(ALLEGATO D)

ISTRUZIONI IMPARTITE AI SOGGETTI CHE AGISCONO SOTTO L'AUTORITÀ DEL TRATTAMENTO AI SENSI DELL'ART. 29 DEL REG (UE) 679/2016 (GDPR)- "AUTORIZZATI PRIVACY DI 2° LIVELLO"

Il presente documento comprende istruzioni, generali e specifiche, impartite ai soggetti che agiscono sotto l'autorità del Titolare del trattamento ai sensi dell'art. 29 del REG (UE) 679/2016 (GDPR).

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

IMPARTISCE AI PROPRI COLLABORATORI E DIPENDENTI CHE TRATTANO DATI PERSONALI SOTTO LA SUA AUTORITÀ LE SEGUENTI ISTRUZIONI PER OPERARE UN CORRETTO TRATTAMENTO DEI DATI PERSONALI

Art. 1. Il divieto di effettuare trattamenti non autorizzati o, comunque, illeciti. L'obbligo di acquisire correttamente il consenso al trattamento dei dati personali e di rispettare i generali principi del trattamento. Documentazione e trasparenza delle operazioni di trattamento compiute dai soggetti autorizzati.

In questa sede è fatto espresso divieto a tutti i Soggetti Autorizzati dal Titolare che operano attività di trattamento sotto la sua autorità, di effettuare ulteriori e diverse attività di trattamento di dati personali non autorizzate, per le quali gli Interessati non sono stati debitamente informati o, comunque, illecite.

Nei limiti delle finalità del trattamento, i dati personali degli interessati devono essere sempre trattati secondo i principi generali di trasparenza, correttezza, finalità, proporzionalità e necessità e per il tempo strettamente necessario a realizzare la finalità per i quali questi sono stati trattati.

Il collaboratore ed il dipendente che opera sotto l'autorità del Titolare deve prima di procedere al trattamento dei dati personali dell'interessato informare adeguatamente l'interessato inviando l'informativa agli interessati anche via email e chiedendo di sottoscriverla per presa visione.

<u>Art. 2</u>. L'obbligo di rettificare eventuali irregolarità nell'ambito delle operazioni di trattamento e di limitare i dati personali trattati. L'autorizzazione delle operazioni precedentemente compiute e la richiesta di revoca del consenso.

Nel caso in cui il consenso dell'Interessato non sia stato raccolto nei modi e nei termini indicati dal precedente articolo, il collaboratore ed il dipendente devono adoperarsi per sanare ogni irregolarità rilevata e darne tempestiva notizia al Titolare oppure al Referente Data Protection nominato.

In caso di mancata esibizione dell'Informativa all'Interessato: occorre inviare l'informativa via email chiedendo all'Interessato di sottoscriverla per presa visione oppure chiedere la sottoscrizione cartacea del modulo in occasione della prima visita alla struttura da parte dell'interessato.

In caso di mancata autorizzazione dell'Interessato a trattamenti facoltativi: occorre richiedere l'autorizzazione successiva al trattamento dei dati personali da parte dell'interessato in modo tale da ratificare ogni operazione di trattamento compiuta in assenza di precedente consenso o con un consenso non idoneo ad autorizzare al trattamento. In particolare, il Collaboratore o il Dipendente hanno l'obbligo di interrompere ogni trattamento non autorizzato preventivamente dall'interessato.

Si deve documentare ogni richiesta di revoca o di autorizzazione successiva al trattamento da parte dell'Interessato.

<u>Art. 3</u>. L'obbligo di verifica della correttezza dei dati personali trattati e di aggiornamento.

Occorre verificare, prima di procedere con le operazioni di trattamento, che i dati personali trattati siano riferibili al soggetto interessato cui la pratica è riferita e che questi siano pertinenti, aggiornati, corretti, completi, esatti e non eccedenti rispetto alle finalità di trattamento.

Se, all'esito delle verifiche emerge che i dati personali raccolti sono insufficienti, inesatti od incompleti il Collaboratore ha il dovere di chiedere all'interessato ogni opportuno riscontro, integrazione, precisazione e chiarimento dei dati personali forniti che reputi necessario.

I Soggetti Autorizzati devono trattare unicamente i dati necessari perseguire le finalità espresse in informativa o per le quali il trattamento è stato autorizzato ed eliminare ogni dato personale, conferito dall'Interessato o comunque raccolto, eccedente e/o non necessario.

<u>Art. 4</u>. La verifica dell'Identità dell'Interessato in sede di accesso.

In particolare, il Collaboratore e/o il Dipendente preposto al controllo degli accessi alla struttura devono limitarsi a verificare l'identità dell'interessato tramite il cartellino identificativo o badge dato in dotazione dalla Struttura, senza chiedere, a meno che non sia necessario, ulteriori dati identificavi e/o l'esibizione di documenti di identità.

Nel caso in cui suddetta prassi si riveli insufficiente a verificare l'identità dell'Interessato, il Soggetto Autorizzato deve sospendere temporaneamente l'accesso ai locali, realizzare le procedure di verifica valutate come necessarie e, solo in caso di esito positivo delle procedure, autorizzare l'accesso all'Interessato.

In caso in cui le predette procedure diano esito negativo si deve sempre negare l'accesso ai locali al Richiedente.

Nessun trattamento di categorie particolari di dati dell'Interessato può essere effettuato laddove lo stesso non sia stato previamente autorizzato, dall'Interessato e dal Titolare, e nei limiti di quanto necessario ad eseguire la prestazione richiesta.

In caso di eventuali dubbi sulla liceità del trattamento che riguarda categorie particolari di dati personali occorre sempre riferirsi al Referente *Data Protection* o direttamente al Titolare prima di procedere al trattamento degli stessi.

Art. 5. Dovere di riservatezza di collaboratori e dipendenti. Divieto di divulgare e di comunicare a terzi non autorizzati dal titolare i dati personali degli Interessati.

I collaboratori ed i dipendenti si obbligano ad un generale dovere di riservatezza nei confronti degli Interessati e si impegnano a non comunicare, diffondere né divulgare, se non nei limiti e per le finalità e nei modi stabiliti in informativa, i dati personali degli Interessati.
La comunicazione e/o diffusione autorizzata ai sensi del precedente comma deve avvenire sempre nel rispetto dei principi generali di trasparenza, correttezza, finalità, proporzionalità e necessità e per il tempo strettamente necessario a realizzare la finalità per le quali tali dati sono stati trattati e previa ed espressa autorizzazione in tal senso dell'Interessato e del Titolare del trattamento.

I Collaboratori e Dipendenti che trattano dati personali, da ultimo, devono avere cura che anche coloro i quali prestano la propria attività lavorativa, anche saltuariamente presso la struttura del Titolare che non sono autorizzati al trattamento dei dati personali non vi accedano.

Art. 6. L'obbligo di informare il soggetto interessato nell'ipotesi di comunicazione dei suoi dati a terzi al di fuori delle ipotesi indicate in informativa.

Nel caso in cui l'espletamento dell'Incarico richieda di conferire i dati personali dell'interessato a Soggetti Terzi non indicati in informativa o con modalità o per finalità diverse rispetto a quanto stabilito in informativa, occorre che l'Interessato ne sia debitamente informato o che il nuovo trattamento sia debitamente autorizzato tanto dall'Interessato quanto dal Titolare del trattamento.

Nel caso in cui il trattamento richieda l'autorizzazione dell'interessato occorre ottenere espressa autorizzazione da parte dell'interessato prima di effettuare qualsiasi attività di trattamento.

<u>Art. 7.</u> Il divieto di divulgare e di comunicare a terzi non autorizzati dal titolare i dati personali dei soggetti interessati.

I dati personali degli interessati possono essere comunicati a soggetti Terzi nei limiti di quanto stabilito in informativa e solo se la comunicazione dei dati personali a terzi è necessaria o funzionale per un migliore svolgimento dell'incarico professionale conferito.

Se lo svolgimento dell'incarico richiede di conferire i dati personali dell'interessato a Soggetti Terzi non indicati in informativa o con modalità o per finalità diverse rispetto a quanto stabilito in informativa, l'Interessato ne deve essere, se del caso, debitamente informato anche sentito il parere, se del caso, del Referente Generale Data Protection oppure del Titolare del Trattamento.

Il Collaboratore ed il dipendente, al di fuori dei limiti stabiliti dal comma precedente, non può né diffondere né comunicare dati riferibili all'interessato a Terzi in assenza di previa ed espressa autorizzazione da parte del Titolare del trattamento e di rilascio dell'apposita informativa all'Interessato.

Laddove la comunicazione o la diffusione a terzi di dati personali sia stata autorizzata dal Titolare o dal Suo Referente, il Collaboratore ed il dipendente devono comunque minimizzare, ove possibile, i dati personali degli Interessati che formano oggetto di comunicazione nel rispetto dei principi generali di trasparenza, correttezza, finalità, proporzionalità e necessità e per il tempo strettamente necessario a realizzare la finalità per i quali questi sono stati trattati.

In ogni caso, nessun dato valutato eccedente deve essere comunicato o diffuso a Terzi pure se debitamente autorizzati e tutti i dati personali trattati, se possibile, devono essere minimizzati, resi anonimi o pseudonimizzati.

<u>Art. 8</u>. L'obbligo di prevenire e gestire correttamente il rischio relativo al trattamento di dati personali.

I collaboratori hanno l'obbligo di prevenire ove possibile e comunque limitare ogni rischio discendente o collegato alle attività di trattamento realizzate.

In particolare, i soggetti autorizzati devono adottare, secondo i canoni di ragionevolezza e trasparenza, ogni comportamento volto ad evitare la distruzione, la perdita, la modifica e la divulgazione non autorizzata, l'accesso accidentale o illegale ai dati personali trasmessi, memorizzati o comunque trattati, in formato digitale e/o cartaceo.

In caso di dubbio su come gestire determinate operazioni di trattamento, di violazione di dati personali/*Data Breach* (od anche solo di pericolo di verificarsi dello stesso) è fatto obbligo ai collaboratori di riferirsi immediatamente al Titolare od al Referente *Data Protection* designato.

<u>Art. 9</u>. L'obbligo di verificare periodicamente l'attuazione delle misure di sicurezza fisiche.

I collaboratori devono verificare che:

- le porte e le finestre ed ogni altro accesso ai locali siano sempre chiuse nel momento in cui accedono ed abbandonano la struttura,

- siano serrati i lucchetti di accesso agli archivi, anche cartacei, ed al server contenenti dati personali, al fine di evitare accessi abusivi da parte di soggetti non autorizzati,

- sia sempre escluso l'accesso ai dati personali, soprattutto se particolari/sensibili, a soggetti non autorizzati dal Titolare,

- tutte le misure fisiche di sicurezza adottate assicurino sempre standard adeguati di sicurezza, anche determinati dal Titolare, dal Referente *Data Protection* o da altri soggetti preposti.

Art. 10. L'obbligo di verificare periodicamente l'attuazione delle misure di sicurezza digitali.

I collaboratori che trattano dati personali attraverso PC in dotazione alla struttura devono verificare che:

- i sistemi di sicurezza informatica adottati garantiscano la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento di dati personali, nonché il ripristino tempestivo, la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.

- vengano adottate adeguate misure di protezione informatica quali: una procedura di autenticazione, l'adozione di procedure di gestione delle credenziali di autenticazione, l'utilizzazione di un sistema di autorizzazione, l'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o la manutenzione degli strumenti elettronici, la protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici, l'adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi.

- i sistemi operativi, gli antivirus, i programmi di rimozione *malware* installati nei PC siano aggiornati e che le procedure di backup dei dati predisposte vengano operate con regolarità e correttamente.

- ogni altra misura di sicurezza digitale adottata offra adeguati standard di sicurezza e l'assenza di rischi di vulnerabilità.

Art. 10 *bis*. Password Personale

I soggetti autorizzati devono adottare Password non inferiori ad 8 caratteri**,** con almeno 1 carattere maiuscolo, 1 carattere minuscolo, una sequenza numerica di almeno tre numeri. Le Password adottate vengono periodicamente aggiornate (ogni 6 mesi – o secondo altre indicazioni fornite dal Titolare) con altra Password di uguale complessità.

Nelle password di accesso ai sistemi informatici non devono mai essere inseriti dati personali dell'utente all'interno della password, come ad esempio nome, cognome, data di nascita o simili associazioni.

Art. 10 *ter*. Sicurezza e Prudenza

I soggetti autorizzati hanno il dovere:

- di proteggere e salvaguardare le proprie credenziali di accesso al sistema e di astenersi da comportamenti che potrebbero metterle a rischio, di non cedere le stesse a terzi e, comunque, di astenersi dall' adottare alcun comportamento che metta a rischio l'integrità dei dati personali trattati;

- di modificare sempre ed immediatamente le proprie credenziali di accesso nel caso di sospetto che Terzi non autorizzati abbiano acceduto abusivamente o compiuto un tentativo di accesso non autorizzato al proprio sistema;

Ricevono istruzioni nel senso di:

- richiedere all'interessato di inoltrare via email o con altri sistemi di trasferimento da remoto i file necessari per l'esecuzione dell'incarico;
- evitare di utilizzare, ove possibile, chiavette USB portate da Terzi le quali possono essere potenziali veicoli di virus informatici ed altri malware; nel qual caso, il dispositivo mobile dell'Interessato ed i file che lo stesso contiene devono essere sempre integralmente scansionati con l'antivirus installato.

Se il controllo con antivirus del dispositivo mobile esterno dà esito positivo i soggetti autorizzati devono interrompere ogni operazione di download ed invitare l'Interessato a comunicare con altri mezzi i documenti; se il controllo dà, invece, esito negativo si può procedere ad aprire e scaricare il documento.

Art. 10 *quater*. Allontanamento ed abbandono della postazione lavorativa

Il collaboratore e/o il dipendente, se si allontanano per un periodo di tempo superiore a 20 (venti) minuti dalla postazione lavorativa, devono sempre verificare che il PC sia spento.
Nessun PC deve essere lasciato acceso alla conclusione della giornata e della settimana lavorativa.

Art. 11. La gestione corretta della posta elettronica, dei download e navigazione sicura su internet.

I collaboratori e dipendenti devono astenersi:

- dall'aprire email sospette inviate da soggetti sconosciuti ed aprire solamente link ed allegati che ritengono essere attendibili, verificando caso per caso l'attendibilità dei contenuti delle mail;

- dallo scaricare (download) e dall'installare programmi od applicazioni di cui non abbiano chiare le funzionalità, che non si conoscano oppure provenienti da mittente sconosciuto, sospetto o non identificabile;

- dal cliccare su vari ed eventuali *popup* aperti in sede di navigazione oppure contenuti nelle mail;

- dal navigare su siti web non attendibili ed, in generale, per motivi non attinenti allo svolgimento dell'incarico professionale;
- dall'aprire allegati che contengano estensioni di file del tipo EXE, BAT, VBS e SCR o file di word e excel provvisti di macro se provenienti da mittenti non conosciuti o sospetti, posto che queste estensioni sono vettori di virus/malware od infezioni di altro tipo. Gli allegati alle mail ed i download devono essere aperti solo laddove questi non siano sospetti e, comunque, unicamente nel caso in cui l'apertura di questi sia necessaria o funzionale a svolgere l'incarico lavorativo. In caso di allegato sospetto, occorre operare una scannerizzazione dello stesso con il sistema antivirus e/o antimalware.

Si invitano i Soggetti interessati a:

- diffidare delle mail HTML, soprattutto se provenienti da mittenti non identificabili, sconosciuti e/o sospetti;
- disabilitare l'apertura automatica delle mail, anche solo come visualizzazione di anteprima onde evitare l'attivazione automatica di script all'interno della mail stessa;
- accedere alle mail tramite web browser;
- disabilitare i cookie traccianti di terze parti dal browser internet.

Si invitano i Collaboratori ad:

- utilizzare Web Browser (Google Chrome, Mozzilla Firefox, Opera)e *Client* di posta affidabili (Mozzilla Thunderbird e Microsoft Outlook).

- inserire in calce alla mail professionale specifiche formule privacy dove viene specificato che l'interessato acconsente ed autorizza al trattamento dei propri dati personali.

Art. 12. *Data Breach* ed altre problematiche nell'ambito delle attività di trattamento ed altri eventi rischiosi.

Art. 12.1 *Data Breach*

Il Collaboratore e/o il dipendente hanno l'obbligo, in caso di avvenuta violazione dei dati personali:

- di riferire immediatamente al Titolare, al Referente Privacy oppure al Soggetto preposto alla compilazione del registro dei Data Breach l'avvenuta violazione

- di indicare ogni aspetto utile e descrittivo della violazione stessa, di cui sono venuti a conoscenza, necessario per la compilazione del Registro dei Data Breach

- di indicare ogni altro soggetto che sa essere a conoscenza di circostanze che riguardano l'avvenuta violazione.

<u>Art 12.2</u> Problematiche nell'ambito di attività di trattamento ed altri eventi rischiosi

Nel caso in cui vi siano dubbi sulla liceità dell'attività di trattamento o si ravvisino dubbi o difficoltà su come operare determinate attività di trattamento o su altri aspetti applicativi relativi all'implementazione ed all'attuazione di misure organizzative e di sicurezza fisiche o logiche (anche nell'ottica di prevenzione e corretta gestione di potenziali violazioni di dati personali/*data breach*) occorre riferirsi al Titolare, al Referente Data Protection o ad altro soggetto Indicato nell'organigramma aziendale, per chiedere ogni chiarimento od istruzione operativa necessaria.

Il Titolare, potrà, una volta valutata la gravità e le conseguenze della violazione, valutare se riferirsi ad un Consulente e se comunicare la violazione al Garante della Privacy ed agli Interessati che l'hanno subita.

<u>Art. 13</u>. L'obbligo di formazione ed aggiornamento dei collaboratori e dipendenti

I dipendenti e/o collaboratori dell'Ente hanno l'obbligo di formarsi ed aggiornarsi periodicamente in materia di privacy e data protection e sulle misure di sicurezza, nei termini e nei modi stabiliti ed indicati dal Titolare del trattamento, secondo le necessità operative individuate.

<u>Art. 14.</u> Il divieto dei collaboratori e dipendenti di continuare a trattare dati personali all'esito della risoluzione del rapporto di lavoro con il titolare.

All'esito della risoluzione del rapporto di collaborazione con il Titolare è fatto divieto al Collaboratore e al Dipendente di continuare a trattare, per Suo conto o per conto di Terzi, i dati personali dei quali è venuto a conoscenza sotto l'autorità del Titolare del Trattamento.

Nel caso in cui il Collaboratore ed il dipendente abbiano ricevuto dispositivi e device mobili da parte del Titolare questi vanno restituiti nella loro integrità senza che alcun documento in essi contenuto sia cancellato, alterato o trasferito.

Il collaboratore ed il dipendente su ordine del Titolare possono provvedere a cancellare attraverso sistemi di cancellazione sicura e nei modi indicati dal Titolare i dati trattati per conto di questi e sotto la Sua autorità.

Il Collaboratore e/o dipendenti firmano, all'esito della conclusione del rapporto di lavoro, un verbale dove dichiara l'avvenuta restituzione del dispositivo elettronico nonché l'avvenuta cancellazione sicura dei dati su dispositivi in Suo possesso.

<u>Art. 15</u>. Rilascio di copia e pubblicazione.

Del presente documento è rilasciata copia ad ogni dipendente e collaboratore che tratta dati personali sotto l'autorità del Titolare del trattamento.
Il Titolare è, altresì, disponibile a fornire ogni chiarimento necessario e/o opportuno richiesto dal soggetto autorizzato ed a rilasciare ulteriori copie al soggetto autorizzato che ne faccia richiesta.

Il presente documento, ed ogni successivo aggiornamento e/o integrazione dello stesso, è pubblicato ed esposto all'interno degli spazi e aziendali[1] attraverso affissione in un luogo accessibile a tutti i dipendenti e collaboratori e con modalità tali da renderlo ben visibile.

<u>Art. 16</u>. Integrazione ed aggiornamento del presente documento.

Il presente documento è, altresì, integrato da altri disciplinari speciali adottati dal Titolare per il trattamento di particolari categorie di dati, per particolari trattamenti o effettuati con particolari strumenti i quali integrano e prevalgono, in caso di conflitto, sulle diposizioni in questa sede convenute.
Ogni aggiornamento ed integrazione al presente documento viene letta e comunicata a tutti i collaboratori e dipendenti, che ne riceveranno altresì copia.

Il Titolare delle attività di trattamento

I Soggetti Autorizzati ed Istruiti dal Titolare del trattamento dichiarano che il contenuto del presente documento e delle relative istruzioni è stato etto, compreso integralmente ed in ogni sua parte e di averne ricevuto copia.

NOME	**COGNOME**	**FIRMA**
----------	----------	----------
----------	----------	----------
----------	----------	----------
----------	----------	----------
----------	----------	----------
----------	----------	----------
----------	----------	----------
----------	----------	----------
----------	----------	----------
----------	----------	----------