A chiunque sia autorizzato a consultare, modificare, trasmettere, cancellare ovvero compiere qualsivoglia attività di trattamento a dati personale e che agisca nell'ambito dell'autorità che gli viene concessa

Data .....

Obbligo di confidenzialità

Premesso che:

a) per svolgere le mansioni previste dal contratto di lavoro in essere deve trattare dati personali;
b) è stato adeguatamente informato del fatto che ogni informazione che consente l'identificazione, diretta o indiretta, di una persona fisica, costituisce dato personale, ivi incluse informazioni quali: numeri identificativi, indicatori di posizioni, identificatori online, caratteristiche dell'identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale di tale persona fisica etc.;
c) le sono state fornite esaustive istruzioni in merito al trattamento dei dati personali ai sensi del Regolamento Generale sulla Protezione dei Dati Personali (GDPR) e delle altre disposizioni applicabili in materia.

Tutto ciò premesso, che forma parte integrante e sostanziale della presente disposizione contrattuale, le viene rammentato l'obbligo a svolgere in modo diligente la sua attività nell'ambito delle mansioni a lei assegnate e, in particolare a:

1. **trattare** dati personali unicamente in base alle istruzioni ricevute e, in ogni caso, in conformità con la normativa applicabile in materia di protezione dei dati personali, ivi incluso il GDPR;
2. **garantire** che i dati personali siano trattati in ossequio ai principi e alle norme applicabili di legge e in stretta osservanza alle istruzioni fornite;
3. **mettere** in atto ogni azione utile affinché i dati personali oggetto di trattamento nello svolgimento delle sue mansioni lavorative siano trattati solo se necessario e solo nella misura strettamente necessaria al raggiungimento delle legittime finalità del trattamento ("*minimizzazione dei dati*");
4. **assicurare** che i dati siano sempre corretti e, se necessario, aggiornati; conservati in modo tale da consentire l'identificazione degli interessati solo per il periodo di tempo necessario al raggiungimento delle finalità per le quali vengono trattati;
5. **operare** nell'ambito delle mansioni a lei assegnate affinché i dati siano trattati in modo tale da assicurare un adeguato livello di sicurezza, ivi inclusa la tutela da accessi o trattamenti non autorizzati o illeciti e da perdita accidentale, distruzione o danneggiamento, ricorrendo ad idonee misure tecniche ed organizzative ("*integrità e confidenzialità*");
6. **osservare** la più stretta confidenzialità con riferimento ai dati personali che tratterà, o ai quali avrà accesso nell'ambito dell'attività svolta e a non rivelarli ad alcuna altra persona fisica o giuridica, ivi inclusi colleghi ed altri membri del personale, che non siano espressamente autorizzati all'accesso per istruzione del datore, contratto o legge;
7. **garantire** che l'obbligo di non divulgazione e confidenzialità continui anche qualora dovesse cessare il rapporto di lavoro perdurando fino a quando non sussistano rischi per la dignità e/o la libertà dell'interessato.

Sulla scorta della formazione, informazione e sensibilizzazione ricevuta le viene rammentato che qualsiasi violazione dell'obbligo di confidenzialità o, in generale, delle norme di legge poste a tutela dei dati personali può comportare, nei confronti del Titolare del trattamento o del Responsabile, l'imposizione di rilevanti sanzioni ai sensi dell'art. 83 GDPR o di altre disposizioni applicabili europee o nazionali, nonché causare danni a persone fisiche o giuridiche.
La presente, quindi, a confermarle la natura contrattuale vincolante delle istruzioni fornitele e che la eventuale trasgressione a tali istruzioni, anche singolarmente o per episodi unici, e alle norme contenute nel presente, comporterà l'irrogazione nei suoi confronti delle sanzioni disciplinari previste dal contratto di lavoro e dalla normativa applicabile, oltre al risarcimento del danno eventualmente arrecato in esito alle violazioni perpetrate.

Nota contrattuale attinente l'obbligo di confidenzialità a validità immediata e fino a comunicazione contraria. La presente viene divulgata e pubblicizzata attraverso i canali comunicativi propri del Titolare del trattamento.

Misure di sicurezza minime da adottare ai fini della protezione dei dati

Premesso che:

- poiché il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali deve trattare tali dati secondo le istruzioni qui contenute redatte dal titolare del trattamento, fatto salvo il diritto dell'Unione o degli Stati membri;
- considerato che le istruzioni qui contenute sono da intendersi aggiuntive rispetto agli obblighi derivanti dalla legislazione applicabile, dal disposto del CCNL applicato e dai regolamenti e disposizioni interne che qui si danno per desunti.

Nel dettaglio, il responsabile del trattamento e chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, attraverso l'adozione delle misure qui indicate, **deve garantire** al titolare del trattamento un livello di sicurezza adeguato al rischio, provvedendo se del caso:

a) alla pseudonimizzazione od alla cifratura dei dati personali;
b) alla capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) alla capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) all'applicazione periodica (di norma almeno ogni 12 mesi) di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
e) all'eliminazione di qualsiasi operazione che deliberatamente presenti rischi ulteriori al trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Quanto sopra fatto salvo la possibilità concessa al responsabile del trattamento ad implementare le misure di protezione.

Ai fini della trasparenza, liceità e correttezza del trattamento dei dati personali al fine della tutela del diritto inviolabile alla dignità ed alla libertà da parte dell'interessato, si dispone quanto segue con decorrenza immediata e fino ad avviso contrario:

Trattamento dei dati in modalità cartacea

1. Il dato trattato in modo cartaceo deve essere archiviato in appositi luoghi con destinazione specifica, identificati in modo univoco, consultato e/o modificato solo per scopi legittimi, cancellato solo per decorso tempo di trattamento ovvero decorso obbligo normativo, ovvero esplicita richiesta da parte dell'interessato.
2. I dati in modalità cartacea devono essere sottoposti a backup elettronico.
3. Eventuali copie cartacee successive al backup sono da considerarsi illegittime fatto salvo:
   - ✓ requisito normativo;
   - ✓ requisito contrattuale;
   - ✓ specifica richiesta da parte dell'interessato.
4. Il dato cartaceo deve essere segregato con chiave fisica garantita dall'incaricato.
5. Deve essere utilizzata carta e inchiostri prodotti da fornitori che possano garantire un tempo di decomposizione superiore al tempo di conservazione del dato.
6. Giornalmente deve essere data priorità al corretto utilizzo delle misure antintrusione presenti.
7. Il dato cartaceo deve essere utilizzato per il tempo strettamente necessario e prioritariamente nella stessa sede di archiviazione.
8. Ad ogni trattamento deve essere eseguito il controllo sistematico della corretta imputazione del dato.
9. Tutti i dati cartacei, periodicamente, devono essere sottoposti a Backup elettronico.
10. Le copie non autorizzate devono essere immediatamente distrutte.
11. Le copie c.d. "temporanee" devono essere distrutte entro la fine dell'operazione di trattamento.
12. I Dati personali a carattere speciale c.d. "Sensibili" e/o "Giudiziari" trattati in modalità cartacea sono oggetto di misure di protezione aggiuntive, nello specifico:
    - o quando consultabili da parte di terzi, gli stessi saranno rinchiusi in cartelle non trasparenti con sigillo inamovibile e archiviati in apposito luogo con resistenza al fuoco almeno REI 60 chiuso a chiave garantita dall'incaricato;
    - o quando non consultabili da parte di terzi, gli stessi saranno archiviati in luogo con resistenza al fuoco almeno REI 60 chiuso a chiave garantita dall'incaricato.

Trattamento dei dati in modalità elettronica

1. Effettuare periodicamente il Backup in cloud tramite procedura di disaster recovery.
2. Divieto assoluto di aggiornamento ovvero installare software operativi se non sono state previste misure di prevenzione dal Responsabile di Sistema.
3. Applicazione di firewall, antivirus, antispam di ultima generazione.
4. Obbligo di gestione degli accessi tramite credenziali personali
5. Eventuali copie elettroniche successive al backup sono da considerarsi illegittime fatto salvo:
   - ✓ requisito normativo;
   - ✓ requisito contrattuale;
   - ✓ specifica richiesta da parte dell'interessato.
6. Verifica giornaliera dell'istallazione a monte dell'ingresso di alimentazione di UPS.
7. Divieto assoluto di utilizzo delle porte USB (con esclusione della keys per la firma digitale).
8. Recupero della password tramite procedura aziendale in revisione corrente.
9. Giornalmente deve essere data priorità al corretto utilizzo delle misure antintrusione presenti.
10. Obbligo di attuazione della procedura di gestione degli accessi nei luoghi di lavoro.
11. Assoluto divieto di non presidiare utenze attive.
12. Impegno costante al corretto utilizzo delle procedure aziendali in materia di divulgazione dati con mezzi elettronici.
13. I Dati personali a carattere speciale c.d. "Sensibili" e/o "Giudiziari" trattati in modalità elettronica sono oggetto di misure di protezione aggiuntive, nello specifico:
    - o criptati con chiave elettronica con grado di sicurezza sufficiente a essere elusa solo in modo fraudolento. La cifratura della chiave e le modalità di esecuzione del blocco / sblocco devono essere custoditi in luogo separato dall'archivio elettronico.
14. Per quanto qui non indicato si fa specifico rimando al regolamento dell'azienda per l'utilizzo del sistema informatico in revisione corrente.

Si ricorda che è fatto esplicito divieto di trattare, in qualsiasi forma, dati personali **non afferenti all'attività lavorativa** con strumenti cartacei e/o elettronici del Titolare del trattamento ovvero nei luoghi di lavoro sotto la responsabilità del Titolare del Trattamento.

Qualsivoglia situazione di rischio che possa configurare data breach, violazione dei dati ovvero diffusione non autorizzata o che possa aumentare il rischio di danno a libertà e/o dignità degli interessati deve essere immediatamente comunicata in modo circostanziale al Titolare del Trattamento.

Copia conforme all'originale in edizione e revisione di cui sopra composta da 3 (tre) pagine compresa la presente.
La presente viene consegnata ai Responsabili del Trattamento ed a chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento che abbia accesso a dati personali (c.d. "incaricati") quale supporto alle attività di formazione e sensibilizzazione in essere. La stessa viene divulgata tramite i canali informativi (es. bacheca aziendale, intranet, ecc.) propri del Titolare del trattamento.

Promosso in data .....

Fatto, il Titolare del Trattamento

Visto, il DPO aziendale

Giuliano Palotto

Per ricevuta, lettura e comprensione del contenuto.
In pari data, l'incaricato al trattamento dei dati .....