GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

CAA liberi professionisti s.r.l.
CENTRO AUTORIZZATO ASSISTENZA AGRICOLA

Sede Centrale: Via Carlo Alberto, 30
10123 TORINO (TO) - ITALY
Telefono: 011.541338
Fax: 011.5623332
E-mail: info@caaitalia.it
pec: caaliberiprofessionisti@peccaaitalia.it

Codice di condotta aziendale per tutti i soggetti autorizzati al trattamento dei dati personali

Rev. 25/5/2018

Codice di condotta aziendale per tutti i soggetti autorizzati al trattamento dei dati personali

PREMESSA

Di seguito vengono descritte le principali norme a cui gli incaricati/autorizzati devono attenersi nell'esecuzione dei compiti che implicano un trattamento di dati personali con riferimento agli adempimenti normativi del Regolamento (UE) 2016/679 d'ora in poi chiamato GDPR.

Preliminarmente va evidenziato che, al fine di evitare che soggetti estranei possano venire a conoscenza dei dati personali oggetto del trattamento, l'autorizzato deve osservare le seguenti regole di ordinaria diligenza, nonché tutte le altre ulteriori misure ritenute necessarie per garantire il rispetto di quanto disposto dalla normativa in ambito privacy:

- tutte le operazioni di trattamento devono essere effettuate in modo tale da garantire il rispetto delle misure di sicurezza, la massima riservatezza delle informazioni di cui si viene in possesso considerando tutti i dati confidenziali e, di norma, soggetti al segreto d'ufficio;
- le singole fasi di lavoro e la condotta da osservare devono consentire di evitare che i dati siano soggetti a rischi di perdita o distruzione, che vi possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati stessi sono stati raccolti;
- in caso di allontanamento, anche temporaneo, dalla propria postazione di lavoro si devono porre in essere tutte le misure necessarie affinché soggetti terzi, anche se dipendenti, non possano accedere ai dati personali per i quali era in corso un qualunque tipo di trattamento, sia esso cartaceo sia automatizzato;
- non devono essere eseguite operazioni di trattamento per fini non previsti tra i compiti assegnati dal responsabile del trattamento, ben delineati nel registro/mappature delle attività di trattamento consegnato all'autorizzato;
- devono essere svolte le sole operazioni di trattamento necessarie per il raggiungimento dei fini per i quali i dati sono stati raccolti;
- deve essere costantemente verificata l'esattezza dei dati trattati e la pertinenza rispetto alle finalità perseguite nei singoli casi.

Quanto sopra descritto impone, in altri termini, di operare con la massima attenzione in tutte le fasi di trattamento, dalla esatta acquisizione dei dati, al loro aggiornamento, alla conservazione ed eventuale distruzione.

Nei successivi paragrafi si riportano le norme che gli autorizzati devono adottare sia che trattino dati in formato elettronico sia cartaceo.

ACCESSO AI DATI DALLA POSTAZIONE DI LAVORO

La postazione di lavoro deve essere:

- utilizzata solo per scopi legati alla propria attività lavorativa;
- protetta, evitando che terzi possano accedere ai dati che si sta trattando.

Occorre, inoltre, precisare che è dovere dell'autorizzato al trattamento:

- non utilizzare in Azienda risorse informatiche private;
- non installare alcun software se non preventivamente autorizzati e istruiti dall'Amministratore di sistema/Responsabile del sistema informatico;
- non lasciare sulla scrivania informazioni riservate su qualunque supporto esse siano archiviate (carta, CD, dischetti, pendrive, ecc…);
- richiamare le funzioni di sicurezza del sistema operativo (con la sequenza dei tasti CTRL+ALT+CANC) ed assicurarsi della attivazione della funzione Lock Workstation in caso di abbandono momentaneo del proprio PC;
- non lasciare il computer portatile, smartphone, palmari o tablet aziendali incustoditi sul posto di lavoro (al termine dell'orario lavorativo, durante le pause di lavoro, o durante riunioni lontane dalla propria postazione);
- non utilizzare fax e/o telefono per trasmettere informazioni riservate e personali se non si è assolutamente certi dell'identità dell'interlocutore o del destinatario e se esso non è legittimato a riceverle.

GESTIONE DELLE PASSWORD

Per una corretta gestione delle password, ciascun autorizzato deve aver cura di:

- modificare, alla prima connessione, quella che il responsabile del sistema informatico/amministratore di sistema ha attribuito di default;
- cambiarla alla scadenza (6 mesi per il trattamento di dati comuni, 3 mesi per quelli sensibili/giudiziari) o immediatamente nei casi in cui sia compromessa;
- comporla utilizzando almeno 8 caratteri o, nel caso in cui lo strumento elettronico non lo consenta, con un numero di caratteri pari al massimo consentito;
- usare sia lettere che numeri e almeno un carattere maiuscolo;
- non basare la scelta su informazioni facilmente deducibili quali, ad esempio, il proprio nome, il nome dei propri familiari, le date di nascita, i codici fiscali, ecc.,
- mantenerla riservata e non divulgarla a terzi;
- non permettere ad altri utenti (es. colleghi) di operare con il proprio identificativo utente;
- non trascriverla su supporti (es. fogli, post-it) facilmente accessibili a terzi, né lasciarla memorizzata sul proprio PC;
- salvare le proprie credenziali in un file criptato e proteggerlo con una password (annotata in busta chiusa firmata sui lembi) e consegnarlo al custode delle password. In caso di prolungata assenza o impedimento dell'autorizzato stesso in presenza di circostanze che rendano indispensabile e indifferibile l'intervento per esclusive necessità di operatività e di sicurezza del sistema, in tal caso, il responsabile del trattamento dei dati ne autorizzerà l'uso. L'autorizzato non sarà responsabile dei trattamenti effettuati durante questo periodo e al suo rientro modificherà le sue credenziali di accesso.

ANTIVIRUS

I Personal Computer (PC) in dotazione agli utenti e altri dispositivi portatili (computer portatile, smartphone, palmari o tablet aziendali), pur protetti contro gli attacchi dei virus informatici mediante appositi programmi, rimangono potenzialmente esposti ad aggressioni di virus non conosciuti.
Per ridurre le probabilità del verificarsi di tali attacchi è necessario che vengano osservate le seguenti regole:

- controllare che il programma antivirus installato sia aggiornato periodicamente e sia attivo;
- chiudere correttamente i programmi in uso;
- non aprire, se si lavora in rete, files sospetti e di dubbia provenienza;
- non scaricare o installare applicazioni/software che non siano state preventivamente approvate e autorizzate dal responsabile del sistema informatico o dall'amministratore di sistema;
- verificare con l'ausilio del programma antivirus in dotazione ogni supporto magnetico contenente dati (pendrive, floppy disk o CD-DVD), prima dell'esecuzione dei file in esso contenuti;
- non utilizzare pendrive,CD-DVD o altri supporti elettronici di provenienza incerta;
- porre la necessaria attenzione sui risultati delle elaborazioni effettuate e sulle eventuali segnalazioni anomale inviate dal PC;
- usare correttamente e solo per esigenze di lavoro i servizi di posta elettronica e di Internet;
- non modificare le configurazioni impostate sul proprio PC;
- spegnere il PC al termine della giornata di lavoro;

Alla verifica di un malfunzionamento del PC, che può far sospettare la presenza di un virus, è bene che l'autorizzato al trattamento:

1. sospenda ogni operazione sul PC evitando di lavorare con il sistema infetto;
2. contatti immediatamente il responsabile del sistema informatico;
3. chiuda il sistema e le relative applicazioni.

SALVATAGGIO DEI DATI

Tutti i dati devono essere salvati nelle apposite cartelle del server con l'uso dei software installati sui sistemi, non è consentito salvare dati sul PC locale. Non è consentito fare copie di salvataggio su qualsiasi altro tipo di supporto esterno.

PROTEZIONE DEI SISTEMI INFORMATICI PORTATILI (computer portatile, smartphone, palmari o tablet aziendali)

Un sistema informatico portatile presenta maggiori vulnerabilità rispetto ad una postazione di lavoro fissa.

Fatte salve tutte le disposizioni dei paragrafi precedenti, di seguito vengono illustrate le ulteriori precauzioni da adottare nell'uso dei dispositivi portatili:

- conservare lo strumento in un luogo sicuro alla fine della giornata lavorativa;
- non lasciare mai incustodito il sistema in caso di utilizzo in ambito esterno all'azienda;
- avvertire tempestivamente il responsabile del sistema informatico e il responsabile del trattamento dei dati, che darà le opportune indicazioni, in caso di furto;
- essere sempre ben consapevole delle informazioni archiviate sul portatile il quale è maggiormente soggetto a furto e smarrimento rispetto alla postazione fissa;
- operare sempre nella massima riservatezza quando si utilizza il dispositivo informatico portatile in pubblico: i dati, ed in particolare le password, potrebbero essere intercettati da osservatori indiscreti.

USO DI INTERNET E POSTA ELETTRONICA

Gli strumenti di comunicazione telematica (Internet e Posta elettronica) devono essere utilizzati solo ed esclusivamente per finalità lavorative. Sono vietati comportamenti che possano arrecare danno all'Azienda.
In particolare, l'utente dovrà osservare le seguenti regole:

- è consentita la navigazione internet solo in siti attinenti e necessari per lo svolgimento delle mansioni assegnate;
- non è consentito scaricare software gratuiti (freeware o shareware) prelevati da siti Internet;
- non è consentita la registrazione a siti internet o partecipare a Forum di discussione;
- non è consentito l'utilizzo funzioni di instant messaging o navigazione in social network;
- è vietato aprire e-mail e file allegati di origine sconosciuta o che presentino degli aspetti anomali (quali ad esempio, un mittente o oggetto non chiaro);

- non è consentito rispondere a messaggi provenienti da un mittente sconosciuto o di dubbio contenuto in quanto tale atto assicura al mittente l'esistenza del destinatario;
- è vietato l'utilizzo della posta elettronica per comunicare informazioni riservate, dati personali o dati critici, senza garantirne l'opportuna protezione;
- occorre sempre accertarsi che i destinatari della corrispondenza per posta elettronica siano autorizzati ad entrare in possesso dei dati che ci si appresta ad inviare;
- occorre sempre essere consapevoli che posta elettronica e navigazione internet sono veicoli per l'introduzione sulla propria macchina (e quindi in azienda) di virus e altri elementi potenzialmente dannosi;
- è consentito solo l'utilizzo dei programmi ufficialmente installati;
- è vietato installare autonomamente programmi, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti, di violare la legge sul diritto d'autore non disponendo delle apposite licenze d'uso acquistate dall'ente;
- è vietato modificare le caratteristiche impostate sulle dotazioni od installare dispositivi di memorizzazione, comunicazione o altro (ad esempio masterizzatori, modem, wi-fi o connect card), collegare alla rete aziendale qualsiasi apparecchiatura (ad es. switch, hub, apparati di memorizzazione di rete, ecc), effettuare collegamenti verso l'esterno di qualsiasi tipo (ad es. tramite modem o connect card ecc.) utilizzando un pc che sia contemporaneamente collegato alla rete aziendale (creando così un collegamento tra la rete aziendale interna e la rete esterna);
- al fine di ottimizzare le risorse a disposizione della posta elettronica aziendale e migliorare le prestazioni del sistema si evidenzia che la casella di posta deve essere "tenuta in ordine" cancellando periodicamente o comunque se sono superati i limiti di spazio concessi, documenti inutili o allegati ingombranti.
- va sempre prestata la massima attenzione nell'utilizzo dei supporti di origine esterna (per es. chiavi USB, dischi esterni ecc.), avvertendo immediatamente il responsabile del sistema informatico nel caso in cui siano rilevati virus.
- L'azienda, in caso di assenza improvvisa o prolungata dell'utente o comunque non programmata e per improrogabili necessità di sicurezza o di operatività del

sistema, si riserva, di accedere alla casella di posta elettronica dell'utente assente: per i dettagli si rimanda al paragrafo "Accesso ai dati dell'utente".

Particolari cautele nella predisposizione dei messaggi di posta elettronica.

Nell'utilizzo della posta elettronica ciascun utente deve tenere in debito conto che i soggetti esterni possono attribuire carattere "ufficiale di comunicazione aziendale" alla corrispondenza ricevuta da dipendenti aziendali. Pertanto si deve prestare particolare attenzione agli eventuali impegni contrattuali e precontrattuali contenuti nei messaggi.

La formulazione dei messaggi deve pertanto far uso di un linguaggio appropriato, corretto e rispettoso che tuteli la dignità delle persone, l'immagine e la reputazione dell'Azienda.

L'Azienda formula inoltre le seguenti regole di comportamento a cui gli utenti devono attenersi:

a. conservare le comunicazioni inviate o ricevute, in particolare quelle dalle quali si possano desumere impegni e/o indicazioni operative provenienti dalla committenza;
b. prestare attenzione ai messaggi di posta elettronica ed ai file, programmi e oggetti allegati, ricevuti da mittenti sconosciuti, con testo del messaggio non comprensibile o comunque avulso dal proprio contesto lavorativo. In tali casi gli utenti devono non aprire il messaggio, evitare di aprire gli allegati o cliccare sui "link" eventualmente presenti, segnalare l'accaduto al responsabile del sistema informatico e sotto sua autorizzazione cancellare il messaggio e svuotare il "cestino" della posta
c. evitare comunque di cliccare sui collegamenti ipertestuali dubbi presenti nei messaggi di posta;
d. in caso di errore nella spedizione o ricezione, contattare rispettivamente il destinatario cui è stata trasmessa per errore la comunicazione o il mittente che, per errore, l'ha spedita, eliminando quanto ricevuto (compresi allegati) senza effettuare copia;

e. evitare di predisporre messaggi che contengano materiali che violino la legge sul diritto d'autore, o altri diritti di proprietà intellettuale o industriale.

TRASMISSIONE E RIPRODUZIONE DEI DOCUMENTI

Al fine di prevenire eventuali accessi ai dati aziendali da parte di soggetti terzi non autorizzati, occorre adottare delle cautele nella trasmissione e riproduzione dei documenti contenenti dati personali.
Quando le informazioni devono essere trasmesse telefonicamente occorre essere assolutamente certi dell'identità dell'interlocutore e verificare che esso sia legittimato ad ottenere quanto domandato.
Quando il dato deve essere inviato a mezzo fax, posta elettronica, SMS, ecc. e, in particolar modo, nel caso in cui vengano inviati documenti contenenti dati sensibili occorre:

- prestare la massima attenzione affinché il numero telefonico o l'indirizzo e-mail immessi siano corretti;
- verificare che non vi siano inceppamenti di carta o che dalla macchina non siano presi più fogli e attendere sempre il rapporto di trasmissione per un ulteriore verifica del numero del destinatario e della quantità di pagine inviate;
- nel caso di documenti inviati per posta elettronica accertarsi, prima di confermare l'invio, di avere allegato il file giusto;
- in caso di trasmissione di dati particolarmente delicati è opportuno anticipare l'invio chiamando il destinatario della comunicazione al fine di assicurare il ricevimento nelle mani del medesimo, evitando che terzi estranei o non autorizzati conoscano il contenuto della documentazione inviata.
- Tutti coloro che provvedono alla duplicazione di documenti con stampanti, macchine fotocopiatrici o altre apparecchiature, in caso di copia erronea o non leggibile correttamente, da cui potrebbero essere desunti dati personali, sono tenuti a distruggere il documento mediante apposita macchina "distruggi documenti" o con qualunque altro mezzo che ne renda impossibile la ricostruzione in modo da escludere qualunque possibilità da parte di estranei di venire a conoscenza dei dati medesimi.

ARCHIVI CARTACEI

Tutto il materiale cartaceo contenente dati personali non deve essere lasciato incustodito sulle scrivanie e, a fine lavoro, deve essere riposto in un luogo sicuro. Inoltre, occorre usare la medesima perizia nello svolgimento delle normali quotidiane operazioni di lavoro, per evitare che il materiale risulti facilmente visibile a persone terze o, comunque, ai non autorizzati al trattamento.
In caso di trattamento di dati particolarmente sensibili (condizione di salute, dati giudiziari, ecc.), tutta la documentazione cartacea deve essere conservata in armadi/cassetti chiusi a chiave o stanze chiuse a chiave in caso di allontanamento, anche temporaneo, dalla postazione di lavoro.
L'accesso a tutti i locali aziendali deve essere consentito solo a personale preventivamente autorizzato dalla Titolarità.

ACCESSO AI DATI DELL'UTENTE

L'Amministratore di Sistema e il responsabile del sistema informatico può accedere ai dati trattati dall'utente tramite posta elettronica o navigazione in rete esclusivamente per motivi di sicurezza e protezione del sistema informatico (ad es., contrasto virus, malware, intrusioni telematiche, fenomeni quali spamming, phishing, spyware, etc.), ovvero per motivi tecnici e/o manutentivi e/o di regolare svolgimento dell'attività lavorativa (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware). Fatta eccezione per gli interventi urgenti che si rendano necessari per affrontare situazioni di emergenza e massima sicurezza, il personale incaricato accederà ai dati su richiesta dell'utente e/o previo avviso al medesimo.

Ove sia necessario per garantire la sicurezza, l'assistenza tecnica e la normale attività operativa, il personale incaricato avrà anche la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni.
Lo stesso Amministratore di Sistema e il responsabile del sistema informatico possono, nei casi suindicati, procedere a tutte le operazioni di configurazione e gestione necessarie a garantire la corretta funzionalità del sistema informatico aziendale (ad es. rimozione di file o applicazioni pericolosi).
L'Amministratore di Sistema, in caso di assenza improvvisa o prolungata dell'utente o comunque non programmata e per improrogabili necessità di sicurezza o di operatività del sistema è abilitato ad accedere con le credenziali dell'utente contenute

nel file criptato accessibile tramite apertura della busta password dell'utente che il custode delle password metterà a disposizione. L'utente non sarà responsabile dei trattamenti effettuati durante questo periodo e al suo rientro modificherà le sue credenziali di accesso.

USO DEL CELLULARE PRIVATO DURANTE IL PERIODO DI LAVORO

Il titolare dispone che l'uso del cellulare privato durante il periodo di lavoro è vietato fatte salve le deroghe per motivi che verranno valutati.

CONTROLLI DA PARTE DELLA TITOLARITA'

Con il presente capitolo portiamo all'attenzione degli autorizzati al trattamento la possibilità di questa Azienda di effettuare controlli sulle proprie apparecchiature tecnologiche al fine di preservare la sicurezza informatica dei dati personali in esse contenuti.

A tale proposito si sottolinea che la strumentazione tecnologica/informatica e quanto con essa creato è di proprietà dell'Azienda in quanto mezzo di lavoro. E' pertanto fatto divieto di utilizzo del mezzo tecnologico/informatico e delle trasmissioni interne ed esterne con esso effettuate per fini ed interessi non strettamente coincidenti con quelli dell'Azienda stessa.

Nel rispetto dei principi di pertinenza e non eccedenza, le verifiche sugli strumenti informatici saranno realizzati dall'Azienda nel pieno rispetto dei diritti e delle libertà fondamentali degli utenti e del presente Regolamento.

In caso di anomalie, l'Azienda, per quanto possibile, privilegerà preliminari controlli anonimi e quindi riferiti a dati aggregati nell'ambito di intere strutture lavorative o di sue aree nelle quali si è verificata l'anomalia.

In tali casi, il controllo si concluderà con un avviso ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

In caso di successive, perduranti anomalie, ovvero ravvisandone comunque la necessità, l'Azienda si riserva di effettuare verifiche anche su base individuale, comunque finalizzate esclusivamente alla individuazione di eventuali condotte illecite.

In nessun caso verranno realizzate verifiche prolungate, costanti o indiscriminate, fatte salve le verifiche atte a tutelare gli interessi aziendali.

RESPONSABILITÀ E SANZIONI

L'utente, al fine di non esporre sé stesso e l'Azienda a rischi sanzionatori, è tenuto ad adottare comportamenti puntualmente conformi alla normativa vigente ed alla regolamentazione aziendale.

Gli utenti sono responsabili del corretto utilizzo dei servizi di Internet e Posta Elettronica. Pertanto sono responsabili per i danni cagionati al patrimonio, alla reputazione e alla Committenza.

Tutti gli utenti sono pertanto tenuti ad osservare e a far osservare le disposizioni contenute nel presente Regolamento il cui mancato rispetto o la cui violazione, costituendo inadempimento contrattuale potrà comportare:

- per il personale dipendente oltre che l'adozione di provvedimenti di natura disciplinare previsti dal Contratto Collettivo Nazionale di Lavoro tempo per tempo vigente, le azioni civili e penali stabilite dalle leggi tempo per tempo vigenti;
- per i collaboratori esterni oltre che la risoluzione del contratto le azioni civili e penali stabilite dalle leggi tempo per tempo vigenti.