ALLEGATI REG. 27 DEL 2020

Art. 6
(Inserimento degli allegati II, LL, MM e NN al r.r.1/2002 e successive modificazioni)

1. Dopo l'allegato HH del r.r. 1/2002 e successive modificazioni sono inseriti i seguenti:

"ALLEGATO II (art. 474, c.1)
SCHEMA REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

Denominazione Trattamento	Denominazione del trattamento
Descrizione Trattamento	Breve descrizione dei trattamenti effettuati e indicazione se il trattamento è su larga scala.
Finalità	Finalità perseguite dal trattamento.
Base giuridica e fonte normativa	E' riportata la base giuridica del trattamento ai sensi dell'art. 6 del RGPD e la fonte normativa che disciplina le attività svolte.
Categoria di interessato	Persona fisica cui si riferisce il dato trattato.
Categoria del dato	Tipologia di dato trattato, in base alla seguente classifica: • personale (art. 4, punto 1) RGPD) • personali giudiziari (art. 10 del RGPD) • personali sensibili (art. 9 del RGPD)
Trasferimento all'estero dei dati	Indica se il trattamento prevede il trasferimento dei dati all'estero.
Termine di cancellazione dati	Termine di cancellazione dei dati previsto da eventuali normative.
Modalità del trattamento	Nome delle applicazioni software/sistemi utilizzate a supporto del trattamento e indicazione di eventuali archivi cartacei
Destinatari dei dati	Soggetti cui i dati possono essere comunicati.
Responsabili del Trattamento	Soggetti che effettuano operazioni di trattamento di dati per conto della Regione Lazio.
Contitolari del Trattamento	Eventuali soggetti contitolari
Misure di sicurezza tecnica e organizzative	Descrizione delle misure

ALLEGATO LL (art. 474, c. 7)

DISCIPLINARE TECNICO PER AMMINISTRATORI DI SISTEMA

Premessa

Il presente disciplinare tecnico descrive le basilari regole tecniche ed organizzative che gli amministratori di sistema devono applicare per garantire la sicurezza dei dati e delle informazioni trattate con l'utilizzo di strumentazioni informatiche nella Regione.

Tenendo conto di quanto esplicitato nel Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 (Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema) pubblicato sulla G.U. n. 300 del 24.12.2008, e successive modificazioni, la definizione di "amministratori di sistema", ai fini dell'applicazione del presente disciplinare, è la seguente:

"sono le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti (quali ad es. gli amministratori di dominio e di server), nonché le altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi."

Gli amministratori di sistema così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente «responsabili» di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

Attività tecniche quali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti «in chiaro» le informazioni medesime.

Pertanto, considerata la delicatezza di tali peculiari mansioni e i rischi ad esse associati, la designazione di un amministratore di sistema non può prescindere da alcune considerazioni e accorgimenti:

a) valutazione delle caratteristiche soggettive: l'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza;

b) designazioni individuali: la designazione quale amministratore di sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;

c) elenco degli amministratori di sistema: gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante. Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori, la Regione rende nota o conoscibile l'identità degli amministratori di sistema con comunicazione effettuata nell'ambito del portale di comunicazione interna Intranet;

d) servizi in outsourcing: nel caso di servizi di amministrazione di sistema affidati in outsourcing la Regione conserva, presso la direzione competente in materia di

Sistemi Informativi, ognuno per la parte di propria competenza, direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema;

e) verifica delle attività: l'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del titolare del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti;

f) registrazione degli accessi: devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste.

Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Ai fini del presente disciplinare, si intende per sistema informativo il complesso dei dati, delle applicazioni, delle risorse tecnologiche, delle risorse umane, delle regole organizzative e delle procedure deputate all'acquisizione, memorizzazione, consultazione, elaborazione, conservazione, cancellazione, trasmissione e diffusione delle informazioni. Esempi di sistemi informativi sono server (file, database, web, mail, ecc.), applicazioni, apparati di rete (router, switch, ecc.), strumenti di sicurezza (firewall, IPS, ecc.).

Applicabilità

Le regole illustrate nel disciplinare tecnico si applicano a tutti i dipendenti appartenenti all'organico della Regione e a tutti coloro che a vario titolo svolgono attività, compiti, mansioni come amministratori di sistema.

Principi generali

È compito di ogni amministratore di sistema comprendere le minacce di sicurezza incombenti sui propri sistemi e adottare le contromisure di sicurezza necessarie ad assicurare confidenzialità, integrità e disponibilità dei dati e delle informazioni.

A titolo esemplificativo tali minacce possono essere:

- *minacce incombenti sui dati* (furto di dati, incluse credenziali di accesso a basi dati; distruzione anche accidentale di dati; modifica di dati, anche intenzionale, per introdurre informazioni false e fuorvianti);
- *minacce incombenti sulle applicazioni e sui sistemi operativi* (attacchi di vario tipo quali virus, spamming, SQL injection, Denial of Service; accessi non autorizzati, anche non intenzionali);
- *minacce incombenti sull'infrastruttura* (furto di apparecchiature; danneggiamento/distruzione di apparecchiature sia intenzionale che accidentale; smarrimento di apparecchiature o credenziali; reazione inadeguata ad incidenti/disastri).

Sicurezza fisica

L'accesso fisico ai locali della Regione è regolato dall'apposito disciplinare tecnico regionale in materia.

La scelta dei locali in cui installare, conservare o utilizzare sistemi informatici deve essere fatta tenendo in considerazione i potenziali rischi di sicurezza sui dati causati tanto da eventi accidentali quanto da dolo. In funzione dell'analisi dei rischi devono essere valutate e adottate idonee misure di protezione, quali sistemi di antintrusione, sistemi antincendio, sistemi di rilevazione fumi, sistemi antiallagamento.

La scelta delle misure di sicurezza dei locali deve, in ogni caso, tenere conto dei vincoli imposti dalla normativa in materia di tutela della salute e di sicurezza dei lavoratori.

La protezione dei server e degli apparati di rete considerati critici per il funzionamento e la disponibilità dei sistemi informativi deve prevedere sistemi di protezione elettrica quali stabilizzatori di corrente ed apparecchiature UPS e sistemi di condizionamento dell'aria nei locali per garantire il mantenimento di una costante ed adeguata temperatura di esercizio.

La scelta dei locali per gli armadi deve essere fatta individuando ambienti idonei, possibilmente dedicati e ad accesso limitato (solo agli amministratori di sistema e ad un eventuale custode incaricato). Gli armadi medesimi devono essere chiusi a chiave e le relative chiavi devono essere in possesso dei soli amministratori di sistema (e di un eventuale custode specificatamente incaricato). Le chiavi di accesso a locali o armadi possono essere conservate presso le portinerie della Regione.

Controllo dell'accesso ai dati

L'accesso ai dati ed alle strumentazioni informatiche utilizzate per trattarli deve essere concesso al solo personale espressamente autorizzato (nel caso di dati personali i cosiddetti incaricati del trattamento). L'elenco del personale incaricato deve essere aggiornato almeno a cadenza annuale.

In nessun modo devono essere concessi permessi di accesso ai sistemi senza preventiva autorizzazione formale del responsabile funzionale o del referente regionale di progetto. Le modalità con cui viene formulata tale autorizzazione possono variare a seconda del tipo di trattamento.

Autenticazione

L'accesso ai dati trattati con strumentazioni informatiche deve essere concesso esclusivamente previa opportuna autenticazione.

Gli strumenti di autenticazione devono essere progettati in funzione del valore dei dati trattati. Deve essere prevista l'ipotesi di utilizzo di sistemi di autenticazione forte ove necessario (smart card, token hardware, dispositivi one-time password, sistemi biometrici).

Devono essere previsti meccanismi di separazione dei privilegi, sia a livello di sistema operativo che a livello applicativo, per consentire l'accesso ai dati e le operazioni effettuate sugli stessi, in misura corrispondente ai diversi profili degli utenti.

Autorizzazione

È necessario introdurre dei criteri generali di definizione dei ruoli amministrativi e di gestione delle autorizzazioni, pur nel pieno rispetto dei principi di delega e di autonomia dei referenti di applicazioni e sistemi che gestiscono porzioni del sistema informativo.

Il principio generale a cui attenersi è che i ruoli amministrativi critici non si devono sovrapporre. Ad esempio, gli sviluppatori non devono essere anche sistemisti, gli amministratori della sicurezza non devono essere sistemisti o sviluppatori e così via. Qualora non fosse possibile dal punto di vista organizzativo mantenere o adottare questa separazione di ruoli, devono essere introdotti controlli compensativi che permettano di

tracciare puntualmente le operazioni eseguite (ad esempio tramite l'utilizzo di strumenti evoluti di monitoraggio, audit puntuali, notifiche via e-mail).

Gestione delle credenziali
Le credenziali consentono all'utente di accedere ai dati e pertanto è necessario che la loro assegnazione segua procedure codificate e condivise. Tali procedure possono essere diverse in funzione sia del valore dei dati da trattare che dei sistemi coinvolti.

In generale, le richieste delle credenziali di autenticazione devono essere fatte dai responsabili funzionali o referenti regionali di progetto. In ogni caso, deve essere tenuta traccia della richiesta che ha generato la creazione di una credenziale di autenticazione sul sistema. Le modalità con cui sono formulate le richieste variano in funzione della criticità dei dati o dei sistemi (per esempio e-mail, lettera protocollata, determinazione).

Ogni credenziale di autenticazione deve riferirsi ad un singolo utente. Non è consentito l'utilizzo di credenziali condivise. Fanno eccezione a questa regola le credenziali amministrative di accesso ai sistemi (es. root, administrator), che devono comunque essere assegnate ad un numero limitato di incaricati e devono essere utilizzate solo nel caso di interventi particolari sui sistemi. Ove possibile, bisogna privilegiare sempre l'utilizzo di credenziali nominative anche nel caso di operazione di amministrazione dei sistemi.

La gestione delle credenziali deve seguire le procedure documentate per i vari sistemi di autenticazione. La policy di scadenza delle credenziali non utilizzate è normalmente di 180 giorni. Fa eccezione a questa regola il dominio applicativo esterno per la peculiarità di alcune applicazioni che sono utilizzate dagli utenti con periodicità annuale: in questo caso le credenziali non utilizzate sono disabilitate dopo un anno. Le policy di gestione delle password devono essere allineate sui diversi sistemi e comunque conformi ai dettami delle norme in materia di protezione dei dati personali.

Le credenziali amministrative non nominative di gestione dei sistemi non sono vincolate alle stesse regole delle credenziali nominative, non scadono dopo un periodo di inutilizzo, non vengono bloccate dopo un certo numero di tentativi errati, non hanno la password che scade e non ne viene richiesta la modifica al primo accesso. Perciò gli amministratori dei sistemi sono tenuti ad adottare politiche manuali di modifica delle password dei loro sistemi e a monitorare gli eventuali tentativi di accesso non autorizzato. Le credenziali amministrative non nominative create al solo scopo di avviare servizi sui server non devono poter effettuare l'accesso interattivo sui sistemi stessi o, ove ciò non fosse tecnologicamente possibile, deve essere comunque monitorato il loro utilizzo per scopi diversi rispetto all'ambito per cui sono state create.

Le credenziali di autenticazione con privilegi amministrativi non devono essere inviate via e-mail: in tali casi, è necessario convocare l'utente e fornirgli le credenziali verbalmente, oppure mediante un sistema di scambio informazioni sicuro.

Gli amministratori dei sistemi sono tenuti a rispettare le procedure adottate e a non creare particolarità o eccezioni nella gestione delle credenziali utente.

La gestione delle credenziali amministrative deve seguire regole molto rigide e stringenti: devono essere identificate le persone autorizzate a richiedere l'aggiunta o la modifica di amministratori dei sistemi o delle applicazioni e deve essere previsto un sistema di notifica che avvisi gli altri amministratori del cambiamento.

In generale una procedura di gestione delle credenziali deve prevedere:

a) l'identificazione di chi può chiedere la creazione, la modifica, la disabilitazione, la cancellazione di un'utenza, le operazioni di sblocco dell'utente o il reset della password; tale identificazione, qualora avvenga tramite telefono, deve essere fatta chiedendo alcuni dati personali al richiedente;

b) la modalità di inoltro della richiesta: alcune operazioni quali la creazione o la modifica dovranno essere fatte via e-mail o fax, altre quali il reset della password potranno anche essere fatte verbalmente dall'utente interessato tramite telefono, previa la verifica da parte degli amministratori dell'identità dell'interessato (es. tramite richiesta di alcuni dati personali);

c) l'elenco dei destinatari della richiesta: ad esempio i referenti dell'applicazione, gli amministratori dei sistemi, il servizio di help desk;

d) la tempistica di evasione della richiesta;

e) l'archiviazione e il backup delle richieste pervenute via e-mail e delle risposte relative all'attività svolta. Se la richiesta è in formato cartaceo deve essere acquisita agli atti;

f) la modalità di risposta al richiedente per comunicare l'avvenuta attivazione dell'utenza, il nome utente e la password (a tale proposito valutare se sia opportuno crittografarla, ovvero comunicarla verbalmente all'utente, ove possibile).

Le procedure di gestione delle credenziali debbono essere documentate, mantenute aggiornate e messe a disposizione in apposita sezione di Intranet ad accesso riservato per la consultazione sia da parte degli amministratori di sistema, sia da parte dei soggetti incaricati per quanto di propria competenza.

Gestione delle password
La lunghezza minima consentita per le password deve essere impostata ad almeno otto caratteri. Ove la tecnologia non lo consenta, la lunghezza delle password deve essere impostata al massimo consentito dal sistema.

La durata della password dovrebbe essere impostata in base al grado di criticità di sistemi e basi dati. Inoltre, una eventuale password di "single sign on" è opportuno abbia una durata inferiore a quella delle password che sostituisce.

Per contrastare attacchi alle password di tipo "brute-force" i sistemi informatici devono prevedere opportuni meccanismi per la disabilitazione di un account dopo un intervallo finito di tentativi di accesso non riusciti. Devono comunque essere previsti meccanismi di difesa da attacchi di tipo *denial of service* causati dal blocco volontario di account legittimi. Un esempio di tali meccanismi di difesa è di consentire per un account un limite massimo di cinque tentativi di accesso non riusciti, prevedendo il blocco dell'account per un periodo di trenta minuti nel caso in cui tale limite venga superato.

Ove tecnologicamente possibile, deve essere data agli utenti la possibilità di modificare la propria password senza l'intervento degli amministratori.

Devono essere previsti meccanismi di implementazione dei sistemi tali da garantire all'utente la modifica della propria password al primo accesso al sistema.

Le password non devono essere conservate in chiaro, né trasmesse su canali non cifrati. Per la loro conservazione devono essere utilizzati adeguati meccanismi di cifratura anche in funzione del valore dei dati, per esempio, hash calcolati con funzioni irreversibili per la conservazione su disco; analogamente per la loro trasmissione devono essere utilizzati protocolli di comunicazione cifrati come SSL.

In caso di trattamento di dati sensibili (articolo 9 del RGPD) e/o giudiziari (articolo 10 del RGPD) o comunque di rilevanza strategica, devono essere previsti sistemi di controllo delle password per consentire il solo utilizzo di password "resistenti" ad attacchi "brute-force". Per esempio, password formate con valori alfanumerici maiuscoli e minuscoli, simboli e caratteri speciali.

Al momento dell'installazione, su tutti i sistemi, devono essere modificate le password di default utilizzate dal produttore/installatore.

Protezione dei dati

Backup

Per garantire la disponibilità dei dati devono essere previste idonee procedure di backup in funzione del valore dei dati trattati. Tali procedure devono essere formalizzate per iscritto e tenute aggiornate con cadenza almeno annuale.

Con cadenza periodica (perlomeno annuale) devono essere effettuati controlli a campione (su un campione opportunamente numeroso: es. una copia per ogni mese) sulle copie di backup per verificarne la disponibilità e l'integrità.

A fronte di cambiamenti intervenuti nel sistema di backup o nei sistemi che devono essere archiviati devono essere fatti dei test di backup e restore per verificare la consistenza dei dati salvati.

Tutti i test vanno documentati in un "diario" che riporti la data del test, il sistema coinvolto, la persona che ha eseguito il test e l'esito delle operazioni effettuate.

Le copie di backup devono essere conservate in locali fisicamente separati da quelli dei sistemi origine dei dati, per garantire la disponibilità delle copie in caso di eventi accidentali quali incendi o disastri naturali. Le copie dei backup devono essere riposte, possibilmente, in casseforti le cui chiavi sono conservate da personale identificato. L'elenco del personale autorizzato deve essere regolarmente mantenuto aggiornato.

Gli amministratori devono censire e tenere aggiornate le informazioni sul backup dei sistemi da loro gestiti. In particolare, devono richiedere alla struttura competente l'attivazione del backup per i nuovi sistemi e applicazioni e devono segnalare esigenze particolari di backup che esulino dalle politiche in essere di backup centralizzato.

Gli amministratori del sistema di backup devono monitorare l'esito dei task eseguiti e, qualora rilevassero problemi, darne pronta segnalazione agli amministratori dei sistemi coinvolti.

Il sistema di backup, sia per quanto riguarda il software di base che il software applicativo, deve essere mantenuto aggiornato, in particolare relativamente alle patch/hot-fixes di sicurezza. Qualora venissero rilasciate patch/hot-fixes di sicurezza per la parte client, gli aggiornamenti sui singoli sistemi devono essere pianificati in accordo con gli amministratori degli stessi.

Le politiche di backup debbono essere documentate, mantenute aggiornate e messe a disposizione in apposita sezione di Intranet ad accesso riservato per la consultazione sia da parte degli amministratori di sistema, sia da parte dei soggetti incaricati per quanto di propria competenza.

Procedure di dismissione dei sistemi: protezione dei dati
Ogni qualvolta si dismette un dispositivo elettronico o informatico che contiene dati personali, è necessario adottare idonei accorgimenti e misure, anche attraverso soggetti terzi, tecnicamente qualificati, che attestino l'esecuzione delle operazioni effettuate o che si impegnino ad effettuarle.

Chi procede al riutilizzo di dispositivi elettronici o informatici è comunque tenuto ad assicurarsi dell'inesistenza o della non intelligibilità di dati personali sui supporti, acquisendo ove possibile, l'autorizzazione a cancellarli o a renderli non intellegibili.

Il processo di rimozione dei dati dai dischi dei computer è denominato *disk sanitizing*, *cleaning*, *purging*, o *wiping*. Il metodo scelto per "disinfettare" un disco dipende dalla criticità dei dati in esso contenuti.

Cancellare un file comporta in effetti la sola rimozione del puntatore al file. Esistono strumenti software in grado di recuperare file cancellati e quindi i dati in essi contenuti. Pertanto, per garantire la cancellazione sicura delle informazioni le tecniche possibili sono:

- Sovrascrittura: il numero di ripetizioni del procedimento considerato sufficiente a raggiungere una ragionevole sicurezza (da rapportarsi alla delicatezza delle informazioni di cui si vuole impedire l'indebita acquisizione) varia e incide proporzionalmente sui tempi delle procedure;
- Formattazione "a basso livello" (LLF) dei dispositivi di tipo hard disk, laddove possibile, attenendosi alle istruzioni fornite dal produttore e tenendo conto delle possibili conseguenze tecniche su di esso, fino alla possibile sua successiva inutilizzabilità;
- Smagnetizzazione (degaussing) dei dispositivi di memoria basati su supporti magnetici o magneto-ottici, in grado di garantire la cancellazione rapida delle informazioni anche su dispositivi non più funzionanti sui quali potrebbero non essere applicabili le procedure di cancellazione software;
- Distruzione fisica dei dispositivi.

La sovrascrittura è in genere sufficiente a garantire che i dati prima presenti non siano più recuperabili e dunque leggibili.

Smagnetizzare o distruggere fisicamente il disco garantisce l'inutilizzabilità futura del disco medesimo e dunque previene qualsiasi tentativo di recupero dei dati.

Le procedure utilizzate in caso di reimpiego o di smaltimento dei dispositivi e degli strumenti informatici debbono essere documentate, mantenute aggiornate e messe a disposizione in apposita sezione di Intranet ad accesso riservato per la consultazione sia da parte degli amministratori di sistema, sia da parte dei soggetti incaricati per quanto di propria competenza.

Protezione delle applicazioni
Design, sviluppo, deployment e gestione
Le applicazioni devono essere sviluppate dispiegate e gestite secondo i principi di privacy by design e privacy by default, secondo quanto definito da specifico disciplinare.

Protezione dei sistemi
È compito di ogni amministratore mantenere un elenco aggiornato e completo delle risorse gestite. L'elenco, nel caso di server, deve contenere almeno:

- i riferimenti fisici e logici del server (nome e indirizzo di rete), la sua ubicazione e i riferimenti relativi al backup;

- le versioni dell'hardware e del sistema operativo;
- le funzioni e applicazioni principali oppure il ruolo all'interno dell'infrastruttura regionale.

Precedentemente alla progettazione, implementazione, installazione o gestione di un sistema, deve essere effettuata un'analisi dei rischi per determinare le misure di sicurezza da adottare.

Tutti gli interventi tecnici che coinvolgono la creazione, modifica o eliminazione di uno dei meccanismi di sicurezza indicati nel disciplinare tecnico, devono essere opportunamente documentati ed autorizzati da parte del proprio referente funzionale.

Server
Gli amministratori dei sistemi server devono tener conto delle seguenti policy generali e devono documentare qualsiasi eccezione a queste regole.

Policy generale

1. Hardware, sistemi operativi, servizi ed applicazioni installati devono essere approvati dalla direzione competente in materia di Sistemi Informativi.

2. Tutte le patch/hotfixes di sicurezza rilasciate dai fornitori devono essere installate nel minor tempo possibile valutando a priori, in base al rischio, la verifica in ambiente di pre-produzione. Sono ammesse eccezioni basate su specifiche esigenze di servizio della Regione, adeguatamente giustificate, documentate e riportate dagli amministratori alla direzione competente in materia di Sistemi Informativi. I servizi non necessari devono essere rimossi/disabilitati, compatibilmente con le dipendenze del sistema in oggetto. È compito degli amministratori mantenersi costantemente aggiornati sulle patches/hotfixes da installare.

3. Servizi non sicuri devono essere sostituiti da equivalenti oggetti sicuri, ove ciò sia possibile. Per esempio servizi con traffico in chiaro (telnet) devono essere sostituiti da servizi con traffico cifrato (SSH).

4. Relazioni di fiducia tra sistemi possono essere configurate solo per specifiche esigenze di servizio. Devono essere documentate dagli amministratori ed approvate dalla direzione competente in materia di Sistemi Informativi.

5. Qualsiasi attività di amministrazione remota deve essere effettuata utilizzando canali sicuri (es. connessioni di rete con crittografia, che utilizzino SSH o IPSEC). Qualora non sia disponibile una modalità di accesso remoto sicuro, dovrebbero essere utilizzate "one-time" password per tutti i livelli di accesso.

6. I server di produzione devono essere fisicamente localizzati in un ambiente ad accesso controllato, con un impianto di condizionamento adeguato alle esigenze, ovvero in grado di mantenere la temperatura e l'umidità entro i limiti che consentono la normale operatività dei server.

7. È vietata l'installazione di hardware e software non autorizzato. Tutte le attività di modifica di hardware o software devono essere preventivamente autorizzate, preferibilmente mediante definizione e schedulazione delle attività di aggiornamento (upgrade sistema operativo, modifica hardware, ecc.).

8. Tutti i server di produzione devono essere collegati ad un sistema di UPS (Uninterruptible Power Supplies) più Gruppo Elettrogeno oppure solo UPS che consenta una disconnessione (shutdown) automatica dei server prima dell'esaurimento delle batterie.

Le modalità operative di installazione, configurazione ed aggiornamento, debbono essere documentate, mantenute aggiornate e messe a disposizione in apposita sezione di Intranet ad accesso riservato per la consultazione sia da parte degli amministratori di sistema, sia da parte dei soggetti incaricati per quanto di propria competenza.

Apparati di rete
Gli amministratori di rete, nell'attività di configurazione e gestione degli apparati di rete di produzione, devono basarsi sulle seguenti regole generali e documentare le eventuali deroghe o eccezioni.

Policy generale

1. Tutti i router dovrebbero usare un protocollo di accounting per autenticare gli utenti. L'accesso con account locali è consentito solo in situazioni d'emergenza ovvero quando non fosse disponibile il sistema centralizzato di autenticazione.

2. La password di enable deve essere configurata utilizzando il meccanismo di "enable secret" che ne permette la cifratura sicura.

3. Disabilitare le seguenti funzioni (alcuni termini inglesi non sono stati tradotti perché così sono conosciuti in ambito tecnico):

- IP directed broadcast;
- pacchetti in ingresso con indirizzi non validi come da RFC1918;
- TCP small services;
- UDP small services;
- tutti i source routing;
- tutti i servizi web;
- Protocollo CDP o similari.

4. Usare la community SNMP adottata dalla Regione e comunque diversa da *public* o *private*, oppure limitare l'accesso agli apparati impostando opportuni filtri.

5. Le regole di accesso devono essere aggiunte o modificate aderendo alle necessità della Regione.

6. I router devono avere un banner di login che notifichi a chi accede che l'apparato è proprietà della Regione e che l'accesso è consentito al solo personale autorizzato.

7. Gli apparati di rete devono essere inclusi nel sistema di gestione dei sistemi di produzione adottato dalla Regione e quindi censiti riportando i riferimenti dei responsabili tecnici.

8. Deve essere utilizzato il protocollo SSH per gestire i router.

Le modalità operative di installazione, configurazione ed aggiornamento, come pure gli schemi della rete debbono essere documentate, mantenute aggiornate e messe a disposizione in apposita sezione di Intranet ad accesso riservato per la consultazione sia da parte degli amministratori di sistema, sia da parte dei soggetti incaricati per quanto di propria competenza.

Postazioni di lavoro
Gli amministratori dei client devono tener conto delle policy generali di cui all'articolo 474 bis, comma 1, lettera e), del presente regolamento, relative alle postazioni di lavoro e devono documentare qualsiasi eccezione a queste regole.

Policy generale

1. Il software utilizzato sulle postazioni di lavoro deve essere associato ad una licenza, in accordo con le specifiche del fornitore/produttore;

2. Le postazioni di lavoro assegnate al personale dell'Ente devono essere utilizzate solo per gli scopi designati;

3. E' vietato installare hardware e software addizionale senza autorizzazione della direzione competente in materia di Sistemi Informativi ed è vietato alterare o cancellare software o modificare configurazioni su una postazione di lavoro della Regione senza autorizzazione da parte della medesima direzione.

4. Le modalità operative di installazione, configurazione ed aggiornamento, debbono essere documentate, mantenute aggiornate e messe a disposizione in apposita sezione di Intranet ad accesso riservato per la consultazione sia da parte degli amministratori di sistema, sia da parte dei soggetti incaricati per quanto di propria competenza.

Dispositivi portatili
I dispositivi portatili seguono le stesse policy indicate per le postazioni di lavoro con un'attenzione maggiore alla protezione dei dati personali e alla tutela rispetto ai possibili tentativi di furto.

In caso di furto o smarrimento di un dispositivo portatile, l'amministratore di tali dispositivi deve agire tempestivamente, anche su segnalazione verbale del possessore, previa verifica dell'identità dello stesso tramite, ad esempio, la richiesta di alcuni dati identificativi personali (es. matricola, codice fiscale, ecc.).

Policy generale

Impostare la password di accesso al BIOS su tutti i dispositivi. Disabilitare, inoltre, da BIOS il boot da supporto rimovibile. Se il firmware consente di proteggere con password l'hard disk, e se lo si ritiene necessario per casi particolari e documentati, si abiliti anche questa funzionalità. La medesima password per BIOS e hard disk deve essere utilizzata su tutti i dispositivi, per accelerare gli interventi tecnici approvati.

I dispostivi portatili non devono essere lasciati in ufficio ma devono essere portati via al termine dell'orario di lavoro.

Le modalità operative di installazione, configurazione ed aggiornamento debbono essere documentate, mantenute aggiornate e messe a disposizione in apposita sezione di Intranet ad accesso riservato per la consultazione sia da parte degli amministratori di sistema, sia da parte dei soggetti incaricati per quanto di propria competenza.

Gestione dei log
È compito di ogni amministratore monitorare costantemente i sistemi gestiti per prevenire e limitare gli effetti di eventuali incidenti di sicurezza. Il metodo principale per effettuare il monitoraggio è costituito dalla raccolta ed analisi dei file di log.

La definizione ed il rilevamento degli eventi di sistema deve essere effettuata in funzione del valore dei dati ed in modo tale da consentire la verifica dell'efficacia e dell'efficienza delle procedure di sicurezza. Ove possibile devono comunque essere rilevati:

- autenticazione (login e logout, riusciti e non);

- accesso ai dati classificati sensibili dal punto di vista della sicurezza (lettura e scrittura);
- modifica di funzioni amministrative (es. la disabilitazione delle funzioni di logging, la gestione dei permessi, ecc.);
- connessioni di rete (in ingresso ed in uscita).

Ove possibile ogni voce di log deve contenere:

- data/ora dell'evento;
- luogo dell'evento (macchina, indirizzo IP, ecc.);
- identità dell'utente;
- identificativo del processo che ha generato l'evento;
- connessioni di rete (in ingresso ed in uscita) relative all'evento;
- descrizione dell'evento.

In virtù del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e successive modificazioni, i log devono essere conservati in file su cui è possibile effettuare solo la scrittura incrementale o eventualmente su supporti non riscrivibili (es. CD-R). I log, opportunamente normalizzati e filtrati devono essere conservati su host dedicati. In ogni caso, deve essere possibile poter effettuare il backup dei log secondo le normali procedure di backup previste dalla Regione.

L'accesso ai log deve essere concesso al minor numero possibile di incaricati preventivamente individuati.

La frequenza di rotazione dei log è dipendente dalla frequenza di generazione degli eventi del sistema e da eventuali vincoli tecnici o legali. In ogni caso deve essere previsto un meccanismo che, successivamente al backup, sovrascriva i log esistenti ad intervalli regolari.

Ove possibile, gli amministratori devono mantenere on line i file di log contenenti gli eventi di sicurezza per almeno 1 mese.

I log devono essere conservati per un periodo di almeno 6 mesi ai sensi del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e successive modificazioni. E' opportuno che la conservazione avvenga su supporto di memorizzazione offline non accessibile in scrittura ad alcuno.

Gestione degli incidenti di sicurezza

Tutti gli amministratori devono reagire agli incidenti di sicurezza con prontezza e con spirito di cooperazione, segnalando al proprio responsabile e alla direzione competente in materia di Sistemi Informativi le violazioni di sicurezza interna o gli eventi che possono portare a credere che vi sia stata un'elusione delle misure di sicurezza previste.

Gli amministratori, dopo una prima verifica dell'accaduto, devono registrare le operazioni svolte e contattare la direzione competente in materia di Sistemi Informativi.

Per gestire correttamente gli incidenti è indispensabile avere un elenco aggiornato dei beni (assets) che permetta di identificare i sistemi/applicazioni e il relativo livello di criticità.

Le macro fasi di gestione dell'incidente sono le seguenti:

- rilevazione incidente;
- identificazione e analisi dell'incidente;

- contenimento, raccolta evidenze, rimozione e ripristino;
- chiusura dell'incidente.

Le procedure dettagliate di gestione delle violazioni di sicurezza sono oggetto di apposito disciplinare tecnico sulla gestione dei data breach.

Controlli di sicurezza

Analisi dei rischi

E' obbligo di ogni amministratore valutare i potenziali rischi di sicurezza derivanti dal design, l'installazione, l'utilizzo e la gestione dei sistemi informatici di competenza.

Ogni progetto che prevede l'installazione, l'utilizzo, la modifica, l'eliminazione di uno o più sistemi informatici, deve quindi essere preceduto da un'adeguata analisi dei rischi che tenga conto del valore delle risorse da proteggere, delle potenziali minacce di sicurezza, dei meccanismi di sicurezza.

Security audit

I sistemi informatici sono periodicamente valutati ed analizzati per identificare il livello di rischio cui le risorse sono esposte.

Opportune verifiche sono regolarmente effettuate per valutare l'efficacia e l'efficienza dei meccanismi di sicurezza utilizzati.

I security audit possono essere affidati a fornitori esterni di servizi. In tal caso è necessario farsi rilasciare da questi ultimi apposita attestazione di conformità del servizio fornito ai requisiti previsti dalla normativa vigente in materia di protezione dei dati personali.

Documentazione tecnica

Gli amministratori di sistema hanno il compito di provvedere alla documentazione e al tempestivo aggiornamento della stessa, in relazione a tutti i sistemi, banche dati, apparati di rete e sicurezza, applicazioni software di qualunque natura e complessità, nonché alle procedure operative di installazione, configurazione ed aggiornamento delle strumentazioni informatiche e telematiche di competenza. Tale documentazione deve essere messa a disposizione in apposita sezione di Intranet ad accesso riservato per la consultazione sia da parte degli amministratori di sistema, sia da parte dei soggetti incaricati per quanto di propria competenza.

ALLEGATO MM (art. 476 bis)

POLICY PER LA GESTIONE DELLE ISTANZE DEI SOGGETTI INTERESSATI AI SENSI DEL RGPD

SOMMARIO

1. Premessa

Il Regolamento Generale sulla protezione dei dati delle Persone fisiche (Regolamento UE 679/2016) - RGPD - ha stabilito nuove ed uniformi norme all'interno dell'Unione Europea con riferimento alla protezione dei dati personali delle persone ivi residenti. Esso garantisce diritti specifici ai soggetti interessati nei confronti del titolare del trattamento con riferimento alla possibilità di accesso, verifica e controllo, cancellazione dei propri dati personali.

1.1 Obiettivo

Finalità del presente documento è definire le attività, i ruoli e le responsabilità che la Regione, in qualità di Titolare dei dati trattati, pone in essere per la gestione delle richieste ricevute da parte dei soggetti interessati per l'esercizio dei propri diritti, così come previsto dall'articolo 12 del RGPD, fermo restando che, per quanto qui non riportato, si applicano le disposizioni previste nel suddetto regolamento.

1.2 Soggetti destinatari

I soggetti ai quali si rivolge il contenuto del presente documento sono:

- il Titolare;
- i soggetti designati dal titolare, ovvero:
  - il Capo di Gabinetto;
  - i Direttori di direzioni e agenzie regionali;
  - l'Avvocato Coordinatore;

2. Ambito di applicazione

Ambito di riferimento del presente documento sono i processi di conformità che devono essere rispettati con riferimento all'evasione delle richieste dei soggetti interessati.

Tali richieste rientrano nell'ambito dell'esercizio dei diritti di quest'ultimi, ai sensi degli articoli da 15 a 22 del RGPD (ferme restando le limitazioni di cui all'articolo 23 del RGPD), ossia diritti di:

a) accesso ai dati (art. 15 del RGPD), ed eventuale esercizio del diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato (art. 22 del RGPD);

b) rettifica dei dati (art. 16 del RGPD) ed eventuale notifica ai destinatari dei dati (art. 19 del RGPD);

c) cancellazione dei dati (diritto all'oblio, art. 17 del RGPD) ed eventuale notifica ai destinatari dei dati (art. 19 del RGPD);

d) limitazione del trattamento (art. 18 del RGPD) ed eventuale notifica ai destinatari dei dati (art. 19 del RGPD);

e) portabilità dei dati (art. 20 del RGPD);

f) opposizione (art. 21 del RGPD).

La possibilità di esercitare tali diritti è prevista all'interno dell'informativa resa al soggetto interessato.

2.1. Diritto di accesso

L'interessato ha il diritto di richiedere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in caso affermativo, di ottenere l'accesso agli stessi e alle informazioni indicate dall'articolo 15 del RGPD (quali, ad esempio, le finalità del trattamento e le categorie di dati trattati).

Tale accesso non deve ledere i diritti e le libertà altrui; qualora i dati richiesti contengano anche riferimenti a soggetti terzi rispetto all'interessato, il titolare del trattamento deve valutare se la comunicazione di tali dati possa ledere i diritti di libertà dei soggetti terzi. In caso affermativo, occorre applicare una soluzione operativa, quale quella di oscurare i dati relativi a terzi.

In base al Considerando 63 del RGPD, nel caso in cui l'interessato effettui una richiesta di accesso troppo generica, non chiarendo a quali dati si riferisce, si può chiedere un'ulteriore specificazione, in ragione del fatto che la Giunta regionale tratta una notevole quantità di informazioni potenzialmente riferibili all'interessato.

2.2. Diritto di rettifica

L'interessato ha il diritto di richiedere la rettifica dei dati personali inesatti che lo riguardano e/o l'integrazione dei dati personali incompleti. La rettifica e/o l'integrazione devono avvenire senza ingiustificato ritardo.

2.3. Diritto all'oblio

L'interessato ha il diritto di ottenere la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo. La richiesta del soggetto interessato può essere effettuata solo per uno dei seguenti motivi che il Soggetto designato o il Soggetto incaricato hanno l'onere di verificare:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

b) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1 del RGPD e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;

c) i dati personali sono stati trattati illecitamente;

d) i dati personali devono essere cancellati per adempiere un obbligo legale.

Il diritto all'oblio non può essere esercitato se il trattamento è necessario:

a) per l'esercizio del diritto alla libertà di espressione e di informazione;

b) per l'adempimento di un obbligo legale che richieda il trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito l'Ente;

c) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, del RGPD, nella misura in cui il diritto di cui all'articolo 17, paragrafo 1, rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;

d) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Quando la richiesta dell'interessato, a seguito di valutazione, è ritenuta fondata, occorre altresì verificare se i dati di cui si chiede la cancellazione siano stati indicizzati, nel qual caso occorre chiedere ai motori di ricerca (ad esempio Google, Bing, Yahoo, etc) la deindicizzazione dei contenuti relativi ai dati personali riferiti all'interessato.

2.4. Diritto di limitazione del trattamento

L'interessato può richiedere la temporanea esecuzione della sola operazione di conservazione dei dati personali trattati dalla Regione, con conseguente inutilizzabilità e inaccessibilità dei dati per tutto il periodo di limitazione, nei casi di seguito indicati:

a) quando sia contestata l'esattezza dei dati personali che lo riguardano, eventualmente esercitando il diritto di rettifica di cui all'articolo 16 RGPD; in tali casi la limitazione di trattamento potrà durare per il periodo di tempo necessario a procedere alla verifica dei dati di cui la Regione è in possesso;

b) quando l'interessato sostiene che il trattamento dei dati personali è illecito, ma si oppone alla cancellazione dei propri dati personali e chiede che ne sia limitato l'utilizzo;

c) qualora i dati personali siano necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, seppure non più utili alla Regione;

d) nel caso in cui l'interessato si sia opposto al trattamento dei dati ai sensi dell'articolo 21 del RGPD.

Nonostante sia stata disposta la limitazione di trattamento, i dati personali possono essere eccezionalmente trattati nei seguenti casi:

a) il trattamento sia necessario per l'accertamento, l'esercizio o la difesa di un diritto della Regione in sede giudiziaria;

b) per tutelare i diritti di una persona fisica o giuridica diversa dall'interessato istante;

c) per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

A titolo esemplificativo, si rappresentano le modalità attraverso le quali dare seguito a tale richiesta:

- trasferire temporaneamente i dati personali contrassegnati verso un altro sistema di trattamento;

- contrassegnare i dati personali come inaccessibili agli utenti del sistema di trattamento dei dati;

- rimuovere temporaneamente i dati contrassegnati dal sito web istituzionale.

2.5 Diritto di portabilità dei dati

L'interessato ha il diritto di ricevere, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano, forniti a un Titolare del trattamento, e di trasmetterli a un altro Titolare del trattamento, senza impedimenti da parte del Titolare del trattamento cui li ha forniti, qualora siano verificate entrambe le seguenti condizioni:

 il trattamento si basi sul consenso dell'interessato al trattamento dei propri dati personali per una o più finalità specifiche, salvo il caso in cui il diritto dell'Unione o degli Stati membri disponga che l'interessato non possa revocare il divieto di trattare categorie particolari di dati ai sensi dell'articolo 9, paragrafo 1, del RGPD ovvero il trattamento sia necessario per l'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

 il trattamento sia effettuato con mezzi automatizzati.

Nell'esercitare i propri diritti relativamente alla portabilità dei dati, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un Titolare del trattamento ad un altro, laddove risulti essere tecnicamente fattibile.

Il diritto alla portabilità dei dati non pregiudica il diritto di cancellazione. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio di autorità pubbliche attribuite al Titolare.

Il diritto alla portabilità dei dati non pregiudica i diritti e le libertà altrui.

2.6. Diritto di opposizione al trattamento

Ai sensi dell'articolo 21 del RGPD l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), del RGPD, compresa la profilazione.

Tale opposizione è volta ad inibire unicamente un determinato utilizzo dei dati personali dell'interessato.

I Soggetti designati e incaricati possono continuare a trattare, a seguito di propria valutazione, i dati al cui trattamento l'interessato si è opposto, rappresentando allo stesso interessato l'esistenza di motivi legittimi cogenti per procedere al trattamento, che prevalgono sugli interessi o sui diritti e sulle libertà fondamentali che lo riguardano.

2.7. Limitazioni ai diritti dell'interessato

È possibile che i diritti dell'interessato di cui ai punti da 2.1 a 2.6 siano limitati da particolari interessi pubblici o di altri privati. In particolare, nell'ambito del bilanciamento tra i diritti riconosciuti all'interessato ai sensi degli articoli da 15 a 22 del RGPD e determinate ipotesi concrete, in cui possa ricorrere l'esercizio degli stessi, il legislatore italiano individua specifici ambiti e materie privilegiate la cui tutela, in certe ipotesi, può determinare una compressione dei diritti dell'interessato.

Con riferimento ai limiti all'esercizio dei diritti previsti dagli articoli da 15 a 22 del RGPD, si applicano, in particolare, gli articoli 2-undecies (limitazioni ai diritti dell'interessato), 2-duodecies (limitazioni per ragioni di giustizia) e 2-terdecies (diritti riguardanti le persone decedute) del d.lgs. 196/2003 e successive modificazioni.

In particolare, ai sensi dell'articolo 2-undecies del suddetto decreto legislativo, i diritti non possono essere esercitati in ragione della possibilità che possa derivare un pregiudizio effettivo e concreto:

a) agli interessi tutelati in base alle disposizioni in materia di riciclaggio;

b) agli interessi tutelati in base alle disposizioni in materia di sostegno alle vittime di richieste estorsive;

c) all'attività di Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;

d) alle attività svolte da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad una espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;

e) allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria;

f) alla riservatezza dell'identità del dipendente che segnala, ai sensi della legge 30 novembre 2017, n. 179, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio;

g) agli interessi tutelati in materia tributaria e allo svolgimento delle attività di prevenzione e contrasto all'evasione fiscale.

3. Esercizio dei diritti degli interessati

Gli interessati che vogliano esercitare uno o più dei diritti ad essi spettanti, devono presentare la relativa domanda all'Ufficio per le Relazioni con il Pubblico (URP), che la inoltra ai Soggetti designati dal Titolare e tiene traccia delle domande stesse, nonché dei rispettivi riscontri. I Soggetti designati dal Titolare valutano le domande e provvedono al soddisfacimento delle stesse, tenendo traccia di tutti i passaggi del procedimento relativo a ciascuna di esse.

3.1. Modalità di presentazione delle istanze

Le istanze devono essere formulate in modo che sia possibile una identificazione certa dell'interessato richiedente. In particolare:

a) qualora la richiesta provenga direttamente dall'interessato, dovranno essere richiesti gli estremi del documento di identità in corso di validità;

b) qualora la richiesta provenga da parte di un terzo a ciò delegato, incluso un familiare, dovranno essere richiesti gli estremi del documento di identità in corso di validità di chi presenta la richiesta, gli estremi del documento di identità (fotocopia) in corso di validità dell'interessato, la delega scritta e firmata dell'interessato (non necessaria, invece, in caso di genitore che esercita la potestà genitoriale su un minore; in tal caso è richiesta la documentazione che attesti il legame di parentela);

c) qualora la richiesta provenga da parte di un legale dovranno essere richiesti gli estremi del documento di identità (fotocopia) in corso di validità dell'interessato, la richiesta su carta intestata del legale recante gli estremi necessari per la verifica dell'iscrizione all'albo, il mandato conferito nell'ambito della propria professione o la delega scritta e firmata dell'interessato.

Nei casi di istanze presentate telematicamente, ai fini della verifica dell'identità dell'istante, si richiama quanto disposto dall'articolo 65 del decreto legislativo 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale) e successive modificazioni.

Le istanze per l'esercizio dei diritti sopra citati sono trasmesse dai richiedenti direttamente all'URP con una delle modalità previste dalla normativa vigente.

Per tutte le istanze pervenute l'URP comunica al richiedente, nella stessa forma in cui avviene la richiesta, se le informazioni date sono complete, e provvede a dare evidenza dell'avvenuta presa in carico.

L'URP in particolare:

a) inoltra le domande ai Soggetti designati dal Titolare;
b) invita gli interessati a formulare le richieste a mezzo di apposito modulo messo a disposizione dalla Regione sul proprio sito istituzionale e presso la sede dell'URP;
c) tiene un registro di tutte le richieste e dei riscontri forniti dai Soggetti designati dal Titolare.

Nel caso in cui, per errore, i Soggetti designati dal Titolare, il DPO o altro organo regionale riceva direttamente un'istanza, dovrà inoltrare la stessa all'URP per l'avvio della procedura.

3.2 Valutazione e classificazione della richiesta

A seguito della ricezione della richiesta, i Soggetti designati dal Titolare individuano il trattamento cui la stessa si riferisce e procedono alla verifica della sua legittimità, nonché della veridicità e completezza delle informazioni ricevute. Solo per i casi particolarmente complessi gli stessi possono richiedere il supporto del DPO.

La richiesta viene valutata sulla base dei seguenti aspetti:

a) legittimità: valutazione della presenza di eventuali condizioni ostative all'evasione della richiesta (es. impossibilità di cancellazione dei dati per motivi di ordine superiore, quali salute o sicurezza pubblica, etc.);

b) veridicità: valutazione dell'esistenza dei dati che riguardano l'interessato;

c) completezza: verifica che i dati ricevuti siano completi al fine di evadere la richiesta e valutazione dell'identificabilità del richiedente.

A seconda dell'esito della valutazione, la richiesta viene classificata in:

 Evadibile: la richiesta è legittima, completa e non ci sono elementi ostativi alla richiesta. Le modalità di gestione della richiesta sono descritte nei paragrafi successivi;

 Rigettata: la richiesta non è legittima e sussistono motivazioni per il rigetto da parte dei Soggetti designati dal Titolare, i quali ne danno informazione all'URP, che provvede al riscontro formale all'interessato;

 Con informazioni mancanti: i Soggetti designati dal Titolare comunicano all'URP la mancanza di informazioni, e l'URP procede formalmente con la richiesta delle informazioni stesse all'interessato;

3.3. Termini per il riscontro

I Soggetti designati dal Titolare sono tenuti a rispondere, tramite l'URP, alle richieste dell'interessato senza ingiustificato ritardo e al massimo entro un mese.

Il termine decorre dal ricevimento della richiesta che consenta un'identificazione dell'interessato da parte dell'URP. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. L'URP informa l'interessato di tale proroga, nonché dei motivi del ritardo, entro un mese dal ricevimento della richiesta (articolo 12 del RGPD).

3.4. Modalità del riscontro

I Soggetti designati dal Titolare, eventualmente con il supporto della struttura ICT e del partner tecnologico coinvolto, comunicano all'URP l'esito della richiesta.

L'interessato ha il diritto di ottenere una copia dei dati personali oggetto di trattamento.

I dati e le informazioni richieste sono forniti dall'URP per iscritto o con altri mezzi, anche elettronici, (in particolare se la richiesta è presentata con mezzi elettronici e in un formato elettronico di uso comune), salvo diversa indicazione da parte dell'interessato.

Il riscontro deve essere fornito in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice, chiaro e comprensibile. Se richiesto dall'interessato, le informazioni possono essere anche fornite oralmente.

Qualora la richiesta riguardi la portabilità dei dati, i Soggetti designati dal Titolare, eventualmente con il supporto della struttura ICT e del partner tecnologico coinvolto, compilano un modulo interoperabile per trasmettere i dati alla parte terza e l'URP comunica all'interessato l'avvenuto trasferimento.

3.5. Mancato accoglimento

Il mancato accoglimento della richiesta deve essere motivato compiutamente e reso per iscritto, o con altri mezzi, anche elettronici, dall'URP, fornendo l'informazione relativa alla possibilità di proporre reclamo al Garante per la protezione dei dati personali e ricorso giurisdizionale.

Se le richieste dell'interessato sono manifestamente infondate o eccessive, l'URP e i Soggetti designati dal Titolare possono rifiutare di soddisfare la richiesta, dimostrando, con adeguata motivazione, il carattere manifestamente infondato o eccessivo della richiesta.

3.6. Tracciamento del processo

I Soggetti designati dal Titolare hanno l'obbligo di tenere traccia e conservare tutta la documentazione relativa alle richieste raccolte ed evase e di darne comunicazione semestrale al Responsabile Protezione dei Dati (DPO).

La comunicazione deve essere effettuata fornendo almeno le seguenti informazioni:

- numero di protocollo e data di ricezione della richiesta;

- oggetto della richiesta;

- dati identificativi del soggetto interessato richiedente;

- dati identificativi del soggetto eventualmente delegato dall' interessato;

- esito della richiesta;

- data di evasione della richiesta.

ALLEGATO NN (art. 476 ter)

SCHEMI TIPO MODULISTICA

SCHEMA A

(art. 474, c. 3)

ADDENDUM AL CONTRATTO DI LAVORO

CONFERIMENTO DI COMPITI E FUNZIONI IN QUALITA' DI SOGGETTO DESIGNATO AI SENSI DELL'ARTICOLO 2 *QUATERDECIES* D.LGS. 196/2003 (Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 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.) E SUCCESSIVE MODIFICAZIONI. ISTRUZIONI PER L'ESERCIZIO DELLE FUNZIONI CONFERITE.

PREMESSO CHE

L' articolo 474, comma 3, del regolamento regionale 6 settembre 2002, n. 1 (Regolamento di organizzazione degli uffici e dei servizi della Giunta regionale.) e successive modificazioni:

a) stabilisce che la Giunta regionale, in qualità di titolare del trattamento può prevedere, ai sensi dell'articolo 2 quaterdecies del d.lgs. 196/2003 e successive modificazioni, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano conferiti a persone fisiche, che operano sotto la propria autorità, espressamente designate secondo lo schema "A" dell'allegato "NN" del r.r. 1/2002, da allegare quale addendum al contratto di lavoro;

b) individua come Soggetti designati di diritto il Capo di Gabinetto, i Direttori regionali, i Direttori delle Agenzie regionali, l'Avvocato coordinatore e il dirigente cui è attribuita la competenza relativamente alle funzioni previste dal decreto legislativo 6 settembre 1989, n. 322 (Norme sul Sistema statistico nazionale e sulla riorganizzazione dell'Istituto nazionale di statistica, ai sensi dell'art. 24 della legge 23 agosto 1988, n. 400) e alle convenzioni con l'ISTAT per l'attuazione del Programma Statistico Nazionale;

VISTO l'articolo 2-quaterdecies del d. lgs. 196/2003 e successive modificazioni, il quale dispone che *"il Titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità";*

VISTO il decreto legislativo 30 marzo 2001, n. 165 (Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche) e successive modificazioni;

VISTO il 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 (di seguito RGPD), che garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento al diritto di protezione dei dati personali;

ATTESO che le soluzioni tecniche e organizzative relative al trattamento dei dati personali richiedono alla Regione un costante monitoraggio e che tali misure, periodicamente riesaminate ed aggiornate, qualora necessario, devono tener conto dello stato dell'arte e dei costi di attuazione, oltre che della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso;

ATTESO che il titolare del trattamento è tenuto a mettere in atto misure tecniche e organizzative volte ad attuare in modo efficace i principi di protezione dei dati, quali la pseudonimizzazione, la minimizzazione e anche ad integrare, nel trattamento, le necessarie garanzie al fine di soddisfare i requisiti del suddetto regolamento e tutelare i diritti degli interessati alla riservatezza ed all'adeguato trattamento dei dati personali e che è tenuto, altresì, a mettere in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento;

CONSIDERATO che gli obblighi di cui sopra valgono per la quantità dei dati personali raccolti, per la portata del trattamento ed anche per il periodo di conservazione e l'accessibilità e che le misure da adottare devono garantire che, per impostazione predefinita, non siano resi accessibili dati personali ad un numero indefinito di persone fisiche senza l'intervento della persona fisica;

CONSIDERATO che ai fini del RGPD per "trattamento" si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (articolo 4, n. 2) del RGPD);

TENUTO CONTO che, ai sensi dell'articolo 24 del RGPD, il Titolare del trattamento è tenuto a mettere in atto le misure, tecniche ed organizzative, adeguare per garantire ed essere in grado di dimostrare che il trattamento sia effettuato conformemente al RGPD;

TENUTO CONTO che l'articolo 29 del RGPD stabilisce la regola generale per cui *"chiunque agisca sotto l'autorità del responsabile del trattamento o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri";*

DATO ATTO che il <**indicare nome e cognome**> in qualità di Capo di Gabinetto/Avvocato coordinatore/Direttore<**indicare nome della Direzione**>/dirigente responsabile <**indicare nome dell'Area competente in materia di statistica**> è, secondo quanto disposto dall'articolo 474, comma 3, del r.r. 1/2002 e successive modificazioni, soggetto designato al trattamento dei dati ai sensi e per gli effetti di cui all'articolo 2 quaterdecies del d.lgs. 196/2003 e successive modificazioni;

RITENUTO che il <**indicare nome e cognome**> in qualità di Capo di Gabinetto/Avvocato coordinatore/Direttore<**indicare nome della Direzione**>/dirigente responsabile <**indicare nome dell'Area competente in materia di statistica**>, per l'ambito di attribuzioni, funzioni e competenze conferite, abbia le garanzie sufficienti per mettere in atto tutte le misure tecniche ed organizzative adeguate a soddisfare i requisiti del RGPD e garantire la tutela dei diritti degli interessati;

Tutto ciò premesso

SI CONVIENE QUANTO SEGUE

Art. 1
(Obblighi del Soggetto designato)

1. Il **<*indicare nome e cognome*>**, quale Soggetto designato al trattamento dei dati ai sensi dell'articolo 2 *quaterdecies* del d.lgs. 196/2003 e successive modificazioni e dell'articolo 474, comma 3, del r.r. 1/2002 e successive modificazioni, svolge i compiti e assume le responsabilità previste dalle disposizioni vigenti in materia di trattamento di dati personali e osserva scrupolosamente quanto in esse previsto, nonché le seguenti istruzioni.

Art. 2
(Istruzioni per il trattamento dei dati personali)

1. Il **<*indicare nome e cognome*>**, Soggetto designato, nell'ambito delle sue funzioni, presiede ai trattamenti di dati personali di competenza della **<indicare i riferimenti della struttura di afferenza>**, la cui elencazione e descrizione è riportata nel "Registro delle attività di Trattamento" di cui all'articolo 30 del RGPD, attenendosi al rispetto delle seguenti **istruzioni**:

a) i trattamenti devono essere svolti nel pieno rispetto delle previsioni normative vigenti in materia di protezione dei dati personali, nonché tenendo conto dei provvedimenti e dei comunicati ufficiali emessi dall'Autorità Garante per la Protezione dei Dati Personali, di seguito denominata Garante;

b) la raccolta dei dati personali e la loro successiva registrazione devono avvenire per il solo perseguimento delle finalità istituzionali della Regione e, comunque, per scopi:

1) *determinati*, pertanto non è consentita la raccolta come attività fine a sé stessa;

2) *espliciti*, quindi il soggetto interessato deve essere informato sulle finalità del trattamento;

3) *legittimi*, pertanto, oltre al trattamento, anche il fine della raccolta dei dati deve essere lecito;

c) i dati personali trattati sono: dati genericamente di natura personale (articolo 4, n. 1), del RGPD); dati sensibili (articolo 9 del RGPD "Categorie particolari di dati personali"); dati giudiziari (articolo 10 del RGPD);

d) le categorie di interessati sono quelle identificate nelle parti di competenza della **<indicare i riferimenti della struttura di afferenza>** del "Registro delle attività di Trattamento" di cui all'articolo 30 del RGPD;

e) le operazioni di trattamento nell'ambito della struttura di competenza, dovranno essere organizzate in conformità con la normativa in materia di protezione dei dati personali applicabile ed in osservanza delle eventuali indicazioni scritte impartite

dalla Regione, assicurando l'applicazione del principio della protezione dei dati fin dalla progettazione e protezione predefinita di cui all'articolo 25 del RGPD, determinando i mezzi del trattamento e mettendo in atto le misure tecniche e organizzative adeguate, di cui all'articolo 32 del RGPD, prima dell'inizio delle attività. Inoltre, dovrà essere adottata ogni misura adeguata, fisica e logica, atta a garantire che i dati personali siano trattati in ossequio al principio di necessità e che siano trattati solamente per le finalità previste e per il tempo strettamente necessario al raggiungimento delle stesse (privacy by default);

f) in veste di Soggetto designato al trattamento dei dati personali, dovrà collaborare con il Titolare del trattamento affinché siano garantiti tutti i diritti dell'interessato di cui al Capo III del RGPD. In particolare, dovrà attenersi ad ogni istruzione scritta impartita al riguardo dal Titolare;

g) dovranno essere rese disponibili al Titolare del trattamento, tutte le informazioni necessarie per dimostrare il rispetto degli adempimenti previsti dalla normativa in materia di protezione dei dati personali relativamente alla struttura di competenza, consentendo di effettuare periodicamente attività di verifica, comprese ispezioni realizzate dal Titolare stesso, dal Responsabile della Protezione dei Dati o da un altro soggetto incaricato;

h) informare il Titolare del trattamento ed il Responsabile della Protezione dei Dati personali, qualora sorgesse la necessità di effettuare trattamenti su dati personali diversi ed eccezionali rispetto a quelli normalmente eseguiti;

i) i dati devono, inoltre, essere:

1) *esatti*, cioè precisi e rispondenti al vero e, se necessario, aggiornati;

2) *pertinenti*, ovvero il trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali, in relazione all'attività che viene svolta;

3) *completi*: idonei a contemplare specificamente il concreto interesse e diritto del soggetto interessato (da non intendersi nel senso di raccogliere il maggior numero di informazioni possibili);

4) *non eccedenti* in senso quantitativo rispetto allo scopo perseguito, ovvero devono essere raccolti solo i dati che siano al contempo strettamente necessari e sufficienti in relazione al fine, la cui mancanza risulti di ostacolo al raggiungimento dello scopo stesso;

5) *conservati per un periodo non superiore a quello necessario* per gli scopi del trattamento e comunque in base alle disposizioni aventi ad oggetto le modalità ed i tempi di conservazione degli atti amministrativi. Trascorso detto periodo i dati vanno resi anonimi o cancellati e la loro comunicazione e diffusione non è più consentita;

l) ciascun trattamento deve avvenire nei limiti imposti dal principio fondamentale di riservatezza e nel rispetto della dignità della persona dell'interessato al trattamento; deve pertanto essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi;

m) se il trattamento di dati è effettuato in violazione dei principi summenzionati e di quanto disposto dalla normativa vigente in materia di protezione dei dati personali, è necessario provvedere, previa comunicazione al Responsabile della Protezione dei Dati (DPO) della Regione, al blocco dei dati stessi, ossia alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del medesimo trattamento, fornendo, ad esempio, l'informativa omessa, ovvero provvedendo alla cancellazione dei dati se non è possibile procedere alla regolarizzazione.

2. In conformità alla normativa vigente in materia di protezione dei dati personali ed in osservanza delle eventuali indicazioni scritte impartite al riguardo dal Titolare del trattamento, dovrà:

a) individuare e, se presenti, designare le persone autorizzate al trattamento, detti incaricati, che prestano la propria attività all'interno della struttura di propria competenza;
b) controllare l'operato degli incaricati al trattamento, nonché sensibilizzare gli stessi sugli aspetti normativi ed organizzativi in materia di tutela dei dati personali;
c) garantire che i profili di accesso ai sistemi informativi da parte degli incaricati al trattamento siano configurati anteriormente all'inizio del trattamento, nonché verificare, almeno una volta l'anno, che tali profili siano conformi con le mansioni svolte. In caso di sospensione dall'attività lavorativa o revoca/esclusione dall'incarico dovrà essere comunicato alle strutture competenti la necessità di procedere alla disattivazione dell'utenza;
d) assicurare, all'interno della propria struttura, il pieno rispetto degli adempimenti formali nei modi e nei tempi previsti dalla normativa vigente, tra i quali la predisposizione e il rilascio di informative e la gestione dei diritti degli interessati;
e) collaborare con il Garante in caso di ispezioni, al fine di fornire informazioni, documenti e ogni facilitazione di accesso alle banche dati inerenti all'Ufficio di competenza;
f) collaborare nelle verifiche predisposte dal DPO, al fine di fornire informazioni, documenti e ogni facilitazione di accesso alle banche dati;
g) informare prontamente il DPO di ogni questione rilevante in base alla normativa sulla protezione dei dati personali, come la presentazione di eventuali istanze inerenti all'esercizio dei diritti degli interessati ai sensi degli articoli da 15 a 22 del RGPD;
h) informare tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, il DPO di ogni violazione di dati personali (cosiddetto data breach) entro 24 ore dall'avvenuta conoscenza dell'evento. In ogni caso, l'informativa deve essere accompagnata da ogni documentazione utile, per permettere al Titolare, ove ritenuto necessario, di notificare tale violazione al Garante e/o darne comunicazione agli interessati, entro il termine di 72 ore da quando ne è venuto a conoscenza, ai sensi degli articoli 33 e 34 del RGPD;
i) nel caso in cui il Titolare debba fornire informazioni aggiuntive al Garante, supportare il Titolare stesso nella misura in cui le informazioni richieste e/o necessarie per il Garante siano esclusivamente in possesso del Soggetto designato;
l) collaborare, per la struttura di propria competenza, alla redazione ed aggiornamento del Registro delle attività di trattamento di cui all'articolo 30 del RGPD, cooperando con il Titolare e con il Garante, laddove ne venga fatta richiesta ai sensi dell'articolo 30, paragrafo 4, del RGPD;
m) collaborare per i trattamenti della struttura di competenza e, unitamente al DPO, allo svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente a quanto prescritto dall'articolo 35 del RGPD e nella eventuale consultazione del Garante, prevista ai sensi dell'articolo 36 del RGPD;
n) garantire che la protezione dei dati personali all'interno della struttura di propria competenza sia realizzata in base alle misure di sicurezza previste dall'articolo 32 del RGPD idonee a ridurre al minimo i rischi di divulgazione, distruzione, perdita o modifica anche accidentale o illegale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

o) collaborare, in caso di modifica della normativa in materia di protezione dei dati personali e nei limiti delle proprie competenze tecniche/organizzative e delle proprie risorse, con il Titolare e con il DPO, affinché siano sviluppate, adottate ed implementate misure correttive di adeguamento ai nuovi requisiti introdotti;
p) proporre al Titolare la designazione di eventuali ulteriori Responsabili del trattamento individuati in conformità alle relative disposizioni del RGPD;
q) designare gli amministratori di sistema della struttura di appartenenza, nel rispetto di quanto previsto dal Provvedimento del Garante della Protezione dei dati Personali 27 novembre 2008 (Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema) nonché degli ulteriori criteri e modalità definiti dall'allegato "LL" al r.r. 1/2002 e successive modificazioni e darne comunicazione alla direzione regionale competente in materia di sistemi informativi.

Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

Luogo e data:
IL TITOLARE DEL TRATTAMENTO
Per accettazione
Luogo e data
Il SOGGETTO DESIGNATO

SCHEMA B
(art. 474, c. 5)

NOMINA SOGGETTI INCARICATI

(INTESTAZIONE DELLA STRUTTURA)

Oggetto: Nomina soggetto incaricato al trattamento di dati personali ai sensi dell'articolo 474, comma 5, del r.r. 6 settembre 2002, n. 1 (Regolamento di organizzazione degli uffici e dei servizi della Giunta regionale) e successive modificazioni e degli articoli 28, paragrafo 3, lett. b), 29 e 32, paragrafo 4, del Regolamento UE 2016/679 (RGPD).

Visto l'articolo 474, comma 3, del r.r. 1/2002 e successive modificazioni, il quale individua come Soggetti designati di diritto allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali, il Capo di Gabinetto, i Direttori regionali, i Direttori delle Agenzie regionali, l'Avvocato coordinatore e il dirigente cui è attribuita la competenza relativamente alle funzioni previste dal decreto legislativo 6 settembre 1989, n. 322 (Norme sul Sistema statistico nazionale e sulla riorganizzazione dell'Istituto nazionale di statistica, ai sensi dell'art. 24 della legge 23 agosto 1988, n. 400) e alle convenzioni con l'ISTAT per l'attuazione del Programma Statistico Nazionale;

Visto l'articolo 474, comma 5, del r.r. 1/2002 e successive modificazioni, il quale prevede che la Giunta regionale, in qualità di titolare del trattamento e i soggetti designati autorizzano, ai sensi degli articoli 28, paragrafo 3, lettera b), 29 e 32, paragrafo 4, del RGPD, alle operazioni di trattamento dei dati personali, con

specifico atto di nomina redatto secondo lo schema "B" dell'allegato "NN" del r.r. 1/2002, tutti i dipendenti o collaboratori a qualsiasi titolo, detti soggetti incaricati, che effettuano operazioni di trattamento dati sotto l'autorità diretta del titolare o del soggetto designato;

Visto il Regolamento UE 2016/679 del Parlamento e del Consiglio Europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, di seguito RGPD, che garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali delle persone fisiche, con particolare riferimento alla riservatezza e al diritto di protezione dei dati personali.

Considerato che ai fini del RGPD si intende per:

- "*trattamento*", qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (articolo 4, n. 2), RGPD);
- "dato personale" qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (articolo 4, n. 1) del RGPD);
- "categorie particolari di dati personali" si intendono i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale nonché i dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (articolo 9, paragrafo 1, RGPD).

Tenuto conto che la figura del soggetto incaricato risulta coerente con il principio di "responsabilizzazione" dei Titolari del trattamento, la cui attuazione richiede l'adozione di misure atte a garantire proattivamente l'osservanza del RGPD nella sua interezza, come evidenziato dall'Autorità Garante per la Protezione dei dati personali nella "Guida all'applicazione del Regolamento Europeo in materia di protezione dei dati personali";

Tenuto conto che alla luce degli articoli 28, paragrafo 3, lettera b), 29, e 32, paragrafo 4, del RGPD in tema di misure tecniche e organizzative di sicurezza, l'Autorità Garante ritiene opportuno che i Titolari del trattamento mantengano in essere la struttura organizzativa e le modalità di designazione dei soggetti incaricati del trattamento stesso, così come delineatesi negli anni, anche attraverso gli interventi del Garante stesso;

Considerato che la Regione Lazio, ai sensi dell'articolo 30 del RGPD, ha proceduto alla predisposizione del "Registro delle attività di trattamento", riportante, per ciascuna direzione, le informazioni in ordine ai trattamenti effettuati dalla Regione stessa;

Considerato che la Regione Lazio, ai sensi degli articoli 33 e 34 del RGPD, ha proceduto alla redazione della "Procedura di Personal Data Breach", allo scopo di

illustrare le azioni da mettere in atto, a fronte dell'accadimento di un incidente, accertato e classificato come violazione di dati personali (Personal Data Breach);

Tenuto conto delle mansioni già attribuite nel contratto di lavoro in essere con il Titolare e derivanti dall'assegnazione alla struttura amministrativa di afferenza;

DISPONE

1) di nominare il **<*indicare nome e cognome*>**, **soggetto incaricato al trattamento** dei dati personali relativamente alle attività normalmente svolte nell'ambito della Direzione Regionale **<*inserire riferimenti Direzione e Area*>**, in conformità e nei limiti delle proprie competenze espresse negli ordini di servizio e nelle norme del contratto di riferimento;

2) di impartire, ai fini dell'esercizio delle attività di cui al punto 1), le seguenti istruzioni:

- nel trattare i dati personali, si deve operare garantendo la massima riservatezza delle informazioni di cui si viene in possesso considerando tutti i dati personali confidenziali e, di norma, soggetti ad un dovere di riservatezza. Pertanto, non si dovranno divulgare a terzi le informazioni di cui si è venuti a conoscenza;
- si devono adottare tutte le misure necessarie a verificare l'esattezza dei dati raccolti e registrati, e, se necessario, correggerli ed aggiornarli di conseguenza;
- si è tenuti ad informare, tempestivamente e senza ingiustificato ritardo, di ogni evento attinente la sicurezza o violazione di dati personali (cosiddetto data breach), il Soggetto designato al trattamento, per permettere al Titolare, ove ritenuto necessario, di notificare la violazione all'Autorità Garante per la protezione dei dati personali e/o darne comunicazione agli interessati, entro il termine di 72 ore da quando il Titolare ne è venuto a conoscenza;
- la condotta tenuta in ogni fase di lavoro dovrà evitare che i dati personali siano soggetti a rischi di perdita o distruzione anche accidentale; che ai dati possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini istituzionali per i quali i dati sono stati raccolti e per i quali vengono trattati;
- in ogni fase del trattamento non si possono eseguire operazioni per fini non previsti tra i compiti assegnati e si potrà accedere ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere tali compiti;
- per i trattamenti dei dati personali che comportino l'uso di sistemi informatici e telematici (PC, PC portatile o altro), l'accesso a tali dati può avvenire solo attraverso password o codici di accesso secondo quanto disposto dalle regole della Regione. Ogni incaricato deve mantenere segreta la password di accesso al proprio PC, evitando di divulgarla a terzi o di trascriverla su fogli. Nessun dato personale, su supporto magnetico, digitale o cartaceo, potrà essere lasciato incustodito;
- tutto il materiale cartaceo contenente dati personali in argomento deve essere custodito con diligenza e conservato in maniera tale da non risultare facilmente visibile a persone terze o comunque ai non autorizzati al trattamento. Tali misure devono essere applicate anche a tutte le forme di riproduzione dei dati personali (ad esempio pen drive, CD/DVD, fotocopie);
- l'incaricato coadiuva il Titolare e/o il Soggetto designato al trattamento nell'aggiornamento del "Registro delle attività del Trattamento", indicato in premessa;
- l'incaricato è tenuto a comunicare tempestivamente, qualora necessario, al Soggetto designato al trattamento o al Responsabile per la Protezione dei Dati indicato in

premessa, ogni circostanza idonea a determinare pericolo di dispersione o utilizzazione non autorizzata dei dati stessi, nonché ogni evento legato a operazioni di trattamento di dati personali per finalità o con modalità diverse da quelle definite dalla Regione;

- in qualunque circostanza non si abbia la certezza in merito alla correttezza di un'operazione di trattamento, ci si deve rivolgere senza indugio al Soggetto designato al trattamento;
- l'incaricato si impegna all'obbligo legale di riservatezza sui trattamenti effettuati e su qualsiasi informazione o circostanza di cui fosse venuto a conoscenza, così come richiesto dal RGPD;

3) di stabilire che ulteriori istruzioni rispetto a quelle elencate potranno, di volta in volta, essere fornite dal Titolare e/o dal Soggetto designato al trattamento, in base alla normativa vigente;

4) di stabilire che la presente nomina, disposta ai sensi della normativa vigente in materia di protezione dei dati personali, avrà la medesima durata del rapporto di lavoro con la Regione e comunque dell'assegnazione alla struttura amministrativa di afferenza, al termine della quale cesserà l'efficacia dell'autorizzazione ad effettuare alcun tipo di trattamento sui dati.

_____

Il Soggetto designato (Direttore Regionale)
<*inserire nome e cognome*>

SCHEMA C

(art. 474, c. 7)

NOMINA AMMINISTRATORE DI SISTEMA

(INTESTAZIONE DELLA STRUTTURA)

Oggetto: Nomina Amministratore di Sistema/Base dati/Rete ai sensi dell'articolo 474, comma 7, del r.r. 6 settembre 2002, n. 1 (Regolamento di organizzazione degli uffici e dei servizi della Giunta regionale) e successive modificazioni e del Provvedimento Generale del Garante per la protezione dei dati personali del 27/11/2008 (Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema) e successive modificazioni, pubblicato sulla Gazzetta Ufficiale n. 300 del 24/12/2008.

Visto l'articolo 474, comma 3, del r.r. 1/2002 e successive modificazioni, il quale individua come Soggetti designati di diritto allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali, il Capo di Gabinetto, i Direttori regionali, i Direttori delle Agenzie regionali, l'Avvocato coordinatore e il dirigente cui è attribuita la competenza relativamente alle funzioni previste dal decreto legislativo 6 settembre 1989, n. 322 (Norme sul Sistema statistico nazionale e sulla riorganizzazione dell'Istituto nazionale di statistica, ai sensi

dell'art. 24 della legge 23 agosto 1988, n. 400) e alle convenzioni con l'ISTAT per l'attuazione del Programma Statistico Nazionale;

Visto l'articolo 474, comma 7, del r.r. 1/2002 e successive modificazioni, il quale prevede che i soggetti designati, qualora il trattamento dei dati personali venga effettuato con strumenti elettronici direttamente acquisiti dalla struttura di appartenenza, nominano gli amministratori di sistema con specifico atto di organizzazione, redatto sulla base dello schema "C" dell'allegato "NN" al r.r. 1/2002, nel rispetto di quanto previsto dal Provvedimento del Garante della Protezione dei dati Personali 27 novembre 2008 e successive modificazioni, nonché degli ulteriori criteri e modalità definiti dall'allegato "LL" al r.r. 1/2002;

Visto il Regolamento UE 2016/679 del Parlamento e del Consiglio Europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, di seguito RGPD, che garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali delle persone fisiche, con particolare riferimento alla riservatezza ed al diritto di protezione dei dati personali.

Visto il Provvedimento del Garante per la Protezione dei Dati Personali del 27/11/2008 e successive modificazioni;

Considerato che il suddetto Provvedimento richiede che si proceda alla designazione individuale degli Amministratori di Sistema (System Administrator), degli Amministratori di Base Dati (Database Administrator) e degli Amministratori di Rete (Network Administrator) che, nell'esercizio delle proprie funzioni, hanno accesso, anche fortuito, a dati personali;

Considerato che ai fini del RGPD per:

- "*trattamento*" si intende, qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (articolo 4, n. 2), del RGPD);
- "dato personale" qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (articolo 4, n. 1) del RGPD);
- "categorie particolari di dati personali" si intendono i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale nonché i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (articolo 9, paragrafo 1, del RGPD).

Considerato che la Regione, ai sensi dell'articolo 30 del RGPD, ha proceduto alla predisposizione del "Registro delle attività di trattamento", riportante per ciascuna direzione le informazioni in ordine ai trattamenti effettuati dalla Regione stessa;

Considerato che la Regione, ai sensi degli articoli 33 e 34 del RGPD, ha proceduto alla redazione della "Procedura di Personal Data Breach", allo scopo di illustrare le azioni da mettere in atto, a fronte dell'accadimento di un incidente, accertato e classificato come violazione di dati personali (Personal Data Breach);

Tenuto conto delle mansioni già attribuite nel contratto di lavoro in essere con il Titolare e derivanti dall'assegnazione alla struttura amministrativa di afferenza;

Ritenuto che il/la dott./dott.ssa <**inserire nome e cognome**> ha l'esperienza, le capacità e l'affidabilità necessarie a fornire idonee garanzie del pieno rispetto delle disposizioni in materia di trattamento di dati personali, ivi compreso il profilo relativo alla sicurezza;

DISPONE

1) di nominare il/la **dott./dott.ssa <inserire nome e cognome>** quale **Amministratore di Sistema** relativamente alle attività di competenza;

2) di stabilire il seguente elenco degli ambiti di operatività dell'Amministratore di sistema in base al profilo di autorizzazione assegnato: **<inserire profilo di autorizzazione>**:

-

-

3) di stabilire che l'elenco sopra riportato potrà essere modificato al manifestarsi di specifiche necessità della direzione, in quanto le attività di profilazione e creazione delle utenze potranno rendere necessaria la modifica/integrazione degli ambiti di operatività sopra identificati;

4) di impartire, ai fini dell'esercizio delle attività di Amministratore di sistema di cui al punto 2), le seguenti istruzioni:

- nell'adempimento dell'esercizio delle proprie funzioni, l'Amministratore di sistema opera quale soggetto incaricato al trattamento di dati personali, ai sensi dell'articolo 474, comma 5, del r.r. 1/2002 e successive modificazioni e degli articoli 28, paragrafo 3, lett. b), 29 e 32, paragrafo 4, del RGPD ed è tenuto ad osservare le istruzioni, attuali e future, impartite dalle competenti strutture della Regione;

- tutti i dati di cui l'Amministratore di sistema viene a conoscenza devono essere trattati esclusivamente per fini aziendali e con modalità tali da garantire la massima riservatezza, considerando i suddetti dati confidenziali e, di norma, non soggetti ad alcuna divulgazione a terzi;

- in qualunque circostanza non si abbia la certezza in merito alla correttezza di un'operazione di trattamento, ci si deve rivolgere senza indugio al Soggetto designato al trattamento;

- l'Amministratore di sistema si impegna all'obbligo legale di riservatezza sui trattamenti effettuati e su qualsiasi informazione o circostanza di cui fosse venuto a conoscenza, così come richiesto dal RGPD;

5) di stabilire, in conformità a quanto prescritto dal Provvedimento del Garante per la Protezione dei Dati Personali 27/11/2008 e successive modificazioni, indicato in premessa, che questa struttura provvederà a:

- svolgere con cadenza almeno annuale, nei limiti consentiti dalle norme legali e contrattuali, un'attività di verifica dell'operato dell'Amministratore di sistema, previa registrazione degli accessi logici (autenticazione informatica) ai sistemi e conservazione degli stessi per un congruo periodo non inferiore a 6 mesi. I dati registrati a tale scopo dai sistemi non vengono utilizzati in alcun modo per il controllo a distanza dei lavoratori e le tecnologie utilizzate a tal fine sono compatibili con quanto disposto dalla normativa vigente in materia;
- riportare gli estremi identificativi dell'Amministratore di sistema in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante;
- rendere conoscibile, all'interno della propria organizzazione, l'identità dell'Amministratore di sistema, la cui attività riguardi anche indirettamente sistemi che trattano o permettono il trattamento di informazioni di carattere personale dei lavoratori;

6) di stabilire che ulteriori istruzioni rispetto a quelle elencate potranno, di volta in volta, essere fornite dal Titolare e/o dal Soggetto designato al trattamento, in base alla normativa vigente;

7) di stabilire che la presente nomina, disposta ai sensi della normativa vigente in materia di protezione dei dati personali, avrà la medesima durata del rapporto di lavoro con la Regione e comunque dell'assegnazione alla struttura amministrativa di afferenza, al termine della quale cesserà l'efficacia dell'autorizzazione ad effettuare alcun tipo di trattamento sui dati.

_____

Il Soggetto Designato (Direttore Regionale)
<inserire nome e cognome>

SCHEMA D
INFORMATIVA DATI PERSONALI

PER IL PERSONALE IN SERVIZIO

"**Informativa per il personale in servizio**"
(Regolamento UE 2016/679 "RGPD")

Il Regolamento (UE) 2016/679 del Parlamento e del Consiglio Europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito RGPD) ed il decreto legislativo 196/2003 e successive modificazioni, garantiscono che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, al diritto e alla protezione dei dati personali.

Per questi motivi la Regione Lazio in qualità di Titolare del trattamento di dati personali effettuato per finalità di gestione del personale, nell'ambito delle proprie competenze, è tenuta a fornirLe, ai sensi dell'articolo 13 del RGPD, una precisa informativa che Le permette di conoscere i dati personali in possesso della Regione stessa o che dovranno o potranno essere raccolti nell'ambito dell'esercizio del rapporto di lavoro instaurato.

1. BASE GIURIDICA DEL TRATTAMENTO E FINALITÀ

La base giuridica del trattamento è quella prevista dall'articolo 6, paragrafo 1, lett. b), del RGPD: "*il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso*".

I dati personali oggetto del trattamento saranno trattati per le sole finalità strettamente connesse e strumentali alla nascita e gestione del rapporto contrattuale di lavoro nei limiti stabiliti da espressa disposizione di legge e regolamenti o da accordi sindacali.

In particolare, i dati da Lei forniti possono riguardare dati anagrafici e fiscali Suoi e dei Suoi eventuali familiari a carico o comunque componenti il Suo nucleo familiare, nonché eventuali diversi beneficiari di programmi assicurativi; gli estremi del suo conto corrente bancario, i dati professionali (competenze acquisite prima o nel corso del rapporto di lavoro con la Regione Lazio, ruoli svolti).

Tali dati saranno trattati per le finalità di seguito riportate:

- per assolvere agli obblighi della Regione Lazio (in materia fiscale, di previdenza ed assistenza, di igiene e sicurezza del lavoro, di tutela della salute nonché di sicurezza sociale)
- per la gestione ed esecuzione del contratto di lavoro, anche sotto il profilo economico ed amministrativo, ivi compresi gli adempimenti connessi all'organizzazione di eventuali missioni/trasferte connesse ad attività lavorative.

Si fa presente che in occasione delle operazioni di trattamento dei Suoi dati personali, la Regione Lazio può venire a conoscenza di dati che la legge definisce "Categorie particolari di dati personali", detti anche sensibili (articolo 9 del RGPD), in quanto gli stessi sono idonei, tra l'altro, a rivelare uno stato di salute, l'adesione ad un sindacato, l'adesione ad un partito politico; dati che la legge definisce giudiziari (articolo 10 del RGPD) in quanto relativi a condanne penali e reati od a connesse misure di sicurezza. Tali dati saranno trattati con la massima riservatezza e per le sole finalità previste dalla legge e dal CCNL vigente.

I dati relativi all'adesione ad un sindacato potranno essere comunicati alle Organizzazioni sindacali o di categoria per il controllo delle ritenute solo con riferimento ai propri iscritti. I dati relativi all'adesione ad un partito politico o alle convinzioni religiose saranno trattati esclusivamente per le finalità inerenti alla gestione del rapporto di lavoro, nei limiti previsti da leggi e regolamenti.

Sono inoltre presenti eventuali dati personali relativi a Suoi familiari, di natura anche sensibile, da Lei trasmessi a Regione Lazio in loro nome e per conto, necessari per ottemperare ad adempimenti di legge, regolamento e contrattuali (dichiarazione dei redditi, detrazioni fiscali, assegni familiari, permessi per malattia figli, permessi per assistenza a portatori di handicap, certificazioni di matrimonio, ecc.).

Infine, per completezza, si precisa che Regione Lazio si riserva di verificare, nei limiti consentiti dalle norme di legge e contrattuali, l'integrità dei propri sistemi (informatici e di telefonia). In particolare la Regione Lazio non effettua apposite registrazioni per il controllo dell'attività lavorativa del personale ma solo registrazioni volte a salvaguardare la sicurezza ed il mantenimento dell'efficienza dei sistemi nonché a garantire la corretta gestione della rendicontazione delle spese. I dati registrati a tale scopo dai sistemi non sono utilizzati in alcun modo per il controllo a distanza dei lavoratori.

2. MODALITÀ DEL TRATTAMENTO

Il trattamento dei Suoi dati, ed eventualmente dei Suoi familiari, sarà effettuato mediante l'ausilio di strumenti manuali, informatici e telematici con logiche strettamente correlate alle suddette finalità e, comunque, in modo da garantire la sicurezza e la riservatezza dei dati stessi. I dati potranno essere trattati esclusivamente dal personale e dai collaboratori della Regione Lazio o dalle imprese espressamente nominate come Responsabili del trattamento.

Alcuni dati, quali, ad esempio, il nominativo, potranno essere resi disponibili sulla intranet aziendale.

3. NATURA OBBLIGATORIA O FACOLTATIVA DEL CONFERIMENTO DEI DATI

Il conferimento dei Suoi dati personali per le suddette finalità è necessario per l'instaurazione, la prosecuzione e corretta gestione del contratto di lavoro; pertanto l'eventuale rifiuto a fornire tali dati potrà causare la mancata instaurazione del rapporto contrattuale, ovvero in corso di tale rapporto, l'impossibilità di proseguirlo.

4. AMBITO DI COMUNICAZIONE E DIFFUSIONE DEI DATI

I Suoi dati personali saranno comunicati nei limiti previsti dalla vigente normativa, dagli accordi sindacali nonché dalla normativa in materia di protezione dei dati personali. I Suoi dati saranno comunicati agli enti ed alle Autorità competenti in adempimento agli obblighi di legge nella misura strettamente necessaria. In particolare, a titolo esemplificativo e non esaustivo, si evidenzia che i dati potranno essere comunicati alla Corte dei conti (per la gestione dei trattamenti previdenziali), alle Commissioni medico ospedaliere (per la concessione della pensione privilegiata ordinaria e pensione di inabilità, per la concessione del prolungamento del periodo di assenza per malattia, per la risoluzione del rapporto di lavoro per infermità, per nuovo inquadramento per inidoneità fisica), agli Enti preposti alla vigilanza in materia di igiene e sicurezza del lavoro (compresi l'INAIL e l'Autorità locale di pubblica sicurezza per le comunicazioni concernenti gli infortuni sul lavoro), all'INAIL (per la gestione dei trattamenti previdenziali e pensionistici nonché per prestazioni creditizie), alle ASL e strutture sanitarie competenti (per la richiesta di visita fiscale e per gli accertamenti sanitari relativi allo stato di salute del dipendente assente per malattia), ai Centri per l'impiego (per le assunzioni di personale appartenente a categorie protette), alla Presidenza del Consiglio dei Ministri -Dipartimento della Funzione Pubblica (in relazione alla gestione ed alla

rilevazione annuale dei permessi per cariche sindacali).
I dati potranno inoltre essere comunicati agli Istituti bancari appositamente indicati per il versamento delle somme a qualsiasi titolo spettanti nonché, su espressa e separata richiesta degli interessati, a enti ed organismi vari per l'adempimento di specifiche prestazioni aggiuntive facoltative a favore del personale (ad esempio polizze sanitarie, polizze vita ed infortuni, previdenza integrativa).
La Regione Lazio Le garantisce la massima cura affinché la comunicazione dei dati personali Suoi e degli eventuali Suoi familiari ai predetti destinatari riguardi esclusivamente i dati necessari per il raggiungimento delle specifiche finalità cui i dati stessi o la comunicazione sono destinati.
Si ricorda, infine, l'assunzione da parte Sua delle responsabilità connesse alla trasmissione alla Regione Lazio di eventuali dati personali riguardanti i Suoi familiari per l'ammissione ai benefici cui la raccolta è finalizzata. A tal fine, si prega di curare direttamente ogni adempimento che la renda possibile.
E' prevista, con le cautele disposte dalla normativa in materia di protezione dei dati personali, la diffusione dei dati personali nei casi in cui la normativa vigente preveda forme di pubblicità (ad esempio pubblicazione dei ruoli di anzianità del personale, graduatorie di concorsi o procedure selettive).

Si precisa, infine, che non è effettuato alcun trasferimento dei Suoi dati all'estero.

5. TITOLARE DEL TRATTAMENTO

Titolare del trattamento è la Regione Lazio, con sede in via Rosa Raimondi Garibaldi n. 7– 00147 Roma.

6. RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD)

La Regione Lazio ha proceduto a designare, con DGR n. …. del ……, il Responsabile della Protezione dei Dati personali (DPO), contattabile presso il seguente indirizzo e-mail:

dpo@regione.lazio.it

7. TEMPI DI CONSERVAZIONE

I dati personali sono conservati per tutta la durata del rapporto contrattuale e successivamente alla cessazione del rapporto per un periodo di **<indicare tempi di conservazione>.**

8. DIRITTI DELL'INTERESSATO

Ai sensi degli artt. da 15 a 22 del RGPD, Lei ha il diritto, in qualunque momento, di:

a) chiedere al Titolare del trattamento l'accesso ai dati personali, la rettifica, l'integrazione, la cancellazione degli stessi laddove applicabile, la limitazione del trattamento dei dati che la riguardano o di opporsi al trattamento degli stessi qualora ricorrano i presupposti previsti dal RGPD;
b) esercitare i diritti di cui sopra inviando idonea comunicazione alla casella di posta certificata dpo@regione.lazio.legalmail.it , citando: Rif. Privacy;

c) proporre un reclamo al Garante per la protezione dei dati personali, seguendo le procedure e le indicazioni pubblicate sul sito web ufficiale dell'Autorità: www.garanteprivacy.it.

SCHEMA E

INFORMATIVA PER IL TRATTAMENTO DEI DATI PERSONALI

INFORMATIVA PER IL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ARTICOLO 13 DEL REGOLAMENTO EUROPEO 2016/679 - RGPD

1. Premessa

Ai sensi dell'articolo 13 del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la Direttiva 95/46/CE (di seguito Regolamento UE n. 2016/679), la Regione Lazio, in qualità di Titolare del trattamento, è tenuta a fornirle informazioni in merito all'utilizzo dei suoi dati personali.

2. Identità e i dati di contatto del Titolare del trattamento

Il Titolare del trattamento dei dati personali di cui alla presente informativa è Regione Lazio, Via R. Raimondi Garibaldi 7– 00147 Roma. Al fine di semplificare le modalità di inoltro e ridurre i tempi per il riscontro si invita a presentare alla Regione Lazio le richieste di esercizio diritti di cui al successivo punto 10, scrivendo ai seguenti indirizzi e-mail: dpo@regionelazio.it e PEC: DPO@regione.lazio.legalmail.it.

3. Il Responsabile della protezione dei dati personali

Il Responsabile della protezione dei dati designato è contattabile all'indirizzo e-mail dpo@regione.lazio.it, all'indirizzo DPO@regione.lazio.legalmail.it, oppure a seguente indirizzo: protocollo@regione.lazio.legalmail.it.

4. Responsabili del trattamento

La Regione Lazio può avvalersi di soggetti terzi per l'espletamento di attività che comportano trattamenti di dati di cui la Regione stessa è Titolare. Conformemente a quanto stabilito dalla normativa, tali soggetti assicurano livelli di esperienza, capacità e affidabilità tali da garantire il rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza dei dati.

Le istruzioni, i compiti e gli oneri in capo a tali soggetti terzi sono formalizzati con la designazione degli stessi a "Responsabili del trattamento" ai sensi dell'articolo 28 del Regolamento UE 2016/679. I Responsabili designati sono sottoposti a verifiche periodiche al fine di constatare il mantenimento dei livelli di garanzia registrati in occasione dell'affidamento dell'incarico iniziale.

5. Soggetti autorizzati al trattamento

I Suoi dati personali sono trattati da personale interno previamente autorizzato e designato quale incaricato del trattamento, a cui sono impartite idonee istruzioni in ordine a misure, accorgimenti, modus operandi, tutti volti alla concreta tutela dei Suoi dati personali.

6. Finalità e base giuridica del trattamento

Il trattamento dei Suoi dati personali è necessario per lo svolgimento delle funzioni istituzionali di cui è investita la Regione e, pertanto, è effettuato ai sensi dell'articolo 6 "Liceità del trattamento", paragrafo 1 lett. e) del Regolamento UE 2016/679 ("*il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento*"). I dati personali sono trattati per le seguenti finalità strettamente connesse e necessarie alla fruizione del Portale e dei Servizi richiesti, nonché allo svolgimento di tutte le attività conseguenti, in particolare per:

- l'inserimento nell'Albo fornitori e adempimenti connessi;
- la partecipazione alle gare per l'acquisizione di beni e servizi funzionali allo svolgimento di indagini di mercato come previsto dalla normativa vigente in materia di appalti pubblici;
- l'invio di comunicazioni e di aggiornamenti nell'ambito dei programmi della Regione Lazio.

Inoltre, per garantire l'efficienza del servizio, i dati personali degli utenti potranno essere utilizzati per effettuare prove tecniche e di verifica, o indagini dirette a verificare il grado di soddisfazione degli utenti sul servizio offerto e richiesto.

I dati personali forniti dagli utenti che inoltrano richieste sono utilizzati al solo fine di eseguire il servizio o la prestazione richiesta e sono comunicati a terzi nel solo caso in cui ciò sia necessario per l'adempimento delle richieste (esempio servizio di spedizione della documentazione eventualmente richiesta) o quando la comunicazione sia imposta da obblighi normativi. La Regione Lazio si riserva la facoltà di effettuare attività di comunicazione e aggiornamento nell'ambito delle funzionalità del Portale.

7. Destinatari dei dati personali

I Suoi dati personali non sono oggetto di comunicazione o diffusione.

8. Trasferimento dei dati personali a Paesi extra UE

I Suoi dati personali non sono trasferiti al di fuori dell'Unione europea.

9. Periodo di conservazione

I Suoi dati sono conservati per:

- un periodo di 10 anni a partire dall'aggiudicazione della gara;

- per un periodo di 10 anni dalla data della revoca, nel caso in cui il fornitore richieda la cancellazione dall'Albo.

A tal fine, anche mediante controlli periodici, viene verificata costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto al trattamento.

10. I suoi diritti

Ai sensi degli articoli 13, paragrafo 2, lettere b) e d) e 14, paragrafo 2, lettere d) ed e) nonché degli articoli 15, 16, 17, 18, e 21 del RGPD, ha tra l'altro, il diritto, in qualunque momento, di chiedere al Titolare del trattamento:

- l'accesso ai Suoi dati personali;

- la rettifica e l'integrazione degli stessi;

- la cancellazione dei dati (laddove non sussista un obbligo legale di conservazione);

- la limitazione del trattamento dei dati e di opporsi al trattamento degli stessi dati qualora ricorrano i presupposti previsti dalle disposizioni normative vigenti.

Inoltre, ha il diritto di proporre un reclamo all'Autorità Garante per la protezione dei dati personali, seguendo le procedure e le indicazioni pubblicate sul sito web ufficiale dell'Autorità stessa.

11. Conferimento dei dati

Il conferimento dei Suoi dati è facoltativo, ma necessario per le finalità sopra indicate. Il mancato conferimento comporterà l'impossibilità di ottenere quanto richiesto.

12. Tipi di dati trattati

Dati di navigazione

I sistemi informatici e le procedure software preposte al funzionamento di questo sito web acquisiscono, nel corso del loro normale esercizio, alcuni dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet. Si tratta di informazioni che non sono raccolte per essere associate a interessati identificati, ma che per loro stessa natura potrebbero, attraverso elaborazioni ed associazioni con dati detenuti da terzi, permettere di identificare gli utenti. In questa categoria di dati rientrano gli indirizzi IP o i nomi a dominio dei computer utilizzati dagli utenti che si connettono al sito, gli indirizzi in notazione URI (Uniform Resource Identifier) delle risorse richieste, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal server (buon fine, errore, ecc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente. Questi dati vengono utilizzati al solo fine di ricavare informazioni statistiche anonime sull'uso del sito e per controllarne il corretto funzionamento e vengono cancellati immediatamente dopo l'elaborazione. I dati potrebbero essere utilizzati per l'accertamento di responsabilità in caso di ipotetici reati informatici ai danni del sito.

Dati forniti volontariamente dall'utente

L'invio facoltativo, esplicito e volontario di messaggi di posta elettronica agli indirizzi indicati su questo sito comporta la successiva acquisizione dell'indirizzo del mittente, necessario per rispondere alle richieste, nonché degli eventuali altri dati personali inseriti nella missiva. La registrazione facoltativa, esplicita e volontaria, tramite appositi moduli web (form) presenti sul nostro sito, comporta la successiva acquisizione di tutti i dati riportati nei campi compilati dall'utente ed il trattamento, conformemente a quanto riportato nelle specifiche informative riportate per ogni singolo form, è effettuato esclusivamente in adempimento di attività istituzionali proprie dell'Ente.

Cookies

Un "cookie" è un piccolo file di testo creato da alcuni siti web per immagazzinare informazioni sul computer dell'utente al momento in cui questo accede al sito. I cookie sono inviati da un server web al browser dell'utente e memorizzati sul computer di quest'ultimo; vengono, quindi, re-inviati al sito web al momento delle visite successive. Il sito della Regione Lazio fa uso dei cosiddetti "cookies di sessione", che risiedono esclusivamente nella memoria del computer dell'utente e non vengono memorizzati in modo persistente. Ciò implica la loro cancellazione una volta che il browser viene chiuso. L'uso è strettamente limitato alla trasmissione di identificativi di sessione, costituiti da numeri casuali generati dal server, necessari per consentire l'esplorazione sicura ed

efficiente del sito. L'utilizzo di cookies permanenti è strettamente limitato all'acquisizione di dati statistici relativi all'accesso al sito e/o per mantenere le preferenze dell'utente (lingua, layout, ecc.). Il portale si avvale di un software per la rilevazione degli accessi al proprio sito che ricorre all'utilizzo di cookies permanenti, allo scopo di raccogliere informazioni statistiche sui "visitatori unici" (persone diverse) del sito. Questi cookies, definiti come "Unique Visitor Cookies", contengono un codice alfanumerico che identifica i computer di navigazione, senza tuttavia alcuna ulteriore raccolta di dati personali.

Link a siti esterni

Questo sito internet contiene collegamenti ipertestuali detti "link" (ossia strumenti che consentono il collegamento ad una pagina web di un altro sito: i siti esterni raggiungibili tramite link attraverso il Portale della Regione Lazio sono sviluppati e gestiti da soggetti sui quali l'Ente non ha alcuna titolarità né controllo e non è in alcun modo responsabile circa contenuti, qualità, accuratezza e servizi offerti. La visita e l'utilizzo dei siti consultati dall'utente dal presente sito tramite link, quindi, è rimessa esclusivamente alla totale discrezionalità e responsabilità dell'utente utilizzatore. La presente informativa, pertanto, è resa solo per il sito della Regione Lazio e non anche per altri siti web eventualmente consultati dall'utente tramite link.

SCHEMA F

INFORMATIVA SUI DATI PERSONALI AI VISITATORI

INFORMATIVA AI VISITATORI

(ai sensi dell'articolo 13 del Regolamento UE 2016/679 - RGPD - in materia di protezione dei dati personali)

La Regione Lazio, in qualità di Titolare del trattamento, con sede in Via R. Raimondi Garibaldi 7– 00147 Roma, ai sensi dell'articolo 13 del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito "RGPD"), che abroga la Direttiva 95/46/CE, Le fornisce di seguito l'informativa circa le modalità di trattamento dei dati personali da Lei conferiti, al fine di accedere alle sedi di Regione Lazio.

Il RGPD garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Conformemente a quanto previsto dall'articolo 13 del RGPD, La informiamo pertanto che:

- la base giuridica del trattamento è quella di cui all'articolo 6, paragrafo 1, lett. e) del RGPD secondo il qaule "*il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*";
- i dati personali forniti verranno utilizzati nei limiti e per il perseguimento delle finalità relative alla registrazione e archiviazione della Sua presenza, nella qualità

di visitatore negli uffici di Regione Lazio, anche per motivi di sicurezza e controllo interno;

- i documenti di identità consegnati al personale di vigilanza verranno custoditi strettamente per il periodo di permanenza del visitatore nei locali di Regione Lazio;
- il conferimento dei dati è facoltativo; resta inteso che l'eventuale rifiuto a fornire tali dati comporterà l'impossibilità di accesso negli uffici della Regione Lazio;
- i dati personali forniti saranno trattati "in modo lecito e secondo correttezza";
- il trattamento sarà effettuato anche con l'ausilio di strumenti elettronici e/o automatizzati, ai quali possono accedere esclusivamente i soggetti autorizzati nel pieno rispetto di quanto previsto dal RGPD;
- i dati potranno essere trattati con la collaborazione di soggetti terzi espressamente nominati Responsabili esterni del trattamento dal Titolare;
- i dati potranno essere comunicati:

  - a tutte le strutture preposte a verifiche e controlli in merito al corretto adempimento delle finalità su indicate;

  - al personale e ai collaboratori in qualità di responsabili e persone autorizzate al trattamento dei dati per le pratiche che La riguardano/interessano; tutti i soggetti sono debitamente informati ed istruiti circa gli adempimenti e le misure da adottare in materia di protezione dei dati personali;

- i dati personali non sono soggetti a diffusione;
- i dati personali saranno conservati per il tempo strettamente necessario al perseguimento delle finalità per cui i dati sono trattati, nei limiti stabiliti dalla normativa vigente e, comunque, non oltre il termine di 3 mesi dall'ultimo accesso alle sedi della Regione Lazio.

La informiamo altresì che:

- Titolare del trattamento è la Regione Lazio, con sede in Via R. Raimondi Garibaldi 7– 00147 Roma;
- come previsto dall'articolo 37 del RGPD, la Regione Lazio ha proceduto a designare, con DGR n. …… del ……, il Responsabile della Protezione dei Dati personali (DPO), contattabile presso il seguente indirizzo e-mail: dpo@regione.lazio.it oppure all'indirizzo PEC: dpo@regione.lazio.legalmail.it.

Ai sensi degli articolo 13, paragrafo 2, lettere b) e d) e 14, paragrafo 2, lettere d) e e) nonché degli articoli 15, 16, 17, 18 e 21 del RGPD, i soggetti cui si riferiscono i dati personali hanno il diritto, in qualunque momento, di chiedere al Titolare del trattamento l'accesso ai dati personali, la rettifica, l'integrazione, la cancellazione degli stessi laddove applicabile, la limitazione del trattamento dei dati che la riguardano o di opporsi al trattamento degli stessi qualora ricorrano i presupposti previsti dal RGPD.

I diritti di cui sopra possono essere esercitati dall'interessato inviando una richiesta al seguente indirizzo di posta elettronica: urp@regione.lazio.it e PEC: urp@regione.lazio.legalmail.it .

L'interessato ha il diritto di proporre un reclamo al Garante per la protezione dei dati personali, seguendo le procedure e le indicazioni pubblicate sul sito web ufficiale dell'Autorità: www.garanteprivacy.it.

SCHEMA G

(art. 474, c. 2)

NOMINA RESPONSABILE DEL TRATTAMENTO

ATTO DI NOMINA A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

(*ove necessario* **Allegato al CONTRATTO DEL XX.XX.XXXX)**

TRA

La Regione Lazio, con sede in Via R. Raimondi Garibaldi 7– 00147 Roma, nella persona del Dott……;

E

La **<*indicare ragione e denominazione sociale della Società*>**, di seguito, per brevità, anche Società, con sede in ……in persona del legale rappresentante pro tempore Dott. …….;

PREMESSO CHE

la Regione Lazio, in qualità di Titolare del trattamento svolge attività che comportano il trattamento di dati personali nell'ambito dei servizi istituzionalmente affidati;

la Regione Lazio, in qualità di Titolare del trattamento è consapevole di essere tenuta a mettere in atto misure tecniche e organizzative volte ad attuare in modo efficace i principi di protezione dei dati e adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

VISTO l'articolo 474, comma 2, del r.r. 6 settembre 2002, n. 1 (Regolamento di organizzazione degli uffici e dei servizi della Giunta regionale) e successive modificazioni, il quale prevede che il titolare del trattamento, con specifico atto negoziale di incarico ai singoli responsabili del trattamento, disciplina i trattamenti affidati al responsabile, i compiti e le istruzioni secondo quanto previsto dall'articolo 28, paragrafo 3, del RGPD e in coerenza con le indicazioni del DPO; nell'atto di incarico è, altresì, definita la possibilità di nomina di un sub-responsabile, secondo quanto previsto dall'articolo 28, paragrafi 2 e 4, del RGPD;

VISTO il 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 (di seguito RGPD), il quale garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento al diritto alla protezione dei dati personali;

CONSIDERATO che detto Regolamento è divenuto efficace in data 25 maggio 2018, con conseguente abrogazione delle parti del decreto legislativo 30 giugno 2003 n. 196 non compatibili con il predetto Regolamento;

VISTO il decreto legislativo 196/2003 "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 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" e successive modificazioni;

CONSIDERATO che le attività, erogate in esecuzione del Contratto ***<indicare riferimenti del contratto>***, in essere tra Regione Lazio e ***<indicare ragione e denominazione sociale della Società>,*** implicano da parte di quest'ultima, il trattamento dei dati personali di cui è Titolare la Regione Lazio, ai sensi di quanto previsto dal Regolamento (UE) 2016/679;

PRESO ATTO che l'articolo 4, n. 2) del RGPD definisce «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

PRESO ATTO che l'articolo 4, n. 7) del RGPD definisce "Titolare del Trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

PRESO ATTO che l'art. 4, n. 8) del RGPD definisce "Responsabile del Trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

VISTO il Provvedimento del Garante per la Protezione dei Dati Personali 27/11/2008 (Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema) e successive modificazioni, pubblicato sulla Gazzetta Ufficiale n. 300 del 24/12/2008;

CONSIDERATO che il suddetto Provvedimento richiede che si proceda alla designazione individuale degli Amministratori di Sistema (System Administrator), degli Amministratori di Base Dati (Database Administrator), degli Amministratori di Rete (Network Administrator) e degli Amministratori di Software Complessi, che, nell'esercizio delle proprie funzioni, hanno accesso, anche fortuito, a dati personali;

VISTO il provvedimento dell'AgID (Misure minime di sicurezza ICT per le Pubbliche Amministrazioni), adottato in attuazione della Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015 (di seguito per brevità "Misure minime AgID"), il quale ha dettato le regole da osservare per garantire un uso appropriato dei privilegi di Amministratore;

RITENUTO che, ai sensi dell'articolo 28, paragrafo 1 del RGPD, la Società presenta garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento dei dati personali di cui la Regione Lazio è Titolare soddisfi i requisiti e il pieno rispetto delle disposizioni previste dal RGPD;

Quanto sopra premesso, le parti stipulano e convengono quanto segue:

Articolo 1

<***indicare ragione e denominazione sociale della Società***>, in qualità di **RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI** in virtù del presente atto di designazione, ai sensi e per gli effetti delle vigenti disposizioni normative di cui agli articoli 4, n. 8) e 28 del RGPD, con riguardo alle operazioni di trattamento connesse all'esecuzione del suddetto contratto, dichiara di essere edotta di tutti gli obblighi che incombono sul Titolare del trattamento e si impegna a rispettarne e consentirne ogni prerogativa, obbligo, onere e diritto che discende da tale posizione giuridica, attenendosi alle disposizioni operative contenute nel presente atto.

Articolo 2

Il Responsabile del trattamento dei dati personali nell'effettuare le operazioni di trattamento connesse all'esecuzione del suddetto contratto dovrà attenersi alle seguenti disposizioni operative:

- I trattamenti dovranno essere svolti nel pieno rispetto delle previsioni legislative vigenti in materia di protezione dei dati personali, nonché tenendo conto dei provvedimenti e dei comunicati ufficiali emessi dall'Autorità Garante per la Protezione dei Dati Personali. In particolare:
  - i trattamenti sono svolti per <***indicare le finalità per cui il fornitore tratta i dati (es. ai fini di assistenza e manutenzione)***>;
  - i dati personali trattati in ragione delle attività di cui ai suddetti contratti hanno ad oggetto: dati di natura personale (articolo 4, n.1) del RGPD); dati sensibili (articolo 9 del RGPD "Categorie particolari di dati personali"; dati giudiziari (articolo 10 del RGPD); <***eliminare le eventuali tipologie di dati non oggetto di trattamento***>
  - le categorie di interessati sono <***indicare le tipologie di interessato cui i dati afferiscono***>.

- La Società è autorizzata a procedere all'organizzazione di ogni operazione di trattamento dei dati nei limiti stabiliti dai contratti in essere tra le parti e dalle vigenti disposizioni contenute nel RGPD. A tale scopo, *per "trattamento"* si intende ai sensi dell'articolo 4, n. 2) del RGPD, "*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*".

- La Società si impegna, già in fase contrattuale, al fine di garantire il rispetto del principio della "Protezione dei dati fin dalla progettazione e protezione predefinita" di cui all'articolo 25 del RGPD, a determinare i mezzi del trattamento e a mettere in atto le misure tecniche e organizzative adeguate, di cui all'articolo 32 del RGPD, prima dell'inizio delle attività.
- La Società dovrà eseguire i trattamenti funzionali alle attività ad essa attribuite e comunque non incompatibili con le finalità per cui i dati sono stati raccolti. Qualora sorgesse la necessità di effettuare trattamenti su dati personali diversi ed eccezionali rispetto a quelli normalmente eseguiti, la Società dovrà informare il Titolare del trattamento ed il Responsabile della Protezione dei Dati (DPO) della Regione Lazio.

- La Società si impegna a garantire, senza ulteriori oneri per l'Amministrazione, l'esecuzione di tutti i trattamenti individuati al momento della stipula del contratto e dei quali dovesse insorgere in seguito la necessità ai fini dell'esecuzione del contratto stesso.

- La Società dovrà attivare le necessarie procedure aziendali per identificare ed istruire le persone autorizzate al trattamento dei dati personali ed organizzarne i compiti in maniera che le singole operazioni di trattamento risultino coerenti con le disposizioni di cui alla presente nomina, facendo in modo, altresì, che, sulla base delle istruzioni operative loro impartite, i trattamenti non si discostino dalle finalità istituzionali per cui i dati sono stati raccolti e trattati. La Società garantirà, inoltre, che le persone autorizzate al trattamento siano vincolate da un obbligo, legalmente assunto, di riservatezza.

- La Società si attiverà per garantire l'adozione delle misure di sicurezza di cui all'articolo 32 del RGPD. In particolare, tenuto conto delle misure di sicurezza in atto, adottate a protezione dei trattamenti dei dati per conto della Regione Lazio come previste dal contratto vigente, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento e, sulla base delle risultanze dell'analisi dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, che derivano in particolare dalla distruzione, perdita, modifica, divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati, porrà in essere le opportune azioni organizzative per l'ottimizzazione di tali misure, per garantire un livello di sicurezza adeguato al rischio. Tali misure comprendono, tra le altre:
  a) la pseudonimizzazione e la cifratura dei dati personali;
  b) misure idonee a garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
  c) misure idonee a garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico;
  d) procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

  In aggiunta la Società, ove applicabile, dovrà adottare le misure minime di sicurezza ICT per le PP.AA. di cui alla circolare AgID del 18 aprile 2017, n. 2/2017, nonché le eventuali ulteriori misure specifiche stabilite dal Titolare, nel rispetto dei contratti vigenti.

- La Società dovrà predisporre e tenere a disposizione del Titolare la documentazione tecnica relativa sia alle misure di sicurezza in atto sia alle modifiche in seguito riportate; inoltre renderà disponibili al Titolare tutte le informazioni necessarie per dimostrare il rispetto degli adempimenti normativi previsti dal RGPD, consentendo di effettuare periodicamente attività di verifica, comprese ispezioni realizzate dal Titolare stesso o da un altro soggetto da questi incaricato.

- La Società adotterà le politiche interne e attuerà le misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure (*privacy by design*); adotterà ogni misura adeguata a garantire che i dati personali siano trattati in ossequio al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il tempo strettamente necessario al raggiungimento delle stesse (*privacy by default*).

- La Società, ai sensi dell'articolo 30 del RGPD e nei limiti di quanto in esso previsto, è tenuta a tenere un Registro delle attività di Trattamento effettuate sotto la propria responsabilità e a cooperare con il Titolare e con l'Autorità Garante per la protezione dei dati personali, laddove ne venga fatta richiesta ai sensi dell'articolo 30, paragrafo 4, del RGPD.

- La Società è tenuta ad informare di ogni violazione di dati personali (cosiddetta *data breach*) il Titolare ed il Responsabile della Protezione dei Dati (DPO) della Regione Lazio, tempestivamente e senza ingiustificato ritardo, entro 24 ore dall'avvenuta conoscenza dell'evento. Tale notifica – da effettuarsi tramite PEC da inviare all'indirizzo protocollo@regione.lazio.legalmail.it e dpo@regione.lazio.legalmail.it, deve essere accompagnata da ogni documentazione utile, ai sensi degli articoli 33 e 34 del RGPD, per permettere al Titolare, ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali e/o darne comunicazione agli interessati, entro il termine di 72 ore da quando il Titolare ne è venuto a conoscenza. Nel caso in cui il Titolare debba fornire informazioni aggiuntive alla suddetta Autorità Garante, la Società supporterà il Titolare nella misura in cui le informazioni richieste e/o necessarie per l'Autorità Garante siano esclusivamente in possesso del Responsabile Esterno e/o di suoi sub-Responsabili.

- La Società, su eventuale richiesta del Titolare, è tenuta inoltre ad assistere quest'ultimo nello svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente a quanto prescritto dall'articolo 35 del RGPD e nella eventuale consultazione del Garante per la protezione dei dati personali, prevista dall'articolo 36 del RGPD.

- La Società, qualora riceva istanze degli interessati in esercizio dei loro diritti ai sensi degli articoli da 15 a 22 del RGPD, è tenuta a:
  - darne tempestiva comunicazione scritta al Titolare e al Responsabile della Protezione dei Dati (DPO) della Regione Lazio, allegando copia della richiesta;
  - valutare con il Titolare e con il DPO della Regione Lazio la legittimità delle richieste;
  - coordinarsi con il Titolare e con il DPO della Regione Lazio al fine di soddisfare le richieste ritenute legittime.

- Laddove fosse espressamente autorizzata dalla Regione Lazio la sub-fornitura / il sub-appalto, la Regione Lazio è tenuta a procedere alla designazione di detti sub-fornitori / sub-appaltatori, preventivamente autorizzati dalla Regione stessa, quali Responsabili del trattamento, imponendogli, mediante contratto o altro atto giuridico, i medesimi obblighi in materia di protezione dei dati contenuti nella presente nomina, prevedendo, in particolare, garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del RGPD. Qualora l'altro Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, la Società conserverà nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi dell'altro Responsabile ai sensi dell'articolo 28, paragrafo 4 del RGPD.

- La Società garantisce gli adempimenti e le incombenze anche formali verso l'Autorità Garante quando richiesto e nei limiti dovuti, adoperandosi per collaborare tempestivamente, per quanto di competenza, sia con il Titolare sia con l'Autorità garante per la protezione dei dati personali. In particolare:
  - fornisce informazioni sulle operazioni di trattamento svolte;

- consente l'accesso alle banche dati oggetto delle operazioni di trattamento;
- consente l'esecuzione di controlli;
- compie quanto necessario per una tempestiva esecuzione dei provvedimenti inibitori, di natura temporanea.

- La Società si impegna ad adottare, su richiesta del Titolare e nel rispetto degli obblighi contrattuali assunti, nel corso dell'esecuzione dei contratti, ulteriori garanzie quali l'applicazione di un codice di condotta applicato o di un meccanismo di certificazione approvato ai sensi degli articoli 40 e 42 del RGPD, laddove adottati. Il Titolare potrà in ogni momento verificare l'adozione di tali ulteriori garanzie.

- La Società non può trasferire i dati personali verso un paese terzo o un'organizzazione internazionale, salvo che non abbia preventivamente ottenuto l'autorizzazione scritta da parte del Titolare.

- La Società è tenuta a comunicare al Titolare ed al DPO della Regione Lazio il nome ed i dati del proprio DPO, laddove la società stessa lo abbia designato conformemente a quanto prescritto dall'articolo 37 del RGPD. Il DPO collaborerà e si terrà in costante contatto con il DPO della Regione Lazio.

Articolo 3

(laddove le prestazioni contrattuali implichino l'erogazione di servizi di amministrazione di sistema)

In conformità a quanto prescritto dal Provvedimento del Garante del 27/11/2008 e successive modificazioni ed alle citate Misure minime AgID relativamente alle utenze Amministrative, laddove le prestazioni contrattuali implichino l'erogazione di servizi di amministrazione di sistema, la Società, in qualità di Responsabile del trattamento, si impegna a:

- individuare i soggetti ai quali affidare il ruolo di Amministratori di Sistema (System Administrator), Amministratori di Base Dati (Database Administrator), Amministratori di Rete (Network Administrator) e/o Amministratori di Software Complessi e, sulla base del successivo atto di designazione individuale, impartire le istruzioni a detti soggetti, vigilando sul relativo operato;
- assegnare ai suddetti soggetti una user id che contenga riferimenti agevolmente riconducibili all'identità degli Amministratori e che consenta di garantire il rispetto delle seguenti regole:
  - divieto di assegnazione di user id generiche e già attribuite anche in tempi diversi;
  - utilizzo di utenze amministrative anonime, quali "root" di Unix o "Administrator" di Windows, solo per situazioni di emergenza; le relative credenziali devono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso;
  - disattivazione delle user id attribuite agli Amministratori che non necessitano più di accedere ai dati;
- associare alle user id assegnate agli Amministratori una password e garantire il rispetto delle seguenti regole:
  - utilizzare password con lunghezza minima di almeno 14 caratteri, qualora l'autenticazione a più fattori non sia supportata;

  - cambiare la password alla prima connessione e successivamente almeno ogni 30 giorni (password again).
  - le password devono differire dalle ultime 5 utilizzate (password history);
  - conservare le password in modo da garantirne disponibilità e riservatezza;
  - registrare tutte le immissioni errate di password. Ove tecnicamente possibile, gli account degli Amministratori devono essere bloccati dopo un numero massimo di tentativi falliti di login;
  - assicurare che l'archiviazione di password o codici PIN su qualsiasi supporto fisico avvenga solo in forma protetta da sistemi di cifratura;
- assicurare la completa distinzione tra utenze privilegiate e non privilegiate di amministratore, alle quali devono corrispondere credenziali diverse;
- assicurare che i profili di accesso, in particolare per le utenze con privilegi amministrativi, rispettino il principio del need-to-know, ovvero che non siano attribuiti diritti superiori a quelli realmente necessari per eseguire le normali attività di lavoro. Le utenze con privilegi amministrativi devono essere utilizzate per il solo svolgimento delle funzioni assegnate;
- mantenere aggiornato un inventario delle utenze privilegiate (Anagrafica AdS), anche attraverso uno strumento automatico in grado di generare un alert quando è aggiunta una utenza amministrativa e quando sono aumentati i diritti di una utenza amministrativa;
- adottare sistemi di registrazione degli accessi logici (log) degli Amministratori ai sistemi e conservare gli stessi per un congruo periodo non inferiore a 6 mesi. Qualora la Società utilizzi sistemi messi a disposizione dalla Regione, comunicare agli Amministratori che la Regione stessa procederà alla registrazione e conservazione dei log;
- impedire l'accesso diretto ai singoli sistemi con le utenze amministrative. In particolare, deve essere imposto l'obbligo per l'Amministratore di accedere con una utenza normale e solo successivamente dargli la possibilità di eseguire, come utente privilegiato, i singoli comandi;
- utilizzare, per le operazioni che richiedono utenze privilegiate di amministratore, macchine dedicate, collocate in una rete logicamente dedicata, isolata rispetto ad internet. Tali macchine non devono essere utilizzate per altre attività;
- comunicare al momento della sottoscrizione del presente atto, e comunque con cadenza almeno annuale ed ogni qualvolta se ne verifichi la necessità, alla Regione gli estremi identificativi delle persone fisiche preposte quali Amministratori di Sistema, di Base Dati, di Rete e/o di software Complessi, specificando per ciascuno di tali soggetti:
  - il nome e cognome;
  - la user id assegnata agli Amministratori;
  - il ruolo degli Amministratori (ovvero di Sistema, Base Dati, di Rete e/o di Software Complessi);
  - i sistemi che gli stessi gestiscono, specificando per ciascuno il profilo di autorizzazione assegnato;

- eseguire, con cadenza almeno annuale, le attività di verifica dell'operato degli Amministratori e consentire comunque alla Regione ove ne faccia richiesta, di eseguire in proprio dette verifiche;
- nei limiti dell'incarico affidato, mettere a disposizione del Titolare e del DPO della Regione quando formalmente richieste, le seguenti informazioni relative agli Amministratori: log in riusciti, log in falliti, log out. Tali dati dovranno essere resi disponibili per un congruo periodo non inferiore a 6 mesi;

- durante l'esecuzione dei Contratti, nell'eventualità di qualsivoglia modifica della normativa in materia di protezione dei dati personali, che generi nuovi requisiti (ivi incluse nuove misure di sicurezza di natura fisica, logica e/o organizzativa), la Società. si impegna a collaborare, nei limiti delle proprie competenze tecniche/organizzative e delle proprie risorse, con il Titolare affinché siano sviluppate, adottate ed implementate misure correttive di adeguamento ai nuovi requisiti.

La presente nomina avrà efficacia fino al termine del suindicato contratto in essere tra Regione Lazio e la Società.

All'atto della cessazione dei contratti in essere con la Regione Lazio, la Società, sulla base delle determinazioni della Regione Lazio, restituirà i dati personali oggetto del trattamento oppure provvederà alla loro integrale distruzione, salvo che i diritti dell'Unione e degli Stati membri ne prevedano la conservazione. In entrambi i casi rilascerà un'attestazione scritta di non aver trattenuto alcuna copia dei dati.

La validità del presente atto si intende altresì estesa ad ulteriori, eventuali, proroghe contrattuali.

Titolare del Trattamento

_____

Sottoscrivendo il presente atto, ***<indicare ragione e denominazione sociale della Società>***:

□ conferma di conoscere gli obblighi assunti in relazione alle disposizioni del RGPD e di possedere i requisiti di esperienza, capacità ed affidabilità idonei a garantire il rispetto di quanto disposto dal medesimo regolamento e sue eventuali modifiche ed integrazioni;
□conferma di aver compreso integralmente le istruzioni qui impartite e si dichiara competente e disponibile alla piena esecuzione di quanto affidato;
□accetta la nomina di Responsabile del trattamento dei dati personali e si impegna ad attenersi rigorosamente a quanto ivi stabilito, nonché alle eventuali successive modifiche ed integrazioni disposte dal Titolare, anche in ottemperanza alle modifiche normative in materia.

Responsabile del Trattamento

Legale Rappresentante

_____

SCHEMA H

CLAUSOLE DEI CONTRATTI IN CUI IL FORNITORE DEVE ESSERE NOMINATO RESPONSABILE DEL TRATTAMENTO

“Protezione dei dati personali”

La Regione Lazio, in qualità di Titolare del Trattamento, con atto formale riportato in allegato (**inserire riferimenti dell’Allegato**) al presente Contratto e parte integrante dello stesso, nomina la Società, Responsabile del trattamento dei dati ai sensi degli articoli 4, n. 8) e 28 del 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.

Con la sottoscrizione del presente contratto, la Società si obbliga ad accettare la nomina a Responsabile del Trattamento, nonché a sottoscrivere l’atto di nomina di cui all’Allegato (**inserire riferimenti dell’Allegato**) contestualmente al contratto e comunque entro e non oltre il termine di quindici giorni dalla data di stipula del contratto stesso.

Sottoscritto l’atto, la Società garantisce l’osservanza delle prescrizioni in esso contenute da parte del proprio personale dipendente, nonché di quello incaricato per l’esecuzione del Contratto.

STIPULA CONTRATTO <testo valido anche per Convenzione/Protocollo d’Intesa>

Art. … - Trattamento dei dati personali

Le parti dichiarano di avere rilasciato, prima della sottoscrizione del presente contratto, tutte le informazioni di cui all’articolo 13 del Regolamento UE 2016/679 (di seguito RGPD) circa il trattamento dei dati personali conferiti per l’esecuzione del contratto stesso e di essere a conoscenza dei diritti che spettano alle persone fisiche in qualità di interessati in virtù dell’articolo 13, paragrafo 2, lettere b) e d) e 14, paragrafo 2, lettere d) e e), nonché degli articoli 15, 16, 17, 18, e 21 del RGPD, che potranno essere esercitati, in qualunque momento, presso i recapiti indicati nelle policy privacy pubblicate sui siti web di ciascuna Parte.

Le parti si impegnano a improntare il trattamento dei dati raccolti per la gestione del contratto e l’esecuzione economica ed amministrativa dello stesso, nonché per l’adempimento degli obblighi legali ad esso connessi e per fini di studio e statistici, ai principi di correttezza, liceità e trasparenza, nel pieno rispetto di quanto previsto dal RGPD e dal decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni.

In particolare le parti s’impegnano a trattare i dati, il cui conferimento è obbligatorio per l’esecuzione del contratto, esclusivamente con la collaborazione di personale autorizzato al trattamento, nonché di soggetti terzi espressamente nominati Responsabili del trattamento ai sensi dell’articolo 28 del RGPD. Il trattamento sarà effettuato tramite l’utilizzo di procedure informatizzate ovvero mediante trattamenti manuali. I dati non saranno oggetto di comunicazione e/o trasferimento verso paesi terzi e saranno conservati per il tempo strettamente necessario al perseguimento delle finalità per cui i dati sono trattati, nei limiti stabiliti da leggi o regolamenti e, comunque, non oltre il termine di 10 anni dall’ultimo atto o comunicazione inerente il procedimento stesso.

CLAUSOLA DA INSERIRE NEI CONTRATTI LADDOVE il Soggetto Terzo debba essere nominato Responsabile al trattamento dei dati personali ai sensi dell’articolo 28 del RGPD

Articolo … - Responsabile del Trattamento dei Dati Personali

Le attività oggetto del presente contratto implicano, da parte della Società, il trattamento dei dati personali di cui è Titolare la Regione Lazio, ai sensi del Regolamento UE 2016/679 (di seguito RGPD).

Regione Lazio, ai sensi dell'articolo 28 del RGPD, riconosce che la Società dispone delle garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento dei dati personali di cui la Regione Lazio è Titolare soddisfi i requisiti e il pieno rispetto delle disposizioni previste dal RGPD.

La Regione Lazio, in qualità di Titolare del Trattamento, con atto formale riportato in allegato (Allegato n. …) al contratto e parte integrante dello stesso, nomina la Società quale Responsabile del trattamento dei dati ai sensi degli articoli 4, n. 8) e 28 del RGPD. Con la sottoscrizione del presente contratto, la Società si impegna ad accettare la nomina a Responsabile del Trattamento. La Società si impegna, inoltre, a sottoscrivere l'atto di nomina di cui all'Allegato n. …, entro il termine di quindici giorni, dalla data di stipula del presente contratto.

Allegato n. …

Oggetto "Nomina a Responsabile del trattamento dei dati personali ai sensi degli articoli 4, n. 8) e 28 del RGPD – Regolamento (UE) 679/2016 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".

Va compilato secondo il modello di cui allo schema "G"

SCHEMA I

CLAUSOLE DISCIPLINARI DI GARA

"Protezione dei dati personali"

La Regione Lazio, in qualità di Titolare del Trattamento, garantisce che i dati personali saranno trattati ai sensi del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito RGPD), che abroga la Direttiva 95/46/CE, e ai sensi del decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni.

I dati personali saranno utilizzati esclusivamente per il perseguimento delle finalità istituzionali proprie della Regione Lazio, nei limiti stabiliti da espresse disposizioni normative e saranno trattati per finalità connesse e strumentali al presente disciplinare di gara e all'eventuale stipula ed esecuzione del contratto.

La Regione Lazio può venire a conoscenza, oltre che di dati di natura personale, anche di quelli relativi a condanne penali e reati (articolo 10 del RGPD). Tali dati saranno trattati

per le sole finalità previste dalla normativa vigente, mediante l'ausilio di strumenti manuali, informatici e telematici con logiche strettamente correlate alle finalità stesse e, comunque, in modo da garantire la sicurezza, la riservatezza, l'integrità e la disponibilità degli stessi.

I dati saranno trattati, direttamente dal Titolare o dal personale espressamente autorizzato al trattamento nonché da soggetti terzi espressamente nominati Responsabili del trattamento dal Titolare ai sensi dell'articolo 28 del RGPD.

STIPULA CONTRATTO <testo valido anche per Convenzione/Protocollo d'Intesa>

Art. …. - Trattamento dei dati personali

Le parti dichiarano di avere rilasciato, prima della sottoscrizione del presente contratto tutte le informazioni di cui all'articolo 13 del Regolamento UE 2016/679 (di seguito RGPD) circa il trattamento dei dati personali conferiti per l'esecuzione del contratto stesso e di essere a conoscenza dei diritti che spettano alle persone fisiche in qualità di interessati in virtù dell'articolo 13, paragrafo 2, lettere b) e d) e 14, paragrafo 2, lettere d) e e), nonché degli articoli 15, 16, 17, 18 e 21 del citato RGPD, che potranno essere esercitati, in qualunque momento, presso i recapiti indicati nelle policy privacy pubblicate sui siti web di ciascuna parte.

Le parti si impegnano a improntare il trattamento dei dati raccolti per la gestione del contratto e l'esecuzione economica ed amministrativa dello stesso, nonché per l'adempimento degli obblighi legali ad esso connessi, e per fini di studio e statistici, ai principi di correttezza, liceità e trasparenza nel pieno rispetto di quanto definito dal RGPD e ai sensi del decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni.

In particolare le parti si impegnano a trattare i dati, il cui conferimento è obbligatorio per l'esecuzione dell'atto, esclusivamente con la collaborazione di personale autorizzato al trattamento, nonché da soggetti terzi espressamente nominati Responsabili del trattamento ai sensi dell'articolo 28 del RGPD. Il trattamento sarà effettuato tramite l'utilizzo di procedure informatizzate ovvero mediante trattamenti manuali. I dati non saranno oggetto di comunicazione e/o trasferimento verso paesi terzi e saranno conservati per il tempo strettamente necessario al perseguimento delle finalità per cui i dati sono trattati, nei limiti stabiliti da leggi o regolamenti e, comunque, non oltre il termine di 10 anni dall'ultimo atto o comunicazione inerente il procedimento stesso.

CLAUSOLA DA INSERIRE NEI CONTRATTI LADDOVE il Soggetto Terzo debba essere nominato Responsabile al trattamento dei dati personali ai sensi dell'articolo 28 del RGPD.

Articolo …. - Responsabile del Trattamento dei Dati Personali

Le attività oggetto del presente contratto implicano, da parte della Società, il trattamento dei dati personali di cui è Titolare Regione Lazio, ai sensi del Regolamento UE 2016/679 (di seguito definito per brevità anche il "RGPD").

Regione Lazio, ai sensi dell'articolo 28 del RGPD, riconosce che la Società dispone delle garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento dei dati personali di cui la Regione Lazio è Titolare soddisfi i requisiti e il pieno rispetto delle disposizioni previste dal RGPD.

Regione Lazio, in qualità di Titolare del Trattamento, con atto formale riportato in allegato (Allegato n. …) al contratto e parte integrante dello stesso, nomina la Società quale Responsabile del trattamento dei dati ai sensi degli articoli 4, n. 8) e 28 del RGPD. Con la sottoscrizione del presente contratto, la Società si impegna ad accettare la nomina a Responsabile del Trattamento. La Società si impegna, inoltre, a sottoscrivere l'atto di nomina di cui all'Allegato n. …, entro il termine di quindici giorni, dalla data di stipula del presente contratto.

Allegato n. …

Oggetto "Nomina a Responsabile del trattamento dei dati personali ai sensi degli articoli 4, n. 8) e 28 del RGPD – Regolamento (UE) 679/2016 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".

Va compilato secondo il modello di cui allo schema "G".