L'AQUILONE COOPERATIVA SOCIALE
Via Manara Valgimigli, 1 - 24020 Vilminore di Scalve (BG)

POLICY INTERNA AZIENDALE GDPR
ai sensi del Regolamento UE 679/2016
FORMAZIONE DEI SOGGETTI INCARICATI AL TRATTAMENTO DEI DATI
(Regole di condotta ed obblighi in relazione all'uso degli strumenti di lavoro)

1. SEZIONE I –AMBITO DI APPLICAZIONE

1.1. Scopo

La presente si applica a tutti i dipendenti e collaboratori (denominati d'ora in poi: incaricati) di L'AQUILONE COOPERATIVA SOCIALE che utilizzano strumenti informatici (ad esempio PC, laptop, smartphone e tablet).

1.2 Premessa

L'ambito lavorativo porta la nostra azienda a gestire una serie di "**informazioni**", proprie e di terzi, per poter erogare i servizi che le vengono contrattualmente richiesti.

Tali informazioni possono essere considerate, ai sensi del GDPR 679/16, "**dati personali**" quando sono riferite a **persone fisiche** e, per la loro gestione (Trattamento), sia analogica che digitale, è necessario che l'azienda adotti una serie di misure idonee.

Per "**dati analogici**" si intende l'insieme di informazioni su supporto manuale o cartaceo, per "**dati digitali**" invece si intende le informazioni che vengono memorizzate o semplicemente transitano attraverso apparecchiature digitali.

Altre informazioni, pur non essendo "dati personali" ai sensi di legge, sono in tutto e per tutto "**informazioni riservate**", ovvero informazioni tecniche, commerciali, contrattuali, di business o di altro genere per le quali l'azienda è chiamata a garantire la riservatezza per tutela del patrimonio aziendale.

Ai fini di questa policy si specifica, pertanto, che con il termine "**dati**" deve intendersi l'insieme più ampio di informazioni di cui un dipendente o un collaboratore può venire a conoscenza e di cui deve garantire la riservatezza e la segretezza e non solo i "dati personali" intesi a norma di legge.

In linea generale, ogni dato, nell'accezione più ampia sopra descritta, di cui l'incaricato viene a conoscenza nell'ambito della propria attività lavorativa, è da considerarsi riservato e non deve essere comunicato o diffuso a nessuno (anche una volta interrotto il rapporto lavorativo con l'azienda stessa), salvo specifica autorizzazione esplicita dell'azienda.

Anche tra colleghi e collaboratori esterni, è necessario adottare la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l'attività lavorativa richiesta.

La progressiva diffusione delle nuove tecnologie informatiche ed in particolare l'accesso alla rete internet dal computer aziendale espone l'azienda a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa, creando problemi alla sicurezza e all'immagine dell'azienda stessa.

Premesso che i comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, tra i quali rientrano l'utilizzo delle risorse informatiche e telematiche, devono sempre ispirarsi al principio di diligenza e correttezza, l'azienda ha adottato la presente policy interna diretta ad evitare che condotte inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati o delle attrezzature aziendali.

Una gestione dei dati analogici, un uso dei computer e di altri dispositivi elettronici mobili (di seguito device), nonché dei servizi di internet e della posta elettronica, difforme dalle regole contenute nella presente policy potrebbe esporre l'azienda ad aumentare la minaccia di accessi non autorizzati ai dati e/o al sistema informatico aziendale, furti o divulgazioni di informazioni riservate, nonché furti o danneggiamenti del sistema informatico e/o malfunzionamenti in generale dell'intero sistema informatico.

1.3. Finalità del trattamento e base giuridica del trattamento

I dati saranno trattati per le seguenti finalità:

- Gestione degli strumenti regolati dalla presente policy;
- Gestione del rapporto contrattuale in essere con l'interessato e con i connessi obblighi di legge;
- Garantire la sicurezza del sistema informatico aziendale;
- Difendere i diritti dell'interessato e del titolare del trattamento;
- Effettuare controlli permessi dalla presente policy, in particolare il trattamento dei dati degli interessati nell'ambito di controlli con finalità di effettuare verifiche sulla funzionalità e la sicurezza;
- Contrastare l'utilizzo indebito di posta elettronica e internet e dei dispositivi mobili aziendali;
- Accertare eventuali abusi;
- Effettuare indagini riferite a fughe di notizie riservate e confidenziali;
- Effettuare controlli per la tutela del patrimonio aziendale (D.Lgs. 8 giugno 2003 n. 233).

2. SEZIONE II – USO DI STRUMENTI ELETTRONICI

2.1. Utilizzo di Desktop e Laptop

Ricordando che l'incaricato non può utilizzare gli strumenti con finalità diverse dall'attività lavorativa.
È vietato tra l'altro:

- Effettuare download non autorizzati di materiale non attinente all'attività lavorativa;
- Installare software non autorizzati;
- Modificare, in tutto o in parte, eventuali software e le loro configurazioni di aggiornamento;
- Modificare, aggiungere o rimuovere dispositivo hardware e le loro connessioni;
- Disattivare, anche solo temporaneamente, il sistema antivirus;
- Formattare, alterare, manomettere gli strumenti o rendere intellegibili i dati in esso contenuti.

Alla cessazione del rapporto di lavoro i dispositivi che fanno parte degli strumenti di lavoro devono essere restituiti al Titolare del trattamento.

2.2. Accesso alla rete e alle risorse aziendali

L'incaricato non può accedere alle risorse aziendali e alla rete con finalità diverse dall'attività lavorativa.
L'accesso alle stazioni di lavoro sulla rete aziendale è subordinato al possesso di un codice identificativo personale (User_ID), da associare ad una parola chiave (password).
La presenza di un User_ID e di password personali è quindi condizione necessaria per accedere alla rete aziendale per l'attivazione di una postazione di lavoro.
Per definire la qualità della parola chiave (password), si rimanda al contenuto della sezione successiva.

2.3. Antivirus

I virus possono essere trasmessi tramite scambio di file via internet, via mail, tramite scambio di supporti removibili, filesharing e chat. L'azienda impone su tutte le postazioni di lavoro l'utilizzo di un sistema antivirus correttamente installato, attivato continuamente e aggiornato automaticamente con frequenza almeno quotidiana.
L'incaricato, da parte sua, deve impegnarsi a controllare il corretto funzionamento e aggiornamento del sistema antivirus installato sul proprio computer, e, in particolare, deve rispettare le regole seguenti:
1. Comunicare ogni anomalia o malfunzionamento del sistema antivirus;
2. Comunicare eventuali segnalazioni di presenza di virus o file sospetti.
Inoltre, all'incaricato:
1. è vietato accedere alla rete aziendale senza servizio antivirus attivo e aggiornato sulla propria postazione;
2. è vietato ostacolare l'azione dell'antivirus aziendale;
3. è vietato disattivare l'antivirus senza l'autorizzazione espressa dell'azienda, anche e soprattutto nel caso sia richiesto per l'installazione di software sul computer;
4. è vietato aprire allegati di mail provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di mail di persone conosciute ma con testi inspiegabili o in qualche modo strani (SPAM).
Contattare Il Titolare del Trattamento e/o i Responsabili nominati prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra.

3. SEZIONE III – PASSWORD

3.1. Le password

Le password sono un metodo di autenticazione assegnato dall'azienda per garantire l'accesso protetto ad uno strumento hardware oppure ad un applicativo software.
La prima caratteristica di una password è la segretezza, cioè il fatto che non venga svelata ad altri soggetti. La divulgazione delle proprie password o la trascuratezza nella loro conservazione può causare gravi danni al proprio lavoro, a quello dei colleghi e dell'azienda nel suo complesso. Nel tempo anche la password più sicura perde la sua segretezza, per questo motivo è buona norma cambiarle con una certa frequenza.
L'azienda ha implementato alcuni meccanismi che permettono di aiutare e supportare gli incaricati in una corretta gestione delle password, in particolare, per quanto riguarda le password di accesso al Dominio (ove previsto), è in funzione un sistema automatico di richiesta di aggiornamento delle stesse, impostato dall'azienda secondo il livello di sicurezza richiesto dall'azienda stesso e, comunque, in linea con quanto richiesto dalla normativa privacy.
Altra buona norma è quella di non memorizzare la password su supporti facilmente intercettabili da altre persone. Il miglior luogo in cui conservare una password è la propria memoria.
Le password degli incaricati che non vengono utilizzate per un periodo superiore ai sei mesi verranno disattivate.

In qualsiasi momento l'azienda si riserva il diritto di revocare all'Incaricato il permesso di accedere ad un sistema hardware o software a cui era precedentemente autorizzato, rimuovendo user id o modificando/cancellando la password ad esso associata.

3.2. Regole per la corretta gestione delle password

L'Incaricato, da parte sua, per una corretta e sicura gestione delle proprie password, deve rispettare le regole seguenti:

1. Le password sono assolutamente personali e non vanno mai comunicate ad altri;
2. Occorre cambiare immediatamente una password non appena si abbia alcun dubbio che sia diventata poco "sicura";
3. Le password devono essere lunghe almeno 8 caratteri e devono contenere anche lettere maiuscole, caratteri speciali e numeri;
4. Le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, Post-It (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare);
5. Le password devono essere sostituite nei tempi indicati dall'azienda, a prescindere dall'esistenza di un sistema automatico di richiesta di aggiornamento password;
6. In presenza di altri soggetti che possono vedere la tastiera (anche se colleghi), evitare di digitare la propria password;
7. Non lasciare incustodito e accessibile lo strumento elettronico, durante una sessione di trattamento, neppure in ipotesi di breve assenza; le sessioni utente in ogni caso si disattivano in automatico entro 3 minuti di inattività e per riattivare il sistema va introdotta la password;
8. Nei casi di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, potrebbe però rendersi necessario disporre della password dell'incaricato, per accedere agli strumenti ed ai dati. A tale fine, agli incaricati sono state fornite istruzioni scritte, affinché essi scrivano le credenziali su un foglio di carta, da inserire in una busta che deve essere chiusa, sigillata e consegnata a chi custodisce le copie delle parole chiave, il cui nominativo viene loro indicato al momento dell'attribuzione della password;
9. La custodia della copia delle credenziali è organizzata in modo tale da garantirne la relativa segretezza: per questo, viene individuato per iscritto e preventivamente il soggetto incaricato a tale scopo. Solo al verificarsi delle condizioni, sopra esposte, che rendono necessario accedere agli strumenti elettronici, utilizzando la copia della parola chiave, il titolare del trattamento o un responsabile potranno richiedere la busta che la contiene, a chi la custodisce; dell'accesso effettuato provvederanno ad informarla tempestivamente.
10. Modificare la password, con la seguente tempistica:

- immediatamente, al primo accesso e successivamente, almeno ogni 3 (tre) mesi;

In alcuni casi, sono implementati meccanismi che consentono all'Incaricato fino ad un numero limitato di tentativi errati di inserimento della password, oltre ai quali il tentativo di accesso viene considerato un attacco al sistema e l'account viene bloccato per alcuni minuti, in caso di necessità contattare il Titolare.

3.3. Divieto di uso

Al fine di una corretta gestione delle password, l'azienda stabilisce il divieto di utilizzare come propria password:

1. Nome, cognome e loro parti;
2. Username assegnato;
3. Un indirizzo di posta elettronica (e-mail);
4. Parole comuni (in Inglese e in Italiano);
5. Date, mesi dell'anno e giorni della settimana, anche in lingua straniera;
6. Una password già impiegata in precedenza.

3.3.1. Alcuni esempi di password non ammesse

La password ideale deve essere complessa, senza alcun riferimento, ma facile da ricordare. Una possibile tecnica è usare sequenze di caratteri prive di senso evidente, ma con singoli caratteri che formano una frase facile da memorizzare (es.: "NIMzz5DICmm!", Nel Mezzo Del Cammin, più il carattere 5 e il punto esclamativo). Decifrare una parola come questa può richiedere giorni, una come "radar" meno di dieci secondi. Alcuni esempi di password assolutamente da evitare:

1. Se Username = "mariorossi", password = "mario", o ancora peggio, password = "mariorossi";
2. Il nome della moglie/marito, fidanzato/a, figli, ecc. anche a rovescio;
3. La propria data di nascita, quella del coniuge, ecc.;
4. Targa della propria auto;
5. Numero di telefono proprio, del coniuge, ecc.;
6. Parole comuni tipo "Kilimangiaro", "Password", "12345678" (troppo facili), parole banali e/o di facile intuizione, ad es. Security e palindromi (simmetria: radar); esse non possono contenere riferimenti agevolmente riconducibili all'interessato (non solo nomi, cognomi, soprannomi, ma neppure date di nascita proprie, dei figli o degli amici), né consistere in nomi noti, anche di fantasia (pippo, pluto, paperino, pippobaudo…) ripetizioni di sequenze di caratteri (es. abcabcabc);

3.4. La password nei sistemi

Ogni Incaricato può variare la propria password di accesso a qualsiasi sistema aziendale in modo autonomo, qualora il sistema in questione metta a disposizione una funzionalità di questo tipo (Change password), oppure facendone richiesta al Titolare. La password può essere sostituita dal Titolare, anche qualora l'incaricato l'abbia dimenticata.

3.5. Audit delle password

Nell'ambito delle attività riguardanti la tutela della sicurezza della infrastruttura tecnologica, il titolare del trattamento potrebbe effettuare analisi periodiche sulle password degli incaricati, al fine di verificarne la solidità, le policy di gestione e la durata, informandone preventivamente gli stessi.

Nel caso in cui l'audit abbia, tra gli esiti possibili, la decodifica della password, questa viene bloccata e all'Incaricato richiesto di cambiarla.

4. SEZIONE IV – OPERAZIONI A PROTEZIONE DELLA POSTAZIONE DI LAVORO

In questa sezione vengono trattate le operazioni a carico dell'Incaricato e il quadro di riferimento generale per l'esecuzione di operazioni a protezione della propria postazione di lavoro, nel rispetto della sicurezza e dell'integrità del patrimonio aziendale.

4.1. Login e logout

Il "Login" è l'operazione con la quale l'Incaricato si connette al sistema informativo aziendale o ad una parte di esso, dichiarando il proprio Username e Password (ossia l'Account), aprendo una sessione di lavoro. In molti casi è necessario effettuare più login, tanti quanti sono gli ambienti di lavoro (ad es. applicativi web, Intranet), ognuno dei quali richiede un username e una password.

In questi casi, sebbene sia preferibile che ogni utente abbia un suo specifico username e password, l'azienda potrà assegnare un univoco username e password per gruppi di Utenti per l'accesso alla macchina fisica, mentre rimarranno separati ed univoci per l'accesso agli applicativi che contengono dati.

Il "Logout" è l'operazione con cui viene chiusa la sessione di lavoro. Al termine della giornata lavorativa, tutte le applicazioni devono essere chiuse secondo le regole previste dall'applicazione stessa. La non corretta chiusura può provocare una perdita di dati o l'accesso agli stessi da parte di persone non autorizzate.

Il "blocco del computer" è l'operazione con cui viene impedito l'accesso alla sessione di lavoro (tastiera e schermo disattivati) senza chiuderla.

4.2. Obblighi

L'utilizzo dei dispositivi fisici e la gestione dei dati ivi contenuti devono svolgersi nel rispetto della sicurezza e dell'integrità del patrimonio dati aziendale.

L'incaricato deve quindi eseguire le operazioni seguenti:

1. Se si allontana dalla propria postazione dovrà mettere in protezione i suoi strumenti di lavoro, affinché persone non autorizzate non abbiano accesso ai dati protetti;
2. Bloccare il suo PC e i device prima delle pause e, in generale, ogni qualvolta abbia bisogno di allontanarsi dalla propria postazione;
3. Chiudere la sessione (Logout) a fine giornata;
4. Spegnere il PC dopo il Logout.

5. SEZIONE V – INTERNET: MODALITÀ DI UTILIZZO

La capacità di lavorare in una rete di comunicazione estesa e di interloquire tempestivamente con partner, fornitori, risorse informatiche esterne e, in particolare, con clienti è altresì fondamentale. Il collegamento ad Internet è uno strumento di produttività e deve essere utilizzato esclusivamente per realizzare la propria attività in azienda.

Nell'utilizzare il servizio internet è pertanto necessario seguire le regole aziendali sotto riportate:

- Si devono utilizzare solo quei servizi strettamente connaturati all'attività lavorativa svolta, nonché concordati con il proprio responsabile diretto nell'ambito della pianificazione delle attività;
- È vietato l'utilizzo di chat line o di programmi di messaggistica istantanea non autorizzati;
- È vietato l'utilizzo di social network per attività diverse da quelle professionali;
- È vietato l'utilizzo di giochi, anche online;
- Non è ammessa la partecipazione, per motivi non professionali, a forum o affini;
- Ogni accesso viene tracciato dal sistema, tramite username e password di accesso, è in grado di verificare chi ha utilizzato il sistema, in modo da intervenire con sollecitudine in caso di azioni scorrette;
- Gli utenti non hanno la possibilità di manomettere o installare software sul proprio terminale, in quanto non sono loggati come amministratori e tale attività è riservata solo a questi ultimi, le uniche persone abilitate e autorizzate all'installazione, modifica, cancellazione o aggiornamenti dei software sono il titolare del trattamento o personale incaricato da quest'ultimo;

- Per la navigazione in internet è stabilita una politica aziendale e resa nota agli incaricati, in particolare, sono stabiliti quali comportamenti sono considerati illeciti (per esempio, la navigazione su siti pornografici, violenti, illegali, ecc.), il sistema è comunque dotato di un firewall che blocca gli accessi tramite l'immissione di parole chiave e siti non raggiungibili (firewall e router configurati per neutralizzare attacchi DoS (Denial of Service);

6. SEZIONE VI – POSTA ELETTRONICA

Il sistema di posta elettronica è di proprietà del titolare del trattamento e costituisce uno strumento di lavoro dovrà quindi essere utilizzato esclusivamente per l'espletamento delle attività professionali.
Non è consentito:

- L'invio di messaggi e/o allegati non inerenti a scopi professionali, che interferisca con i processi di comunicazione del personale dell'azienda ed interrompa le normali operazioni della rete aziendale;
- La falsificazione e/o modificazione di messaggi e-mail;
- La lettura, la copia o modifica di messaggi e-mail o file di altri utenti senza il loro consenso, sia per ottenere informazioni riservate o violare la loro privacy, sia per approvazione ad intercettazione dei loro messaggi, anche per mezzo di strumenti d'intercettazione audio, registrazioni immagini od ogni altro mezzo di comunicazione;
- L'invio o l'inoltro improprio di "messaggi" del tipo "a catena" o "piramide";
- L'apertura di file di dubbia provenienza senza prima consultare la funzione aziendale dedicata;
- L'invio di messaggi od immagini di natura illegale, offensiva, diffamatoria, inappropriata o con contenuto discriminatorio riguardo genere, età, sesso, inabilità o materiale che promuove molestie sessuali o pornografiche;
- Lo scambio di messaggi di posta elettronica con oggetto e contenuto estraneo all'attività lavorativa;
- L'utilizzo di posta elettronica aziendale per scopi privati.
- Rispondere allo spam, né per protestare, né per "dis-iscrivervi".
  Inoltre verificate di applicare le regole di seguito elencate:
- Date il vostro indirizzo soltanto alle persone strettamente indispensabili, avvisandoli di non darlo a nessuno senza il vostro consenso;
- Non immettete il vostro indirizzo nel browser;
- Non date il vostro indirizzo ai siti che ve lo chiedono, a meno che abbiano una reputazione cristallina;
- Scegliete un nome utente lungo almeno dieci caratteri;
- Usate e fate usare SEMPRE la "copia carbone nascosta" una variante della "copia carbone" che si chiama "copia carbone nascosta" (CCN) o BCC (dalle iniziali dell'equivalente inglese blind carbon copy) ed ha l'immenso pregio di nascondere gli indirizzi dei destinatari. Nessun destinatario vede gli indirizzi degli altri;
- Usate programmi di posta che non visualizzano automaticamente la grafica o che almeno permettono di disattivare questa visualizzazione (questo significa che se qualcuno vi manda un'immagine porno, ve la trovate subito sullo schermo appena aprite la posta, per evitare questo problema è sufficiente usare programmi che non visualizzano le immagini o perlomeno permettono di disattivarne la visualizzazione);
- Se lo spammer è italiano, mandare una diffida piuttosto efficace e, se necessario, procedere alla denuncia.
- Evitare di aderire a catene di Sant'Antonio, prima di spaventarsi, conviene quindi consultare il Sarc (http://www.sarc.com/avcenter/hoax.html), la clinica della Symantec dove vengono analizzati tutti i virus, compresi quelli falsi (hoaxes); Negli altri casi, si possono segnalare i messaggi non richiesti o spamming di virus all'indirizzo abuse@na.nic.it. Le segnalazioni vengono immediatamente ridistribuite ai gestori dei servizi di sicurezza dei vari provider italiani. Sono i provider stessi a prendere provvedimenti nei confronti del loro cliente colpevole di spamming, anche troncandone l'abbonamento.

ALCUNI CONSIGLI ANTI-SPAMMING.

- Caselle riservate: meglio avere 2 indirizzi e-mail, uno serio e uno per lo spamming.
- Cancellazioni: usate il tasto "unsubscribe" per dichiarare che non volete più ricevere messaggi. Non sempre funziona: proprio il fatto che vi siate preoccupati di cancellarvi è un mezzo usato dagli spammer per verificare che il vostro indirizzo sia quello usato davvero.
- Indagini: segnalate lo spammer al suo provider, che spesso è felice di rimuoverlo!
- Consigli: consultate il vostro provider e verificate quali strumenti possiede contro lo spamming. Molti fornitori di e-mail gratuite, infatti, hanno filtri per individuare e scartare i messaggi non richiesti.
- Verificate le proprietà della MAIL CHE VI ARRIVA, è semplice, basta andare sulla mail che vi è arrivata, col pulsante destro cliccate su proprietà, lì vi appare una cosa simile:

Return-Path: <>
Received: from Standard (212.171.144.97) by mail.tiscalinet.it (5.5.025)
id 3AE3F651000B7A87 for ventoi@tiscalinet.it; Thu, 26 Apr 2001 14:20:59 +0200
Date: Thu, 26 Apr 2001 14:20:59 +0200 (added by postmaster@mail.tiscalinet.it)
Message-ID: <3AE3F651000B7A87@mail.tiscalinet.it> (added by postmaster@mail.tiscalinet.it)
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="--VEUNOT6Z0PMJWLM3G1IFW5YJ4P6BW5IV0H"

Bene, quel numerino **212.171.144.97** messo tra parentesi dopo "from Standard", è l'indirizzo IP dell'utente che vi ha mandato la mail, magari anonima…. Per inviare la segnalazione di spamming, o abuso al Provider corretto, si può verificare l'appartenenza dell'IP (gli IP sono tantissimi!!!) presente nell'ultimo received dell'header del messaggio sul sito www.ripe.net selezionando la voce whois, nel risultato della ricerca, generalmente c'è anche l'indirizzo e-mail per comunicazioni relative agli abusi: qui di seguito ve ne elenco alcuni:

abuse@tiscalinet.it - abuse@inwind.it - abuse@tin.it - abuse@libero.it

Per saperne di più si consulta:

Su Internet *http://mail-abuse.org* il sito americano dell'azienda spamming.

Infine in caso di assenza da lavoro per esempio ferie o altri motivi si riporta quanto indicato dalla Corte di Cassazione:
CASS. N. 47096/2007 NON INTEGRA IL REATO DI CUI ALL'ART. 6/6 DEL CODICE PENALE LA CONDOTTA DEL SUPERIORE GERARCHICO che prenda cognizione della posta elettronica contenuta nel PC del dipendente assente dal lavoro, dopo AVER A TAL FINE UTILIZZATO LA PASSWORD in precedenza comunicatagli in conformità al protocollo aziendale.
L'accesso alla posta elettronica aziendale può essere sospeso previa necessaria informazione dell'Interessato
Qualora il rapporto di lavoro con l'interessato cessi per qualsiasi ragione, l'indirizzo di posta elettronica fornito a quest'ultimo verrà immediatamente disattivato: il responsabile di riferimento ha la facoltà di indicare uno o più indirizzi alternativi a cui inoltrare in automatico i messaggi destinati all'interessato (Provvedimento 22, dicembre 2016 – 3.2. Trattamenti effettuati sulla posta elettronica aziendale dopo la cessazione del rapporto di lavoro. Disattivazione account. Con riferimento ai trattamenti effettuati sulla posta elettronica aziendale dopo la cessazione del rapporto di lavoro, come già precisato dal Garante in precedenti occasioni, in conformità ai principi in materia di protezione dei dati personali, gli account riconducibili a persone identificate o identificabili devono essere rimossi previa disattivazione degli stessi e contestuale adozione di sistemi automatici volti ad informarne i terzi ed a fornire a questi ultimi indirizzi alternativi riferiti all´attività professionale del titolare del trattamento. L´interesse del titolare ad accedere alle informazioni necessarie all´efficiente gestione della propria attività, pertanto, deve essere contemperato con la legittima aspettativa di riservatezza sulla corrispondenza da parte dei dipendenti nonché dei terzi [v. provvedimenti 30 luglio 2015, n. 456, doc. web n. 4298277; 5 marzo 2015, n. 136, doc. web n. 3985524 e 27 novembre 2014, n. 551, doc. web n. 3718714]).
Il contenuto degli account di posta elettronica disattivati verrà registrato in un file di backup. Successivamente alla cessazione del rapporto di lavoro, il titolare del trattamento potrà liberamente accedere al contenuto del file di backup, del personale computer e alla casella di posta elettronica assegnata all'interessato durante il rapporto di lavoro, per ragioni di continuità dell'attività, per finalità di sicurezza del sistema informatico e qualora fosse necessario per prevenire o accertare condotte illecite, o comunque ai fini di difendere i diritti del titolare del trattamento.
Il titolare del trattamento non effettuerà trattamenti di dati personali mediante sistemi hardware e/o software che mirino alla lettura sistematica dei messaggi di posta elettronica, dei dati di traffico e delle e-mail, al di là di quanto tecnicamente necessario per svolgere il servizio.
Per motivi di sicurezza delle informazioni e di controllo funzionale del sistema di posta elettronica, il titolare del trattamento effettua operazioni di verifica in maniera statistica sulle funzionalità, sulle prestazioni, sugli utilizzi. Tali verifiche sono condotte nel rispetto dei principi di necessità e di correttezza sanciti dal regolamento UE 679/2016.

7. SEZIONE VII – USO DI ALTRI DEVICE (PERSONAL COMPUTER PORTATILE, TABLET, CELLULARE, SMARTPHONE E DI ALTRI DISPOSITIVI ELETTRONICI)

7.1. L'utilizzo del notebook, tablet o smartphone

Il computer portatile, il tablet e il cellulare (di seguito generalizzati in "device mobile") possono venire concessi in uso dall'azienda agli incaricati che durante gli spostamenti necessitino di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete dell'azienda:

L'Incaricato è responsabile dei device mobili assegnatigli dall'azienda e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai device mobili si applicano le regole di utilizzo previste per i computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna. In particolare i files creati o modificati sui device mobili devono essere trasferiti sulle memorie di massa aziendali al primo rientro in ufficio e cancellati in modo definitivo dai device mobili (Wiping). Sui device mobili è vietato installare applicazioni (anche gratuite), se non espressamente autorizzate dall'azienda. I device mobili utilizzati all'esterno (convegni, visite in azienda, ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto. In caso di perdita o furto dei device mobili, deve far seguito la denuncia alle autorità competenti. A tale scopo, si deve avvisare immediatamente l'azienda che provvederà – se del caso – ad occuparsi delle procedure connesse alla privacy. All'Incaricato è vietato lasciare i device mobili incustoditi e a vista dentro l'auto o in una stanza d'albergo, nell'atrio dell'albergo o nelle sale d'attesa delle stazioni ferroviarie e aeroportuali, anche di giorno, durante l'orario di lavoro, all'Incaricato non è consentito lasciare incustoditi i device mobili.

I device mobili che permettono l'attivazione di una procedura di protezione (PIN) devono sempre essere abilitabili solo con la digitazione del PIN stesso e non possono essere lasciati privi di PIN.

Laddove il device mobile sia accompagnato da un'utenza, l'Incaricato è chiamato ad informarsi preventivamente dei vincoli ad essa associati (es. numero minuti massimo, totale gigabyte dati, …) e a rispettarli. Qualora esigenze lavorative richiedessero requirements differenti, l'Incaricato è tenuto ad informare tempestivamente e preventivamente l'azienda.

In relazione alle utenze mobili, salvo autorizzazione dell'azienda, è espressamente vietato ogni utilizzo all'estero e anche in caso di autorizzazione dell'azienda, gli utilizzi all'esterno devono essere preventivamente comunicati, per permettere l'attivazione di opportuni contratti di copertura con l'operatore mobile di riferimento.

7.2. Memorie esterne (chiavi usb, hard disk, memory card, cd-rom, dvd, ecc.)

Agli incaricati può essere assegnata una memoria esterna (quale una chiave USB, un hard disk esterno, una memory card, …), su cui copiare temporaneamente dei dati per un facile trasporto, o altri usi (es. macchine fotografiche con memory card, videocamere con dvd, …).

Questi dispositivi devono essere gestiti con le stesse accortezze di cui all'articolo precedente e devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnate a terzi.

- Prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti removibili (floppy disk, dischi zip, cd, supporti removibili), nei quali siano contenuti dati personali e/o particolari: per quanto concerne i supporti removibili contenenti dati personali, l'azienda ha ritenuto di estendere tali precetti ai supporti contenenti dati personali di qualsiasi natura, anche comune, prescrivendo agli incaricati del trattamento quanto segue:

1 - I supporti devono essere custoditi ed utilizzati in modo da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti, in particolare, essi devono essere conservati in cassetti chiusi a chiave, durante il loro inutilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi;

2 - Le registrazioni trasferite su supporti rimovibili vengono protette con tecniche crittografiche per proteggere i dati in transito (illeggibili anche in caso di perdita o furto del supporto).

3 - Una volta cessate le ragioni per la conservazione dei dati, si devono in ogni caso porre in essere gli opportuni accorgimenti, finalizzati a rendere i dati contenuti nei supporti non leggibili e non ricostruibili tecnicamente. Tali dati devono quindi essere cancellati, se possibile, e, se necessario per i fini in esame, si deve arrivare a distruggere il supporto.

4 - Ogni estrazione di dati viene effettuata con procedure crittografiche, le tracce digitali, le altre informazioni acquisite e le eventuali copie di sicurezza (backup) vengono conservate in forma cifrata.

5 - In caso di errore comportamentale involontario con conseguente danneggiamento di dati, il titolare del trattamento può recuperare l'originale sulle copie di BK;

7.3. Device personali

Ai dipendenti è permesso l'utilizzo della posta elettronica aziendale sui loro device personali.

In tal caso è necessario che il device abbia password di sicurezza stringenti approvate dall'azienda e l'eventuale furto o smarrimento del device deve essere immediatamente segnalato anche all'azienda per eventuali provvedimenti di sicurezza.

Gli interessati non dipendenti (ovvero i consulenti e collaboratori esterni), possono utilizzare i propri device personali per memorizzare dati dell'azienda solo se espressamente autorizzati dall'azienda stessa e assumendone formalmente e personalmente l'intera responsabilità del trattamento.
Tali device dovranno essere preventivamente valutati dall'azienda, per la verifica della sussistenza di misure minime ed idonee di sicurezza.

7.4. Distruzione dei device

Ogni Device ed ogni memoria esterna affidati agli incaricati (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), al termine del loro utilizzo, dovranno essere restituiti all'azienda, che provvederà a distruggerli o a ricondizionarli, seguendo le norme di legge in vigore al momento.
In particolare l'azienda provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati.

8. SEZIONE VIII – SISTEMI IN CLOUD

8.1. Cloud computing

In informatica, con il termine inglese cloud computing (in italiano nuvola informatica) si indica un paradigma di erogazione di risorse informatiche, come l'archiviazione, l'elaborazione o la trasmissione di dati, caratterizzato dalla disponibilità on demand attraverso Internet, a partire da un insieme di risorse preesistenti e configurabili.
Le risorse non vengono pienamente configurate e messe in opera dal fornitore apposta per l'interessato, ma gli sono assegnate, rapidamente e convenientemente, grazie a procedure automatizzate, a partire da un insieme di risorse condivise con altri utenti lasciando all'interessato parte dell'onere della configurazione. Quando l'interessato rilascia la risorsa, essa viene similmente riconfigurata nello stato iniziale e rimessa a disposizione nel pool condiviso delle risorse, con altrettanta velocità ed economia per il fornitore.
Utilizzare un servizio di cloud computing per memorizzare dati personali o particolari espone l'azienda a potenziali problemi di violazione della privacy. I dati personali vengono memorizzati nei server farms di aziende, che spesso risiedono in uno stato diverso da quello dell'azienda. Il cloud provider, in caso di comportamento scorretto o malevolo, potrebbe accedere ai dati personali per eseguire ricerche di mercato e profilazione degli utenti.
Con i collegamenti wireless, il rischio sicurezza aumenta e si è maggiormente esposti ai casi di pirateria informatica, a causa della minore sicurezza offerta dalle reti senza fili. In presenza di atti illegali, come appropriazione indebita o illegale di dati personali, il danno potrebbe essere molto grave per l'azienda, con difficoltà di raggiungere soluzioni giuridiche e/o rimborsi nel caso in cui il fornitore risieda in uno stato diverso da paese dell'interessato.
Nel caso di industrie o aziende, tutti i dati memorizzati nelle memorie esterne sono seriamente esposti a eventuali casi di spionaggio industriale.

8.2. Utilizzo di sistemi cloud

È vietato agli incaricati l'utilizzo di sistemi cloud non espressamente approvati dall'azienda. Per essere approvati, i sistemi cloud devono rispondere ad almeno i seguenti requisiti:

- Essere sistemi cloud esclusivi e non condivisi;
- Essere sistemi cloud posizionati fisicamente in Italia;
- L'azienda che fornisce il sistema in cloud deve essere preventivamente nominata Responsabile al Trattamento dei dati da parte dell'azienda;
- L'azienda che fornisce il sistema in cloud deve comunicare all'azienda, almeno una volta all'anno, i nominativi degli amministratori di sistema utilizzati;
- Dovranno essere verificate tutte le indicazioni e prescrizioni previste dal Garante della Privacy nei suoi provvedimenti sugli Amministratori di Sistema e sul cloud.

9. SEZIONE IX – GESTIONE DATI ANALOGICI

9.1. Clear desk policy

Gli incaricati sono responsabili del controllo e della custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.
Gli incaricati sono invitati dall'azienda ad adottare una "politica della scrivania pulita". Ovvero si richiede agli Utenti di trattare dati analogici solo se necessario, privilegiando, ove possibile, l'utilizzo degli strumenti digitali messi a disposizione dell'azienda.
I principali benefici di una politica della scrivania pulita sono:
1) Una buona impressione a clienti e fornitori che visitano la nostra azienda;
2) La riduzione della possibilità che informazioni confidenziali possano essere viste da persone non abilitate a conoscerle;

3) La riduzione che documenti confidenziali possano essere sottratti all'azienda.
In particolare, si invita a non lasciare in vista sulla propria scrivania dati analogici quando ci si allontana dalla stessa, oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza dei dati in essi contenuti.
Pc e altri strumenti non devono essere orientati verso utenti esterni;
Prima di lasciare la propria postazione (per esempio per la pausa pranzo o per una riunione), sarà cura degli Utenti riporre in luogo sicuro (armadio, cassettiera, archivio, …) i dati analogici ad esso affidati, affinché gli stessi non possano essere visti da terzi non autorizzati (es. addetti alle pulizie) o da terzi (visitatori) presenti nell'azienda.
A fine giornata deve essere previsto il riordino della scrivania e la corretta archiviazione di tutte le pratiche d'ufficio, in modo da lasciare la scrivania completamente sgombra: non lasciare cartelline/dossier a vista o sulle scrivanie;
La copertina delle cartelline "visibili" devono riportare solamente il nominativo del cliente e non dati personali che saranno indicati al suo interno;
Ove possibile, si invita ad evitare la stampa di documenti digitali, anche ai fini di ridurre l'inquinamento ed il consumo delle risorse in ottica ecologica.
Ove possibile, si invita ad effettuare la scansione dei documenti analogici ed archiviarli digitalmente.
È necessario rimuovere immediatamente ogni foglio stampato da una stampante o da un'apparecchiatura fax, per evitare che siano prelevati o visionati da soggetti non autorizzati.
È buona norma eliminare i documenti analogici attraverso apparecchiature distruggi documenti.

10. SEZIONE X - CONTROLLO

(Art. 4, comma 3, Legge 300/1970, Linee Guida Garante – 1 marzo 2007)

Il titolare del trattamento si riserva la facoltà di effettuare controlli occasionali per verificare l'integrità dei propri sistemi informatici e ai fini di ordinaria valutazione degli stessi. In tale sede si riserva di sollecitare e segnalare eventuali abusi commessi dagli interessati.
Le informazioni memorizzate nel file log verranno trattate esclusivamente da personale con funzione dedicata, appositamente incaricato.
Il titolare del trattamento si riserva pertanto di monitorare i propri sistemi in caso di:

- Necessità di effettuare verifiche sulla funzionalità e sulla sicurezza;
- Constatare l'utilizzo di posta elettronica internet o dei dispositivi mobili aziendali;
- Abusi;
- Indizi relativi a fughe di informazioni confidenziali o riservate.

Nei casi sopra citati, il titolare del trattamento effettua verifiche preventive su informazioni appartenenti a gruppi collettivi di incaricati, tramite attività statistiche aggregate (Linee Guida Garante – 1 marzo 2007, 6.1. Graduazione dei controlli: Deve essere per quanto possibile preferito un controllo preliminare su dati aggregati, riferiti all´intera struttura lavorativa o a sue aree).
Il controllo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e ad istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie, non è di regola giustificato effettuare controlli su base individuale (Linee Guida Garante – 1 marzo 2007, 6.1. Graduazione dei controlli: Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all´area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale).
Il titolare del trattamento si riserva di inoltrare prima avvisi collettivi di diffida dallo svolgere attività non consentite e, successivamente, a seguito di reiterazione di attività segnalate, di attivare controlli individuali sugli strumenti forniti al singolo interessato (per esempio mediante accesso alla memoria di massa del PC, laptop, ecc.).
Tale controllo non può avere ad oggetto un arco temporale eccedente la finalità per il quale il controllo è effettuato.
La direzione dovrà informare preventivamente l'interessato soggetto a tali controlli, salvo il caso in cui una preventiva informativa possa pregiudicare il buon esito delle indagini e la possibilità di difendere i diritti del titolare del trattamento.
Tutte le informazioni relative al controllo, alle sue finalità e alla relativa procedura sono di natura confidenziale e non possono essere rivelate a terzi.
La documentazione redatta all'esito dei suddetti controlli verrà conservata per un tempo necessario in considerazione alle finalità per le quali il controllo è stato effettuato; in ogni caso, nei limiti della prescrizione dei diritti tutelati per mezzo dei controlli effettuati. In caso di indagine da effettuarsi per conto di una Pubblica Autorità, potranno essere effettuati controlli anche secondo differenti modalità e con procedure eventualmente prescritte dall'Autorità. I dati contenuti nei file di log verranno conservati per un periodo di tempo di 6 (sei) mesi, fatto salvo il raggiungimento della massima capienza disponibile. Solo per far fronte a tecniche o di sicurezza, o in caso di difesa di diritto in sede giudiziaria, o ancora nel caso si custodiscano i dati per ottemperare ad una specifica

richiesta delle Autorità, il periodo di conservazione potrà essere prolungato a seconda delle necessità del caso, nel pieno rispetto delle finalità descritte (Linee Guida Garante – 1 marzo 2007, 6.2. Conservazione: I sistemi *software* devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente - attraverso procedure di sovraregistrazione come, ad esempio, la cd. rotazione dei *log file* - i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria. In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all´uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario – e predeterminato – a raggiungerla (*v. art. 11, comma 1, lett. e), del Codice*). Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione: ad esigenze tecniche o di sicurezza del tutto particolari; all´indispensabilità del dato rispetto all´esercizio o alla difesa di un diritto in sede giudiziaria; all´obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell´autorità giudiziaria o della polizia giudiziaria).
L'utilizzo degli strumenti regolati dalla presente policy, la gestione del personale incaricato dal titolare del trattamento degli stessi strumenti e l'applicazione dei controlli potranno comportare trattamento dei dati personali dell'interessato (art. 4, comma 3, Legge 300/1970; art. 12 regolamento UE 679/2016; Linee Guida Garante – 1 marzo 2007: All´onere del datore di lavoro di prefigurare e pubblicizzare una *policy* interna rispetto al corretto uso dei mezzi e agli eventuali controlli, si affianca il dovere di informare comunque gli interessati ai sensi dell´art. 13 del Codice, anche unitamente agli elementi indicati ai punti 3.1. e 3.2.).

11. SEZIONE XI – DISPOSIZIONI FINALI

Quando cessa il rapporto di lavoro, i dati presenti sugli strumenti aziendali dell'interessato e gli strumenti stessi dovranno essere restituiti al titolare del trattamento.
L'interessato si impegna a non conservare copia di tali informazioni, né a comunicarle o diffonderle.
Il mancato rispetto o la violazione delle regole contenute nella presente policy è perseguibile con provvedimento disciplinare previsto dal CCNL di categoria applicabile, ed altresì con azioni civili e penali previste dalle leggi vigenti, qualora si verificassero gli estremi della sussistenza delle responsabilità civili o penali.
Nel caso dei collaboratori (anche occasionali), la violazione delle regole contenute nella presente policy può comportare sanzioni sul piano contrattuale, che possono arrivare anche alla risoluzione del rapporto di lavoro, fatte salve azioni civili e penali previste dalle leggi vigenti, qualora si verificassero gli estremi della sussistenza delle responsabilità civili o penali.

12. SEZIONE XII – VALIDITA', AGGIORNAMENTO E DIFFUSIONE E DISPOSIZIONI FINALI .

12.1. Validità

La presente policy interna aziendale ha validità a partire da: 09/10/2018.
Per quanto non espressamente previsto nella presente policy sarà fatto riferimento alla normativa vigente in materia

12.2. Aggiornamento e Diffusione.

La presente policy interna sarà oggetto di aggiornamento ogni volta che se ne ravvisi la necessità, in caso di variazioni tecniche dei sistemi dell'azienda o in caso di mutazioni legislative.
È fatto obbligo di adeguare i propri comportamenti alle disposizioni previste nella presente policy ed a chiunque competa di osservarla.
Ogni variazione del presente sarà comunicata agli incaricati.

_____
Il Titolare del trattamento dei dati

Data ____/____/____
In data odierna la presente policy interna GDPR composta da n. 12 pagine numerate progressivamente dal n. 1 al 12 è stata consegnata all'Incaricato Sig. _____, che con la firma della presente dichiara di essere stato informato e formato sul contenuto, di averla ricevuta in copia e di averla compresa, impegnandosi ad attuare quanto in essa contenuto fin da subito senza eccezione alcuna è **per ogni richiesta di chiarimento in merito, per l'esercizio dei propri diritti e doveri, si potrà rivolgere al titolare del trattamento.**

_____
Firma della persona incaricata al trattamento