|  |  |  |
| --- | --- | --- |
|  | **Istruzioni rivolte agli Incaricati del trattamento dei dati**  **(All. Beta)** |  |

**PRINCIPI GENERALI DA OSSERVARE**

In relazione alle istruzioni di cui al presente documento è doveroso ricordare che in ambito “privacy” il lavoratore subordinato assume il duplice ruolo di interessato, e quindi soggetto di tutela in riferimento ai propri dati personali trattati dal titolare/datore di lavoro per adempiere a tutte le obbligazioni previsti per l’esecuzione del contratto di lavoro, e delegato dal titolare del trattamento allorquando per eseguire le mansioni affidate debba trattare dati personali di altri interessati (clienti, fornitori, dipendenti) per conto del titolare.

Per quanto detto il dipendente nella sua qualità di interessato è informato in merito ai suoi diritti con specifica informativa dedicata ai dipendenti e collaboratori mentre con il presente documento vengono declinati i doveri ai quali attenersi per eseguire le mansioni affidate con il contratto di lavoro.

Tutto ciò premesso al fine di una corretta applicazione del Reg. UE n. 679/2016, di seguito più brevemente denominato “GDPR” e del D.Lgs. n.196/03 “Codice della Privacy”, di seguito più brevemente denominato “Codice”, i soggetti nominati Incaricati del trattamento di dati personali dovranno attenersi alle **seguenti istruzioni** sotto la vigilanza del Responsabile del trattamento dei dati della Struttura di assegnazione:

* effettuare le operazioni di trattamento dei dati personali (ivi compresi i dati sanitari, etnici e giudiziari- di seguito “dati”) strettamente necessarie allo svolgimento delle attività cui si è preposti secondo i propri ~~gli~~ ambiti di trattamento così come regolamentati all’interno della Struttura di assegnazione;
* trattare tutti i dati di cui si viene a conoscenza nell’ambito dello svolgimento delle proprie funzioni, in modo lecito e secondo correttezza e, comunque, in modo tale da garantire, in ogni operazione di trattamento, la massima riservatezza;
* verificare che i dati trattati siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati. In particolare secondo il principio di “minimizzazione” trattare i dati particolare ulteriori rispetto a quelli personali e sanitari, come per esempio i dati etnici e giudiziari, solo quando strettamente necessario per la tutela dell’interessato,
* accedere unicamente alle banche dati presenti presso l’Unità Organizzativa in cui si presta la propria attività lavorativa;
* mantenere assoluto riserbo sui dati di cui si viene a conoscenza nell’esercizio delle proprie funzioni;
* evitare l’uso di strumenti informatici personali ed il cellulare per il trattamento dei dati acquisiti durante l’attività di servizio anche per pareri e consulenze;
* utilizzare il PC, internet e la posta elettronica in conformità con le linee guida del Garante per la protezione dei dati personali in materia, con la Politica Aziendale della Privacy (A1107\_P22\_POL01) pubblicata in intranet, nonché con le prescrizioni emanate dai Sistemi Informatici Aziendali per l’uso di internet, del sistema di posta elettronica ed in genere di tutti gli strumenti informatici, disponibili sul sito aziendale ed in intranet quando pubblicate;
* prendere nota e conseguentemente attenersi alle disposizione contenute nella Politica Aziendale in materia di Privacy in tema di conservazione ed archiviazione dei dati e di accesso agli archivi locali e centralizzati di raccolta dei dati.

**PER I TRATTAMENTI EFFETTUATI SENZA L’AUSILIO DI STRUMENTI ELETTRONICI**

* I documenti contenenti dati personali, sanitari, etnici e giudiziali (di seguito “dati”) devono essere custoditi in modo da non essere accessibili a persone non incaricate del trattamento (es. armadi o cassetti chiusi a chiave).
* I documenti contenenti dati prelevati dagli archivi per l’attività quotidiana devono esservi riposti a fine giornata.
* I documenti contenenti dati non devono rimanere incustoditi su scrivanie o tavoli di lavoro. In caso di allontanamento, anche temporaneo, dal posto di lavoro, adottare le misure in atto a propria disposizione, secondo le istruzioni ricevute, per evitare l’accesso ai dati trattati o in trattamento, da parte di terzi, anche se dipendenti, a meno che non siano autorizzati.
* I documenti contenenti dati non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (anche se queste persone sono a loro volta incaricate del trattamento).
* Qualora sia necessario distruggere i documenti contenenti dati, questi devono essere distrutti utilizzando gli appositi apparecchi “distruggi documenti” o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.
* I documenti che contengono dati sanitari e/o giudiziari devono essere oggetto di particolare attenzione nei controlli e custodia degli Incaricati, che devono impedire l’accesso a persone prive di autorizzazione.
* L’archiviazione dei documenti cartacei contenenti dati sanitari e/o giudiziari deve avvenire in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave.
* Nel caso di trattamento dei dati è necessario trattare i soli dati la cui conoscenza sia strettamente necessaria per adempiere i compiti di ufficio.

**PER I TRATTAMENTI EFFETTUATI CON L’AUSILIO DI STRUMENTI ELETTRONICI**

* Il trattamento di dati personali, sanitari, etnici e giudiziali (di seguito “dati”) con strumenti elettronici è consentito agli Incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'Incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'Incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
* Non scrivere le proprie password su supporti facilmente rintracciabili e soprattutto in prossimità della postazione di lavoro utilizzata.
* Non scegliere password corrispondenti a parole presenti in un dizionario, sia della lingua italiana sia di lingue straniere.
* Non usare come password parole che possano essere facilmente riconducibili all’identità dell’utente.
* La password assegnata all’Incaricato è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sanitari e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
* La password deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.
* Nel digitare la password accertarsi che non ci sia nessuno che osservi e sia in grado di vedere od intuire i caratteri digitati sulla tastiera.
* Nel caso di trattamento di dati effettuato mediante elaboratori non accessibili da altri elaboratori, è necessario utilizzare la parola chiave (password) fornita per l’accesso ai dati.
* Nel caso di trattamento di dati effettuato mediante elaboratori accessibili da altri elaboratori, solo in rete locale, o mediante una rete di telecomunicazioni disponibili al pubblico, è necessario:
* utilizzare la parola chiave (password) fornita per l’accesso ai dati;
* servirsi del codice identificativo personale per l’utilizzazione dell’elaboratore.
* In presenza di ospiti farli attendere in luoghi in cui non siano presenti informazioni riservate o dati.
* Non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento. In caso di allontanamento, anche temporaneo, dal posto di lavoro, adottare le misure in atto a propria disposizione, secondo le istruzioni ricevute, per evitare l’accesso ai dati trattati o in trattamento, da parte di terzi, anche se dipendenti, a meno che non siano autorizzati.
* Se si rileva un problema nell’ambito dell’utilizzo del sistema informatico relativo al trattamento di dati in corso che può compromettere la sicurezza dei dati se ne dà immediata comunicazione al Responsabile del trattamento.
* Accedere unicamente alle banche dati presenti presso l’Unità Organizzativa in cui si presta la propria attività lavorativa.
* Evitare di creare banche dati nuove senza espressa autorizzazione del Titolare o del Responsabile del trattamento dei dati.
* È fatto assoluto divieto di comunicare, diffondere i dati provenienti da banche dati aziendali, in assenza dell’autorizzazione del Titolare o del Responsabile del trattamento.
* Accertarsi che sul proprio computer sia sempre operativo un programma antivirus, aggiornato e con la funzione di monitoraggio attiva.
* Sottoporre a controllo con il programma antivirus installato sul proprio PC, tutti i supporti di provenienza esterna prima di operare con i files in essi contenuti.
* Accertarsi sempre della provenienza dei messaggi di posta elettronica contenenti allegati; nel caso che il mittente dia origine a dubbi, cancellare direttamente il messaggio senza aprire gli allegati.
* Evitare il trattamento di dati tramite e-mail senza la certezza di una protezione dei messaggi. In ogni caso evitare l’inserimento di dati all’interno del corpo mail e prevedere un allegato criptato per i trattamenti con la posta elettronica accertandosi, anche per iscritto, che l’indirizzo mail utilizzato sia quello segnalato e autorizzato dal destinatario del messaggio.
* Utilizzare la connessione ad internet esclusivamente per lo svolgimento dei propri compiti istituzionali.
* Utilizzare i dati di contatto dell’utente (es. telefono, mail) solo se espressamente segnalati ed autorizzati dall’utente stesso annotando per iscritto l’autorizzazione.
* Informare il Responsabile in caso di incidenti di sicurezza o di eventuali anomalie o stranezza di comportamento che coinvolgono i dati.

L’Incaricato dovrà osservare scrupolosamente tutte le misure di sicurezza adottate a livello aziendale (pubblicato sui siti internet e intranet aziendale sezione Privacy) e le eventuali ulteriori istruzioni (in aggiunta a quelle previste nel presente documento) che verranno comunicate dal Titolare o dal Responsabile del trattamento.

**Data, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Firma per presa visione e accettazione: l’Incaricato \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(Nome e Cognome)