o se esso ne è il destinatario. Ciò, tuttavia, solo a condizione che si adottino tutte le misure qui previste per la tutela dall'accesso indesiderato, anche accidentale, ai dati.

5) Norme generali per la navigazione in Internet e la trasmissione dati

L'utilizzo, abituale o saltuario, della navigazione internet e di qualsiasi altro strumento di trasmissione dati per via telematica come strumento di lavoro dovrà avvenire nel pieno rispetto di tutte le norme di legge e delle misure previste per la tutela della privacy e la sicurezza del sistema informatico aziendale. In particolare dovranno essere osservate con scrupolo le seguenti misure specifiche:

L'utilizzo della navigazione o degli strumenti telematici è riservato unicamente ai fini aziendali. Nessun uso privato è consentito, salvo che non venga esplicitamente autorizzato per iscritto dai responsabili aziendali. L'uso per scopi privati avverrà in ogni caso nel rispetto delle stesse modalità e delle stesse procedure stabilite per l'uso aziendale. In particolare, nessuna deroga è ammessa per il rispetto delle norme di legge e per le misure finalizzate alla tutela della riservatezza e della sicurezza del sistema informatico aziendale.

È vietato ogni accesso a siti illegali o il cui contenuto possa recare offesa, disturbo o nocumento, diretto o indiretto, all'azienda, ai suoi collaboratori o a coloro che si trovino ad avere rapporti con essa. È altresì vietato l'accesso a siti che possano rappresentare un pericolo presente o potenziale per l'azienda. È vietata la partecipazione a Newsgroup, Chat Line o altre modalità simili di contatto on-line

Nessun dato potrà essere comunicato, scaricato o inviato da o verso l'azienda se non nell'ambito della normale attività di lavoro e a condizione che ciò rientri nei limiti delle proprie lettere d'incarico al trattamento dati. I dati personali così ricevuti dovranno essere gestiti secondo le direttive aziendali riguardanti il loro trattamento. I dati personali così inviati dovranno essere destinati solo ed esclusivamente a soggetti autorizzati al loro trattamento. In caso di dubbi o problemi si dovrà fare riferimento ai propri superiori gerarchici e/o al responsabile della sicurezza e della privacy.

Nessun programma o applicazione o pacchetto d'installazione potrà essere scaricato dalla rete.
L'unico soggetto autorizzato a tale attività è il responsabile del sistema informatico. A lui si dovrà fare riferimento in caso di necessità.

Nessun accesso a sistemi di terzi (via ftp, telnet, emulazione ecc.) che comporti il trattamento di dati personali è autorizzato, salvo che tale accesso non sia stato concordato con i terzi stessi. In tal caso l'accesso dovrà avvenire a condizione che sussista presso i terzi un idoneo sistema di autenticazione e che sia garantito la riservatezza sulla propria password di accesso.

È vietato agli utenti procedere ad acquisti via internet o assumere impegni od ogni altra obbligazione in nome o per conto dell'azienda salvo che non si disponga delle necessarie autorizzazioni e ciò rientri nella normale attività svolta dagli utenti stessi.

6) Norme generali per il trattamento di documenti cartacei

Il trattamento abituale o saltuario di documenti cartacei, in special modo quelli contenenti dati personali, dovrà avvenire nel pieno rispetto di tutte le norme di legge e delle misure previste per la tutela della privacy e la sicurezza del sistema informativo aziendale. In particolare dovranno essere osservate con scrupolo le seguenti misure specifiche:

L'utilizzo dei documenti aziendali è riservato unicamente ai fini aziendali. Nessun altro uso è consentito.

Ciascun soggetto è responsabile della conservazione e della tutela dei documenti cartacei in proprio possesso, anche in via temporanea. I documenti vanno protetti in ogni momento dall'accesso di terzi non autorizzati alla loro consultazione.

La creazione, il prelevamento o la consultazione di documenti devono avvenire solo in caso di effettivo bisogno. Nessun documento non necessario agli scopi aziendali va detenuto o archiviato: in particolare, i documenti contenenti dati personali non più utili vanno distrutti. Nel caso che i supporti cartacei vengano riciclati per altri usi, i dati personali in essi presenti devono essere resi illeggibili.

Nessuna copia dei documenti in proprio possesso può essere fatta salvo che non sia utile agli scopi aziendali. In caso di distruzione o cancellazione del documento originale, anche tutte le copie eventualmente esistenti in azienda dovranno subire la stessa sorte.

La conservazione dei documenti deve avvenire esclusivamente nei raccoglitori, nelle strutture o nelle aree aziendali destinate all'archiviazione. Nel caso vi sia la necessità di detenere documenti cartacei per lungo periodo, la conservazione degli stessi dovrà avvenire, laddove possibile, in appositi uffici, scaffali, cassetti o raccoglitori chiusi all'accesso di terzi. Nessun documento dovrà essere lasciato in vista sulle scrivanie durante le assenze prolungate o dopo l'orario di lavoro.

La consegna, la spedizione o l'invio di documenti a terzi potrà avvenire solo a condizione che si tratti di soggetti autorizzati alla loro consultazione.

Nel caso si entrasse in possesso di documenti aziendali non di propria competenza, tali documenti dovranno essere restituiti alla persona responsabile o a chi si occupi della loro archiviazione.

Nel caso si entrasse in possesso di documenti di terzi non di competenza aziendale, tali documenti dovranno essere restituiti al terzo se originali o distrutti se copie, previa segnalazione al terzo stesso. In caso di impossibilità di individuazione o di contatto con il terzo i documenti andranno distrutti, qualora non abbiano un contenuto significativo, oppure consegnati ad un responsabile aziendale se si tratta di materiale di una qualche importanza. Quest'ultimo provvederà alla riconsegna ad un'autorità competente.

7) Norme generale per il salvataggio dati e le operazioni di ripristino

La creazione, la conservazione, l'utilizzo e la distruzione di supporti di back-up, in special modo quelli contenenti dati sensibili e/o giudiziali, dovrà avvenire nel pieno rispetto di tutte le norme di legge e delle misure previste per la tutela della privacy e la sicurezza del sistema informativo aziendale. In particolare dovranno essere osservate con scrupolo le seguenti misure specifiche:

Le operazioni di salvataggio dei dati aziendali dovranno svolgersi con cadenza minima giornaliera.

Il salvataggio dei dati dovrà riguardare tutte le informazioni e i dati aziendali memorizzati in formato elettronico presenti sui server gestionali e sui server documentali. Nel caso di dati presenti su singole postazioni client dovranno essere attivate procedure specifiche per il salvataggio di tali dati.

Le operazioni di salvataggio e ripristino dei dati aziendali dovranno essere compiute solo da personale a ciò autorizzato.

La conservazione dei supporti dovrà avvenire in luogo o contenitore a ciò dedicato e non accessibile se non a persone autorizzate. Le caratteristiche del luogo o del contenitore destinato alla conservazione dei supporti dovranno essere quelle stabilite dal responsabile aziendale per il salvataggio dati. Nessun altro uso dei supporti è consentito all'infuori del ripristino dei dati.

I salvataggi effettuati dovranno essere oggetto di verifiche circa il loro buon esito. Qualora queste verifiche siano eseguibili automaticamente (come istruzioni di rilettura e/o verifica dei dati appena salvati su supporto) da parte degli stessi software o delle procedure di back-up, esse andranno messe in atto ad ogni sessione di salvataggio. Qualora invece la verifica possa essere effettuata solo manualmente, essa dovrà avere cadenza almeno mensile. Eventuali inefficienze a carico degli apparati preposti al salvataggio dovranno immediatamente essere portate all'attenzione del responsabile del sistema informatico o del trattamento dati.

Eventuali salvataggi di dati presenti su singole postazioni di lavoro dovranno seguire le stesse norme dei salvataggi aziendali. Responsabile del salvataggio dati di singoli client sarà l'utilizzatore della postazione; nel caso di più utilizzatori contemporanei, responsabile dei salvataggi sarà la persona a ciò preposta oppure, in mancanza di sua indicazione, quella di maggior livello gerarchico, di maggior anzianità o quella presente alla chiusura degli uffici o dei singoli turni di lavoro.

8) Norme di condotta per l'amministratore di sistema ai fini della tutela dei dati personali

L'amministratore di sistema, nella gestione della rete informatica aziendale, dovrà garantire il pieno rispetto di tutte le norme di legge e delle misure previste per la tutela dei dati personali. In particolare dovrà quanto possibile dar corso alle seguenti linee guida, qualora ragioni tecniche/tecnologiche non ne impediscano la realizzazione.

Nessun soggetto dovrà poter accedere al sistema informatico, agli applicativi, ai documenti e a ogni altro dato presente negli archivi aziendali se non dotato di specifica credenziale di autorizzazione. Tale credenziale di autorizzazione dovrà sempre essere composta da un codice di identificazione dell'utente (account) e da una password riservata o altra soluzione analoga (carte magnetiche personali, token ecc.).

Nella costruzione dell'architettura di rete dovranno essere privilegiate, se possibile, soluzioni che tendano a segmentare la rete stessa in gruppi o aree di lavoro omogenee per necessità di sicurezza, profili di autorizzazione, tipo di utenti o accesso alle risorse condivise. Fra i vari gruppi di lavoro dovranno essere attivati, quando opportuni, filtri (firewall) che impediscano l'accesso da/verso i vari gruppi e/o l'esterno. Ove possibile, si dovrà privilegiare la costruzione di uno più domini all'interno della rete aziendale o comunque soluzioni tecniche analoghe che realizzino l'obiettivo del controllo accentrato dell'autenticazione dei client, della distribuzione dei profili di autorizzazione e dei diritti di accesso alle risorse condivise, dell'installazione e aggiornamento delle applicazioni e del monitoraggio dell'attività in rete dei singoli client/utenti.

Le credenziali di autorizzazione, una volta assegnate, non dovranno essere mai più riassegnate ad altri soggetti. Le credenziali devono essere sempre soggette a verifica circa la loro validità: in particolare, esse vanno tempestivamente disattivate o modificate nel caso di perdita o di cambiamento da parte di un soggetto del proprio diritto d'accesso ai dati (per dimissioni, licenziamento, trasferimento, cambio di qualifica ecc.). In ogni caso, le credenziali non utilizzate da più di sei mesi dovranno comunque essere disattivate, salvo che non si tratti degli utenti di amministrazione di una macchina. Per questi ultimi deve essere prevista una tassativa revisione periodica dei diritti di accesso.

Per tutte le postazioni della rete (server aziendali e client), se non disponibili sistemi di autenticazione centralizzati, dovranno essere configurati almeno due credenziali di autorizzazione. La prima sarà destinata alla Direzione aziendale e avrà carattere di Utente di Amministrazione o Superuser. Per tutti gli altri soggetti, invece, le singole credenziali dovranno essere caricate con un profilo di User o Utente di lavoro ordinario. Il profilo Amministratore dovrà essere l'unico a poter installare programmi o modificare le impostazioni di sistema. Il profilo Utente dovrà poter solo utilizzare i programmi indispensabili al singolo soggetto, secondo le sue autorizzazioni, e limitarsi alle operazioni di ordinaria amministrazione quali l'accesso a file, creazione di documenti, stampe ecc. È possibile che, oltre alla Direzione, possano essere caricati altri utenti di Amministrazione o Superuser destinati all'amministratore di sistema, ad uno o più manutentori software o ad altre figure analoghe, sia appartenenti all'azienda che a fornitori esterni. Gli utenti Amministratori assegnati a fornitori o consulenti esterni all'azienda dovranno essere attivati solo al bisogno e successivamente disattivati. Le password dell'utente della Direzione andranno conservate in busta chiusa da parte del custode delle password. Nel caso in cui, per qualche ragione, vi fosse necessità di aprire tale busta, si dovrà procedere al cambio di password dell'account della Direzione e al rideposito della stessa in busta chiusa.

Nello sviluppo o nell'adozione di nuove applicazioni dovrà essere sempre privilegiata, se possibile, un'architettura di tipo Client-Server. Dovranno poi essere impostati uno o più server documentali per permettere agli utenti di accedere in modo controllato ai file di dati, sia aziendali che personali. La presenza di applicazioni o documenti contenenti dati personali su singoli client dovrà costituire fatto eccezionale: in tal caso occorrerà seguire le medesime indicazioni qui riportate per i server aziendali. Occorrerà inoltre provvedere a determinare idonee procedure per lo svolgimento dei back-up e per garantire la continuità del sistema.

Tutti gli archivi e le basi dati dei programmi non dovranno mai essere installati in cartelle accessibili a utenti ordinari, ma solo in quelle riservate agli utenti amministratori.

L'accesso ai server documentali dovrà essere soggetto a verifica delle credenziali e del profilo di autorizzazione di ogni singolo utente. Tale verifica dovrà operare preferibilmente a livello di singolo documento o, quanto meno, a livello di cartella.

Almeno a tutti i server dovrà essere garantita l'alimentazione elettrica grazie all'installazione di appositi gruppi di continuità. Tali gruppi dovranno essere sottoposti a test almeno trimestralmente, al fine di verificare la loro efficienza.

Su tutti i server dovrà essere fatta opera di disabilitazione dei servizi e delle applicazioni non essenziali, limitando al minimo la porzione di sistema operativo installato. A tutti i servizi o le applicazioni che utilizzano utenti di default ineliminabili (es. utenti administrator di database) dovranno essere imposte password di sicurezza dotate dei necessari requisiti di solidità (vedasi Norme per la gestione delle password).

Nel caso una postazione possa avere accesso all'esterno tramite linee di comunicazione, tale accesso dovrà essere protetto con l'attivazione di firewall o a livello della singola postazione di lavoro o a livello di rete. I criteri di protezione devono essere i più restrittivi possibili.

9) Norme di condotta per il controllo dell'accesso agli ambienti, agli uffici e agli archivi

L'accesso agli ambienti, agli uffici, agli archivi ed in generale a qualsiasi struttura aziendale in cui vengano trattati dati personali o si svolgano attività che necessitino di riservatezza dovrà avvenire nel rispetto delle norme di legge a tutela dei dati personali e della privacy. In particolare dovranno essere osservate con scrupolo le seguenti misure specifiche:

Nessuna persona dovrà accedere agli spazi aziendali (o, nel caso di strutture aperte al pubblico, alle aree riservate di tali spazi) se non appartenente all'organico dell'azienda. I soggetti preposti al controllo degli accessi dovranno aver cura di identificare ogni individuo in entrata, indirizzando i terzi estranei verso le aree dedicate all'attesa. Gli incontri con soggetti esterni all'azienda dovranno svolgersi nei luoghi a ciò deputati, evitando quanto più possibile l'accesso agli uffici in cui si svolge la normale attività aziendale. In ogni caso, ai terzi non dovrà essere consentito di muoversi all'interno degli spazi aziendali riservati se non accompagnati dal personale dell'azienda. A coloro che accedono in azienda per ragioni di servizio (manutentori, addetti alle pulizie ecc.) dovrà essere data libertà di movimento solo negli ambienti nei quali dovrà espletarsi l'intervento richiesto. Al termine delle visite o degli interventi, i terzi dovranno essere accompagnati all'uscita dagli spazi aziendali.

L'accesso agli uffici e agli archivi contenti dati personali riservati dovrà essere limitato solo al personale autorizzato al loro trattamento. Al termine dell'orario di lavoro ed in caso di assenza prolungata che lasci l'ufficio sguarnito, tali uffici andranno chiusi a chiave. La custodia delle chiavi, se non riservata al responsabile dell'ufficio, andrà affidata ai soggetti incaricati di tale compito. Quest'ultimi dovranno consegnare le chiavi di accesso agli uffici solo al personale autorizzato all'accesso.

Nella presente struttura, gli uffici ad accesso riservato sono i seguenti:

Ufficio	Personale ammesso	Custodia chiave
La sede non è accessibile a soggetti non autorizzati, in quanto chiusa a chiave.	Personale dell'Ordine degli Assistenti Sociali della Liguria.	Personale addetto.

Ogni chiave o altro dispositivo analogo che consenta l'accesso alla struttura, a singoli uffici o ad archivi contenenti dati personali, qualora non venga affidata in custodia ad uno specifico responsabile, dovrà essere conservata in apposito raccoglitore generale (o cassetto) chiuso. Il raccoglitore generale dovrà comunque contenere copia delle chiavi affidate in via esclusiva ad un singolo responsabile. La chiave di accesso al raccoglitore dovrà essere data in custodia solo ai soggetti autorizzati dalla direzione aziendale a detenerne il possesso; tali soggetti sono responsabili della consegna delle singole chiavi solo al personale autorizzato all'accesso nei vari uffici o archivi aziendali. Per l'accesso ad archivi contenenti dati sensibili o uffici di particolare rilevanza il ritiro e la riconsegna della chiave di accesso, specie se effettuata in giorni o orari non di attività dell'azienda, potrebbe richiedere l'apposizione di una firma su apposito registro; in alternativa è possibile che vengano rilevati log di accesso a tali ambienti.

Quanto al punto 3 non si applica a dispositivi e chiavi di accesso ad armadi, cassetti ecc. di competenza del singolo lavoratore e destinati esclusivamente al deposito ed alla custodia di oggetti personali.

10) Norme di condotta per la comunicazione dell'informativa relativa al trattamento dati e la raccolta del consenso degli interessati

Ogni trattamento dati dovrà avvenire a condizione che sia stata fornita nelle modalità prestabilite la necessaria informativa e venga raccolto, laddove richiesto, il relativo consenso, così come previsto dal Regolamento UE 2016/679 e dal D.lgs. 196/2003. In particolare dovranno essere osservate con scrupolo le seguenti misure specifiche:

A ospiti e fornitori che entrino in contatto con l'azienda l'informativa relativa al trattamento dati dovrà essere inserita nei documenti e moduli di accettazione, nei contratti, nelle offerte, nelle bolle o nelle fatture, a seconda di quale fra questi documenti sia destinato ad essere consegnato ai diversi interessati

A tutti i dipendenti e collaboratori dovrà essere consegnata, in occasione dell'entrata in servizio, l'informativa relativa al trattamento dei dati personali e dovrà obbligatoriamente essere raccolto per iscritto il consenso per il trattamento dei dati sensibili

Nel caso d'incapaci o minori accompagnati da adulti occorrerà porre attenzione a che sia verificata l'effettiva capacità del soggetto accompagnatore a prestare validamente il consenso per conto dell'incapace o del minore

Al raggiungimento della maggiore età o all'eventuale riacquisto della capacità di agire o intendere, i consensi eventualmente prestati in precedenza dai tutori dovranno essere rinnovati facendo riferimento ai diretti interessati

Tutti i consensi raccolti dovranno essere archiviati e conservati fino a cessazione dei rapporti con il soggetto interessato ed eliminazione dal sistema informativo aziendale di ogni dato riguardante il soggetto stesso.

11) Norme di condotta per la gestione dei dati relativi ai dipendenti e alla gestione paghe

Ogni trattamento dati riguardante i dipendenti e collaboratori dovrà avvenire a condizione che sia stata fornita nelle modalità prestabilite la necessaria informativa e venga raccolto, laddove richiesto, il relativo consenso. Tali trattamenti dovranno avvenire nel rispetto di quanto previsto dalle normative in materia di lavoro e dal Regolamento UE 2016/679 nonché dal D.lgs. 196/2003. In particolare dovranno essere osservate con scrupolo le seguenti misure specifiche:

- Tutti i dati dei collaboratori e dipendenti dovranno essere conservati in armadi chiusi accessibili esclusivamente al personale addetto all'ufficio del personale.
- Nessuna comunicazione o accesso ai dati del personale dovrà essere possibile a terzi estranei, con particolare riguardo ai dati sensibili. Qualora si faccia ricorso a consulenti del lavoro o per il calcolo paghe o altre materie collegate alla gestione del personale, occorrerà limitare al minimo indispensabile la comunicazione di informazioni a tali soggetti. Laddove possibile tali informazioni dovranno essere fornite in forma anonima, facendo riferimento alla matricola del dipendente.
- Il deposito presso terzi o la consegna a costoro di copie di documentazione relativa ai dipendenti dovrà avvenire solo sulla base dell'autorizzazione del dipendente stesso ed essere limitata al minimo indispensabile. In ogni caso tale documentazione dovrà essere richiamata o distrutta non appena fossero cessate le ragioni per la detenzione da parte del terzo.
- La gestione e la consegna dei cedolini paga dovrà avvenire singolarmente ed in busta chiusa o in forme tali da garantire una tutela equivalente della riservatezza.
- Ogni colloquio con il personale o richiesta di informazioni che abbia ad oggetto questioni di esclusivo interesse del singolo dipendente dovrà avvenire in modalità e condizioni tali da garantirne la riservatezza.

12) Norme di condotta per i sistemi di videosorveglianza e controllo

Ogni trattamento dati che riguardi la videosorveglianza o il controllo degli ambienti dovrà avvenire nel pieno rispetto di tutte le norme di legge e delle misure previste per la tutela della privacy e la sicurezza del sistema informativo aziendale. In particolare dovranno essere osservate con scrupolo le seguenti misure specifiche

In prossimità delle aree soggette a videocontrollo o videosorveglianza dovrà essere apposto il cartello di segnalazione/informativa sulle modalità del trattamento dei dati

I monitor di videocontrollo dovranno essere posizionati in luoghi riservati o comunque in posizioni tali da poter garantire l'accesso solo al personale autorizzato

La registrazione di immagini dovrà avvenire a circuito chiuso e le stesse dovranno essere conservate per non più di 24/48 h. La cancellazione dei nastri, se non garantita da apposita impostazione tecnica del sistema di registrazione, dovrà essere effettuata manualmente.

La mancata cancellazione delle immagini potrà verificarsi solo nel caso in cui vi siano motivate esigenze di verifica delle registrazioni dovute a violazioni della sicurezza della struttura. In ogni caso la conservazione di tali

immagini dovrà essere limitata al tempo strettamente necessario alle verifiche stesse e solo per le parti rilevanti a tale scopo.

Qualsiasi sistema di controllo dell'attività di soggetti terzi dovrà quanto più possibile limitare il numero e la quantità d'informazioni personali gestite allo stretto indispensabile per il compimento degli scopi previsti. Il numero dei soggetti autorizzati ad accedere alle informazioni dovrà essere quanto più possibile limitato allo stretto indispensabile.

Quanto più possibile le informazioni dei sistemi di controllo dell'attività di soggetti terzi dovranno essere collegate a tali soggetti per via indiretta ed anonima, facendo riferimento ad un codice identificativo, ad una matricola, ad un numero di camera o altro elemento analogo invece che al suo nominativo

Per i sistemi di rilevazioni delle telefonate è opportuno che vengano almeno parzialmente oscurati, sia a video che in stampa, i numeri chiamati. L'eventuale possibilità di accedere ai numeri in chiaro dovrà essere sottoposta a controllo, automatico o procedurale, dovrà essere riservata solo a personale a ciò deputato e consentita solo in caso di verifiche o contestazioni.

Ogni informazione dovrà essere cancellata quando sia trascorso un sufficiente intervallo di tempo ed in ogni caso qualora ne sia cessata ogni utilità.

13) Norme di condotta per il trattamento dei dati sanitari e giudiziari

Il trattamento dei dati sanitari e giudiziari dovrà avvenire nel rispetto delle norme di legge a tutela dei dati personali e della privacy. In particolare dovranno essere osservate con scrupolo le seguenti misure specifiche:

I dati sanitari degli ospiti dovranno essere gestiti ed archiviati in modo da garantire il più possibile la non identificazione del soggetto cui si riferiscono: l'identificazione degli interessati dovrà avvenire, anche per i soggetti autorizzati all'accesso ai dati, in modi tali da essere limitata ai soli momenti di effettiva necessità

Per i trattamenti effettuati con strumenti elettronici la non identificazione dovrà essere ottenuta tramite associazione a codici o con tecniche di cifratura dei dati

Per i trattamenti effettuati con supporti cartacei la non identificazione dovrà avvenire grazie all'utilizzo di fascicoli, copertine o raccoglitori anonimi; l'archiviazione dei fascicoli dovrà avvenire utilizzando codici o soluzioni analoghe

I dati sanitari degli ospiti dovranno essere gestiti ed archiviati in modo da garantire il più possibile l'accesso separato rispetto agli altri dati personali dell'interessato

Per i trattamenti effettuati con strumenti elettronici, la separazione dei dati dovrà essere garantita per mezzo dei sistemi di autenticazione e autorizzazione

Per i trattamenti effettuati con supporti cartacei la separazione dei dati personali dai dati sanitari dovrà avvenire già in fase di apertura del fascicolo del soggetto: tutti i dati di natura amministrativa dovranno essere raccolti in un fascicolo destinato all'amministrazione, mentre quelli di natura sanitaria (referti di analisi, screening iniziali, valutazioni di anamnesi, documentazione medica presentata, consensi informati ecc.) dovranno essere archiviati nella cartella sanitaria del soggetto

Nel caso di utilizzo o consultazione, i fascicoli contenenti dati sanitari e giudiziari sono presi in carico personalmente dagli incaricati i quali devono custodirli ed impedire l'accesso a persone non autorizzate. I fascicoli vanno restituiti non appena terminate le operazioni di cui l'incaricato è stato chiamato ad occuparsi

L'accesso agli archivi contenenti i dati sanitari deve essere consentito solo ai soggetti autorizzati: la verifica è compito degli addetti al controllo degli ingressi, della vigilanza ai piani e dei soggetti cui è affidata la custodia delle chiavi di accesso.

12. **Procedura in caso di Data Breach**

PARTE 1 – IN GENERALE
PARTE 2 – PROCEDURA IN CASO DI DATA BREACH
PARTE 3 – RIEPILOGO
PARTE 4 - SCHEDE

PARTE 1 - IN GENERALE:

1. ***Cosa si intende per "DATA BREACH".*** *Con Data Breach si intende, ai sensi dell'art. 4 del Regolamento UE 2016/679, la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. A mero titolo d'esempio costituisce data breach lo smarrimento di documenti cartacei, il furto di un computer o di una chiave USB aziendale o l'attacco da parte di un virus.*
2. ***Cosa prescrive il Regolamento UE 2016/196?*** *Il Regolamento UE 2016/679 prevedere che il Titolare del trattamento deve provvedere ad effettuare:*
   a) *una notifica all'Autorità Garante, entro 72 ore dal momento in cui è venuto a conoscenza della violazione, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche (art. 33);*
   b) *una comunicazione agli interessati se la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.*

   In entrambi i casi, si tratta quindi di comunicazioni necessarie solo in determinati casi, da valutare attentamente con il Registro dei Trattamenti.
3. ***Come posso riconoscere se la notifica al Garante è necessaria o meno?*** *La notifica al Garante deve essere effettuata in presenza di un rischio, indipendentemente dalla gravità del rischio. È improbabile che la violazione comporti un rischio per i diritti e le libertà delle persone fisiche (c.d. Interessati) se il Titolare ha attuato adeguate misure di sicurezza, destinate a rendere i dati personali incomprensibili, come la cifratura o l'anonimizzatine del dato.*
4. ***Come posso riconoscere se la comunicazione agli Interessati è necessaria o meno?*** *La comunicazione agli Interessati deve essere effettuata in presenza di un elevato rischio: in questo caso è richiesta anche la valutazione della gravità del rischio.*

   L'art. 34 del Regolamento distingue due ipotesi in cui la comunicazione non è necessaria:
   a) *quando le misure messe in atto preventivamente (ad esempio, la cifratura) o successivamente alla violazione, sono idonee a scongiurare il rischio elevato;*
   b) *quando la comunicazione agli Interessati richiede uno sforzo sproporzionato da parte del Titolare. In questo caso, il Titolare effettua una comunicazione pubblica.*
5. ***Qual è il contenuto della notifica?*** *Nella notifica al Garante, il Titolare deve, come previsto dall'33 del Regolamento, comma 3:*
   a) *descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di Interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;*
   b) *comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;*
   c) *descrivere le probabili conseguenze della violazione dei dati personali;*
   d) *descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.*

   La comunicazione agli Interessati, deve descrivere la natura della violazione in un linguaggio semplice e chiaro e deve contenere almeno i punti di cui alle lettere b), c) e d).

PARTE 2 – PROCEDURA IN CASO DI DATA BREACH

1) Chiunque, all'interno della struttura nonché i fornitori in *outsourcing* (cd. Responsabili ex art. 28 del Regolamento) abbia notizia di una violazione è tenuto a segnalarlo senza indugio al Titolare perché prenda le necessarie misure.

2) Il Titolare o il suo delegato, devono informare dell'avvenuta violazione il Responsabile della Protezione dei dati (DPO), se presente.

3) Il Titolare o il suo delegato devono valutare senza indugio:
   a) la categoria di Interessati e il loro numero (anche approssimativo);
   b) la tipologia di dato violato;
   c) la tipologia di violazione;
   d) una ricognizione delle misure di sicurezza applicate.

   Sulla base di tali informazioni, il Titolare deve compiere una valutazione circa i rischi per i diritti e le libertà degli Interessati.
   Per la rilevazione della violazione utilizzare la scheda 1.

4) Nel caso in cui la valutazione di cui al punto 2 rilevi un rischio per i diritti e le libertà delle persone fisiche, il Titolare o il suo delegato devono attuare tutte le misure ritenute opportune al fine di limitare gli effetti della violazione ed evitare più gravi conseguenze.
   A tal fine il Titolare o il suo delegato devono contattare i soggetti, interni o esterni, in grado di predisporre adeguate misure, tecniche ed organizzative, a seconda della tipologia di violazione.

5) Nel caso in cui la valutazione di cui al punto 2 rilevi un rischio per i diritti e le libertà delle persone fisiche, è necessario procedere alla notifica al Garante ai sensi dell'art. 33 GDPR.
   La notifica deve essere trasmessa entro il termine di 72 ore dalla scoperta dell'evento. In caso di superamento del termine è necessario motivare il ritardo.
   La notifica e gli eventuali allegati devono essere trasmessi via pec al seguente indirizzo: protocollo@pec.gpdp.it.
   Ogni notifica deve essere registrata con un numero di protocollo interno da riportare nell'apposito Registro delle violazioni.
   Per la notifica al Garante utilizzare la scheda 2[1].

6) Nel caso in cui la valutazione di cui al punto 2 rilevi un pericolo "elevato", la comunicazione agli Interessati deve essere effettuata per iscritto (via posta ordinaria o via mail) agli Interessati e deve contenere la descrizione dell'evento nonché:
   - il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
   - le probabili conseguenze della violazione dei dati personali;
   - le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

   Nel caso in cui la comunicazione venga inviata via mail e a più destinatari, è necessario utilizzare le impostazioni che consentano di nascondere l'elenco completo dei destinatari al soggetto ricevente.

7) Ogni violazione di cui si abbia notizia, indipendentemente dalla gravità e dall'avvenuta notifica all'Autorità Garante, deve essere annotata nell'apposito "Registro delle violazioni" da parte del Titolare o da un suo delegato.
   Ai fini della tenuta del Registro, è opportuno allegare allo stesso anche le schede di cui al punto 2 e le copie delle comunicazioni effettuate, attribuendo ad ognuna un numero progressivo interno da riportare nel Registro.
   Per il Registro delle violazioni utilizzare la scheda 3.

8) In ogni caso, dopo la violazione devono essere approntati modelli organizzativi, procedure o misure di sicurezza in modo da evitare il successivo verificarsi della stessa violazione.

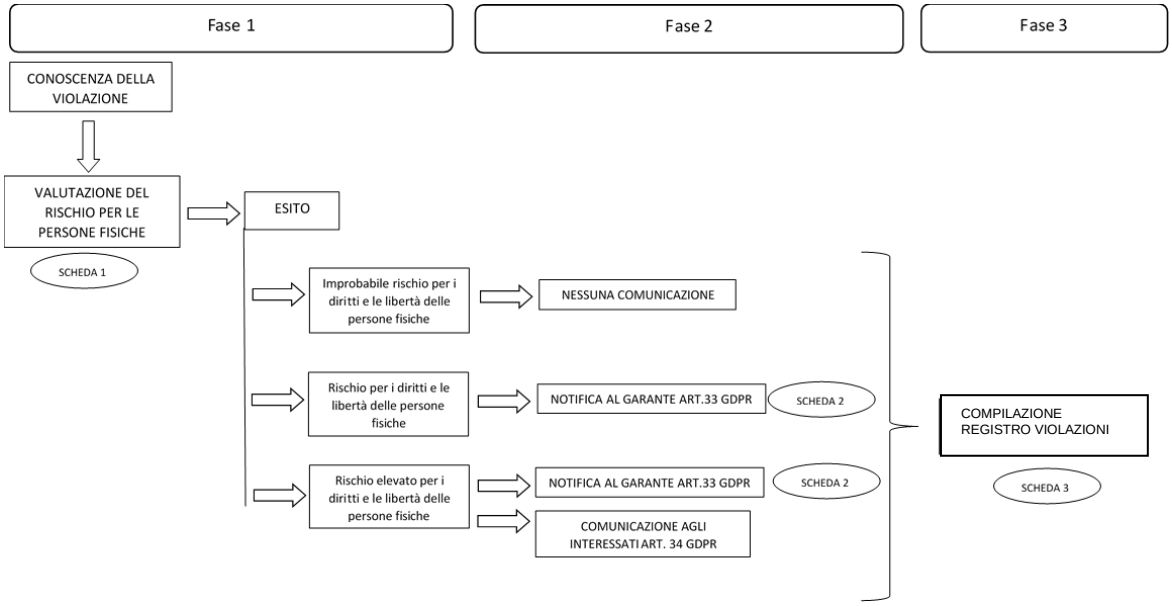
[1] *Nel caso in cui il garante dovesse mettere a disposizione un modulo apposito, si invita ad utilizzare il modulo ufficiale.*

A titolo d'esempio:

a) in caso di accesso illecito ai dati in formato elettronico, si consiglia di cambiare le password esistenti e di installare/aggiornare il firewall;
b) in caso di accesso illecito ai dati in formato cartaceo, si consiglia di sostituire le serrature dei locali e/o degli armadi.

È opportuno tenere traccia degli aggiornamenti e delle modifiche delle misure di sicurezza.

PARTE 3 – RIEPILOGO



PARTE 4 – SCHEDE

Scheda 1: scheda di rilevazione della violazione

<table>
<tr><td colspan="6">Scheda rilevazione violazione dei dati personali</td></tr>
<tr><td colspan="2">Numero progressivo indicato nel Registro delle Violazioni</td><td colspan="4"></td></tr>
<tr><td colspan="2">Giorno e ora avvenuta violazione</td><td colspan="4"></td></tr>
<tr><td colspan="2">Giorno e ora avvenuta scoperta</td><td colspan="4"></td></tr>
<tr><td colspan="2">Breve descrizione dell’evento</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Interessati</td><td>Categoria</td><td colspan="4"></td></tr>
<tr><td>Numero approssimativo</td><td colspan="4"></td></tr>
<tr><td colspan="2">Tipologia di dato</td><td colspan="4">□ dati personali comuni
□ dati personali particolari (sensibili)
□ dati personali giudiziari ex art. 10 GDPR</td></tr>
<tr><td colspan="2">Misure di sicurezza applicate</td><td colspan="4"></td></tr>
<tr><td colspan="6">VALUTAZIONE RISCHIO</td></tr>
<tr><td colspan="2">Descrizione</td><td colspan="4"></td></tr>
<tr><td colspan="6">RISULTATO</td></tr>
<tr><td colspan="6">□ improbabile rischio per i diritti e le libertà delle persone fisiche</td></tr>
<tr><td colspan="6">Presenza rischio per i diritti e le libertà delle persone fisiche
□ rischio basso □ rischio elevato</td></tr>
<tr><td colspan="6">□ Presenza di rischio per i diritti e le libertà delle persone fisiche ma sforzi sproporzionati per il numero degli interessati</td></tr>
<tr><td colspan="6">ESITO</td></tr>
<tr><td colspan="2">Notifica ex art. 33 GDPR</td><td colspan="4">Comunicazione ex art. 34 GDPR</td></tr>
<tr><td>□ nessuna notifica</td><td>□ notifica al Garante</td><td>□ nessuna comunicazione</td><td colspan="2">□ comunicazione agli interessati</td><td>□ comunicazione pubblica</td></tr>
</table>

Scheda 2: modulo notifica al Garante

Notifica all'Autorità Garante per la protezione dei dati personali ai sensi dell'art. 33 del Regolamento UE 2016/679	
1. Dati del Titolare del Trattamento	
Denominazione	
Legale Rappresentante	
Sede legale	
P.IVA	
Indirizzo PEC	
Indirizzo e-mail	
telefono	
Delegato al Trattamento dei dati	
Tipologia di attività	
Responsabile della Protezione dei dati	
2. Breve descrizione della violazione	
Categoria di Interessati	
Tipologia di dati	
Numero approssimativo degli interessati	
Numero delle Registrazioni	
Soggetto coinvolto	
Luogo dell'evento	
Tipologia della violazione	
Breve descrizione della modalità dell'evento	
Indicazione del giorno dell'evento	
Indicazione della notizia dell'evento	
Modalità con cui il Titolare è venuto a conoscenza della violazione	
Motivazione dell'eventuale ritardo	
Descrizioni delle probabili conseguenze della violazione	
3. Misure di sicurezza adottate normalmente	
Descrizione	
4. Misure di sicurezza straordinarie adottate come contromisura per adottare possibili effetti negativi	
Descrizione	
5. Comunicazione agli interessati	
Descrizione	
6. Soggetti ai quali è possibile chiedere ulteriori informazioni	
Indicazione soggetti e loro qualifica	

7. Allegati	
Indicazione del nome del file e breve descrizione del contenuto	
8. Numero della notifica	
Numero assegnato dal Titolare	
9. Sottoscrizione del Titolare	
Data	
Firma	