

DOCUMENTAZIONE DI SISTEMA PRIVACY E PROTEZIONE DATI PERSONALI

EDIZIONE n. (Anno 2018-19)

Istruzione operativa : **Designazione Soggetti Autorizzati 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 da corso agli adempimenti del cosiddetto GDPR "Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" che dal 25 maggio 2018 è pienamente operativo.

DESIGNAZIONE E INFORMATIVA PER SOGGETTO 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) ed 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 ha partecipato in precedenza.

Lei è invitato a prendere visione delle seconde pagine nelle quali trova le principali istruzioni operative a cui conformarsi mentre la rimandiamo alla lettura del documento del Disciplinare interno Privacy che è stato reso disponibile sul manuale del Sistema Privacy e Protezione dei Dati pubblicato sul nostro sito web.

Per conto del Titolare

Presa visione e accettazione

Il Delegato Interno Privacy

Soggetto Autorizzato

.....

.....

Clausola di aggiornamento:

Il presente documento sostituisce e aggiorna quello di "Incaricato al Trattamento" relativo al precedente Sistema di Gestione Privacy conforme al Dlg.vo 196/03

RACCOMANDAZIONI E ISTRUZIONI SULLA GESTIONE DEGLI ACCESSI NEL LUOGO DI LAVORO

- impedire l'intrusione nei locali che gli sono stati affidati in custodia da parte di persone non autorizzate secondo quanto stabilito dal *Responsabile del Trattamento*;
- impedire il danneggiamento, la manomissione, la sottrazione, la distruzione, o la copia di dati nei locali che gli sono stati affidati in custodia da parte di persone non autorizzate secondo quanto stabilito dal *Responsabile del Trattamento*;
- conservare i documenti contenenti i dati sensibili in contenitori muniti di serratura;
- identificare e registrare i soggetti ammessi dopo l'orario di chiusura degli uffici stessi.

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

Purtroppo la sottrazione di personal computer, cellulare o supporto di memoria asportabile è assai frequente, SI RACCOMANDA di proteggere con password forte l'accesso al dispositivo in modo da garantire:

- Protezione contro la perdita fisica dell'apparato
- Protezione contro accesso non autorizzato ai dati
- Copia di rispetto di dati archiviati sull'apparato
- Trasferimento controllato e sicuro dei dati dall'apparato aziendale.
- La protezione contro la sottrazione o smarrimento

RACCOMANDAZIONI DI SICUREZZA DIGITALE

- Utilizzate sempre il codice identificativo personale e le parole chiave, cambiandole ogni qual volta abbiate la sensazione che esse non ne siano sufficientemente sicuro; laddove possibile, utilizzate sempre almeno 8 caratteri, mescolando caratteri maiuscoli e minuscoli.
- La parola chiave deve essere preferibilmente priva di significato e non deve mai essere comunicata a soggetti terzi, anche se fiduciari.

- Ricordate che in caso di trattamento di dati sensibili la parola chiave deve essere cambiata almeno ogni tre mesi, e se questo intervallo viene ridotto, tanto meglio.
- Si raccomanda di evitare di utilizzare la stessa parola chiave sia sui computer portatili che su quelli fissi.
- Non tenete mai insieme la copie di backup ed il personal computer, per evitare che un eventuale furto possa coinvolgere sia i dati del personal computer portatile, che quelli di backup.

ELENCO DELLE CHIAVI GESTITE DALLA S.V.

FISICHE

DIGITALI

IL TITOLARE DEL TRATTAMENTO
DESIGNATO

IL

SPPD

Framework

M.S.P.

