REPUBBLICA ITALIANA

REGIONE SICILIANA
ASSESSORATO REGIONALE DELLA SALUTE
UFFICIO SPECIALE COMUNICAZIONE PER LA SALUTE
Responsabile dott.ssa Daniela Segreto

Prot. 31 /USC del 28-01-2021

OGGETTO: Regolamento Europeo n. 679/2016 sulla protezione dei dati personali, GDPR (General Data Protection Regulation). Prime istruzioni operative per "Incaricati del Trattamento" e trasmissione modulistica per informativa ed acquisizione autorizzazione al trattamento dei dati.

A tutti i componenti dell'Ufficio Speciale "Comunicazione per la salute"
S E D E

E p.c. All'Assessore regionale della Salute
S E D E

Con la presente si fa riferimento al decreto legislativo 18 maggio 2018, n. 51 e al decreto legislativo 10 agosto 2018, n. 101, inerenti l'applicazione delle disposizioni di cui al Regolamento Europeo n. 679/2016 sulla protezione dei dati personali, GDPR (General Data Protection Regulation).

Con **Decreto del Presidente della Regione Siciliana n. 569/Gab del 12 giugno 2018 l'Ing. Sebastiano Lio** – Dirigente di Ruolo dell'Amministrazione regionale Siciliana – **è stato nominato "Responsabile della Protezione dei Dati"** nelle more dell'istituzione di una adeguata struttura organizzativa dedicata alla specifica funzione attribuita. Lo stesso, con note prot. n. 11 del 25 luglio 2018 e n. 12 del 26 luglio 2018, ha richiesto alcune prime informazioni utili alla definizione delle procedure e dei comportamenti da porre in essere.

Il "Responsabile della Protezione dei Dati", con le due note sopra citate, ha chiarito che ***"la figura del Responsabile del trattamento rimane immutata rispetto il Codice della Privacy e corrisponde a colui il quale tratta dati personali per conto del titolare del trattamento ed assiste il titolare mediante l'adozione di adeguate misure organizzative e tecniche per garantire la sicurezza ed assicurando che l'uso dei dati sia conforme alle norme vigenti ed alla finalità per cui***

sono stari raccolti: già in sede di attuazione del Codice della Privacy nell'amministrazione regionale i responsabili dei trattamenti vennero individuati nei dirigenti preposti ai dipartimenti, aree e servizi ed unità operative o a posizioni di collaborazione e coordinamento, nonché nei dirigenti preposti agli uffici speciali, agli uffici di diretta collaborazione ed alle dirette dipendenze, in ragione degli incarichi loro conferiti e dei trattamenti effettuati".

Inoltre il "Responsabile della Protezione dei Dati" ha chiarito che per effetto del Decreto del Presidente della Regione Siciliana n. 569/Gab del 12 giugno 2018, con la individuazione e nomina del Responsabile, in capo allo stesso sussiste ***"il compito di informare e fornire consulenza ai titolari e ai responsabili, sorvegliare l'osservanza del regolamento, fornire pareri sulle valutazioni di impatto di cui all'art. 35 del Regolamento, cooperare con l'Autorità di controllo e fungere da punto di contatto per quest'ultima. Per tali motivi lo stesso svolge le proprie funzioni in autonomia ed indipendenza, senza ricevere istruzioni e in collaborazione diretta con il vertice gerarchico del titolare".***

Orbene, nelle more che il "Responsabile della Protezione dei Dati" fornisca le necessarie istruzioni, nonché il fondamentale ausilio informativo e di consulenza, necessari all'avvio e definizione:

- delle procedure di Audit e Analisi dei rischio, quale prima fase verso la compliance al GDPR;
- delle misure per l'adeguamento del Sistema;
- degli strumenti e programma di Controllo, monitoraggio e risk management;

così come previsto dalla norma, occorre comunque dare attuazione ad una serie di adempimenti minimi che consentano di dare evidenza del fatto che sono state diramate delle prime direttive e adottate sufficienti misure, nonché posti in essere i connessi comportamenti, rispettosi delle disposizioni normative vigenti.

Con **D.A. n. 955 del 15/10/2020** la scrivente Dott.ssa Daniela Segreto è stata designata **"Responsabile del trattamento dei dati"** per l'Ufficio Speciale "Comunicazione per la Salute".

Il Responsabile del trattamento dei dati è chiamato, in ragione del ruolo, a collaborare direttamente, e per il tramite del personale appartenente al comparto assegnato all'Ufficio, al pieno raggiungimento degli obiettivi normativi in materia di privacy, vigilando sul rispetto delle regole in materia.

Tutti i componenti dell'Ufficio Speciale, qualunque sia il ruolo e la mansione ricoperta, sono **"Incaricati dei Trattamenti"** limitatamente alle pratiche di propria competenza, ed hanno l'onere di raccordarsi con il Responsabile del trattamento dei dati supportandolo nell'esercizio delle funzioni; pertanto sono onerati di osservare scrupolosamente le brevi indicazioni che seguono.

Al fine di procedere nella direzione del miglioramento continuo del processo di che trattasi, si rimettono quindi alcune informazioni propedeutiche ritenute utili per potere nel prosieguo definire compiutamente gli adempimenti da porre in essere.

1.0 DEFINIZIONI

Secondo l'articolo 4 del Regolamento (Ue) 2016/679 (GDPR), si definisce:

- **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;
- **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;
- **Violazione dei dati personali** - la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

2.0 ADEMPIMENTI

Ciascun incaricato del trattamento deve:

- **rispettare i principi generali del Regolamento** (Ue) 2016/679 (GDPR) con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi;
- **rispettare l'obbligo di riservatezza e segretezza** e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;
- **utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione** delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti aziendali;
- **rispettare le misure di sicurezza** idonee adottate dall'ufficio, atte a salvaguardare la riservatezza e l'integrità dei dati;
- **segnalare eventuali malfunzionamenti di strumenti elettronici**, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;

- **accedere ai dati strettamente necessari all'esercizio** delle proprie funzioni e competenze;
- in caso di interruzione del lavoro, anche temporanea, **verificare che i dati trattati non siano accessibili a terzi non autorizzati;**
- **mantenere riservate le proprie credenziali di autenticazione;**
- **svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati;** non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- **rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;**
- **informare il responsabile in caso di incidente di sicurezza** che coinvolga dati particolari e non;
- **raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli** di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- **eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni** e nel rispetto delle norme di legge.

3.0 MODALITÀ DI SVOLGIMENTO DELLE OPERAZIONI

Le principali operazioni degli incaricati del trattamento, sono:

- **l'Identificazione dell'interessato** - al momento della raccolta dei dati personali, qualora sia necessario individuare l'identità del soggetto che fornisce le informazioni, è obbligatorio richiedere un documento di identità o di riconoscimento, al fine di verificare la identità e di procedere correttamente alla raccolta e alla registrazione delle informazioni;
- **verifica del controllo dell'esattezza del dato e della corretta digitazione** - al momento della registrazione dei dati raccolti, occorre prestare attenzione alla digitazione e all'inserimento dei dati identificativi e degli altri dati riferiti all'interessato, al fine di evitare errori, che potrebbero generare problemi nella corretta gestione dell'anagrafica e nello svolgimento delle operazioni, che caratterizzano il processo di trattamento;
- **norme logistiche per l'accesso fisico ai locali** - i locali ove sono custoditi i dati personali (ed in particolare quelli di natura sensibile) devono essere soggetti a controllo e a verifica, al fine di evitare che durante l'orario di lavoro possano essere conosciuti o accessibili da parte di soggetti non autorizzati. Si raccomanda, in caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, di adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'organizzazione di appartenenza. Laddove si esegue il trattamento di Dati Personali, deve essere possibile ricoverare in luogo sicuro i documenti cartacei ed i supporti rimovibili contenenti tali dati. Pertanto le porte degli uffici ed almeno un armadio per ufficio devono essere dotati di serratura con chiave. Al termine dell'orario lavorativo, ove la

dinamica delle attività ed il numero di occupanti lo consentano, è necessario chiudere sempre a chiave gli uffici nei quali vengono svolti trattamenti di Dati Personali.

- rilevazione presenze - ogni Incaricato è tenuto ad utilizzare sempre i sistemi di rilevazione presenze disponibili, allo scopo di segnalare la propria presenza e legittimare le attività in corso di svolgimento. In caso di assenza deve sempre avere le necessarie autorizzazioni all'allontanamento e deve assicurare, prima di lasciare la propria postazione, di avere adottato tutti gli accorgimenti e comportamenti che precedono.

4.0 ISTRUZIONI PER L'USO DEGLI STRUMENTI INFORMATICI

Come principio di carattere generale, sia i dispositivi di memorizzazione del proprio PC che le unità di rete, devono contenere informazioni strettamente professionali e non possono essere utilizzate per scopi diversi (immagini, video e documenti personali).

Di seguito sono riportate le indicazioni per la gestione dei diversi strumenti informatici per il trattamento dati:

- Gestione strumenti elettronici (pc fissi e portatili) - Ciascun incaricato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card). Si devono adottare le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei all'organizzazione o non specificamente autorizzati.

Per la gestione della sessione di lavoro sul pc (fisso e portatile), è necessario che:

- al termine delle ore di servizio, il PC deve essere spento, a meno che non stia svolgendo elaborazioni particolari. In tal caso gli uffici debbono tassativamente essere chiusi a chiave;
- Se l'incaricato si assenta momentaneamente dalla propria postazione deve accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone. Pertanto deve chiudere la sessione di lavoro sul PC facendo Logout, oppure in alternativa deve avere attivo un salvaschermo (screen- saver) protetto dalle credenziali di autenticazione;
- Relativamente all'utilizzo dello screen-saver, occorre osservare le seguenti norme:

- Non deve mai essere disattivato;
- Il suo avvio automatico deve essere previsto non oltre i primi 10 minuti di inattività del PC;
- Deve essere messo in funzione manualmente ogni volta che si lascia il PC incustodito ed acceso;

- Quando si esegue la stampa di un documento contenente dati personali, in particolare su una stampante condivisa, occorre ritirare tempestivamente i documenti stampati per evitare l'accesso a soggetti non abilitati al trattamento.

Per l'utilizzo dei PC portatili valgono le regole elencate per i PC connessi alla rete, con le seguenti ulteriori raccomandazioni:

- prima della riconsegna, rimuovere eventuali file ivi elaborati;
- quando il PC portatile è nei locali dell'Ufficio, non lasciarlo mai incustodito; in caso di brevi assenze assicurarlo alla scrivania o ad elementi "sicuri" dell'arredamento (maniglie, intelaiature…) utilizzando gli appositi cavi in acciaio dotati di lucchetto;
- quando il PC portatile è all'esterno dell'Ufficio, evitare di lasciarlo incustodito;
- per assenze prolungate, anche qualora l'ambiente venga ritenuto "affidabile", è necessario custodire il portatile in modo opportuno;
- in caso di furto di un portatile è necessario avvertire tempestivamente il responsabile dell'Ufficio da cui dipende ed il Servizio Informatico, onde prevenire possibili intrusioni ai sistemi aziendali;
- eseguire periodicamente salvataggi dei dati e non tenere tali backup insieme al PC portatile.

- Gestione username e password - L'accesso al PC, sia esso collegato in rete o meno, è protetto da un sistema di autenticazione che richiede all'Incaricato di inserire sulla videata di accesso all'elaboratore un codice utente (username) ed una parola chiave (password). L'adozione ed il corretto utilizzo della combinazione username/password è fondamentale per il corretto utilizzo del PC, in quanto:

- tutela l'utilizzatore ed in generale l'ufficio da accessi illeciti, atti di vandalismo e, in generale, violazioni e danneggiamenti del proprio patrimonio informativo;
- tutela l'Incaricato da false imputazioni, garantendo che nessuno possa operare a suo nome e che, con il suo profilo (ossia con le sue user id e password) solo lui possa svolgere determinate azioni;
- è necessario per gestire correttamente gli accessi a risorse condivise.

Ciascun incaricato deve scegliere le password in base ai seguenti criteri:

- devono essere lunghe almeno otto caratteri;
- non devono fare riferimento ad informazioni agevolmente riconducibili ai soggetti utilizzatori o ai loro famigliari;
- devono contenere una combinazione di numeri e/o segni speciali, lettere, maiuscole e minuscole;
- non deve essere uguali alle precedenti.

Per la corretta gestione della password è necessario:

- Almeno ogni 3 mesi è obbligatorio cambiare la password;
- Ogni password ricevuta va modificata al primo utilizzo;
- La password venga conservata in un luogo sicuro;

• Non rivelare o condividere la password con i colleghi di lavoro, famigliari e amici, soprattutto attraverso il telefono;

• Non utilizzare la funzione, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni.

- **Installazione di hardware e software** - L'installazione di hardware e software, nonché la modifica dei parametri di configurazione, possono essere eseguiti solamente dalle persone del Servizio Informatico all'uopo preposto, su mandato del Responsabile del trattamento per i Sistemi Elettronici. Pertanto si raccomanda agli utenti dei PC di rispettare i seguenti divieti:

• Non utilizzare sul PC dispositivi hardware personali, o comunque non autorizzati dall'amministrazione regionale;

• Non installare sistemi per connessione esterne (es : modem, wifi); tali connessioni, aggirando i sistemi preposti alla sicurezza della rete regionale, aumentano sensibilmente i rischi di intrusioni e di attacchi dall'esterno;

• Non installare programmi, anche in versione demo. In particolare, è vietata l'installazione di giochi, programmi in prova (shareware), programmi gratuiti (freeware), programmi pirata, e in generale tutti i software non autorizzati dal Servizio Informatico;

• Non modificare i parametri di configurazione del proprio PC senza espressa autorizzazione e senza il supporto di personale tecnico qualificato.

Si ricorda che normalmente la condivisione di aree e di risorse del proprio PC è vietata. Può essere autorizzata dal Servizio Informatico, solo in casi eccezionali e solo per il tempo strettamente necessario allo svolgimento delle attività di lavoro. In questi casi devono essere adottate password di lettura e scrittura e la condivisione deve operare solo su singole directory del PC, e non sull'intero disco rigido.

- **Gestione posta elettronica regionale** - Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità dell'Uffico e in stretta connessione con l'effettiva attività e mansioni del lavoratore che utilizza tale funzionalità.

Al fine di non compromettere la sicurezza dell'Ufficio e di prevenire conseguenze legali a carico della stessa, bisogna adottare le seguenti norme comportamentali:

• Se si ricevono mail da destinatari non identificabili contenenti file di qualsiasi tipo, procedere alla loro immediata eliminazione;

• È fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione;

• La casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione.

Nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di dati particolari (ex dati sensibili), si raccomanda di prestare attenzione a che:

- l'indirizzo del destinatario sia stato correttamente digitato,
- l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;
- nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio.

- **Gestione del salvataggio dei dati** - Per i dati ed i documenti che risiedono sui server gestiti centralmente, come ad esempio cartelle di rete e database, il Servizio Informatico esegue i salvataggi con la possibilità di ripristinare in toto oppure selettivamente eventuali files distrutti, ad esempio per guasti hardware oppure per cancellazioni involontarie. Per i dati ed i documenti che risiedono esclusivamente sul PC, ogni Incaricato deve eseguire almeno una volta alla settimana la copia (salvataggio, o backup). Questo allo scopo di garantire la disponibilità ed il ripristino dei Dati Personali nel caso di una generica compromissione delle risorse (cancellazioni accidentali, guasti, furti...). L'Incaricato deve verificare che i supporti informatici utilizzati per il backup, che normalmente sono dischi magnetici esterni, CD, DVD oppure flash disks (chiavette) siano funzionali e non corrotti.

- **Gestione dei supporti rimovibili** - I supporti rimovibili, come ad esempio dischi magnetici esterni, penne USB o CD riscrivibili, quando contengono dati personali devono essere custoditi in luogo protetto e non accessibile (armadio e cassetti chiusi a chiave, etc.). Quando non sono più utilizzati devono essere formattati prima della consegna e se non più utilizzabili devono essere distrutti. Il trasferimento di file contenenti dati personali, dati particolari (ex dati sensibili) o giudiziari su supporti rimovibili, è da eseguire unicamente in via transitoria, ponendo la massima attenzione alla destinazione di trasferimento e cancellando i file appena possibile. I dati particolari (ex dati sensibili) o giudiziari devono essere crittografati.

- **Gestione protezione dai virus informatici** - Per prevenire eventuali danneggiamenti al software causati dalla presenza o dall'azione di programmi virus informatici, su ogni elaboratore dell'Ufficio dovrebbe essere installato un software antivirus che si aggiorna automaticamente all'ultima versione disponibile. Competenza demandata alle apposite strutture dipartimentali.

L'antivirus non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito. Nel caso il programma antivirus installato sul proprio PC riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus è necessario darne immediata segnalazione al responsabile del Servizio Informatico. Si raccomanda di non scaricare, né tantomeno aprire, file provenienti via e-mail da mittenti sconosciuti. Tali file possono essere

portatori di virus e compromettere la funzionalità del PC, l'integrità dei dati in essa contenuti e soprattutto l'integrità dei sistemi collegati al PC stesso.

- Distruzione delle copie cartacee - Coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzano strumenti per la riproduzione cartacea di documenti digitali, sono tenuti a procedere alla relativa distruzione del supporto, qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli, salva l'ipotesi di uso esclusivamente personale per eventuali appunti o brutte copie, da distruggere immediatamente quando non più necessarie;

- Misure di sicurezza - Il trattamento sicuro di documenti contenenti Dati Personali richiede la presenza di misure di sicurezza con le quali l'Incaricato possa interagire ed una serie di accorgimenti direttamente gestibili dall'Incaricato stesso. In particolare, si richiede:

- la presenza e l'uso tassativo di armadi e cassetti dotati di serratura adeguata;
- la presenza e l'uso tassativo, ove si richieda la distruzione di documenti contenenti dati particolari (ex dati sensibili) o giudiziari, di un tritadocumenti.

Alla luce di tutto quanto precede, tenuto conto delle prime informazioni rese disponibili, si rimettono di seguito delle istruzioni operative basilari affinché gli *"Incaricati del trattamento"*, così come sopra individuati, pongano in essere comportamenti "virtuosi" rispettosi della normativa in argomento, attenendosi in particolare alle seguenti prescrizioni:

- in nessun caso è concesso l'accesso a documentazione contenente Dati Personali per motivi non dettati da esigenze di lavoro strettamente connesse ai trattamenti dichiarati, autorizzati e tutelati dal Titolare;
- la documentazione contenente Dati Personali che, per ragioni di praticità operativa, risiede sulle scrivanie degli Incaricati, deve comunque essere rimossa al termine dell'orario di lavoro;
- l'accesso ai documenti contenenti Dati Personali deve essere limitato al tempo necessario a svolgere i Trattamenti previsti;
- i documenti contenenti Dati Personali non devono essere lasciati incustoditi in un ambiente non controllato (ad es. a seguito della stampa, i documenti non devono essere abbandonati nella stampante di rete);
- il numero di copie di documenti contenenti Dati Personali deve essere strettamente funzionale alle esigenze di lavoro;
- cassetti ed armadi contenenti documentazione riservata debbono tassativamente essere chiusi a chiave fuori dell'orario di lavoro;
- l'accesso a documenti contenti Dati particolari (ex dati sensibili) o giudiziari può avvenire esclusivamente da parte di personale incaricato o autorizzato per specifiche esigenze di ufficio;

• la distruzione di documenti contenenti Dati Personali deve essere operata, ove possibile, direttamente dal personale Incaricato;

• ove non siano disponibili strumenti per la distruzione dei documenti (trita documenti), il personale Incaricato ha l'onere di ridurre il documento in condizioni da essere illegibbile;

• quando gli atti e i documenti contenenti dati personali, dati particolari (ex dati sensibili) o giudiziari sono affidati agli Incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli Incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate (fascicolati e pronti per l'archiviazione);

• l'accesso agli archivi contenenti dati particolari (ex dati sensibili) o giudiziari deve essere controllato.

• è severamente vietato utilizzare documenti contenenti Dati personali, dati particolari (ex dati sensibili) o giudiziari come carta da riciclo o da appunti.

Inoltre, per perfezionare la procedura di tracciabilità occorrerà adottare un registro informatico ricorrendo all'ausilio del **Format Excel** reso disponibile dal Dipartimento regionale della Funzione Pubblica, che verrà aggiornato periodicamente ed inviato al Dipartimento Funzione Pubblica.

Tra tutti gli adempimenti da porre in essere, un ruolo centrale riveste la somministrazione agli interessati dell'informativa sul trattamento dei dati, e l'acquisizione da parte di questi dell'autorizzazione al trattamento dei dati, secondo l'informativa sottoposta.

Al riguardo, si trasmettono in allegato due modelli di informativa (mod. 1 – lavoratori dipendenti, collaboratori, consulenti ed esperti, e mod. 2 – utenti), finalizzati a rendere note le modalità di trattamento dati ed all'acquisizione dell'autorizzazione al trattamento, da sottoporre e fare firmare alle due categorie di soggetti interessati, in ragione delle peculiarità delle attività poste in essere dall'Ufficio Speciale "Comunicazione per la Salute".

Ogni Informativa, compilata e sottoscritta dagli interessati, dovrà costituire corredo delle pratiche poste in capo ai dipendenti inquadrati presso l'Ufficio Speciale "Comunicazione per la Salute" in quanto Incaricati del trattamento, e limitatamente al rispettivo carico di lavoro. Si raccomanda la puntuale osservanza della presente direttiva.

Si rammenta infine che il Titolare del trattamento ed il Responsabile del trattamento sono esonerati dalla responsabilità del mancato o non corretto trattamento dei dati, se dimostrano che l'evento dannoso non gli è imputabile in alcun modo. Si sollecita pertanto l'osservanza puntuale delle istruzioni impartite.

Per tutto quanto precede, nei primi giorni del mese di febbraio 2021 è indetta una riunione operativa, la cui data sarà convenuta nel prosieguo, a cui dovranno prendere parte **tutti i**

componenti dell'Ufficio al fine di fornire eventuali chiarimenti, raccogliere suggerimenti, acquisire le informazioni richieste già disponibili, e concordando sui successivi comportamenti e procedure da porre in essere, in raccordo, per assicurare il rispetto del Regolamento Europeo n. 679/2016 sulla protezione dei dati personali.

Ufficio Speciale
"Comunicazione per la Salute"
Dott.ssa Daniela Segreto

REPUBBLICA ITALIANA

REGIONE SICILIANA
ASSESSORATO REGIONALE DELLA SALUTE
UFFICIO SPECIALE COMUNICAZIONE PER LA SALUTE
Responsabile dott.ssa Daniela Segreto

Mod. 1

INFORMATIVA PER IL TRATTAMENTO DEI DATI PERSONALI E PARTICOLARI DI LAVORATORI DIPENDENTI, COLLABORATORI, CONSULENTI, ESPERTI

I dati personali dei Dipendenti, Collaboratori, Consulenti, Esperti, sono utilizzati **dall'Ufficio Speciale "Comunicazione per la Salute"**, che è titolare per il trattamento, nel rispetto dei principi di protezione dei dati personali stabiliti dal Regolamento GDPR 2016/679.

MODALITÀ E FINALITÀ DEL TRATTAMENTO DATI

1) La informiamo che i dati a vario titolo forniti verranno trattati con il supporto dei seguenti mezzi:

   a) Cartacei (contratto, moduli di dichiarazione, autocertificazioni, ecc.);
   b) Informatici (software gestionali, contabili, ecc.);
   c) Telematici;

   - per l'inquadramento e/o la contrattualizzazione dei dipendenti/dirigenti interni all'amministrazione, per l'eventuale assunzione di esterni, per il conferimento di incarico a Consulenti ed Esperti;
   - per l'adempimento degli obblighi legali e contrattuali, anche collettivi, connessi al rapporto di lavoro;
   - per la rilevazione delle presenze e l'elaborazione dei dati necessari ai fini del pagamento della retribuzione;

L'eventuale rifiuto nel consentire il trattamento dei dati comporta l'impossibilità di usufruire del servizio richiesto dall'utente. Fatto salvo esplicito diniego da parte dell'interessato, i dati dell'utente saranno trattati per le seguenti finalità:

- l'inquadramento e/o la contrattualizzazione dei dipendenti/dirigenti interni all'amministrazione, per l'eventuale assunzione di esterni, per il conferimento di incarico a Consulenti ed Esperti;

Accetta		Non accetta	

- adempimento degli obblighi legali e contrattuali, anche collettivi, connessi al rapporto di lavoro;

Accetta		Non accetta	

- per la rilevazione delle presenze e l'elaborazione dei dati necessari ai fini del pagamento della retribuzione;

Accetta		Non accetta	

BASE GIURIDICA

2) Il conferimento dei dati è obbligatorio per tutto quanto è richiesto dagli obblighi legali e contrattuali e pertanto l'eventuale rifiuto a fornirli in tutto o in parte può dar luogo all'impossibilità di dare esecuzione al contratto o di svolgere correttamente tutti gli adempimenti, connessi al rapporto di lavoro da instaurarsi.

CATEGORIE DI DESTINATARI

3) Ferme restando le comunicazioni eseguite in adempimento di obblighi di legge e contrattuali, tutti i dati raccolti ed elaborati potranno essere comunicati esclusivamente per le finalità sopra specificate a:

   - Enti pubblici (Dipartimenti regionali, Ragioneria Centrale, Corte dei Conti, INPS, INAIL, Direzione provinciale del lavoro, Uffici fiscali, ISTAT, ect.);
   - Enti ed organismi di controllo e vigilanza;

- Fondi o casse di previdenza e assistenza;
- ASL e/o Studi medici in adempimento degli obblighi in materia di igiene e sicurezza del lavoro;
- Società e/o Enti di assicurazioni, ove previsto e/o richiesto dal lavoratore;
- Istituti di credito, Finanziarie ed altri organismi legittimati alla concessione del credito, in ragione di specifiche richieste dei dipendenti, collaboratori, esperti;
- Organizzazioni sindacali cui è stato conferito specifico mandato.

Nella gestione dei dati, inoltre, possono venire a conoscenza degli stessi le seguenti categorie di persone autorizzate e/o responsabili interni ed esterni individuati per iscritto ed ai quali sono state fornite specifiche istruzioni scritte circa il trattamento dei dati:

- Dipendenti regionali per l'espletamento delle pratiche inerenti la gestione del personale, per la contabilità, per la predisposizione delle Buste Paga, per la liquidazione degli emolumenti;
- Dipendenti di Enti ed Organismi terzi che per conto della Regione Siciliana gestiscono alcuni aspetti operativi inerenti la gestione dei rapporti contrattuali;

In relazione al rapporto di lavoro, l'**Ufficio Speciale "Comunicazione per la Salute"** potrà trattare dati che la legge definisce "particolari" in quanto idonei a rilevare ad esempio:

a) lo stato generale di salute (assenze per malattia, maternità, infortunio, ect.) idoneità o meno a determinate mansioni (quale esito espresso da personale medico a seguito di visite mediche preventive/periodiche o richieste da Lei stesso/a);
b) l'adesione ad un sindacato (assunzione di cariche e/o richiesta di trattenute per quote di associazione sindacale);
c) la titolarità di cariche pubbliche elettive (permessi od aspettativa), convinzioni religiose (festività religiose fruibili per legge), preferenze sessuali, ect.;
d) dati, informazioni ed esperienze personali riguardanti il curriculum vitae e studiorum del lavoratore;

I dati di natura particolare, concernenti lo stato di salute, che tratta il medico competente nell'espletamento dei compiti previsti dal D.Lgs. 81/08 e dalle altre disposizioni in materia di salute e sicurezza sui luoghi di lavoro, per l'effettuazione degli accertamenti medici preventivi e periodici, verranno trattati dallo stesso medico quale autonomo titolare/responsabile del trattamento, per il quale l'Amministrazione regionale chiede espresso consenso.

PERIODO DI UTILIZZAZIONE E CONSERVAZIONE

4) Tutti i dati predetti e gli altri costituenti lo stato di servizio verranno conservati anche dopo la cessazione del rapporto di lavoro per l'espletamento di tutti gli eventuali adempimenti connessi o derivanti dalla conclusione del rapporto di lavoro stesso.

DIRITTI DELL'INTERESSATO

5) Ai sensi del Regolamento europeo 679/2016 (GDPR) e della normativa nazionale, l'interessato può, secondo le modalità e nei limiti previsti dalla vigente normativa, esercitare i seguenti diritti:
   - richiedere la conferma dell'esistenza di dati personali che lo riguardano (diritto di accesso);
   - conoscerne l'origine;
   - riceverne comunicazione intelligibile;
   - avere informazioni circa la logica, le modalità e le finalità del trattamento;
   - richiederne l'aggiornamento, la rettifica, l'integrazione, la cancellazione, la trasformazione in forma anonima, il blocco dei dati trattati in violazione di legge, ivi compresi quelli non più necessari al perseguimento degli scopi per i quali sono stati raccolti;
   - nei casi di trattamento basato su consenso, ricevere i propri dati forniti al titolare, in forma strutturata e leggibile da un elaboratore di dati e in un formato comunemente usato da un dispositivo elettronico;
   - il diritto di presentare un reclamo all'Autorità di controllo.

   Le richieste vanno rivolte al Titolare del trattamento.

INFORMATIVA SUI SISTEMI DI VIDEOSORVEGLIANZA

6) L'Amministrazione regionale potrebbe utilizzare sistemi di videosorveglianza degli accessi, al solo fine di garantire la sicurezza ed il patrimonio regionale e per prevenire atti illeciti.
Le eventuali immagini riprese dalle telecamere saranno acquisiste, trattate e conservate, esclusivamente secondo le modalità ed i termini previsti dalla normativa vigente, e rese disponibili nel caso in cui si debba aderire a specifica richiesta investigativa e dell'Autorità Giudiziaria o di Polizia Giudiziaria.
Le immagini saranno consultabili solo dal personale incaricato e/o dall'autorità giudiziaria o di polizia.

TITOLARE, RESPONSABILE E SUB- RESPONSABILE DEL TRATTAMENTO

7) Il Titolare del trattamento dei Suoi dati personali è l'Assessore regionale pro tempore della Salute, il Responsabile del Trattamento dei dati è il Dirigente Responsabile dell'Ufficio Speciale "Comunicazione per la Salute" – con uffici in Via Mario Vaccaro n. 5 – 90145 Palermo - Recapiti telefonici: 091 /7079380-7079276
   mail: *ufficiocomunicazione.salute@regione.sicilia.it*
   pec*: ufficiocomunicazione.salute@certmail.regione.sicilia.it;*

8) Il Presidente della Regione Siciliana ha nominato quale DPO (Data Protection Officer) Responsabile della Protezione dei dati della Regione Siciliana l'Ing. Sebastiano Lio (DP 569/Gab del 12/06/2018)
mail : dpo@certmail.regione.sicilia.it;

La presente privacy policy può subire modifiche nel tempo – anche connesse all'eventuale entrata in vigore di nuove normative di settore, all'aggiornamento o erogazione di nuovi servizi ovvero ad intervenute innovazioni tecnologiche

AUTORIZZAZIONE

Il/la sottoscritto/a _____ nato/a a _____ il _____, in relazione a tutto quanto precede, autorizza l'Ufficio Speciale "Comunicazione per la Salute" – Via Mario Vaccaro n. 5 – 90145 Palermo – al trattamento dei dati forniti inerenti le finalità sopra meglio specificate.

Palermo lì _____

Per autorizzazione al trattamento

_____

(allegare copia documento d'identità
in corso di validità)

Il Funzionario che riceve il presente consenso al trattamento

_____

REPUBBLICA ITALIANA

REGIONE SICILIANA
ASSESSORATO REGIONALE DELLA SALUTE
UFFICIO SPECIALE COMUNICAZIONE PER LA SALUTE
Responsabile dott.ssa Daniela Segreto

Mod. 2

INFORMATIVA PER IL TRATTAMENTO DEI DATI PERSONALI

DEGLI UTENTI

I dati personali dell'utente sono utilizzati **dall'Ufficio Speciale "Comunicazione per la Salute"**, che è titolare per il trattamento, nel rispetto dei principi di protezione dei dati personali stabiliti dal Regolamento GDPR 2016/679.

MODALITÀ E FINALITÀ DEL TRATTAMENTO DATI

1) La informiamo che i dati a vario titolo forniti verranno trattati con il supporto dei seguenti mezzi:
   a) Cartacei (moduli di registrazione, istanze di accesso ad atti e documenti, richieste di finanziamenti e patrocini, ecc.);
   b) Informatici (software gestionali, contabili, ecc.);
   c) Telematici;

   con le seguenti finalità:
   - erogazione dei servizi richiesti dall'utente;
   - avvio e conclusione dell'iter istruttorio di competenza, di cui è parte l'utente;
   - fini amministrativi e contabili correlati alla richiesta dell'utente.

L'eventuale rifiuto nel consentire il trattamento dei dati comporta l'impossibilità di usufruire del servizio richiesto dall'utente. Fatto salvo esplicito diniego da parte dell'interessato, i dati dell'utente saranno trattati per le seguenti finalità:

- erogazione dei servizi richiesti dall'utente;

Accetta		Non accetta	

- avvio e conclusione dell'iter istruttorio di competenza, di cui è parte l'utente;

Accetta		Non accetta	

- fini amministrativi e contabili correlati alla richiesta dell'utente.

Accetta		Non accetta	

BASE GIURIDICA

2) Il conferimento dei dati, se necessario per le finalità, impone l'obbligatorietà dell'autorizzazione al consenso, e pertanto l'eventuale rifiuto a fornirla, in tutto o in parte, può dar luogo all'impossibilità di fornire i servizi richiesti.
   L'Ufficio tratta i dati degli utenti in base al consenso, ossia mediante l'approvazione esplicita della presente policy privacy e in relazione alle modalità e finalità di seguito descritte.

CATEGORIE DI DESTINATARI

3) Ferme restando le comunicazioni eseguite in adempimento di obblighi di legge, tutti i dati raccolti ed elaborati potranno essere comunicati, esclusivamente per le finalità sopra specificate, alle seguenti categorie di interessati:

   - Altri uffici dell'amministrazione regionale;
   - Uffici ed organismi di vigilanza e controllo;
   - Altri in ragione di specifici interessi tutelati per legge;

PERIODO DI UTILIZZAZIONE E CONSERVAZIONE

4) I dati forniti sono utilizzati per il tempo necessario allo svolgimento delle attività di competenza dell'ufficio e successivamente conservati, con il ricorso ai necessari ausili di sicurezza, per il periodo previsto dalla normativa di settore.

DIRITTI DELL'INTERESSATO

5) Ai sensi del Regolamento europeo 679/2016 (GDPR) e della normativa nazionale, l'interessato può, secondo le modalità e nei limiti previsti dalla vigente normativa, esercitare i seguenti diritti:
   - richiedere la conferma dell'esistenza di dati personali che lo riguardano (diritto di accesso);
   - conoscerne l'origine;
   - riceverne comunicazione intelligibile;
   - avere informazioni circa la logica, le modalità e le finalità del trattamento;
   - richiederne l'aggiornamento, la rettifica, l'integrazione, la cancellazione, la trasformazione in forma anonima, il blocco dei dati trattati in violazione di legge, ivi compresi quelli non più necessari al perseguimento degli scopi per i quali sono stati raccolti;
   - nei casi di trattamento basato su consenso, ricevere i propri dati forniti al titolare, in forma strutturata e leggibile da un elaboratore di dati e in un formato comunemente usato da un dispositivo elettronico;
   - il diritto di presentare un reclamo all'Autorità di controllo.

   Le richieste vanno rivolte al Titolare del trattamento.

INFORMATIVA SUI SISTEMI DI VIDEOSORVEGLIANZA

6) L"Amministrazione regionale potrebbe utilizzare sistemi di videosorveglianza degli accessi, al solo fine di garantire la sicurezza ed il patrimonio regionale e per prevenire atti illeciti.
Le eventuali immagini riprese dalle telecamere saranno acquisiste, trattate e conservate, esclusivamente secondo le modalità ed i termini previsti dalla normativa vigente, e rese disponibili nel caso in cui si debba aderire a specifica richiesta investigativa e dell'Autorità Giudiziaria o di Polizia Giudiziaria.
Le immagini saranno consultabili solo dal personale incaricato e/o dall'autorità giudiziaria o di polizia.

TITOLARE, RESPONSABILE E SUB- RESPONSABILE DEL TRATTAMENTO

7) Il Titolare del trattamento dei Suoi dati personali è l'Assessore regionale pro tempore della Salute, il Responsabile del Trattamento dei dati è il Dirigente Responsabile dell'Ufficio Speciale "Comunicazione per la Salute" – con uffici in Via Mario Vaccaro n. 5 – 90145 Palermo - Recapiti telefonici: 091/7079380-7079276
   mail*: ufficiocomunicazione.salute@regione.sicilia.it;*
   pec*: ufficiocomunicazione.salute@certmail.regione.sicilia.it;*

8) Il Presidente della Regione Siciliana ha nominato quale DPO (Data Protection Officer) Responsabile della Protezione dei dati della Regione Siciliana l'Ing. Sebastiano Lio (DP 569/Gab del 12/06/2018)
   mail : *dpo@certmail.regione.sicilia.it;*

La presente privacy policy può subire modifiche nel tempo – anche connesse all'eventuale entrata in vigore di nuove normative di settore, all'aggiornamento o erogazione di nuovi servizi ovvero ad intervenute innovazioni tecnologiche

AUTORIZZAZIONE

Il/la sottoscritto/a _____ nato/a a _____ il _____, in relazione a tutto quanto precede, autorizza l'Ufficio Speciale "Comunicazione per la Salute" – Via Mario Vaccaro n. 5 – 90145 Palermo – al trattamento dei dati forniti inerenti le finalità sopra meglio specificate.

Palermo lì _____

Per autorizzazione al trattamento

_____

(allegare copia documento d'identità
in corso di validità)

Il Funzionario che riceve il presente consenso al trattamento

_____