ISTITUTO NAZIONALE PER L'ASSICURAZIONE CONTRO GLI INFORTUNI SUL LAVORO

Direzione generale
Direzione centrale per l'organizzazione digitale

Circolare n. 19

Roma, 12 maggio 2020

Al Direttore generale vicario
Ai Responsabili di tutte le Strutture centrali e territoriali

e p.c. a: Organi istituzionali
Magistrato della Corte dei conti delegato all'esercizio del controllo
Organismo indipendente di valutazione della performance
Comitati consultivi provinciali

Oggetto

Designazione degli autorizzati al trattamento dei dati personali, relative istruzioni operative e contestuale pubblicazione della nuova versione dell'informativa per l'utilizzo di posta elettronica e internet da parte dei dipendenti.

Quadro normativo

- **Decreto legislativo 30 giugno 2003, n. 196:** "Codice in materia di protezione dei dati personali".
- **Provvedimento del Garante 1 marzo 2007** e successive modificazioni: "Lavoro: le linee guida del Garante per posta elettronica e internet".
- **Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio (GDPR)** 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.
- **Circolare Inail 23 febbraio 2018, n. 12:** "Codice disciplinare per il personale delle aree destinatario dei precedenti Ccnl del comparto Enti pubblici non economici".
- **Determinazione del Presidente Inail 22 marzo 2018, n. 149:** "Regolamento unico per la disciplina del diritto di accesso ai documenti amministrativi ai sensi degli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, e del diritto di accesso

a documenti, dati e informazioni ai sensi degli articoli 5 e seguenti del decreto legislativo 14 marzo 2013, n. 33".

- **Determinazione del Presidente Inail 22 maggio 2018, n. 234:** "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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)» - RGPD. Designazione del Responsabile della protezione dei dati personali (RPD) - art.37 Regolamento UE 2016/679".

- **Decreto legislativo 10 agosto 2018, n. 101:** "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni 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, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)".

- **Determinazione del Presidente Inail 8 ottobre 2019, n. 297:** "Regolamento unico per la disciplina del diritto di accesso ai documenti amministrativi ai sensi degli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, e del diritto di accesso a documenti, dati e informazioni ai sensi degli articoli 5 e seguenti del decreto legislativo 14 marzo 2013, n. 33. Modifiche".

- **Determinazione del Presidente Inail munito dei poteri del Consiglio di amministrazione 12 marzo 2020, n. 53:** "Nuovo modello organizzativo della privacy e della protezione dei dati personali ai sensi del Regolamento UE 2016/679 (GDPR)".

- **Circolare Inail 6 maggio 2020, n. 16:** "Codice disciplinare per i dirigenti appartenenti all'Area delle Funzioni centrali e per i dirigenti dell'ex Ispesl transitati all'Inail".

- **Circolare Inail 6 maggio 2020, n. 17:** "Codice disciplinare per i professionisti e i medici".

Premessa

Il modello organizzativo della *privacy* e della protezione dei dati, modificato in base al Regolamento UE 2016/679 (General data protection regulation - GDPR), di cui alla determina del Presidente Inail munito dei poteri del Consiglio di amministrazione del 12 marzo 2020, n. 53, conferisce, nell'ambito dell'organizzazione dell'Istituto, specifiche responsabilità a vari livelli, finalizzate alla conformità al GDPR relativamente ai trattamenti di cui l'Istituto è titolare. Tali trattamenti, così come richiesto dall'art. 30 del GDPR, sono censiti in un apposito registro, presente nel sistema documentale che l'Istituto ha reso disponibile per rendere più efficiente e fruibile il sistema di gestione della protezione dei dati. Tale sistema contiene documenti, informazioni, note operative e istruzioni in relazione alla protezione dei dati. Inoltre, registra le evidenze necessarie a comprovare la conformità al regolamento, in linea con il principio di responsabilizzazione espresso nel regolamento stesso.

In relazione al modello organizzativo, la presente circolare:

- disciplina le modalità di designazione degli autorizzati al trattamento dei dati personali;
- fornisce agli autorizzati le istruzioni necessarie per operare in conformità, come previsto nell'ambito "politiche in materia di sicurezza e protezione dei dati e adozione delle contromisure" del modello organizzativo;
- tra le istruzioni di cui al punto precedente, rammenta agli autorizzati le azioni a loro carico relativamente all'ambito di "gestione delle violazioni di dati personali (*data breach*)" presente nel modello organizzativo.

La presente circolare costituisce, inoltre, informativa ai dipendenti per l 'utilizzo dei servizi di posta elettronica e di accesso a internet.

Designazione

Tutti i dipendenti in forza sono designati come autorizzati al trattamento dei dati personali, in relazione agli incarichi, ai compiti e alle funzioni svolte dagli stessi nell'ambito dei processi e delle attività lavorative alle quali sono addetti, alla natura dei dati, alle finalità e alle modalità di trattamento nonché agli strumenti utilizzati.

L'autorizzazione ai trattamenti discende direttamente dagli incarichi e dalle mansioni derivate dal ruolo o assegnate dal diretto responsabile in base alle effettive necessità lavorative. Il diretto responsabile, in generale, rappresenta il responsabile gerarchico del dipendente, inteso come la persona per cui il dipendente rappresenta un riporto diretto, come il Direttore di Sede.

Gli incarichi ai trattamenti e le relative abilitazioni dei dipendenti per l'accesso ai dati, alle applicazioni e ai dispositivi, conferiti con modalità informatiche, sono equivalenti alle designazioni formali realizzate per iscritto.

Il responsabile ha il compito di monitorare e mantenere aggiornate le abilitazioni dei propri dipendenti, specie in seguito agli eventi che modificano le necessità di accesso ai dati. Considerata la complessità ed eterogeneità del contesto dei sistemi e delle abilitazioni, il responsabile potrà avvalersi, oltre che degli strumenti informatici di cui è dotato, anche del supporto della Direzione centrale per l'organizzazione digitale (Dcod).

Le abilitazioni non più necessarie devono essere immediatamente rimosse. Tale rimozione può avvenire in modalità automatica, agganciandosi a eventi quali il pensionamento, il trasferimento o la variazione di incarico oppure in modalità manuale da parte del responsabile. Esempi di abilitazioni che prevedono un'attività di rimozione manuale sono quelle relative agli applicativi istituzionali (GRA, GRAI, ecc.) e le abilitazioni per l'accesso ai dati in convenzione con enti esterni (Inps, Agenzia delle Entrate, ecc.).

È comunque responsabilità e dovere del dipendente segnalare abilitazioni non più necessarie o frutto di errore e, in questi casi, è comunque fatto divieto di usufruirne per accessi a dati ovvero procedure e/o applicativi che sarebbero considerati non leciti.

Gli autorizzati al trattamento dei dati personali devono puntualmente attenersi ai principi e agli obblighi del GDPR, nonché al modello organizzativo *privacy* dell'Istituto di cui alla determina del Presidente Inail munito dei poteri del Consiglio di amministrazione 12 marzo 2020, n. 53.

Gli autorizzati devono inoltre attenersi alle linee guida, alle *policy* di sicurezza dell'Istituto e alle istruzioni operative impartite nella presente circolare e dettagliate nel seguito, che costituiscono un estratto delle politiche di sicurezza delle informazioni in essere. Sarà compito della Dcod emanare evoluzioni, aggiornamenti e ulteriori istruzioni, pubblicandole nella sezione sicurezza del *repository* ufficiale di Inail.

A ogni modo gli autorizzati, nell'operare per conto dell'Istituto, devono osservare il codice disciplinare previsto nell'ambito del ruolo e dell'attività svolta.

L'Istituto, in qualità di titolare del trattamento dei dati personali, in esecuzione degli obblighi derivanti dalla normativa vigente in materia di protezione dei dati personali, è tenuto a verificare l'osservanza delle disposizioni di cui alle seguenti istruzioni. La violazione parziale o totale delle istruzioni impartite potrà comportare provvedimenti disciplinari commisurati alla gravità della violazione e, nei casi più gravi, conseguenze penali.

Istruzioni operative per gli autorizzati al trattamento

Rispetto dei principi del GDPR

Nel trattare i dati personali, indipendentemente dalla loro natura ordinaria (dati comuni) o particolare (dati di carattere sanitario o giudiziari), gli autorizzati al trattamento sono tenuti a:

- operare garantendo la massima riservatezza delle informazioni di cui vengono a conoscenza, considerando tutti i dati personali confidenziali e, di norma, soggetti al segreto d'ufficio, fatta eccezione per i soli dati anonimi, generalmente trattati per elaborazioni statistiche, e quelli desumibili da liste ed elenchi pubblici;
- evitare, nelle procedure di lavoro e nello svolgimento delle operazioni di trattamento, che i dati personali siano soggetti a rischi di distruzione e perdita anche accidentale;
- evitare che ai dati possano accedere persone non autorizzate e che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati sono stati raccolti;
- operare con la massima diligenza e attenzione in tutte le fasi di trattamento, dal momento dell'acquisizione dei dati, all'eventuale loro aggiornamento, alla conservazione, fino all'eventuale cancellazione o distruzione;
- eseguire operazioni di trattamento esclusivamente in ottemperanza ai compiti assegnati dal responsabile diretto e, comunque, riferiti alle disposizioni e ai regolamenti (processi e procedure) interni vigenti;
- mantenere il segreto verso chiunque, in ordine alle informazioni delle quali siano venuti a conoscenza nello svolgimento dell'incarico; tale segreto deve essere mantenuto in ogni caso anche quando sia venuto meno l'incarico stesso, salvo legittima richiesta dell'Autorità giudiziaria. Per i funzionari pubblici il reato di rivelazione del segreto d'ufficio scatta non solo per la divulgazione di notizie coperte da segreto ma anche per la semplice comunicazione di notizie «accessibili» a chi però non ha diritto di riceverle;
- mantenersi informato rispetto ai propri obblighi connessi ai propri incarichi assumendo atteggiamento consapevole in tema di protezione dei dati maneggiati.

Gestione dell'abilitazione informatica

Nel caso in cui il trattamento avvenga per mezzo di un'applicazione informatica, l'incarico al trattamento si accompagna a una abilitazione che permette l'accesso ai dati. Come detto, gli incarichi ai trattamenti e le relative abilitazioni dei dipendenti per l'accesso ai dati, alle applicazioni e ai dispositivi, conferiti con modalità informatiche (per esempio tramite la *consolle* di profilazione o mediante apertura di un *ticket* per l'abilitazione a una applicazione), sono equivalenti a designazioni formali realizzate per iscritto.

L'accesso ai dati è lecito solo in presenza di un'abilitazione valida, connessa all'incarico lavorativo, che non derivi da errori o da precedenti incarichi, e deve avvenire esclusivamente per un'effettiva esigenza lavorativa relativa alla pratica. Quindi, anche nel caso di abilitazioni valide è comunque vietato l'accesso ai dati senza una motivazione lavorativa quale, per esempio, l'assegnazione della pratica o la richiesta diretta da parte di un interessato allo sportello.

Tali abilitazioni derivano dagli incarichi e dalle mansioni di ogni dipendente, ovvero:

- sono derivate dal ruolo mediante degli automatismi legati al profilo lavorativo;
- vengono assegnate dal diretto responsabile tramite apposite *consolle* di profilazione oppure vengono richiesti, sempre per il tramite del diretto responsabile, alla Dcod.

I responsabili:

- assegnano le abilitazioni in modo corretto, in funzione dell'incarico lavorativo del dipendente e in relazione a una effettiva esigenza lavorativa;
- prestano particolare attenzione a tutti gli eventi che possano determinare una differente esigenza di accesso ai dati e quindi una variazione delle abilitazioni dei dipendenti. Tra gli eventi più significativi si evidenziano:
  - il pensionamento, a seguito del quale molte abilitazioni interne come l'accesso alla intranet e alle applicazioni istituzionali interne (per esempio GRA, GRAI, Cartella Clinica) decadono automaticamente. Altre abilitazioni, invece, come quelle sui sistemi esterni all'Istituto (per esempio nei casi di accessi a dati in convenzione con altri enti), rimangono attive e vanno fatte cessare tempestivamente a cura del responsabile stesso;
  - il cambio di incarico di un dipendente, situazione in cui sarà sempre cura del responsabile aggiornare le abilitazioni o assicurarsi che lo siano state;
  - il trasferimento di un dipendente ad altra Sede o altra Unità organizzativa, che prevede che:
    - il responsabile uscente, ovvero colui che rilascia la risorsa, provveda alla rimozione delle abilitazioni non più necessarie;
    - il responsabile entrante, ovvero colui che riceve la risorsa, prenda in carico il compito di verifica e controllo delle abilitazioni del dipendente.

I dipendenti:

- accedono ai dati a fronte di abilitazione valida e solo in relazione a una specifica necessità lavorativa;
- segnalano abilitazioni non più necessarie, o frutto di errore, di cui sono a conoscenza e, comunque, non utilizzano in alcun modo tali abilitazioni per accessi a dati che sarebbero considerati non leciti.

Gestione delle violazioni di dati personali (*data breach*) e segnalazione degli incidenti di sicurezza

Una violazione dei dati personali è una 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. Esempi di violazione dei dati personali sono: la perdita di un dispositivo contenente dati personali, l'invio per errore di dati personali a terzi non autorizzati, l'infezione della propria postazione di lavoro da parte di un *ransomware*, ecc.

Un incidente di sicurezza è, più in generale, qualsiasi evento o insieme di eventi indesiderati o imprevisti che sottintendono una violazione delle politiche di sicurezza fonte di danno per gli *asset* Inail, ovvero per il patrimonio informativo dell'organizzazione. Esempi di incidenti di sicurezza sono, la ricezione di *e-mail* malevole come quelle di *phishing* o contenenti *malware*, tentativi di accesso non autorizzato alle informazioni, ecc.

In questo ambito tutti i dipendenti:

- nel caso abbiano evidenza di una situazione che possa comportare o ha comportato violazione di dati personali ne danno immediata segnalazione al proprio responsabile che, a propria volta, ne dà immediata comunicazione al Responsabile della protezione dei dati (RPD);
- nel caso abbiano evidenza di una situazione che possa determinare o abbia determinato un incidente di sicurezza delle informazioni, ne danno immediata comunicazione al CERT Inail, mediante la casella di posta elettronica cert@inail.it.

Gestione delle *password*

Le *password* rappresentano l'attuale metodo dell'Istituto per la verifica dell'identità degli utenti, la cui efficacia verrà ulteriormente innalzata mediante l'introduzione di meccanismi di autenticazione forte. Pertanto la sicurezza della *password* è di importanza fondamentale per poter proteggere l'utente, la postazione di lavoro, la rete interna e i dati.

In accordo con le Linee guida gestione password di accesso ai sistemi informativi l'utente è tenuto ad adottare i seguenti criteri per la gestione della propria *password* di accesso:

- non deve in nessun caso comunicare ad altri la propria *password*, per esempio tramite posta elettronica o al telefono, nemmeno in risposta a una richiesta esplicita;
- non deve trascrivere mai la propria *password* su carta o su *file* non opportunamente crittografato;
- non deve usare *password* che:
  - contengano la propria matricola o il proprio nome e/o cognome;
  - contengano sequenze digitate alla tastiera (per esempio "qwerty") o sequenze di caratteri ripetuti;
- deve adottare i criteri per aumentare la complessità della *password* suggeriti nelle già citate Linee guida gestione password di accesso ai sistemi informativi;
- non può usare le credenziali personali per l'iscrizione a siti esterni al perimetro dell'Istituto;
- è obbligato a cambiare la *password* di accesso in caso di accertata o sospetta compromissione.

Gestione degli strumenti elettronici

È fondamentale che i dipendenti adottino le Linee guida per l'utilizzo degli strumenti elettronici. In merito, al fine di salvaguardare la riservatezza delle informazioni, l'utente non deve:

- usare impropriamente il sistema informativo e i dispositivi dell'Istituto (per esempio per diffusione o memorizzazione di inserzioni commerciali o personali, petizioni, pubblicità o per qualsiasi altro uso non autorizzato, come l'uso di strumenti non autorizzati per lo scambio di dati personali);
- portare all'esterno delle Sedi dell'Inail apparecchiature, informazioni o *software* di proprietà dell'Istituto senza preventiva autorizzazione;
- accedere o tentare l'accesso alle informazioni per le quali non si hanno privilegi;
- fare copie di dati dell'Istituto o divulgare a terzi informazioni se non autorizzati.

L'utente è inoltre obbligato a:

- rispettare la legge sul *copyright* o diritto d'autore;
- riferire al CERT Inail eventuale ricezione di messaggi di posta elettronica contenente materiale inappropriato o illegale.

Inoltre, relativamente alla postazione di lavoro, la cui gestione è cruciale al fine di ridurre il rischio di accesso non autorizzato a informazioni dell'Istituto, i dipendenti sono tenuti a:

- seguire politiche di *clear desk* e di *clear screen* (ovvero tenere libere da dati e informazioni non utili in quel momento sia la scrivania fisica che lo schermo del proprio computer);
- ogni qualvolta si abbia la necessità di allontanarsi dal posto di lavoro, chiudere i documenti non in uso e bloccare il Pc utilizzando il comando Ctrl-Alt-Canc o Blocca computer;
- distruggere o custodire in luoghi sicuri stampe e documenti cartacei con informazioni di dominio non pubblico e non lasciare stampe incustodite alle stampanti;
- mantenere impostato il salva schermo (*screen saver*).

Utilizzo della posta elettronica

La sicurezza della posta elettronica è centrale per tutelare le informazioni dei dipendenti e i dati dell'Istituto stesso.

Le indicazioni sulla sicurezza delle informazioni relative alla posta elettronica sono contenute all'interno delle Linee guida per l'utilizzo dei servizi di posta elettronica e di accesso a internet. Tale documento rappresenta l'informativa ai dipendenti da parte del datore di lavoro sull'utilizzo di tali strumenti, prevista dal Provvedimento del Garante 1 marzo 2007, e costituisce parte integrante di questa circolare. Il documento è stato aggiornato di recente in occasione delle ultime modifiche derivanti dal cambiamento di tecnologia. Tutti i dipendenti sono invitati a prenderne visione tenendo presente che questa circolare comprende anche l'accettazione di tale informativa, la cui presa visione comporta pertanto presa visione e accettazione dell'informativa.

Di seguito se ne riporta un estratto:

- prestare la massima attenzione nell'apertura dei *file* allegati alle *e-mail* (per esempio Word, Excel, PDF, ZIP, Immagini) poiché possibili veicoli di virus o *ransomware*;
- prestare la massima attenzione nell'apertura di *link* presenti nel corpo della *e-mail*, poiché potrebbero indirizzare a siti malevoli;
- non diffondere notizie a carattere riservato, né inviare documenti di lavoro a indirizzi di posta elettronica esterni alla rete informatica dell'Istituto, se non necessario per l'attività lavorativa, in considerazione del fatto che la posta può essere intercettata da chiunque;
- in caso di dubbio e per effettuare un controllo in automatico sui messaggi di posta sospetta, si invita a inoltrare il messaggio all'indirizzo di posta elettronica horus@inail.it; qualora si necessiti di ulteriori informazioni è possibile contattare la casella di posta elettronica presidiata postasospetta@inail.it.

Utilizzo di internet

Nelle suddette Linee guida per l'utilizzo dei servizi di posta elettronica e di accesso a internet sono identificate le regole, che costituiscono un saldo presupposto per un comportamento *online* corretto da parte di dipendenti con l'obiettivo di tutelare la sicurezza nella navigazione *web*.

In generale, l'utente è tenuto a:

- utilizzare l'accesso alla rete internet senza mettere a rischio l'integrità, la riservatezza e la disponibilità dei dati, delle informazioni e dell'intero sistema informatico dell'Istituto;
- non visitare siti non attendibili poiché, dopo la posta elettronica, la navigazione internet rappresenta il veicolo principale per le minacce di sicurezza.

Uso dei dispositivi mobili

I dispositivi mobili aziendali rappresentano di fatto delle estensioni del *network* dell'Istituto al di fuori del suo perimetro fisico. Pertanto, se vulnerabili, possono esporre l'Istituto a rischi di sicurezza informatica.

Sulla base delle Politica dei dispositivi mobili, si riportano di seguito alcune delle regole dettate dall'Istituto che impongono ai dipendenti il divieto di:

- installare applicazioni non provenienti dagli *App Store* ufficiali resi disponibili dai fornitori dei dispositivi mobili (es. *Google Play, App Store*), salvo diverse indicazioni da parte dell'Istituto;
- installare applicazioni il cui utilizzo può arrecare danni di reputazione oppure economici all'Istituto, nonché quelle che violino le normative nazionali e internazionali;
    - utilizzare reti telematiche insicure o pubbliche per la trasmissione dati, come per esempio le reti Wi-Fi non protette da *password* o protette da meccanismi deboli, quali per esempio il *Wired Equivalent Privacy* (WEP).

Sicurezza nella conservazione e trasferimento dei *files*

L'Istituto, nell'ottica di tutela del patrimonio digitale, sconsiglia fortemente, per la memorizzazione delle informazioni, l'utilizzo di ambienti *cloud* non consentiti o supporti di memoria removibili quali, per esempio, chiavette USB o dischi esterni.

Ai fini della conservazione e del trasferimento delle informazioni, si suggerisce in alternativa di:

- salvare e, se necessario, condividere i *files* tramite InailOneDrive, che permette di archiviare i documenti e di recuperarli in mobilità, evitandone quindi la copia su un supporto mobile o su ambienti *cloud* non consentiti. Tale soluzione permette anche la condivisione sicura con colleghi e persone esterne all'Istituto e garantisce la cifratura dei dati per una adeguata protezione delle informazioni;
- in un'ottica di salvaguardia della disponibilità delle informazioni (*backup*), salvare, ove possibile e opportuno, documenti e dati di interesse dell'Istituto sui server centrali (es. *sharepoint*), soggetti a regole di *backup* periodico.

Resta comunque fondamentale valutare sempre la necessità di condividere e memorizzare dati personali, al fine di garantire la conformità ai principi del GDPR sopra citati, operando in conformità alle Linee guida sulla classificazione delle informazioni. La diffusione e l'accesso non autorizzato alle informazioni può costituire una violazione di dati personali, da cui possono derivare danni per gli interessati ed elevate sanzioni amministrative nei confronti dell'Istituto stesso. Per questo, quando si trattano dati personali si deve sempre porre attenzione alla correttezza e liceità delle azioni che si intraprendono.

Gestione della sicurezza dei dati trattati senza l'ausilio di strumenti elettronici

Gli autorizzati al trattamento devono attenersi alle modalità previste ai fini di una idonea custodia degli atti e dei documenti loro affidati. In particolare:

- non lasciare mai gli atti e i documenti cartacei contenenti dati personali, anche per brevi intervalli di tempo, incustoditi o esposti alla visione di soggetti estranei o non autorizzati al trattamento;
- conservare tutti gli atti e i documenti cartacei contenenti dati personali in armadi, contenitori o cassetti muniti di serratura;
- lasciare chiusi a chiave, fuori dell'orario di apertura degli uffici, i locali dove sono posizionati gli armadi o i contenitori; le persone ammesse dopo l'orario di chiusura, a qualunque titolo, devono essere identificate e registrate;
- chiudere a chiave gli armadi o i contenitori in occasione delle periodiche operazioni di pulizia, di eventuali lavori di manutenzione dei locali o del trasferimento in altri locali di documenti contenenti dati personali;
- rendere inintelligibili i documenti cartacei prima di procedere con la loro dismissione.

Ulteriori istruzioni per incarichi specifici

Nel caso di incarichi specifici (es. accesso ai dati relativi al trattamento di videosorveglianza, accesso ai dati in qualità di amministratore di sistema, ecc.), si rimanda alle istruzioni di dettaglio che verranno fornite al personale interessato.

Il Direttore generale
f.to Giuseppe Lucibello