Disciplinare interno per l'utilizzo degli strumenti informatici

Settore Patrimonio, Reti, Innovazione Tecnologica, Archivi e Protocollo

Indice generale

1. INTRODUZIONE.....2

1.1 Finalità del documento.....3

1.2 Contesto normativo.....3

2. GLOSSARIO E DEFINIZIONI.....3

3. PRINCIPI GENERALI.....5

4. REGOLE PER L'UTILIZZO DEI SISTEMI INFORMATICI.....5

4.1 Credenziali di autenticazione al dominio.....5

4.2 Utilizzo di applicazioni aziendali.....6

4.3 Postazione di lavoro.....7

4.4 Postazione di lavoro portatile.....8

4.5 Altri dispositivi.....8

4.7 Software a corredo.....8

4.8 Navigazione in internet.....9

4.9 Posta elettronica.....9

4.10 Servizi di Unified Communication.....12

4.11 Servizi Cloud e Spazi di condivisione di rete aziendale.....12

4.12 Dispositivi di memorizzazione rimovibili (Hard disk, Pen drive USB, etc.).....12

4.13 Comportamenti non consentiti.....13

4.14 Comportamenti da tenere in caso di furti e danneggiamenti.....14

4.15 Comportamento in caso di assenza programmata.....14

5. CONTROLLI E MONITORAGGI.....14

5.1. Ruolo degli amministratori delle risorse tecnologiche condivise e delle applicazioni.....15

1. INTRODUZIONE

Il presente documento definisce le regole e le condizioni per l'utilizzo degli **strumenti informatici dell'Agenzia Regionale Toscana per l'Impiego** da parte dei dipendenti e di tutti coloro che, in virtù di un rapporto di lavoro a qualsiasi titolo (collaboratori, consulenti, stagisti, fornitori, etc.), utilizzano strumenti informatici dell'Agenzia, nel seguito denominati Utenti.

1.1 Finalità del documento

Il presente documento, redatto a cura del Servizio IT e infrastrutture digitali interne, regolamenta l'accesso e l'uso delle risorse informatiche dell'Agenzia Regionale Toscana per l'Impiego (di seguito ARTI), secondo i principi e le disposizioni della normativa citata (1.2 – Contesto normativo) e le indicazioni in materia di corretto uso delle risorse informatiche, nel rispetto delle politiche e disposizioni definite in accordo con la Direzione dell'Agenzia.

1.2 Contesto normativo

Il presente disciplinare è redatto sulla base dei seguenti e principali riferimenti normativi:

- D. Lgs. 196/2003 e s.m.i (Codice in materia di protezione dei dati personali);
- D. Lgs. 82/2005 e s.m.i. (Codice dell'amministrazione digitale);
- Provvedimenti del Garante per la protezione dei dati personali applicabili al contesto oggetto del presente documento, fra cui le "Linee guida per posta elettronica e Internet" di cui alla deliberazione 13/2007;
- D.P.R 62/2013 (Codice di comportamento dei dipendenti della pubblica amministrazione) e Codice di comportamento ARTI;
- Regolamento (UE) 2016/679 (General Data Protection Regulation, di seguito GDPR)
- Linee guida Agenzia per l'Italia Digitale (AgID)

2. GLOSSARIO E DEFINIZIONI

Ai fini del presente documento si intende per:

- ***Amministratori di sistema**:* figure professionali finalizzate alla gestione e alla manutenzione di un sistema di elaborazione o di sue componenti o figure equiparabili, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi, individuate in conformità al Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, come modificato dal provvedimento del 25 giugno 2009;
- ***Applicazioni aziendali***: si considerano applicazioni aziendali:
    - Prodotti/programmi acquistati o noleggiati dall'amministrazione, di valenza generale o settoriale ed in quest'ultimo caso approvati dai sistemi informativi;
    - Applicazioni e servizio sviluppate ad hoc dai sistemi informativi, da terze parti ma sotto il coordinamento dei sistemi informativi ovvero da altre strutture con un processo di partecipazione e approvazione da parte dei sistemi informativi e che seguono le regole di gestione previste nei casi precedenti;
    - Applicazioni esterne che l'amministrazione utilizza secondo le regole di gestione e di sicurezza delle medesime a titolo di mero esempio possono essere la piattaforma NoiPA, abbonamenti a servizi informativi, portale ANAC, etc.
- ***Dispositivi mobili**:* apparecchi di telecomunicazione portatili (tablet, smartphone, etc.);
- ***File di log:*** registrazioni sequenziali e cronologiche delle operazioni effettuate da un sistema informativo, necessarie per la risoluzione di problemi ed errori; tali operazioni possono essere effettuate da un Utente oppure avvenire in modo totalmente automatizzato;
- ***Utenti***: personale dipendente, personale comandato da altre pubbliche amministrazioni, collaboratori, consulenti, tirocinanti, stagisti, fornitori esterni e coloro che, in virtù di un rapporto di lavoro in essere a qualsiasi titolo con l'Agenzia, siano autorizzati all'utilizzo degli strumenti informatici messi a disposizione dall'Agenzia.

- ***Postazione di lavoro (PdL)****:* personal computer (desktop o portatile) messo a disposizione dall'Agenzia a ciascun Utente per l'espletamento dell'attività lavorativa;
- ***Strumenti informatici****:* personal computer fissi o portatili e relative periferiche, stampanti locali o di rete, programmi e prodotti software, apparecchiature adoperate per la comunicazione unificata (videoconferenza, telefonia fissa e mobile, chat, messaggistica generica, social network, posta elettronica, condivisioni, accessi remoti, etc);

3. PRINCIPI GENERALI

Gli strumenti informatici sono assegnati agli Utenti per lo svolgimento dell'attività lavorativa e devono essere utilizzati con modalità e mediante comportamenti adeguati ai compiti assegnati e alle responsabilità connesse, nel rispetto del Codice di comportamento dei dipendenti della pubblica amministrazione e delle normative e delle direttive interne.

Nell'esecuzione della propria attività lavorativa, gli Utenti sono tenuti ad attenersi alle seguenti istruzioni generali:

a) effettuare la propria attività uniformandosi alle disposizioni dell'Agenzia e alle istruzioni ricevute;

b) custodire con diligenza gli strumenti informatici loro affidati, segnalando tempestivamente alle strutture preposte, secondo le modalità previste, ogni danneggiamento, smarrimento o furto;

c) adottare ogni misura di sicurezza idonea a scongiurare rischi di perdita o distruzione (anche accidentale) dei dati;

4. REGOLE PER L'UTILIZZO DEI SISTEMI INFORMATICI

4.1 Credenziali di autenticazione al dominio

L'accesso alle applicazioni del sistema informativo dell'Agenzia avviene attraverso autenticazione mediante credenziali di dominio che devono essere modificate ogni 6 mesi.

Le credenziali di autenticazione sono strettamente personali e non devono essere comunicate né rese disponibili ad altri soggetti.

In caso di diffusione accidentale, anche solo presunta, le password devono essere immediatamente modificate e l'incidente va immediatamente segnalato a helpdesk-arti@arti.toscana.it.

Il sistema di controllo degli accessi presente in Agenzia implementa le seguenti regole:

- composizione di password complesse, che abbiano una lunghezza minima stabilita e una sequenza di caratteri normali, speciali e/o numerici;
- impossibilità di riuso delle ultime password utilizzate;
- reinizializzazione (reset) della password e riattivazione delle utenze disabilitate, secondo le procedure in vigore.

4.2 Utilizzo di applicazioni aziendali

All'atto della cessazione/interruzione del rapporto di lavoro o dell'attività lavorativa svolta a qualsiasi titolo per conto dell'Agenzia, ferma restando la disabilitazione all'uso degli applicativi e delle funzionalità di ARTI da parte dei Servizi IT e infrastrutture digitali interne, è fatto obbligo di restituzione delle strumentazioni elettroniche (PC portatili, tablet, cellulari, kit di firma elettronica ecc.) già affidate per l'esplicazione delle funzioni connesse al rapporto di lavoro.

In caso di assegnazione temporanea del personale ARTI presso altra pubblica amministrazione, la titolarità della casella di posta elettronica sul dominio dell'Agenzia potrà essere mantenuta nel rispetto delle disposizioni che regolano l'uso di tale risorsa ai sensi del presente disciplinare. All'atto dell'assegnazione temporanea e durante il relativo periodo di servizio, l'Ufficio dei Servizi IT e infrastrutture digitali interne provvede alla disabilitazione all'uso degli applicativi e funzionalità, fermo restando l'obbligo del dipendente di restituzione della strumentazione informatica già assegnata da ARTI per lo svolgimento della prestazione lavorativa.

4.3 Postazione di lavoro

Le postazioni di lavoro (PdL) sono gestite dall'ufficio Servizi IT e infrastrutture digitali interne che le assegna agli Utenti. È vietato qualsiasi utilizzo che deturpi o rovini la PdL e tutti gli accessori/periferiche in assegnazione.

La postazione di lavoro è provvista di software di sicurezza (software antivirus, personal firewall, software per aggiornamento automatico delle patch di sistema, etc.).

L'assegnatario della PdL è profilato come utente senza diritti amministrativi.

La PdL è provvista del software base approvato dall'Agenzia. In caso di particolari necessità, è disponibile una lista di software, la cui installazione può essere richiesta direttamente dall'Utente tramite l'Helpdesk all'ufficio Servizi IT e infrastrutture digitali interne che valuterà anche l'ammissibilità di eventuali, ulteriori necessità lavorative.

In caso di anomalia del funzionamento del computer di dotazione o insolita lentezza nelle comunicazioni con i servizi dell'ente, contattare il servizio Helpdesk;

L'Utente assegnatario della postazione di lavoro è responsabile del suo corretto utilizzo nel rispetto delle seguenti regole comportamentali:

a) la PdL è assegnata all'Utente per lo svolgimento della propria attività lavorativa;

b) la PdL non deve essere accessibile a soggetti non autorizzati;

c) l'Utente non deve apportare modifiche alle configurazioni della PdL che non siano state preventivamente richieste e autorizzate dall'ufficio Servizi IT e infrastrutture digitali interne;

d) tutto il personale ha l'obbligo di salvare la documentazione relativa alla propria attività lavorativa sugli spazi di condivisione dell'Agenzia;

e) durante l'allontanamento dalla PdL, l'Utente deve bloccare la propria postazione tramite la combinazione dei tasti WINDOWS + L, o in alternativa deve essere fatta la disconnessione del proprio utente per

consentirne l'accesso unicamente mediante l'immissione della password.

4.4 Postazione di lavoro portatile

Per quanto riguarda la postazione portatile, oltre alle regole già descritte per le postazioni fisse, è necessario tener presente che:

- il PC portatile è assegnato direttamente all'Utente che ne è responsabile;
- il PC portatile non deve essere lasciato in ufficio al termine dell'orario di lavoro.

Si evidenzia che le stazioni di lavoro portatili sono maggiormente esposte a rischi di sicurezza, quali danneggiamenti conseguenti agli spostamenti, furti, violazione della riservatezza delle informazioni contenute. Tutti gli Utenti, pertanto, devono custodire con cura e diligenza la postazione di lavoro portatile assegnata.

4.5 Altri dispositivi

Con riferimento ad altri dispositivi assegnati ai dipendenti, quali smartphone e/o tablet, valgono le medesime regole comportamentali adottate per le PdL.

4.6 Utilizzo di attrezzature informatiche personali o fornite in dotazione da soggetti terzi

Le attrezzature personali di qualsiasi tipologia (PC, tablet, smartphone ecc.) possono essere collegate alla rete aziendale esclusivamente previa sottoscrizione, per presa visione ed accettazione, da parte del proprietario del dispositivo o del legale rappresentante del soggetto fornitore, del presente disciplinare.

4.7 Software a corredo

L'eventuale utilizzo di software di tipo portable (che non richiedono installazione) o installabili con i permessi dell'Utente è nella completa responsabilità dell'Utente, sia per gli aspetti di diritto di proprietà intellettuale sia per quelli di sicurezza.

4.8 Navigazione in internet

La navigazione in internet è messa a disposizione del personale come fonte di informazione per le finalità di documentazione, ricerca e studio, utili per lo svolgimento della prestazione lavorativa.

Qualsiasi operazione effettuata sulla rete esterna (accesso a siti web per necessità non inerenti l'attività lavorativa, salvataggio di file, partecipazione a forum, etc.) è posta sotto la responsabilità dell'Utente, che deve mantenere un comportamento lecito e tale da non compromettere le attività e il buon nome dell'Agenzia.

Ogni Utente è tenuto a osservare le seguenti regole comportamentali:

- utilizzare internet per fini leciti, astenendosi da qualsiasi comportamento che possa avere natura oltraggiosa e/o discriminatoria verso terzi;
- trasferire sul proprio computer (download) solo file da siti web verificati e affidabili, tenendo presente che quando si trasferisce materiale da internet occorre prestare la massima attenzione al fine di non incorrere in violazioni di diritti di proprietà intellettuale;
- non utilizzare social network, forum, chat e simili per scambiare informazioni riservate o lesive dell'immagine dell'Agenzia e dei colleghi.

Al fine di prevenire l'accesso a siti web e risorse internet potenzialmente nocivi, per la navigazione dalla rete aziendale l'Agenzia adotta soluzioni di sicurezza basate su filtri attraverso i quali l'accesso a specifiche e determinate categorie di siti è bloccato a priori; i tentativi di accesso a tali siti (ad esempio siti malevoli, gioco d'azzardo, siti per adulti) vengono bloccati e all'Utente è inviato un avviso in cui viene spiegato il motivo del blocco.

4.9 Posta elettronica

Tutti gli Utenti sono dotati di una casella di posta elettronica sul dominio dell'Agenzia. Le caselle devono essere utilizzate per l'esercizio della propria attività lavorativa.

L'utilizzo delle caselle PEC gestite in ambito generale o funzionale ad applicazioni dal personale che ne cura le relative applicazioni è coordinato dal dirigente di riferimento.

Quando si utilizza lo strumento della posta elettronica, è opportuno osservare comportamenti consoni, come indicato nell'allegato **Posta elettronica e UC Netiquette.**

Il sistema di posta elettronica prevede:

- la possibilità di imporre limiti all'utilizzo del servizio, ad esempio sul numero dei destinatari di un messaggio, sulla dimensione degli allegati che sarà possibile inviare e/o sulla dimensione complessiva della casella di posta elettronica;
- per le e-mail inviate a destinatari esterni al dominio di posta elettronica dell'Agenzia, è predisposto un avvertimento (disclaimer) inserito automaticamente in calce al messaggio. In tale disclaimer viene dichiarata la natura riservata del contenuto ed è inserito un invito alla cancellazione per chi non fosse il destinatario previsto. Non è consentito inserire disclaimer personalizzati in calce alla comunicazione;
- un sistema automatico di classificazione dei messaggi ricevuti (spam o posta indesiderata), in cui confluiscono tutti i messaggi non reputati leciti dall'algoritmo anti-spamming.

Nell'utilizzo del servizio l'Utente ha l'obbligo di:

- inserire la propria firma utilizzando il format definito dall'Agenzia per l'invio di messaggi verso l'esterno;
- proteggere la privacy dell'interlocutore evitando, qualora non necessario, di inoltrare messaggi altrui senza il previo consenso dell'interessato;
- provvedere ad un invio separato per ciascun destinatario o utilizzare il campo "Ccn" qualora la comunicazione debba essere inviata a più soggetti il cui indirizzo e-mail non appartiene all'organizzazione aziendale (@arti.-

toscana.it), così che non vi sia l'indebita o l'impropria condivisione di indirizzi e-mail tra tutti i destinatari;

- verificare che il mittente dichiarato nelle email ricevute sia compatibile con quanto presente nel campo "Da:";
- evitare di utilizzare la posta elettronica come archivio documentale. Se venisse utilizzata come tale, infatti, in caso di accesso malevolo, l'attaccante accederebbe all'intera base documentale. E` sempre preferibile procedere a caricarli su cartelle condivise e/o sistemi di filesharing dell'Agenzia;
- evitare di automatizzare l'inoltro delle email dal proprio indirizzo di posta istituzionale a domini terzi e viceversa: non è consentito cioè inoltrare sistematicamente quanto ricevuto sull'indirizzo utente1@arti.toscana.it all'indirizzo utente2@gmail.com e viceversa;
- evitare l'invio, tramite le caselle di posta elettronica, di messaggi ingiuriosi, minatori, lesivi dell'immagine dell'Agenzia o che utilizzino linguaggi o immagini oscene, ingannevoli o diffamatorie;
- evitare di creare o rispondere a "catene di Sant'Antonio", appelli o richieste non pertinenti all'attività lavorativa in ARTI;
- evitare l'invio o l'inoltro di messaggi estranei al contesto lavorativo a un gran numero di indirizzi o a liste di distribuzione interne all'Agenzia;
- evitare l'utilizzo dell'indirizzo e-mail per l'iscrizione e/o la partecipazione a social network, mailing list, servizi di instant messaging, forum o altri servizi pubblici su internet di interesse personale e non lavorativo;
- evitare di diffondere, all'esterno dell'Agenzia, indirizzi di posta elettronica di altri colleghi, per motivi non legati all'attività lavorativa.

Fermo restando che i contenuti delle e-mail sono ordinariamente consultabili esclusivamente da parte dell'Utente titolare della casella, vengono adottate le seguenti misure di tipo tecnologico:

- possibilità di attivazione da parte dell'Utente, in caso di sua assenza prolungata, della funzione di risposta automatica con invito al mittente a prendere contatto con l'Ufficio competente dell'Agenzia.

Ulteriori dettagli sull'utilizzo della posta elettronica sono riportati nell'allegato **Posta Elettronica e UC Netiquette.**

4.10 Servizi di Unified Communication

Gli strumenti di Unified Communication (UC), oltre alla posta elettronica, comprendono la telefonia, la videoconferenza e la collaborazione sui documenti. L'oggetto che transita nella UC è la comunicazione. L'Utente che invita ospiti esterni a partecipare alla comunicazione oppure condivide con tali ospiti l'indirizzo e-mail o il numero telefonico aziendale, si assume la responsabilità di tale invito o condivisione ed è tenuto a comunicare, in anticipo, agli altri partecipanti la presenza di questi ultimi.

Durante l'utilizzo di tali strumenti è opportuno adottare comportamenti consoni, come indicato nell'allegato **Posta elettronica e UC Netiquette**.

I partecipanti alla comunicazione hanno la responsabilità del proprio comportamento e del rispetto della netiquette, anche qualora supportati tecnicamente dall'ufficio Servizii IT e infrastrutture digitali interne tramite Helpdesk; i partecipanti, inoltre, sono responsabili della manutenzione dei documenti e della cancellazione dei dati non più necessari.

4.11 Servizi Cloud e Spazi di condivisione di rete aziendale

Gli ***spazi di condivisione*** file server o cloud, devono essere utilizzati per la memorizzazione di file ad uso strettamente lavorativo. I file e i documenti di lavoro devono essere obbligatoriamente memorizzati nello ***spazio di condivisione*** apposito al fine di impedire la perdita di dati aziendali, a seguito di guasti alle PdL.

In caso di comprovato pericolo per la sicurezza dei sistemi, ARTI potrà procedere anche senza preavviso alla rimozione di file e/o applicazioni presenti negli ***spazi di condivisione*** degli Utenti, dandone successiva e tempestiva comunicazione agli interessati.

4.12 Dispositivi di memorizzazione rimovibili (Hard disk, Pen drive USB, etc.)

L'utilizzo di supporti di memorizzazione rimovibili deve essere effettuato con molta cautela ed esclusivamente per le attività lavorative. Al momento della

connessione di un dispositivo esterno viene avviata la scansione automatica antivirus, per permettere al sistema di completare la verifica di sicurezza che non può essere interrotta dall'Utente. È inoltre fondamentale che il dispositivo non venga disconnesso durante la scansione, per non danneggiare e rendere illeggibili i dati.

L'utilizzo di dispositivi rimovibili, utile per esempio per effettuare copie di sicurezza o per trasportare file di grandi dimensioni, rimane in ogni caso sotto la responsabilità dell'utilizzatore.

Qualora il dispositivo sia fornito dall'Agenzia, l'Utente è tenuto a informare immediatamente i dirigenti responsabili della struttura organizzativa di appartenenza, l'ufficio Servizi IT e infrastrutture digitali interne e il Responsabile della Protezione dei Dati, anche ai sensi della procedura di gestione delle violazioni di dati personali, di qualsiasi danno, furto o perdita di apparati, software e/o dati in proprio possesso, fatti salvi gli obblighi di denuncia alle autorità competenti.

4.13 Comportamenti non consentiti

Sono vietati a tutti gli Utenti i seguenti comportamenti:

a) l'utilizzo abusivo di credenziali altrui, la cessione a terzi delle credenziali di utilizzo della smart card di firma digitale (o strumento equivalente), l'accesso non autorizzato a risorse informatiche di ARTI e/o lo scambio di comunicazioni mediante falsa identità;

b) l'installazione, sulla PdL in dotazione, di software non coperto da licenza o, comunque, non preventivamente autorizzato dall'ufficio Servizi IT e infrastrutture digitali interne;

c) l'utilizzo, per comunicazioni personali, di chat, social network o altri strumenti di comunicazione aziendale messi a disposizione da ARTI;

d) l'utilizzo, la distruzione, l'alterazione o la disabilitazione non autorizzata di file e di ogni altra risorsa informatica;

e) l'allontanamento dalle PdL senza la preventiva adozione di opportune precauzioni di sicurezza (ad es. il blocco della PdL);

f) la modifica delle configurazioni di base dei dispositivi assegnati dall'Agenzia senza l'autorizzazione preventiva dell'ufficio Servizi IT e in-

frastrutture digitali interne (non è possibile, ad esempio, configurare account privati nel client di posta);

g) l'utilizzo di strumenti volti a eludere i sistemi di protezione.

4.14 Comportamenti da tenere in caso di furti e danneggiamenti

L'Utente è tenuto a informare immediatamente il dirigente responsabile, l'ufficio Servizi IT e infrastrutture digitali interne e, qualora vi sia la possibilità di una violazione di dati personali, altresì il RPD di qualsiasi danno, furto o perdita di strumentazioni informatiche, software e/o dati in proprio possesso, fermi restando gli obblighi di denuncia alle autorità competenti.

4.15 Comportamento in caso di assenza programmata

In caso di assenza programmata, al fine di garantire la continuità del servizio, l'Utente si impegnerà a:

- rendere disponibile, ove necessario, la relativa documentazione su una share condivisa dell'ufficio;
- attivare eventualmente la funzione di risposta automatica, utilizzando un messaggio contenente il periodo di assenza e l'eventuale contatto alternativo.

5. CONTROLLI E MONITORAGGI

ARTI imposta la propria azione di monitoraggio e controllo sui sistemi informatici dell'Agenzia messi a disposizione per lo svolgimento dell'attività lavorativa nel rispetto della normativa vigente e sul presupposto di un utilizzo responsabile degli stessi da parte degli Utenti, adottando in ogni caso le soluzioni tecnologiche idonee a garantire i profili di sicurezza dei sistemi informativi e dei dati gestiti.

A tal fine, ARTI utilizza sistemi automatizzati per la gestione centralizzata dei cosiddetti "file di log", che consentono di tracciare eventuali anomalie o minacce informatiche che potrebbero colpire i sistemi, compromettendo la

funzionalità e la sicurezza degli apparati informatici di ARTI e delle informazioni ivi contenute.

L'amministratore di sistema, nel caso in cui rilevi anomalie o configurazioni non corrette delle PdL, può provvedere a isolare immediatamente l'origine dell'anomalia o del malfunzionamento anche senza preavvisare l'Utente, per salvaguardare la sicurezza e l'integrità dei sistemi informativi di ARTI. In tal caso, verrà data successiva informativa all'Utente sui motivi dell'avvenuto intervento sulla PdL da parte dell'amministratore di sistema.

Le predette attività sono svolte nel rispetto dei principi di gradualità, pertinenza e non eccedenza stabiliti dal Garante per la protezione dei dati personali nonché dei diritti e delle libertà fondamentali dei lavoratori, sempre mediante funzionalità consentite dalla normativa vigente.

5.1. Ruolo degli amministratori delle risorse tecnologiche condivise e delle applicazioni

Gli Amministratori delle risorse tecnologiche condivise e delle applicazioni svolgono le attività necessarie per garantire la salvaguardia del sistema informativo e delle applicazioni conformemente alle politiche e alle istruzioni impartite dall'Agenzia e nel rispetto della normativa vigente con particolare riferimento alla protezione dei dati personali.

Qualora si renda necessario procedere a operazioni finalizzate al ripristino della funzionalità del Sistema informativo comportanti l'accesso a cartelle, file o archivi di altri Utenti, gli Amministratori sono tenuti a preavvisare gli interessati, limitando il proprio intervento a quanto strettamente necessario.