(ALLEGATO C)

ATTO DI NOMINA A "REFERENTE GENERALE DATA PROTECTION"

ED ISTRUZIONI IMPARTITE AI SENSI DELL'ART. 29 DEL REGOLAMENTO U.E. 2016/679 (G.D.P.R.)

Il Titolare del trattamento - ALFA (Agenzia regionale per il lavoro, la formazione e l'accreditamento) – con Sede Legale in Via San Vincenzo, 4 -16121 Genova – C.F./P.IVA: 02437860998 – E-mail: privacy@alfaliguria.it – Pec: direzione@pec.alfaliguria.it, nella persona del Suo Legale Rappresentante – Dott. Fabio Liberati, con il presente atto, nomina

il Dott. /la Dott.ssa ……....

quale "**Referente Generale Data Protection" o "Referente Privacy di 1° livello**, ai fini del Regolamento U.E. 2016/679 in materia di protezione dei dati personali.

Il Referente Generale Data Protection è una figura indispensabile per una corretta gestione dei processi di trattamento dei dati personali che si svolgono nell'Ente.

a. Il Soggetto individuato dal Titolare come Referente Generale Data Protection ha tutte le caratteristiche richieste dalla normativa vigente ed è dotato della necessaria esperienza, capacità e di particolari requisiti tecnico-organizzativi, di onorabilità, professionali, morali o di condotta ed ha ricevuto formazione specifica in materia di privacy;

b. Il Referente Generale Data Protection garantisce il pieno rispetto della normativa ed assicura la generale adeguatezza delle misure di carattere tecnico ed organizzative adottate dal Titolare e, con il supporto dell'Amministratore di Sistema, è tenuto a garantire anche la sicurezza delle banche dati e la corretta gestione delle reti telematiche dell'Ente, la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali e vigila sul corretto utilizzo dei sistemi informatici di Alfa.

Il Titolare del Trattamento

Garantisce:

1. la necessaria autonomia ed indipendenza al Referente Data Protection individuato ed eroga i fondi necessari per realizzare l'adozione delle misure tecniche ed organizzative individuate e programmate;
2. che sia resa nota o conoscibile l'identità del Referente Data Protection nell'ambito delle proprie organizzazioni;
3. adeguata formazione ed istruzione al Referente *Data Protection* in materia;
4. l'adozione delle seguenti misure tecniche ed organizzative:

   a) verifica almeno annuale della rispondenza dell'operato dei Referenti Data Protection in relazione alle misure organizzative, tecniche e di sicurezza previste dalla legge per i trattamenti di dati personali effettuati nell'Ente;

   b) redazione dell'elenco dei Referenti Generali Data Protection come previsto nello specifico organigramma aziendale, reso disponibile in caso di accertamenti da parte del Garante, dove sono indicati gli estremi identificativi dei Referenti Generali Data Protection dell'Ente e l'elenco delle funzioni loro attribuite.

Parte A: Compiti generali del Referente *Data Protection dell'Ente*.

1. **Gestione delle richieste degli interessati**:

1.1 Il Referente ottempera alle richieste degli interessati nel termine di 30 (giorni) da quando queste pervengono se gli interessati sono Lavoratori il termine è di giorni 7 (sette).
1.2 Nel caso in cui sia impossibile ottemperare nel termine suddetto ne dà notizia all'interessato e provvede non oltre 90 giorni alla richiesta.

2. Gestione dei Registri: il Referente cura la compilazione dei registri delle attività di trattamento (art. 30 GDPR), delle violazioni (art. 33 GDPR) e della formazione dei dipendenti.

3. Procedura per la gestione dei *Data Breach*/Violazioni subite

3.1 Il Referente ha il compito di rilevare la violazione subita, la annota sul registro compilandone i campi.
3.2 Deve dare notizia, immediatamente e non oltre 48 ore, al Titolare del trattamento della violazione subita dopo avere provveduto all'annotazione della violazione.
3.3. Se del caso, deve riferirsi al Consulente *data protection* o all'assistente informatico per valutare tempestivamente la gravità della violazione.
3.4 Nel caso, ha il compito di notificare la gestione della violazione al Garante della protezione dei dati personali, anche con il supporto del consulente e, se necessario di comunicare agli Interessati l'avvenuta violazione dei dati che li riguardano.

e dispone, inoltre, che:

Il **Referente Generale Data Protection** curi l'adozione di tutte le misure tecnico-organizzative e di carattere generale nel prosieguo descritte:

Parte B: Misure tecnico-organizzative di carattere generale

Il Referente Generale Data Protection:

5. impartisce, ai soggetti autorizzati ad effettuare le operazioni di trattamento, dovute istruzioni generali scritte finalizzate ad una corretta gestione delle operazioni di trattamento di dati personali e della gestione degli atti e dei documenti contenenti dati personali delle categorie di interessati,
6. individua categorie omogenee di soggetti autorizzati e non autorizzati ad effettuare attività di trattamento di dati personali e ne cura l'aggiornamento periodico con cadenza almeno annuale,
7. cura che le istruzioni operative ai Soggetti Autorizzati siano debitamente esposte negli appositi spazi aziendali comuni (*intranet*) e che i Soggetti Autorizzati siano effettivamente istruiti ad effettuare corrette operazioni di trattamento dei dati personali,
8. cura altresì che i soggetti non autorizzati al trattamento di dati personali ricevano adeguate e specifiche istruzioni operative volte a preservare la segretezza, riservatezza ed integrità dei dati dati personali trattati in azienda,
9. è preposto alla gestione e alla manutenzione dei sistemi elettronici con i quali vengono effettuati trattamenti di dati personali, compresi i *client* intesi come "*postazioni di lavoro informatizzate*";
10. cura la realizzazione di copie di sicurezza (operazioni di *backup* e *recovery* dei dati), di custodia delle credenziali alla gestione dei sistemi di autenticazione e di autorizzazione, l'accesso a tutti i server in lettura/scrittura, la predisposizione delle procedure di disaster recovery, la creazione di nuovi utenti di rete e/o loro modifica, l'attribuzione nuovi nome computer del dominio e dei permessi di accesso agli utenti di rete, la creazione o modifica di aree condivise in rete, il monitoraggio degli eventi e dei servizi offerti dai servers, l'installazione e configurazione del sistema operativo, la manutenzione ed aggiornamento dei sistemi operativi ed antivirus dei server, l'installazione di software applicativo.

Parte B: Per le attività di trattamento effettuate con strumenti elettronici.

1. **Sistema di autenticazione informatica:**

1.1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

1.2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

1.3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

1.4. Con le istruzioni impartite ai soggetti autorizzati ed istruiti è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

1.5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

1.6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

1.7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

1.8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

1.9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

1.10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

1.11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

2. Sistema di autorizzazione:

2.1. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

2.2 I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

2.3 Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

3. Altre misure di sicurezza:

3.1 Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

3.2 I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

3.3 Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

3.4 Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

4. Ulteriori misure in caso di trattamento di dati sensibili o giudiziari:

4.1 I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

4.2 Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

4.3 I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

4.4 Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni

4.5 Il trattamento dei dati categorie particolari di dati personali ai sensi dell’art. 9 e 10 GDPR viene effettuato al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali comuni identificativi e di contatto. Se possibile, le categorie particolari di dati sono trattate esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi ed il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

5. Misure di sicurezza e garanzia:

5.1 Il titolare che adotta misure adeguate di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

Parte C: Per le attività di trattamento effettuate senza l'ausilio di strumenti elettronici:

1.1 Quando gli atti e i documenti contenenti categorie particolari di dati sono affidati a soggetti autorizzati al trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera tale da preservarli da accessi abusivi da parte di persone prive di autorizzazione e sono restituiti al termine delle operazioni affidate.

1.2 L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato e le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate.

1.3 Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

IL TITOLARE DEL TRATTAMENTO

IL REFERENTE GENERALE DATA PROTECTION
