DOCUMENTAZIONE DI SISTEMA PRIVACY E PROTEZIONE DATI PERSONALI

EDIZIONE 2024

Istruzione operativa : Designazione Operatori Autorizzati al Trattamento (aziendali / Terzi / Destinatari)
Versione : Rif. : ALLEGATI A e B compilati dal TDT del soggetto Candidato
Ultima revisione : INCARICHI SOGGETTI PRIVACY INTERNI ED ESTERNI GDPR-EU/REG.2016/679

Il presente documento dà corso agli adempimenti del cosiddetto GDPR "Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio" e s.s.m., relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che dal 25 maggio 2018 è pienamente operativo, e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

DESIGNAZIONE E INFORMATIVA PER
OPERATORE AUTORIZZATO AL TRATTAMENTO DEI DATI PERSONALI
ISTRUZIONI E RICHIESTA DI INFORMAZIONI

Tipologia Sogg. Autorizzato: ☐ **Interno Azienda** ☐ **Terzo** ☐ **Destinatario**

Nome Cognome e funzione : .....

In qualità di *"Titolare del Trattamento"* dei dati personali, adempiente a quanto stabilito dal Regolamento UE 679/2016 e Normativa Italiana, lei viene designato "Soggetto Autorizzato" al trattamento dei dati personali gestiti al fine di adempiere alle attività operative assegnate dal Titolare.

Per favorire il Suo lavoro, la nostra organizzazione ha designato anche un Delegato Interno Privacy (DIP) e un Amministratore di Sistema IT (ADS) a cui lei farà riferimento secondo le istruzioni e le informazioni ricevute durante il Piano di Formazione a cui lei ha partecipato.

Lei è invitato a prendere visione delle pagine che seguono, nelle quali trova le principali istruzioni operative a cui conformarsi; la rammentiamo inoltre la lettura del documento del Disciplinare interno Privacy disponibile nel manuale del Sistema Privacy e Protezione dei Dati, pubblicato sul nostro sito web specifico.

Clausola di aggiornamento:
Il presente documento sostituisce e aggiorna quello di "Incaricato al Trattamento" relativo al precedente Sistema di Gestione Privacy

La presente scheda è un estratto delle diligenze dovute per legge e adeguate nella nostra organizzazione nel documento del Disciplinare Interno per lei disponibile sulla bacheca, in amministrazione nel Manuale del Sistema Privacy e Protezione dei Dati (SPPD) e consultabile sul sito web aziendale.

RACCOMANDAZIONI E ISTRUZIONI SULLA GESTIONE DEGLI ACCESSI NELLE POSTAZIONI DI LAVORO

- ***Impedire, nei locali dove lei opera, l'intrusione di estranei sugli apparati in dotazione che le sono stati affidati da parte delle persone autorizzate ad operare a nome e per contro del Titolare del Trattamento;***
- ***seguire le istruzioni ricevute durante il Piano di Formazione Privacy aziendale così da impedire il danneggiamento, la manomissione, la sottrazione, la distruzione, o la copia di dati nei locali dove svolge la sua funzione;***
- ***conservare i documenti cartacei contenenti i dati sensibili in contenitori muniti di serratura e trattare quelli in formato elettronico solo sui supporti previsti dall'ADS;***
- ***identificare e registrare i soggetti ammessi dopo l'orario di chiusura degli uffici stessi usando il modulo RAFO679 predisposto nel nostro Manuale SPPD.***

GESTIONE DEI DISPOSITIVI ELETTRONICI, COMPUTER, TELEFONI AZIENDALI, PORTATILI.

Per scongiurare la sottrazione di computer, cellulari (BYOD) o supporti di memoria mobili, le raccomandiamo di utilizzare il sistema di credenziali definito nella nostra organizzazione, per l'uso di dispositivi affidati, in modo da garantire:

- ***Protezione contro la perdita fisica dell'apparato***
- ***Protezione contro accessi non autorizzati ai dati***
- ***Minimizzazione di promiscuità di uso di dati aziendali su apparati BYOD***
- ***Trasferimento controllato e sicuro dei dati dall'apparato aziendale fuori dalla sede***
- ***La protezione contro la sottrazione o smarrimento***

RACCOMANDAZIONI DI SICUREZZA DIGITALE

- **Utilizzare sempre il codice identificativo personale e le parole chiave assegnate, cambiandole periodicamente; laddove possibile, utilizzate sempre almeno 8 caratteri, mescolando caratteri maiuscoli,minuscoli e numeri.**
- **La parola chiave deve essere preferibilmente priva di significato e non deve mai essere comunicata a soggetti altri, anche se fiduciari e/o ADS.**
- **Ricordare che in caso di trattamento di "dati di particolare natura", la parola chiave deve essere cambiata almeno ogni tre mesi, o meno.**

- **Evitare di utilizzare la stessa parola chiave sia sui computer portatili che su quelli fissi.**
- **Mai tenere insieme la copie di *backup* e il computer, per evitare che un eventuale furto possa coinvolgere sia i dati del computer portatile, che quelli di backup. Seguire il sistema di Stoccaggio ingegnerizzato in modo automatico dall'ADS nominato dal Titolare a questo scopo.**
- **INSERIRE EVENTUALI DISPOSIZIONI PECULIARI PER OAT (operatore autorizzato)**

.....

.....

CHIAVI A LEI ASSEGNATE

Indicare descrittivamente eventuali attività a lei assegnate per le quali utilizzare passwords, certificati digitali, chiavi e/o *passphrase*

FISICHE : _____

DIGITALI : _____

Per conto del Titolare	**Presa visione e accettazione**
Il Delegato Interno Privacy	**Operatore Autorizzato**
.....	.....

Data _____