REGOLAMENTO PER LA GESTIONE DEI SISTEMI INFORMATICI

AZIENDA SOCIALE COMUNI INSIEME

Approvato con Delibera del Consiglio di Amministrazione n. 36 del 13.11.2019

n. revisione	data	oggetto
0	13.11.2019	Emissione e approvazione del CdA

PREMESSA

Il Garante per la protezione dei dati personali, con Provvedimento del 1.03.2007 pubblicato sulla G.U.R.I. del 10.03.2007, n. 58, ad oggetto "Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori" raccomanda l'adozione da parte dei datori di lavoro pubblici e privati, di un disciplinare interno, in cui siano indicate le regole per l'uso di Internet, della posta elettronica e della tenuta di file della rete interna, tenendo in debita considerazione quanto stabilito dal Regolamento UE 679/16 ("GDPR") nonché dalla Legge 20.05.1970, n. 300 (Statuto dei lavoratori).

Con il presente regolamento sono definite le condizioni di utilizzo delle risorse informatiche di comunicazione che l'Azienda Sociale Comuni Insieme (di seguito "L'Azienda") mette a disposizione dei propri dipendenti per l'esecuzione delle attività di propria competenza.

Sono tenuti alla vigilanza sul rispetto delle disposizioni: il CdA, il Direttore Generale, il DPO (Responsabile Protezione Dati ai sensi art. 37 del GDPR), i Responsabili del Trattamento, i Sub-Responsabili del Trattamento, gli Incaricati Autorizzati, l'Amministratore di Sistema, Il Responsabile esterno dei sistemi informatici, i Dipendenti designati "Incaricati Autorizzati Trattamento" dei dati personali e particolari ai sensi del Regolamento UE 679/16 ("GDPR").

Il controllo e la vigilanza sul rispetto delle disposizioni fa capo al Responsabile esterno dei sistemi Informatici, al dipendente che assume la veste di Amministratore di Sistema e al DPO (Responsabile Protezione Dati ai sensi art. 37 del Regolamento UE 6791/6) dell'Azienda.

L'Azienda ha inoltre adottato il presente Regolamento sui sistemi informatici, diretto ad evitare che comportamenti, anche inconsapevoli, possano innescare rischi di commissione di reati o minacce alla sicurezza nel trattamento dei dati, a norma del D.Lgs. 231/01.

In particolare si ricorda a tutti i dipendenti che il D.Lgs 231/2001 prevede specifici reati:

- in materia informatica e di privacy che fanno capo all'art. 24-bis del D.Lgs 231/2001 "Delitti informatici e trattamento illecito di dati";
- in materia di diritto d'autore che fanno capo all'art. 25 novies "Reati in materia di violazione del diritto di autore";
- in materia di pornografia che fanno capo all'art. 25 quinquies "Delitti contro la personalità individuale".

Art. 1 - Accesso al sistema informativo aziendale

All'atto dell'assunzione ogni dipendente dell'Azienda riceve gli strumenti di lavoro essenziali per svolgere la propria mansione e, tra questi, può essere previsto l'uso di personal computer, di apparati telefonici, smartphone/tablet con accesso alla rete internet ed alla posta elettronica.
Per il primo accesso al sistema viene fornita dall'Amministratore di Sistema al dipendente una ID personale ed una password temporanea, che il dipendente avrà compito di modificare tempestivamente.
Ulteriori specifici account (ID utente e password) personali possono essere forniti sempre dall'Amministratore di Sistema e il Responsabile esterno dei sistemi informatici, per l'accesso a siti e banche dati esterne, laddove previsto in base alla mansione svolta.
Ogni assegnazione al dipendente di account per l'accesso a risorse informatiche aziendali o esterne (comprese banche dati), deve essere registrata (ed aggiornata nel tempo) a cura dell'Amministratore di Sistema su segnalazione proveniente dal Responsabile di Area.
E' dato incarico a tutti i responsabili di ambito comunicare tempestivamente eventuali cambi di mansione che comportino modifiche o revoche di autorizzazione all'accesso delle risorse informatiche, sia al Responsabile del trattamento che all'Amministratore di Sistema, per iscritto, al fine di rendere possibili le modifiche dei profili di accesso alle risorse e la sostituzione delle password ove necessario.

Art. 2 - Utilizzo del personal computer

Il Personal Computer affidato al personale è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
Si dispone pertanto che tutto il personale usi la massima cura nella gestione delle apparecchiature informatiche di cui è responsabile e si attenga rigorosamente alle seguenti disposizioni:

1. Le apparecchiature informatiche devono essere utilizzate solo per scopi aziendali e non privati.

2. Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita del Responsabile esterno dei sistemi informatici in quanto sussiste il grave pericolo di violare specifiche leggi in materia di diritto d'autore nonché di importare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore; in particolare, installando programmi cosiddetti "di rete" senza le necessarie verifiche di compatibilità, è possibile compromettere il funzionamento del server, dei database ivi contenuti e/o della rete stessa.
3. Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dall'Amministratore di Sistema dell'Azienda.
   L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D.Lgs. 518/92 sulla tutela giuridica del software, L. 633/1941 s.m.i. Legge sul diritto d'autore, L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore; in merito si precisa che anche il software freeware spesso è tale solo per uso personale e non aziendale e pertanto soggetto a licenza d'acquisto.
4. I Personal Computer e i loro componenti (stampanti, casse, CD software etc.) devono essere custoditi con cura unitamente alla documentazione con cui originariamente sono stati consegnati;
5. La postazione di lavoro e le relative periferiche, quali stampanti locali e di rete, scanner, ecc., devono essere spente al termine dell'attività lavorativa o in caso di assenze prolungate dall'ufficio. Eventuali eccezioni dovranno essere formalmente autorizzate dall'Amministratore di Sistema. Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso; pertanto l'utente, ogni qualvolta si allontani dalla propria postazione, deve procedere al blocco della macchina mediante la pressione contemporanea dei tasti CTRL+ALT+CANC seguita da INVIO. Il ripristino della stessa avverrà soltanto attraverso l'immissione della password di accesso a client;
6. E' assolutamente vietato scaricare da Internet dati, immagini, video e/o programmi non strettamente correlati all'attività lavorativa.
7. E' cura degli utilizzatori provvedere alla archiviazione periodica dei dati (non dei programmi): si sottolinea che i dati sono di proprietà aziendale e non personale e che la perdita degli stessi può causare grave danno all'Azienda la cui responsabilità ricade sull'utilizzatore.
8. Non è consentito all'utente modificare le caratteristiche di sistema (nome computer, indirizzi IP, DNS, Firewall, aggiornamenti automatici SW, etc.) preimpostate sul proprio PC, salvo previa autorizzazione esplicita del Responsabile esterno del sistema informatico.
9. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Amministratore di Sistema nel caso in cui vengano rilevati virus.

Art. 3 – Gestione delle password

Si dispone che l'accesso ai computer, ai programmi (applicativi) o ad eventuali banche dati esterne avvenga solo attraverso l'utilizzo di parole chiavi riservate, le password.
Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non devono contenere riferimenti agevolmente riconducibili all'incaricato. In particolare, si raccomanda di usare, preferibilmente, nella composizione della password almeno un carattere numerico, uno maiuscolo e uno speciale e non basarla su informazioni facilmente deducibili, quali il proprio nome, il nome dei famigliari, la data di nascita, il codice fiscale e simili.
Di seguito alcune regole di gestione delle password personali:

- non permettere ad altri utenti (es. colleghi) di operare con il proprio identificativo utente;
- non trascrivere la password su supporti (es. fogli, post-it) facilmente accessibili a terzi;
- non utilizzare le cosiddette "password di gruppo", ovvero generalizzate per area o mansioni di appartenenza. A questa regola generale può derogarsi solo, per condizioni particolari e specifiche, dietro autorizzazione dell'Amministratore di Sistema previa analisi dei rischi correlati all'utilizzo dei dati.

La segretezza delle password utilizzate deve essere custodita dall'incaricato con la massima diligenza e non divulgata.

La password deve essere immediatamente sostituita, dandone comunicazione al custode delle parole chiave, identificato nell'Amministratore di Sistema, nel caso si sospetti che la stessa abbia perso la segretezza.
È necessario procedere alla modifica della password a cura dell'utente del sistema al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati particolari (sensibili) e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi.

Art. 4 - Utilizzo dei supporti magnetici

Tutti i supporti magnetici riutilizzabili (dischetti, DVD, penne USB, cassette) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.
I supporti magnetici contenenti dati particolari (sensibili) e giudiziari devono essere custoditi in archivi chiusi a chiave.

Art. 5 - Uso della rete internet e dei relativi servizi

Il computer abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa.
È pertanto assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.
È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal Responsabile esterno del sistema informatico.
È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).
È fatto assoluto divieto di navigare in siti, scaricare, scambiare ed utilizzare materiale pornografico o pedopornografico che possa fare incorrere nei reati di pornografia minorile (art. 600-ter codice penale) e detenzione di materiale pornografico (art. 600-quater codice penale) e così ledere all'immagine e reputazione dell'Azienda.
L'impiego di internet per l'accesso a banche dati e siti esterni all'Azienda tramite sistema di autenticazione, deve essere limitato alle persone che ne sono state preventivamente autorizzate ed esclusivamente per le esigenze lavorative. Ogni utilizzo che vada oltre le normali esigenze di ufficio o che possa configurare un rischio di commissione di uno dei reati previsti dall'art. 24 bis (Delitti informatici e trattamento illecito di dati) del D.Lgs 231/01, potrà essere sanzionato.

Art. 6 - Utilizzo di dispositivi portatili

L'utente è responsabile del dispositivo portatile (computer, tablet) assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Ai dispositivi portatili si applicano le regole di utilizzo previste per i Pc connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sugli stessi prima della riconsegna.
I dispositivi portatili utilizzati all'esterno (convegni, attività di lavoro fuori sede), in caso di allontanamento, devono essere custoditi in un luogo protetto.
E' fatto divieto di utilizzo dei dispositivi portatili all'esterno del luogo di lavoro senza la previa autorizzazione del Direttore Generale.

Art. 7 - Uso della posta elettronica

La casella di posta, assegnata dall'Azienda all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
È fatto divieto di utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.
È fatto divieto di utilizzare la posta elettronica aziendale per lo scambio di materiale pornografico o pedopornografico che possa fare incorrere nei reati di pornografia minorile (art. 600-ter codice penale) e detenzione di materiale pornografico (art. 600-quater codice penale) e così ledere all'immagine e reputazione dell'Azienda.

Per quanto riguarda le comunicazioni inviate o ricevute a mezzo e-mail che abbiano contenuti rilevanti o contengano impegni contrattuali o precontrattuali per l'Azienda è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria, anche per quanto concerne l'autorizzazione e la firma del documento stesso.
È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali oppure della posta elettronica certificata (PEC).
È obbligatorio controllare i file attachments di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
È vietato inviare catene telematiche.
Nel caso di accesso da parte dell'Amministratore di Sistema o del Responsabile esterno del sistema informatico nelle caselle di posta elettronica dei dipendenti, è prevista una forma di reindirizzo con avviso alla posta elettronica personale del dipendente, ogni qual volta vi sia un accesso, in modo da rendere edotti e consapevoli gli utenti dell'accesso da parte dell'Amministratore di Sistema, riservandosi di chiedere il motivo dell'accesso.

Art. 8 - Disponibilità dei messaggi di posta elettronica.

Il personale dell'Azienda, in caso di assenza programmata (ad es. per ferie o attività di lavoro fuori sede), deve adottare le misure organizzative idonee ad assicurare la corretta gestione dei messaggi necessari al normale svolgimento dell'attività lavorativa ed alla conseguente continuità della stessa.
L'Azienda mette a disposizione di tutti i lavoratori apposite funzionalità di sistema che consentono di impostare un messaggio di risposta automatica (Out of Office Replay). In caso di assenza programmata, l'utente quindi è tenuto ad attivare i messaggi di risposta automatica che comunicano l'assenza dell'utente e devono contenere i riferimenti (sia elettronici che telefonici) di Uffici e/o utenti cui rivolgersi in caso di necessità.
Nel caso, invece, di eventuale assenza improvvisa e/o prolungata (ad es. per malattia) ed il lavoratore non possa attivare la procedura sopra descritta, l'Azienda si riserva la possibilità di attivare analogo accorgimento, avvertendo gli interessati.
Nel caso in cui si preveda la possibilità che, in caso di assenza improvvisa o prolungata, e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica o di altri dati aziendali che siano nella esclusiva disponibilità del dipendente (es. file.PST.), il Responsabile a cui fa capo l'utente, in qualità di fiduciario, può richiedere all'Amministratore di Sistema che venga effettuato il reset della password dell'utente stesso. Di tale attività deve essere redatto, a cura del suddetto Responsabile di Area, apposito verbale e deve essere informato l'utente interessato alla prima occasione utile in modo tale da metterlo in condizione di cambiare la password.

Art. 9 - Interventi sui sistemi informatici aziendali

Gli interventi sui sistemi informatici aziendali (software e hardware) sono di esclusiva competenza del Responsabile esterno del sistema informatico e delle eventuali società esterne incaricate dall'Azienda.
Ogni richiesta di intervento deve essere formalizzata dagli utenti, tramite il sistema interno di posta, all'Amministratore di Sistema il quale, in base all'urgenza ed alla gravità della segnalazione, allerta il Responsabile esterno del sistema informatico per il relativo intervento.

Art. 10 - Connessioni da remoto

Non sono previste ed ammesse connessioni da remoto ai server aziendali se non per lo svolgimento di operazioni di manutenzione da parte di società esterne, a ciò preventivamente autorizzate, limitatamente all'espletamento delle necessarie attività.
L'autorizzazione, anche temporanea e/o per condizioni particolari, all'accesso ai sistemi informatici da parte del personale aziendale deve essere autorizzato preventivamente dal Responsabile trattamento dati e dal Responsabile esterno del sistema informatico e registrato a cura dello stesso.

Art. 11 - Sicurezza dei dati aziendali e privacy

L'Azienda adotta tutte le adeguate misure tecniche ed organizzative di sicurezza previste dal Regolamento UE 679/16 che ogni dipendente è tenuto a rispettare per la sicurezza del trattamento (art. 32 del Regolamento UE 679/16) dei dati personali e particolari (sensibili, art. 9 del Regolamento UE 679/16) e giudiziari (art. 10 del Regolamento UE 679/16).

É fatto obbligo a ciascun dipendente, Incaricato del Trattamento dei dati, di osservare le disposizioni impartite dal Titolare del Trattamento e dai Responsabili, in conformità con quanto previsto dal Regolamento UE 679/16.
Ogni Sub-Responsabile e Incaricato Autorizzato è tenuto ad osservare tutte le misure di protezione e sicurezza atte ad evitare rischi di distruzione, perdita, accesso non autorizzato o trattamento non consentito.
L'attività di Amministratore di sistema, prevista dalla normativa privacy, viene assegnata formalmente dal Titolare del trattamento dei dati, ad una persona fisica (interna all'azienda) dotato delle esperienze, dei requisiti di capacità ed affidabilità adeguate. Il nominativo viene diffuso all'interno dell'Azienda.

Art. 12 - Attività di verifica

A cura dell'Amministratore di Sistema, del Responsabile esterno del sistema informatico e del DPO (Responsabile Protezione Dati) nominato ai sensi art. 37-38 e 39 del Regolamento UE 679/16, sono periodicamente attivati controlli, almeno su base annuale, anche a campione, al fine di verificare la funzionalità e sicurezza del sistema e garantire l'applicazione del regolamento.
In particolare si rende noto che l'Azienda può attivare sistemi di monitoraggio della navigazione aziendale secondo le previsioni di cui al Provvedimento del Garante Privacy del 1 marzo 2007, effettuando il monitoraggio generalizzato ed anonimo dei log di connessione.
Gli archivi di log risultanti da questo monitoraggio contengono traccia di ogni operazione di collegamento effettuata dall'interno della rete societaria verso Internet.
Eventuali attivazioni di controlli specifici saranno preventivamente comunicate; resta inteso che in caso di anomalie, l'Azienda potrà effettuare verifiche dirette a fini di monitoraggio e controllo delle risorse informatiche, che potranno incidentalmente consentire la conoscibilità dei log di connessione relativi anche ad una sola postazione.
In conformità a quanto previsto dall'atto di nomina dell'Amministratore di Sistema, nei casi in cui si verificano una delle seguenti condizioni:

- prolungata assenza o impedimento dell'incaricato,
- intervento è indispensabile e indifferibile,
- concrete necessità di operatività e di sicurezza del sistema,

l'Amministratore di Sistema può accedere al computer per acquisire i dati necessari al proseguimento dell'attività lavorativa, registrando in apposito verbale le operazioni eseguite.
L'Amministratore di Sistema su propria iniziativa o su richiesta sempre di concerto con il DPO e il Responsabile esterno del sistema informatico, potrà effettuare controlli a campione circa il rispetto di quanto contenuto nel presente regolamento e nel Codice Etico aziendale che ciascun dipendente è tenuto a seguire.
Qualsiasi presunta violazione di dati in ambito di sistemi informatici, dovrà essere tempestivamente comunicata entro 24 ore al DPO dell'Azienda per le valutazioni ai fini dell'eventuale segnalazione data breach al Garante entro 72 ore (art. 33 e 34 del GDPR).

Art. 13 - Cessazione del rapporto di lavoro

In caso di cessazione del rapporto di lavoro, l'utente deve mettere a disposizione dell'Azienda qualsiasi risorsa assegnata, sia le attrezzature informatiche sia le informazioni di interesse aziendale:

- la casella di posta elettronica individuale sarà mantenuta attiva per il tempo strettamente necessario a gestire il passaggio di consegne e concludere eventuali contatti aperti;
- l'utente non può cancellare le informazioni di interesse aziendale presenti sulle postazioni di lavoro e/o sulla rete, senza esplicita autorizzazione del Responsabile;
- qualora l'utente abbia inavvertitamente lasciato sulle postazioni di lavoro e/o sulla rete informazioni di interesse non aziendale, le stesse verranno cancellate senza alcuna responsabilità per l'Azienda.

Il Responsabile si dovrà preoccupare di disattivare tutti gli accessi a siti e banche dati esterne registrate a nome del dipendente comunicando successivamente all'Amministratore di Sistema.

Art. 14 - Sanzioni per inosservanza delle norme

Le presenti istruzioni sono impartite ai sensi delle normative vigenti in materia di privacy ed in conformità al Regolamento UE 679/2016.
L'inosservanza delle stesse da parte dell'incaricato può comportare sanzioni anche di natura penale a suo carico ai sensi delle disposizioni di cui agli articoli 83 e 84 del Regolamento UE 679/16.

Inoltre si fa presente che l'inosservanza del presente regolamento potrebbe configurare violazione del Codice Etico e di Comportamento aziendale e, di conseguenza, essere passibile di sanzioni ai sensi del Regolamento interno del personale e del CCNL di riferimento.

Art. 15 - Aggiornamento e revisione

Tutti i dipendenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dal Direttore Generale di concerto con il DPO, il Responsabile esterno del sistema informatico e l'Amministratore di Sistema ed approvate dal C.d.A.
Il presente Regolamento è soggetto a revisione ogni qual volta se ne presenti la necessità. Di ogni revisione successiva sarà data tempestiva comunicazione a tutti i dipendenti.
Il presente Regolamento entra immediatamente in vigore con l'approvazione da parte del C.d.A.