Atto di Nomina ad "*incarico del trattamento dei dati personali*" ai sensi dell'Art. 30 D.Lgs 196/2003

Il sottoscritto _____, Responsabile della Direzione _____ di LAZIOcrea SpA – Società Titolare del Trattamento dei dati personali ai sensi dell'art. 28 D.Lgs. 196/2003 - in qualità di Responsabile del trattamento dei dati personali nominato ai sensi dell'art. 29 D.Lgs 196/2003 dal Consiglio d'Amministrazione della società stessa in occasione della seduta del _____ - nomina i sottoscrittori della presente incaricati del trattamento dei dati personali ai sensi dell'art. 30 D.Lgs 196/2003, nell'ambito delle attività di competenza dell'Area _____, con l'avvertenza che dovranno operare osservando le direttive impartite dal sottoscritto nonché dal Responsabile dell' Area _____ in osservanza della normativa di cui al D.Lgs. n. 196/2003 (Codice della Privacy) e s.m.i.

La nomina si rende necessaria al fine di consentire il lecito svolgimento delle operazioni di trattamento dei dati personali correlate alla corretta esecuzione delle attività lavorative assegnate (vedi Organigramma e Microstruttura Aziendale pubblicati sul sito internet nella sezione società trasparente – declaratoria attività Area _____).

La presente nomina è da intendersi valida per ogni tipologia di trattamento ovvero per qualunque operazione o complesso di operazioni, effettuate con o senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati. Inoltre la stessa è da intendersi valida per qualunque tipologia di dati personali (generici, sensibili e giudiziari) trattati ai fini dell'espletamento delle attività lavorativa affidata.

A tal fine vengono fornite istruzioni e raccomandazioni per l'assolvimento dei compiti assegnati nel rispetto della normativa in materia di Privacy.

- Indicazione in ordine alle operazioni di trattamento dei dati personali

- Le operazione di trattamento dei dati personali devono essere effettuate nel rispetto della normativa vigente in materi di trattamento dei dati personali di cui al D.Lgs. n. 196/2003 e s.m.i. ovvero in osservanza dei principi di necessità, liceità, trasparenza, correttezza e proporzionalità (per ogni approfondimento si rinvia ai regolamenti/procedure aziendali pubblicata sul sito internet e sul sito intranet nelle apposite sezioni dedicata alla Privacy).
  Nel dettaglio.
- Il trattamento dei dati deve essere effettuato in modo lecito e corretto.
- I dati personali devono essere raccolti, registrati e trattati unicamente per le finalità inerenti all'attività svolta.
- Le modalità con cui si effettuano i trattamenti devono essere pertinenti e non eccedenti le finalità perseguite (ovvero l'incaricato risulta autorizzato al trattamento dei dati personali al solo fine di effettuare le proprie mansioni lavorative e/o l'incarico affidato).
- Il trattamento dei dati personali deve avvenire solo se necessario allo svolgimento della propria attività lavorativa, escludendo lo stesso quando le finalità perseguite possono essere realizzate mediante l'utilizzo di dati anonimi e/o mediante modalità che permettano di identificare l'interessato solo in caso di necessità.
- I dati personali oggetto di trattamenti devono essere raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni di trattamento compatibilmente con i predetti scopi.
- Il trattamento dei dati deve essere effettuato secondo il principio di trasparenza, ovvero deve essere assicurata la consapevolezza dell'interessato in ordine al trattamento dei dati che lo riguardano.
- Risulta necessaria la verifica costante dell'esattezza dei dati, il loro aggiornamento e la loro conservazione nel rispetto delle misure/procedure di sicurezza adottate dall'Azienda.
- L'incaricato è tenuto ad assicurarsi che i dati trattati non vadano dispersi e/o acquisiti, anche in modo incontrollato, da terzi non autorizzati al trattamento.
- Risulta necessaria la verifica costante della completezza e pertinenza dei dati trattati il cui trattamento non deve essere eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati.
- Devono essere rispettate le misure di sicurezza riportate nei Regolamenti Aziendali in materia di

trattamento dei dati personali e utilizzo dei mezzi informatici nonché le indicazioni e/o istruzioni fornite dal Titolare del Trattamento e/o dal Responsabile del Trattamento.

- Risulta vietato modificare i trattamenti esistenti e/o introdurre nuovi trattamenti senza l'esplicita autorizzazione del Responsabile del Trattamento dei dati personali.
- Le operazioni di trattamento devono essere effettuate in osservanza delle prescrizioni contenute nel Codice della Privacy nonché nei regolamenti aziendali in materia di Privacy pubblicati sia sul portale dei dipendenti che sul sito internet nelle apposite sezioni dedicate alla Privacy).

- <u>Obblighi di riservatezza</u>

L'incaricato del trattamento deve garantire la massima riservatezza in relazione ai dati personali (soprattutto sensibili) di cui venga a conoscenza nell'espletamento delle proprie attività lavorative ed in particolare:

- Risulta vietato comunicare e/o diffondere dati personali a terzi non autorizzati al trattamento senza la preventiva autorizzazione del Responsabile del Trattamento dei dati.
- Risulta vietato comunicare dati personali ad un collega autorizzato al trattamento in presenza di terzi non autorizzati.
- Risulta vietato parlare ad alta voce quando si comunicano dati personali per telefono, evitando comunque che terzi non autorizzati vengano a conoscenza di informazioni personali ascoltando la conversazione.
- L'accesso ai dati dovrà essere limitato all'espletamento delle proprie attività lavorative ed esclusivamente negli orari di lavoro.
- In caso di interruzione, anche temporanea, del lavoro risulta necessario verificare che i dati trattati non siano accessibili a terzi non autorizzati.
- Le attività, nel cui ambito vengono effettuate le operazioni di trattamento, devono essere svolte secondo le prescrizioni contenute nei Regolamenti/Procedure Aziendali in materia di Privacy e in materia di utilizzo dei mezzi informatici, posta elettronica e internet (pubblicati sia sul portale dei dipendenti che sul sito internet nelle apposite sezioni dedicate alla Privacy) nonchè secondo le istruzioni e/o raccomandazioni del Responsabile del Trattamento dei dati.
- In caso di incidente di sicurezza che coinvolga dati personali (soprattutto dati sensibili) risulta necessario informare tempestivamente il Responsabile del Trattamento e/o l'Amministratore di

Sistema.

- Risulta necessario raccogliere, registrare e conservare i dati presenti nei files informatici e nei documenti cartacei avendo cura che l'accesso agli stessi sia reso possibile solo al personale autorizzato.
- Qualora giungano richieste telefoniche di dati personali da parte dell'Autorità Giudiziaria o degli Organi di Polizia, risulta necessario assicurarsi circa l'identità del chiamante nonché chiedere l'autorizzazione al Responsabile del Trattamento prima di comunicare i dati stessi.
- Risulta opportuno registrare tutte le richieste di comunicazione della documentazione che contiene dati sensibili (eventualmente utilizzare un apposito registro di carico e scarico se autorizzato dal Responsabile del Trattamento).
- Risulta necessario distruggere o comunque rendere illeggibili i documenti cartacei non più utilizzati, prima che gli stessi vengano cestinati.

Gli obblighi di cui sopra, relativi alla riservatezza dei dati trattati, ovvero dei dati personali di cui l'incaricato è venuto a conoscenza per ragioni di lavoro, dovranno essere osservati anche a seguito di modifica dell'incarico e/o di cessazione del rapporto di lavoro.

- Obblighi inerenti al trattamento con l'ausilio di strumenti elettronici

In base a quanto stabilito dalla normativa vigente in materia di Privacy – art. 33, 34 e 36 D.Lgs. 196/2003 e Disciplinare Tecnico in materia di misure minime di sicurezza (Allegato B stesso decreto) - per le operazioni di trattamento dei dati personali effettuate con strumenti elettronici, l'incaricato del trattamento deve osservare le misure di sicurezza adottate dall'Azienda e specificate nei Regolamenti Aziendali in materia di Privacy e in materia di utilizzo di strumenti informatici, internet e posta elettronica pubblicati sul portale dei dipendenti (e/o sul sito aziendale internet) nell'apposita sezione dedicata alla Privacy.

In particolare si elencano di seguito gli obblighi inerenti alle **credenziali di autenticazione (password)**.

L'incaricato deve adottare le necessarie cautele per assicurare la segretezza della componente riservata delle proprie credenziali di autenticazione (password) nonché la diligente custodia dei dispositivi elettronici (computer) in uso esclusivo e/o comunque in possesso dell'incaricato.

Nel dettaglio risulta necessario:

- Elaborare la password secondo le indicazioni dell'Amministratore di Sistema e/o del Responsabile dei Sistemi Infrastrutturali e conservare la segretezza sulla stessa e sulle altre componenti riservate della credenziale di autenticazione (*username*).
- Rispettare i profili di autorizzazione attribuiti ai fini dell'accesso ai dati ovvero all'utilizzo di determinati applicativi informatici e/o piattaforme informatiche nell'ambito delle attività lavorative assegnate;
- Custodire in modo diligente i dispositivi elettronici in possesso e/o in uso esclusivo.

Al riguardo si precisa quanto segue:

- La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri, di cui almeno quatto devono essere di natura numerica.
- Risulta necessario che la parola chiave non contenga riferimenti agevolmente riconducibili all'incaricato; quindi, la parola chiave non deve essere: il nome o il cognome dell'incaricato, il soprannome, la data di nascita propria, dei figli o degli amici, il nome di un hobby o di una passione conosciuta o facilmente conoscibile dai colleghi, il nome e cognome di personaggi famosi, etc.
- Risulta inoltre vietato:
  - rivelare la parola chiave a terzi non autorizzati;
  - scrivere la parola chiave in un messaggio di posta elettronica;
  - rivelare la parola chiave al superiore;
  - dare indicazione in merito al formato ed alla lunghezza della parola chiave;
  - svelare la parola chiave su questionari e/o su formulari di sicurezza,

- La parola chiave deve essere modificata dall'incaricato almeno ogni sei mesi (il sistema prevede in automatico la modifica della parola chiave ogni tre mesi); in caso di trattamento di dati sensibili e/o di dati giudiziari la parola chiave deve essere modificata obbligatoriamente ogni tre mesi.
- L'incaricato ha l'obbligo di terminare la sessione di lavoro, al computer, ogni volta che si deve allontanare, anche solo per poco tempo, dal proprio ufficio;
- Spetta all'incaricato mettere in atto gli accorgimenti ritenuti più opportuni affinché anche in sua assenza, il computer non resti incustodito e/o accessibile a terzi non autorizzati.
- In ogni caso deve essere attivata la funzione *screen saver* qualora l'incaricato si allontani, anche solo per pochi minuti, dal proprio ufficio.
- Risulta, inoltre, importante curare la conservazione e la segretezza della parola chiave evitando di

trascriverla su supporto cartaceo precario o visibile (es. post-*it*) oppure di tenerla nel portafoglio o trascritta nella prima pagina dell'agenda o della rubrica di ufficio o in qualunque altro posto facilmente intuibile;

(N.B. Al fine di tutelare l'integrità dei dati trattati e memorizzati sui files di rete, si precisa che l'azienda ha adottato un sistema di *back up che* opera in automatico a fine giornata lavorativa.

- **Obblighi inerenti ai trattamenti senza l'ausilio di strumenti informatici**

In base a quanto stabilito dalla normativa vigente in materia di Privacy - artt. 33, 35 e 36 D.Lgs. n. 196/2003 e del Disciplinare Tecnico in materia di misure minime di sicurezza (Allegato B al D. Lgs. n. 196 del 30 giugno 2003) - per i trattamenti di dati personali effettuati senza l'ausilio di strumenti elettronici - l'incaricato del trattamento deve osservare le misure minime di sicurezza adottate dall'Azienda e specificate nei Regolamenti/Procedure Aziendali in materia di Privacy. In particolare l'incaricato ha l'obbligo di rispettare le procedure e/o i regolamenti aziendali in ordine alla custodia di atti e documenti affidati per lo svolgimento delle mansioni lavorative assegnate, alla conservazione di determinati documenti in archivi ad accesso selezionato e alle modalità di accesso agli archivi stessi.

Nel dettaglio si elencano di seguito le regole principali che l'incaricato deve osservare nelle operazioni di trattamento dei dati personali.

- I documenti che contengono dati personali non devono essere portati al di fuori dei locali individuati per la loro conservazione, se non in casi del tutto eccezionali, e nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento.
- Nel periodo di tempo in cui i documenti che contengono dati personali si trovano al di fuori dei locali individuati per la loro conservazione, l'incaricato del trattamento non deve lasciarli mai incustoditi.
- L'incaricato del trattamento deve inoltre controllare che i documenti che contengono dati personali, composti da numerose pagine o più raccoglitori, siano sempre completi ed integri.
- Al termine dell'orario di lavoro, l'incaricato del trattamento deve riportare tutti i documenti che contengono dati personali nei locali (Archivi) individuati per la loro conservazione.
- I documenti (Faldoni, Raccoglitori, Fascicoli, etc.) che contengono dati personali non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro.

- Risulta necessario adottare ogni cautela affinché persone non autorizzate non vengano a conoscenza dei dati personali contenuti nei documenti utilizzati per lo svolgimento delle mansioni lavorative.
- Per evitare il rischio di divulgazione dei dati personali si deve limitare l'utilizzo di copie fotostatiche. Particolare cautela deve essere adottata quando i documenti sono consegnati in originale ad un altro incaricato debitamente autorizzato;

Risulta inoltre vietato:

- Effettuare copie fotostatiche o di qualsiasi altra natura - non autorizzate dal Responsabile del Trattamento dei dati personali - di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati personali oggetto del trattamento.
- Sottrarre, cancellare, distruggere - senza l'autorizzazione del Responsabile del Trattamento dei dati personali - stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati personali oggetto del trattamento.
- Consegnare - a persone non autorizzate dal Responsabile del Trattamento dei dati personali - stampe, tabulati, elenchi, rubriche e, più in generale, ogni altro materiale che contiene dati/informazioni personali oggetto del trattamento.

In riferimento, invece, agli obblighi inerenti alla sicurezza degli archivi cartacei nonché alla sicurezza nella cancellazione dei dati si elencano le seguenti regole che l'incaricato deve osservare.

Sicurezza Archivi Cartacei

- L'accesso agli archivi cartacei è limitata al solo personale autorizzato al trattamento e ai soli dati la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati.

(N.B. La chiave degli archivi è fornita ai soli soggetti autorizzati).

Nel caso di dati sensibili e giudiziari, inoltre, devono essere osservate le seguenti regole:

- Le cartelle o fascicoli o supporti cartacei di vario genere che contengono dati personali devono essere conservati in armadi (Archivi) muniti di serratura con chiave che devono essere chiusi al termine della giornata di lavoro dall'incaricato del trattamento.
- Maggiori cautele devono essere utilizzate per i documenti e/o atti che contengono dati sensibili e giudiziari; in particolare i menzionati dati affidati all'incaricato del trattamento, qualora non vengano utilizzati, devono essere conservati in contenitori chiusi a chiave fino al loro rientro in

archivio.

(N.B. Ai fini della sicurezza degli archivi cartacei la LAZIOcrea S.p.A. ha adottato dispositivi di sicurezza passiva come rilevatori di fumo, allarme, estintori).

Sicurezza nella cancellazione dei dati

- La cancellazione dei dati personali può essere effettuata – previa autorizzazione del Responsabile del Trattamento - quando la conservazione degli stessi non è più necessaria per legge e/o per gli scopi per cui sono stati raccolti e successivamente trattati.
- I dati personali possono essere cancellati anche su richiesta dell'interessato, sempre che la conservazione non sia necessaria per legge e/o per la gestione del rapporto di lavoro (e/o contrattuale nel caso di consulenti e/o fornitori), sempre previa autorizzazione del Responsabile del Trattamento.
- L'eventuale distruzione dei dati deve essere effettuata con sistemi meccanici o automatizzati in modo da evitare ogni possibile recupero. In caso di cancellazione dei dati memorizzati sui files elettronici, l'incaricato è tenuto al rispetto dei regolamenti aziendali in ordine alla funzione "svuotamento del cestino in modalità sicura".
- I documenti che contengono dati personali forniti all'Azienda per l'esecuzione della propria attività lavorativa dovranno essere restituiti e/o cancellati – previa autorizzazione del Responsabile del Trattamento - alla cessazione del rapporto di lavoro e/o comunque in tutti i casi in cui il trattamento dei dati personali non risulta essere necessario ai fini dell'espletamento delle mansioni lavorative assegnate, salvo diversa prescrizione di legge.

In ogni caso l'incaricato del trattamento ha l'obbligo di controllare e custodire i dati personali oggetto del trattamento in modo da evitare o, comunque, ridurre al minimo i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta.

Per quanto non previsto nella presente lettera di incarico, si precisa che sarà cura del Responsabile del Trattamento fornire ogni altra istruzione e/o raccomandazione in ordine alle operazioni di trattamento dei dati personali, alla gestione e custodia degli stessi nel rispetto della vigente normativa in materia di Privacy nonché nel rispetto delle normative applicabili alle diverse tipologie di attività effettuate nei singoli

uffici/Aree (es. normativa in materia di Archivio, in materia di Salute e Sicurezza sui luoghi di lavoro, in materia di atti e documenti amministrativi, etc.).

La presente nomina si intende valida per tutta la durata delle attività lavorative assegnate. In caso di cessazione del rapporto di lavoro (anche interruzione temporanea delle attività lavorative come ad es. nei casi di aspettativa, congedi parentali, maternità, etc.) e/o cambiamento delle mansioni affidate, è vietato comunicare e/o diffondere dati personali di cui l'incaricato è venuto a conoscenza nell'espletamento delle mansioni lavorative svolte.

Per ogni altra misura di sicurezza e/o istruzione e/o raccomandazione non contemplate nella presente lettera, si rinvia ai Regolamenti/Procedure Aziendali in materia di trattamento dei dati personali pubblicati sul sito internet e sul portale dei dipendenti nelle apposite sezioni dedicate alla Privacy e/o pubblicati nelle sezioni dedicate ai Fornitori e/o dedicate alla pubblicazione del Modello Organizzativo di Gestione e Controllo della LAZIOcrea SpA.

Roma,

Il Responsabile del Trattamento

Direzione _____

_____

Roma,

Per conoscenza e accettazione

Gli incaricati del trattamento

_____