Allegato "A"

ISTRUZIONI E MISURE DI SICUREZZA SULLE MODALITÀ A CUI L'INCARICATO DEVE ATTENERSI NEL TRATTAMENTO DEI DATI PERSONALI

ISTRUZIONI

1. Trattare i dati esclusivamente per lo svolgimento delle mansioni e dei compiti assegnati.
2. Laddove sia compito dell'Incaricato raccogliere i dati presso l'interessato, consegnare o mostrare o trasmettere all'Interessato, all'atto della raccolta dei dati o, se raccolti presso terzi, all'atto della prima registrazione, l'informativa ai sensi dell'art. 13 comma 2 GDPR, salvo diverse indicazioni del Titolare/Responsabile.
3. Laddove sia compito dell'Incaricato acquisire il consenso dell'Interessato nei casi previsti dall'art. 7, 8, 9 e 10 GDPR, far sottoscrivere l'autorizzazione/consenso previa lettura e/o consegna dell'informativa, salvo diverse indicazioni del Titolare/Responsabile.
4. Trattare i dati nel rispetto dei principi e delle disposizioni di cui al Capo II del GDPR, ed in particolare:
   - trattare i dati in modo lecito, corretto e trasparente;
   - raccogliere i dati solo per le specifiche finalità del trattamento assegnato (principio di limitazione delle finalità);
   - assicurare che i dati siano adeguati, pertinenti e non eccedenti rispetto alle finalità (principio di minimizzazione dei dati)
   - assicurare che i dati siano esatti e se necessario aggiornati (principio di esattezza dei dati), seguendo le eventuali ulteriori direttive del Titolare/Responsabile in ordine al loro aggiornamento;
   - conservare i dati per un periodo non superiore a quello necessario al raggiungimento delle finalità del trattamento (principio della limitazione della

conservazione), seguendo le eventuali ulteriori istruzioni del Titolare/Responsabile in ordine alla cancellazione o alla anonimizzazione;

5. Comunicare e diffondere i dati esclusivamente ai soggetti indicati dal Titolare/Responsabile, secondo le modalità stabilite nell'informativa e/o nel Registro dei Trattamenti.

6. Porre in essere tutte le attività e condotte dirette a garantire un'adeguata sicurezza dei dati, compresa la protezione da trattamenti non autorizzati o illeciti, e ad evitare la perdita, la distruzione o il danno accidentale (principio di integrità e riservatezza).

7. Inoltrare tempestivamente al Titolare o al Responsabile e al RPD le richieste degli interessati volte all'esercizio dei diritti previsti dagli artt. 15, 16, 17, 18, 20, 21 GDPR.

8. Dare immediata comunicazione al Titolare e al Responsabile e al RPD nel caso sospetti o riscontri un problema di sicurezza relativamente al trattamento dei dati personali.

9. Partecipare agli eventi formativi in materia di protezione dei dati personali.

10. Fornire collaborazione al Titolare e al Responsabile per consentire a questi di svolgere correttamente la propria attività di direzione e controllo sulle operazioni di trattamento;

11. Fornire collaborazione al Responsabile della Protezione Dati nell'adempimento dei suoi compiti;

12. Garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui è venuto a conoscenza;

13. Eseguire ogni altra istruzione che sia eventualmente impartita dal Titolare o dal Responsabile o dal RPD in occasioni specifiche.

MISURE DI SICUREZZA

In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario:

• controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro;

• restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato;

• conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate;

• non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Titolare/Responsabile interno, o situazioni di smart working (lavoro agile);

• laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro;

• qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili;

• custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente;

• prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni;

• richiedere autorizzazione al Titolare/Responsabile per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali.

In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario:

• utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una

sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password);

• custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Titolare/Responsabile in caso di smarrimento o sottrazione;

• modificare la password fornita al primo accesso, e poi ogni 3 mesi;

• adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate;

• mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi;

• non utilizzare le stesse credenziali (username e password) per l'accesso ai diversi servizi online (es. Posta elettronica del CISIS, Home banking, Posta elettronica personale, ecc.),

• conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati;

• curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Titolare/Responsabile le segnalazioni di aggiornamento ricevute;

• non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta;

• evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC o dispositivi (es. smartphone) di terzi collegati a Internet.