ISTRUZIONI IN MATERIA DI PRIVACY
PICCOLO VADEMECUM OPERATIVO

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.

E 'necessario modificare le password con cadenza almeno trimestrale.

Regola n. 2 – Conservazione

I soggetti che per mansione sono deputati a trattare dati personali 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 l'autorizzazione dell'ufficio competente per la gestione della privacy.

Gli strumenti elettronici in dotazione non devono essere lasciati incustoditi o accessibili da terzi durante una sessione del trattamento.

Tutti gli incaricati sono tenuti al controllo e alla custodia dei documenti contenenti dati personali per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento loro assegnate. L'accesso ai dati personali dovrà essere limitato a quelli la cui conoscenza sia necessaria e indispensabile per lo svolgimento delle operazioni di trattamento consentite. E' compito dell'incaricato provvedere alla loro idonea archiviazione alla cessazione delle operazioni autorizzate.

Regola n. 3 – Smaltimento documentazione cartacea

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

I documenti cartacei ed informatici devono essere conservati per il periodo previsto dalle leggi vigenti, dal Massimario di scarto e dai criteri definiti dal Titolare del trattamento.

L'eliminazione dei documenti cartacei deve avvenire attraverso il distruggi documenti o in modalità tali da renderli intelligibili.

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 e/o compiere sugli stessi qualsiasi operazione di trattamento.

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 soggetto responsabile per la gestione della privacy.

Regola n. 5 – 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 tramite account aziendali.

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 mail in arrivo per ovviare al rischio di subire malware o altre ipotesi di effrazione.

Regola n. 6 – 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, il soggetto responsabile per la gestione della privacy.

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

Regola n. 7 – Esercizio dei diritti

Qualsiasi richiesta di esercizio dei diritti 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 al soggetto responsabile per la gestione della privacy.

Regola n. 8 – Divieto utilizzo di strumenti elettronici privati

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

È fatto divieto di usare strumenti personali.

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

Regola n. 9 – Esposizione elenchi

È fatto assoluto divieto di esporre 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. 10 – Corretta gestione del data breach

Tutti i collaboratori 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 al soggetto responsabile per la gestione della privacy.

Regola n. 11 – Comunicazione dati

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

Si invita a prestare particolare attenzione quando si consegnano o si trasmettono dati personali e informazioni di persone fisiche, attraverso strumenti cartacei, informatici o per vie telefoniche, avendo cura che la comunicazione abbia luogo solo nei confronti di terzi legittimati alla loro conoscenza.

Qualsiasi altra comunicazione di dati personali a terzi non legittimati e/o loro diffusione è vietata.

Regola n. 12 – 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. 13 – 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.
E 'necessario attenersi al profilo di autorizzazione ricevuto dal titolare.

Regola n. 14 – 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 pubblicare su 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. 15 - Comportamenti	
Il personale è tenuto ad attenersi alle indicazioni ricevute attraverso il materiale fornito da parte del titolare. In caso di dubbi il dipendente è invitato a rivolgersi al soggetto responsabile per la gestione della privacy.	
Regola n. 16 - Misure di sicurezza	
E' necessario osservare scrupolosamente tutte le misure di sicurezza adottate dal titolare rispettando le istruzioni ricevute e e indicazioni fornite dall'amministratore di sistema.	

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, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
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 è incaricato dei seguenti compiti: informare e fornire consulenza al titolare del trattamento o al responsabile del tratta- mento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati; sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative 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, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35; cooperare con l'autorità di controllo; fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
misure di sicurezza	Misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: la pseudonimizzazione e la cifratura dei dati personali; la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
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.