INCOM S.P.A.

MONTECATINI TERME

POLICY AZIENDALE

PER LA SICUREZZA DEI DATI PERSONALI E DEI SISTEMI INFORMATICI

REV. 0.1

(data) 18/03/2022

PREMESSA

Con la presente *"Policy aziendale per la sicurezza dei dati personali e dei sistemi informatici"* (di seguito, per brevità, anche "policy") la Società Incom S.p.A. (di seguito, per brevità, anche "Società") si prefigge lo scopo di determinare criteri di uniformità per tutti i soggetti operanti a qualsiasi titolo all'interno della stessa nella definizione della disciplina afferente all'utilizzo degli strumenti e dei sistemi informatici della Società, al fine di garantire la sicurezza e l'integrità della rete, degli strumenti e dei dati personali trattati attraverso di essi.
Il documento concorre, insieme agli altri adempimenti posti in essere dal Titolare del trattamento, a garantire ed essere in grado di dimostrare la conformità al Regolamento UE 679/2016 (GDPR), così come richiesto ai sensi del suo articolo 24 (principio di *accountability)*, nonché di integrare le misure di sicurezza sotto il profilo organizzativo secondo gli articoli 32 e 29, comma 4, GDPR.

Il modello sarà revisionato e, se necessario, aggiornato, con cadenza almeno annuale.

ISTRUZIONI OPERATIVE

Oltre ai principi e agli obblighi generali già descritti all'interno del proprio atto di nomina come soggetto Designato o Autorizzato al trattamento dei dati personali, ciascun soggetto operante a qualsiasi titolo all'interno della Società dovrà attenersi a quanto di seguito riportato.
Con la presente policy la Società si prefigge lo scopo di determinare criteri operativi di uniformità per tutti i soggetti (siano essi designati o autorizzati al trattamento) operanti a qualsiasi titolo sotto la direzione del Titolare, al fine di garantire la sicurezza e l'integrità dei dati personali di cui la Società è Titolare del trattamento a norma della normativa europea in materia di protezione dei dati

personali (Regolamento UE 679/2016), nonché la sicurezza degli strumenti e dei sistemi informatici e di rete di sua proprietà.

La Società Incom S.p.A. si riserva in ogni caso il diritto di effettuare controlli sui sistemi di rete e informatici volti ad accertare comportamenti illeciti inerenti al patrimonio, alla proprietà e sicurezza dei dati e alla tutela dell'immagine.

DEFINIZIONI

Ai fini di una migliore comprensione dei termini utilizzati nel presente documento, s'intendono:

- «**Dato personale**» (**art. 4, punto 1 e C26-C27-C30 GDPR**): "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

  Dalla definizione si comprende che i principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato.

- «**Dato particolare**» (**artt. 9, comma 1 e 10 GDPR**): si fa riferimento alle categorie particolari di dati di cui all'art. 9, comma 1, (dati che "rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché [...] dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona") all'art. 10 (dati "relativi alle condanne penali e ai reati o a connesse misure di sicurezza") del Regolamento UE 679/2016.

  Mentre i primi (ex 'dati sensibili') possono essere trattati soltanto dietro consenso dell'interessato o qualora si rientri nell'elenco previsto dal legislatore europeo al secondo comma dell'art. 9 Regolamento UE 679/2016, il trattamento dei secondi (ex 'dati giudiziari')

può avvenire soltanto "sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Inoltre, nel caso in cui si rientri nell'elenco di cui all'art. 2-*octies* del codice privacy novellato (D.Lgs 196/2003 così come modificato dal D.Lgs. 101/2018).

- «**Trattamento**» (**art. 4, punto 2, GDPR**): "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".

Dalla definizione appare evidente, dunque, come qualsiasi operazione abbia ad oggetto il dato personale integri la definizione di "trattamento", sia che si tratti di un uso cartaceo che informatico del dato. Nello specifico:

- **Raccolta** dei dati: è la prima operazione e generalmente rappresenta l'inizio del trattamento. Si traduce nell'attività di acquisizione del dato.
- **Registrazione**: memorizzazione dei dati su un qualsiasi supporto, sia cartaceo che informatico.
- **Organizzazione**: classificazione dei dati secondo un metodo prescelto.
- **Strutturazione**: attività di distribuzione dei dati secondi schemi precisi.
- **Conservazione**: mantenere memorizzate le informazioni su un qualsiasi supporto, sia esso cartaceo che informatico.
- **Consultazione**: lettura dei dati personali. Anche la mera visualizzazione dei dati è un trattamento che può rientrare nella definizione in parola.
- **Elaborazione**: attività con la quale il dato personale subisce una modifica sostanziale.
- **Modificazione**: a differenza dell'elaborazione può riguardare anche solo una minima parte del dato personale.
- **Selezione**: individuazione di dati personali nell'ambito di gruppi di dati già memorizzati.
- **Estrazione**: coattività di estrapolazione di dati da gruppi già memorizzati.

- **Raffronto**: operazione di confronto tra dati, sia una conseguenza di elaborazione che di selezione o consultazione.
- **Utilizzo**: attività generica che ricopre qualsiasi tipo di uso dei dati.
- **Interconnessione**: impiego di più banche dati, con riferimento all'uso di strumenti elettronici.
- **Blocco**: conservazione con sospensione temporanea di ogni altra operazione di trattamento.
- **Comunicazione (o cessione)**: fornire la conoscenza di dati personali ad uno o più soggetti *determinati* diversi dall'interessato, dal titolare, dal responsabile e dagli incaricati.
- **Diffusione**: fornire la conoscenza di dati personali a soggetti *indeterminati*, in qualunque forma anche mediante la loro messa a disposizione o consultazione. Si ha diffusione, dunque, anche nel caso di pubblicazione online.
- **Cancellazione**: eliminazione di dati tramite utilizzo di strumenti elettronici.
- **Distruzione**: attività di eliminazione definitiva dei dati.

- «**Titolare del trattamento**» (**art. 4, punto 7, e C74 GDPR**): "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri".

  La norma prevede che sia opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

- «**Designato al trattamento**» (**art. 2-*quaterdecies* D.Lgs 196/2003 così come modificato dal D.Lgs. 101/2018**): secondo l'art. 2-*quaterdecies* del codice privacy novellato, è il soggetto

all'interno dell'organizzazione al quale sono stati attribuiti specifici compiti e funzioni connesse al trattamento dei dati personali da parte del Titolare, sotto la cui autorità opera.

- «**Autorizzato**» **(art. 4, punto 10, GDPR)**: è il soggetto che all'interno dell'organizzazione è stato autorizzato dal Titolare a trattare i dati che sono stati raccolti sotto la responsabilità di quest'ultimo e che, pertanto, come anche riportato al punto 10 dell'art. 4 della normativa europea, rimarranno sotto l'autorità di quest'ultimo.

- «**Data Protection Officer - DPO**» **(o Responsabile per la Protezione dei Dati – RPD) (art. 37 e C97 GDPR)**: È una nuova figura introdotta dall'art. 37 del Regolamento generale sulla Protezione dei Dati, che al comma 1 determina i casi in cui la sua nomina si rende obbligatoria. In tutti gli altri casi è facoltativo.

  Il DPO, che può essere una figura interna o esterna all'organizzazione, deve godere in ogni caso di assoluta autonomia e indipendenza nell'ambito dello svolgimento delle sue attività ed essere connotato da una spiccata conoscenza della normativa (art. 38 GDPR).

  I suoi compiti principali consistono in **un generale dovere di sorveglianza rispetto alla *compliance* della normativa; in un dovere di consulenza e informazione nei confronti del Titolare, del responsabile, dei dipendenti e, più in generale degli interessati; infine, un dovere di assistenza al Titolare in caso di redazione della valutazione d'impatto e della consultazione preventiva, così come una cooperazione con l'Autorità di controllo (art. 39 GDPR)**.

- «**Terzo**» **(art. 4, punto 10, GDPR)**: "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile".

- «**Violazione dei dati personali**» **(art. 4, punto 12, e C85 GDPR)**: "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

INCOM S.P.A.

MONTECATINI TERME

UTILIZZO DEI DISPOSTIVI ELETTRONICI AZIENDALI E PERSONALI

Il Personal Computer (di seguito, per brevità, anche "PC"), il laptop, lo smartphone, il tablet (d'ora in poi anche "dispositivi"), affidato dalla Società a ciascun soggetto operante a qualsiasi titolo all'interno della stessa è uno strumento di lavoro.

Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, ai sensi dell'art. 32 Regolamento UE 679/2016 in materia di protezione dei dati personali, minacce alla sicurezza dei dati trattati.

I dispositivi sopra riportati vanno considerati come strumenti di esclusiva pertinenza della Società e la sua assegnazione è funzionale al corretto svolgimento delle attività inerenti al rapporto professionale o di lavoro o di collaborazione, non essendone in nessun caso consentito l'utilizzo per finalità private.

L'accesso ai dispositivi sarà protetto da una password che, al di là dei casi connessi all'attività lavorativa, sarà nota soltanto al lavoratore o collaboratore affidatario della postazione informatica e/o del dispositivo. La password dovrà essere custodita con la massima diligenza e non potrà essere divulgata a soggetti terzi.

L'eventuale smarrimento della password da parte del lavoratore o collaboratore affidatario dovrà essere comunicato tempestivamente al Titolare, in modo da consentire la celere modifica della parola chiave.

Salvo ragioni di lavoro e dietro espressa autorizzazione della Società, non è consentito installare autonomamente programmi o applicazioni provenienti dall'esterno, onde evitare il grave pericolo di portare minacce informatiche e di alterare la stabilità dei dispositivi e/o delle loro applicazioni.

Non è consentito l'uso di programmi o applicazioni diverse da quelle distribuite e installate sui dispositivi, salvo diversa autorizzazione da parte del Titolare del trattamento. L'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con i software esistenti, può esporre a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software, che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

Salvo ragioni di lavoro, non è consentito all'utente modificare le caratteristiche impostate sui dispositivi messi a disposizione.

Il PC fisso deve essere spento ogni sera prima di lasciare il luogo di lavoro.

Sede legale e amm.va: VIA ROMA N. 47 –51018 PIEVE A NIEVOLE (PT) TEL. +39 0572 7771 FAX +39 0572 777442 CAP. SOC. € 10.000.000,00 I.V.
PARTITA IVA: 00286820972 – IT 00286820972 R.E.A. Pistoia N. 98863 – N.ISC.REG.IMP.PISTOIA e C.F. 03076400484
www.incomitaly.com email: incom@incomitaly.com PEC: incom_cert@legalmail.it Codice Identificativo: ISHDUAE

Non è consentita l'installazione sui dispositivi di nessun supporto rimovibile personale che non sia stato sottoposto al vaglio del Titolare. Inoltre, è vietato salvare dati non riconducibili all'attività lavorativa.

Il PC è protetto da software antivirus aggiornato. Ogni soggetto operante a qualsiasi titolo all'interno della Società deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico della Società mediante virus o mediante ogni altra minaccia informatica. Nel caso di attacco informatico o sospetti malfunzionamenti dei dispositivi occorrerà avvertire immediatamente il soggetto responsabile dei sistemi informatici, sospendendo ogni attività in corso. Il soggetto responsabile dei sistemi informatici potrà accedere ai dispositivi ogniqualvolta si renda necessario il suo intervento (ad esempio per la soluzione dei problemi di natura tecnica).

Non è consentito portare fuori dai locali aziendali pc o altri dispositivi elettronici aziendali senza previa autorizzazione da parte del Titolare. In ogni caso resta in capo al soggetto designato/autorizzato il dovere di porre la necessaria attenzione e adottare le misure affinché si evitino intrusioni, manomissioni, appropriazioni indebite o accessi non autorizzati, in modo da garantire la conservazione lecita dei dati contenuti in detti dispositivi. In caso di perdita, distruzione, furto, tentativi di furto, accessi non autorizzati e in ogni altra ipotesi di *data breach* che si dovessero verificare, il soggetto designato/autorizzato dovrà porre all'attenzione del Titolare l'evento nel più breve termine possibile e comunque entro e non oltre 24 ore dal momento di avvenuta conoscenza.

Anche nell'ambito dell'utilizzo di un dispositivo personale (c.d. BYOD – *Bring Your Own Device*), il dipendente o collaboratore dovrà conservare i dati afferenti all'attività lavorativa con diligenza e in modo da garantirne la riservatezza, prevendendo che sul dispositivo siano presenti misure di sicurezza adeguate (es. password, antivirus, etc.) a prevenire il rischio di accessi non autorizzati o di attacchi informatici. In caso di smarrimento del proprio dispositivo o di malfunzionamenti tali da coinvolgere l'integrità e la sicurezza dei dati personali connessi all'attività lavorativa *ivi* contenuti, dovrà prontamente darne comunicazione al Titolare.

In alcun modo il Titolare potrà avere accesso a file o informazioni contenute all'interno del dispositivo e non inerenti all'attività lavorativa.

NAVIGAZIONE INTERNET

I dispositivi assegnati al singolo dipendente, collaboratore o professionista ed abilitati alla navigazione internet costituiscono uno strumento utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa.

È assolutamente proibita la navigazione in internet sui siti diversi da quelli strettamente legati all'attività lavorativa.

Fermo restando le ragioni di utilizzo connesse all'attività lavorativa, a titolo meramente esemplificativo e non esaustivo, non sarà consentito:

- Il *download* o l'*upload* di software gratuiti (freeware) e shareware, senza autorizzazione e senza aver effettuato una preventiva verifica con il soggetto responsabile dei sistemi informatici;
- L'utilizzo di documenti provenienti da siti *web* se non strettamente attinenti all'attività lavorativa e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il soggetto responsabile dei sistemi informatici);
- L'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di *remote banking*, acquisti *on-line* e simili, fatti salvi i casi connessi all'attività lavorativa;
- Il *download* e il salvataggio di contenuti audio o video non attinenti alla propria attività lavorativa;
- La registrazione a siti non attinenti all'attività lavorativa;
- La partecipazione a siti di messaggistica istantanea, a *forum* o a *blog* non connessi all'attività lavorativa;
- L'accesso a caselle *webmail* di posta elettronica personale;
- La visione, il *download* o l'*upload* di materiale di natura indecorosa, oltraggiosa o scandalistica;
- La condivisione di documenti personali tramite *cloud*;
- L'accesso e l'utilizzo di *social network* non connessi in alcun modo all'attività lavorativa;
- La condivisione o la diffusione online, se non connessa all'attività lavorativa, di archivi o altre risorse informatiche della Società.

La Società si riserva la facoltà di individuare categorie di siti web ai quali limitare l'accesso e altresì di impedire il *download* o l'*upload* di *file* o *software* aventi particolari caratteristiche (dimensionali

o di tipologia di dato), in quanto in alcun modo non necessari all'attività lavorativa dei dipendenti, collaboratori o professionisti.

L'accesso alla rete della Società a fini personali mediante il proprio dispositivo personale (es. PC, *smarthphone* o *tablet* personale) potrà avvenire soltanto collegandosi alla rete wifi "ospiti".

UTILIZZO DELLA POSTA ELETTRONICA

L'utilizzo della casella di posta elettronica (sia essa nominativa o meno) assegnata al soggetto operante a qualsiasi titolo all'interno della Società è consentito esclusivamente per l'espletamento dell'attività di lavoro, essendone pertanto assolutamente vietato l'utilizzo per scopi personali.

Le persone assegnatarie delle caselle di posta elettronica saranno considerate responsabili del corretto utilizzo delle stesse.

Ogni casella di posta elettronica dovrà essere dotata di una password la quale, al di là dei casi connessi all'attività di lavoro, sarà conosciuta esclusivamente dal lavoratore o collaboratore affidatario della casella di posta elettronica aziendale. Quest'ultima dovrà essere custodita con la massima diligenza e soprattutto non potrà essere divulgata.

L'eventuale smarrimento della password da parte del soggetto affidatario dovrà essere comunicato tempestivamente al soggetto responsabile dei sistemi informatici, in modo da consentire la celere modifica della parola chiave.

Nel caso della ricezione di una email sospetta (sotto il profilo, ad esempio, del mittente o del contenuto), occorrerà non aprire eventuali allegati, non fornire risposta e segnalare tempestivamente la mail al soggetto responsabile dei sistemi informatici.

Inoltre, il soggetto, al di là dei casi connessi all'attività lavorativa, non potrà utilizzare la posta elettronica per:

- L'invio e/o la ricezione di allegati contenenti filmati o brani musicali (es. *mp3*);
- L'invio e/o la ricezione di messaggi personali legati, ad esempio, alla partecipazione a dibattiti su forum, aste *on line*, concorsi, o mailing-list;
- L'invio di messaggi personali legati alla partecipazione a catene telematiche (o di Sant'Antonio); peraltro, laddove i dipendenti o collaboratori dovessero ricevere messaggi di tale tipo, correrà l'obbligo di comunicarlo immediatamente al soggetto responsabile dei sistemi informatici: non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi o a fornire una risposta;

Sede legale e amm.va: VIA ROMA N. 47 – 51018 PIEVE A NIEVOLE (PT) TEL. +39 0572 7771 FAX +39 0572 777442 CAP. SOC. € 10.000.000,00 I.V.
PARTITA IVA: 00286820972 – IT 00286820972 R.E.A. Pistoia N. 98863 – N.ISC.REG.IMP.PISTOIA e C.F. 03076400484
www.incomitaly.com email: incom@incomitaly.com PEC: incom_cert@legalmail.it Codice Identificativo: ISHDUAE

• L'invio, in nessun caso, di messaggi dal contenuto indecoroso e/o oltraggioso.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

È possibile, nei periodi di assenza (es. ferie o festività), impostare un messaggio di risposta automatica.

È obbligatorio porre la massima attenzione nell'apertura dei file *attachements* di posta elettronica prima del loro utilizzo (non eseguire *download* di file eseguibili o documenti da siti *Web* o *Ftp* non conosciuti.

Nel caso di invio a più destinatari all'esterno dell'organizzazione, è fatto obbligo l'utilizzo del campo CCN.

In particolare, si raccomanda ad ogni professionista, collaboratore o dipendente di seguire pedissequamente le indicazioni che eventualmente riceverà, anche via mail, sulle cautele da utilizzare nell'uso delle mail, nelle aperture delle stesse (raccomandazioni, alert, comunicazioni, etc).

Ogni soggetto operante all'interno della Società non dovrà aprire le mail provenienti da indirizzi sconosciuti o da indirizzi conosciuti ma che nascondono nel mittente false mail e che possano contenere allegati infetti. In generale in caso di dubbio circa la provenienza il soggetto operante all'interno della Società non potrà e non dovrà aprire la mail, ma valutare con il Responsabile IT la sua pericolosità.

In calce alla firma, all'interno della propria casella di posta elettronica, ogni comunicazione dovrà riportare il seguente disclaimer:

Le informazioni contenute in questa comunicazione sono riservate e destinate esclusivamente alla/e persona/e o all'ente sopra indicata/e. È vietato ai soggetti diversi dai destinatari qualsiasi uso, copia, diffusione di quanto in esso contenuto sia ai sensi dell'art. 616 c.p., che ai sensi del Regolamento UE 679/2016 e del D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018. Se questo messaggio Vi è pervenuto per errore, Vi preghiamo di non leggerlo, comunicarcelo rispondendo a questa mail o telefonandoci e cancellarlo dal Vostro sistema.

Il soggetto responsabile dei sistemi informatici potrà accedere alla casella di posta aziendale affidata al dipendente, collaboratore o professionista, ogniqualvolta si renda necessario il suo intervento (ad esempio per la soluzione dei problemi di natura tecnica).
Le comunicazioni che dovessero giungere dopo la cessazione del rapporto di lavoro verranno deviate verso un diverso indirizzo di posta elettronica aziendale per la gestione della corrispondenza aziendale attraverso l'adozione di sistemi automatici volti ad informare terzi ed a fornire a questi ultimi indirizzi alternativi, per un periodo di tempo a discrezione di Incom S.p.a. stessa.
Le email del dipendente cessato (sia quelle in entrata che in uscita) saranno conservate da Incom S.p.a. all'interno dei propri server aziendali per motivi di legge e per dare esecuzione ad eventuali obblighi contrattuali o per la difesa in giudizio con strumenti adeguati di protezione dei dati personali. Nello specifico l'accesso sarà protetto mediante credenziali di accesso note solo al Titolare e a soggetti autorizzati della funzione coperta dall'ex dipendente.

UTILIZZO DEL TELEFONO AZIENDALE

Il telefono aziendale (fisso e/o portatile oppure tablet con scheda SIM) eventualmente affidato all'utente è uno strumento di lavoro. L'uso del telefono è consentito esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti all'attività lavorativa stessa. Qualora venisse assegnato un cellulare aziendale al soggetto, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare aziendale si applicano le medesime regole sopra previste per l'utilizzo del telefono fisso aziendale: in particolare è vietato l'utilizzo del dispositivo messo a disposizione per inviare o ricevere messaggi di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa. Non è consentito scaricare sul dispositivo programmi o app non espressamente autorizzate dal Titolare.

UTILIZZO E CONSERVAZIONE DEI SUPPORTI RIMOVIBILI

Tutti i supporti rimovibili (es. CD, HDD esterni, *per drive*, etc.) contenenti informazioni legate all'attività lavorativa o al *know-how* della Società, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

Il soggetto resterà, in ogni caso, responsabile della custodia dei supporti e delle informazioni *ivi* contenute.

Salvo ragioni di servizio, è assolutamente vietato l'utilizzo di supporti rimovibili personali.

Ogni supporto rimovibile di provenienza esterna dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus o un funzionamento sospetto, dovrà essere prontamente fatto verificare dal soggetto responsabile dei sistemi informatici.

Nel caso di utilizzo di supporti rimovibili all'esterno della Società (es. convegni o visite presso i clienti) il dipendente, collaboratore o professionista, dovrà far particolare attenzione alla rimozione del supporto, onde evitare la perdita dei dati o un accesso non autorizzato agli stessi.

Come già espresso con riferimento ai pc e ai dispositivi elettronici aziendali, anche per i supporti rimovibili aziendali è fatto obbligo al soggetto designato/autorizzato richiedere l'autorizzazione al Titolare per utilizzare gli stessi al di fuori dei locali aziendali. In ogni caso resta in capo al soggetto designato/autorizzato il dovere di porre la necessaria attenzione e adottare le misure affinché si evitino intrusioni, manomissioni, appropriazioni indebite o accessi non autorizzati, in modo da garantire la conservazione lecita dei dati contenuti in detti supporti. In caso di perdita, distruzione, furto, tentativi di furto, accessi non autorizzati e in ogni altra ipotesi di *data breach* che si dovessero verificare, il soggetto designato/autorizzato dovrà porre all'attenzione del Titolare l'evento nel più breve termine possibile e comunque entro e non oltre 24 ore dal momento di avvenuta conoscenza.

STAMPANTI E FOTOCOPIATRICI

L'utilizzo dei suddetti strumenti deve avvenire sempre per lo svolgimento dell'attività lavorativa. Non è consentito un utilizzo per fini diversi o privati, salvo una specifica autorizzazione da parte di Incom S.p.A.

È richiesta una particolare attenzione quando si invia sulla stampante condivisa documenti di natura riservata per evitare che persone non autorizzate possano venirne a conoscenza. Si richiede quindi di evitare di lasciare le stampe incustodite e ritirarne immediatamente le copie non appena uscite dalla stampante.

Quando si esegue la scansione di documenti riservati, si raccomanda di fare attenzione affinché questi non siano depositati, anche per poco tempo, in aree di rete a cui possono accedere persone non autorizzate.

INOSSERVANZA

L'inosservanza della presente policy e/o trasgressione alle norme del contratto di lavoro potrebbe comportare l'applicazione dei provvedimenti disciplinari previsti dal contratto nazionale applicato e attualmente in vigore.

Incom S.p.A.