ISTRUZIONI IN MATERIA DI PRIVACY

PICCOLO VADEMECUM PER EVITARE SANZIONI

Regola n. 1 – Password

Tutte le password e le credenziali sono uniche e personali, non possono essere condivise o cedute a terzi e devono essere segrete e non annotate in luoghi facilmente accessibili.

Per gli uffici amministrativi si invita all'utilizzo di un programma specifico per la gestione delle credenziali.

Regola n. 2 – Conservazione

I soggetti che per mansione sono deputati a custodire i dati sono tenuti ad adottare adeguate misure di sicurezza, tra cui l'adozione di password per l'accesso ai sistemi informatici.

È fatto divieto di attivare moduli di acquisizione e raccolta di dati senza comunicazione all'ufficio competente per la gestione della privacy.

Regola n. 3 – Smaltimento rifiuti

Tutti i documenti devono essere conservati attraverso modalità che impediscano l'accesso di persone non autorizzate.

I documenti cartacei ed informatici devono essere conservati per il periodo previsto dal Massimario di scarto.

L'eliminazione dei documenti cartacei deve avvenire attraverso il distruggi documenti.

Regola n. 4 – Profili di autorizzazione

I profili di autorizzazione sono strettamente correlati alle mansioni del dipendente.

È fatto divieto di consultare dati e sistemi non afferenti alle proprie mansioni.

Nel caso in cui il dipendente si accorgesse di poter visionare dati eccedenti il proprio profilo autorizzativo è tenuto a comunicarlo tempestivamente, e comunque il prima possibile, al responsabile.

Regola n. 5 – Sistema di videosorveglianza

La collocazione delle videocamere e della segnaletica deve essere chiara e ben visibile.

Le videocamere devono essere installate in modo da evitare di riprendere luoghi pubblici o privati non di pertinenza dell'ente.

Le immagini sono conservate per finalità di sicurezza per 72 ore.

Le immagini trasmesse tramite monitor non possono essere rese visibili a terzi.

Regola n. 6 – E-mail

Le comunicazioni a più persone devono essere spedite utilizzando il campo di "copia conoscenza nascosta" (CCN).

È fatta unica eccezione quando il messaggio è appositamente inviato a più persone per motivi organizzativi e gestionali.

È necessario prestare adeguata attenzione al contenuto delle e-mail, evitando dove possibile di inviare in chiaro informazioni particolarmente sensibili (password, categorie particolari di dati).

È necessario prestare attenzione alla apertura delle e-mail in arrivo per ovviare al rischio di subire malware o altre ipotesi di effrazione.

Regola n. 7 – Utilizzo dispositivi esterni

In caso di smarrimento di dispositivi esterni tutto il personale è tenuto ad informare, tempestivamente e comunque non oltre le 24 ore, l'ufficio competente, facente capo al Direttore.

È fatto divieto di utilizzare chiavette USB o altri strumenti removibili che non siano espressamente autorizzate.

Regola n. 8 – Esecizio dei diritti

Qualsiasi richiesta da parte degli interessati deve essere presa in carico senza ritardo ed esaudita nella maniera più completa possibile da parte dell'ufficio competente.

Tutte le richieste devono essere inoltrate a segreteria@casariposospiazzo.it .

Regola n. 9 – Utilizzi strumenti elettronici privati

Per le attività lavorative devono essere utilizzati esclusivamente gli strumenti aziendali.

È fatto divieto di usare strumenti personali, se non espressamente autorizzati.

Non è ammesso l'utilizzo di whatsapp, icloud, dropbox e altri servizi non approvati, se non espressamente autorizzati.

Regola n. 10 – Esposizione elenchi

È fatto assoluto divieto di esporre in locali pubblici liste, post-it, elenchi contenenti codici di accesso, dati personali di interessati o di soggetti terzi, soprattutto nei locali accessibili al pubblico salvo diverso obbligo di legge.

Regola n. 11 – Corretta gestione del data breach

Gli interessati devono segnalare tempestivamente e comunque entro 24 ore qualsiasi violazione di dati di cui siano venuti a conoscenza per consentire gli adempimenti previsti, mandando una comunicazione scritta contenente un breve riassunto dell'evento a segreteria@casariposospiazzo.it ..

Regola n. 12 – Comunicazione dati

Si invita a prestare massima cura nella creazione dei fascicoli facendo attenzione alla completezza, alla rettifica e aggiornamento dei dati, evitando di mescolare dati di interessati diversi.

Si invita a prestare particolare attenzione quando si consegnano o si trasmettono dati e informazioni di persone fisiche, attraverso strumenti cartacei, informatici o per vie telefoniche, a terzi interessati.

Qualsiasi altra comunicazione a terzi non legittimati è vietata.

Regola n. 13 – Anonimizzazione

Tutte le comunicazioni che coinvolgono dati relativi allo stato di salute o particolarmente delicati di persone fisiche devono essere laddove possibile anonimizzate.

Regola n. 14 – Utilizzo banche dati a fini privati

È fatto assoluto divieto di utilizzare i dati personali di cui si ha accesso per motivi professionali a fini privati e/o non correlati al motivo per cui sono stati raccolti.

Regola n. 15 – Dati particolari

Si invita a prestare attenzione ai dati relativi alla salute, abitudini sessuali, origine razziale ed etnica, convinzioni filosofiche o religiose e comunque a qualsiasi dato rientrante nelle categorie particolari ai sensi della normativa privacy.

È espressamente vietato di riprendere gli utenti, di pubblicare sui social network, siti internet e in qualsiasi altra forma informazioni relative a persone fisiche di cui si è venuti a conoscenza in ragione della propria professione.

Regola n. 16 - Comportamenti

Il personale è tenuto ad attenersi alle indicazioni ricevute attraverso il materiale fornito da parte dell'amministrazione.

In caso di dubbi il dipendente è invitato a rivolgersi al Direttore.

BREVE GLOSSARIO	
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Categoria particolare di dati personali	Dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
Trattamento di dati personali	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali.
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
Incaricato/autorizzato a trattamento	Persona autorizzata che opera sotto l'autorità diretta del Titolare del trattamento.
DPO (responsabile protezione dei dati)	Soggetto individuato da parte del Titolare del trattamento. Il responsabile della protezione dei dati, ai sensi dell'art. 28 Reg., è incaricato dei seguenti compiti: informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento; sorvegliare l'osservanza della normativa alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; fornire pareri in merito alla gestione dei trattamenti svolti e cooperare con l'autorità di controllo.
Misure di sicurezza	Tutte le misure tecniche e organizzative adeguate per garantire un livello di sicurezza idoneo al rischio, che comprendono, tra le altre.
Data breach	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.