ISTRUZIONI OPERATIVE INCARICATI DEL TRATTAMENTO

SOMMARIO

PREMESSA

Il presente documento contiene le istruzioni operative per gli Incaricati del trattamento dei dati personali dell'Azienda M8 S.R.L., conformemente al Regolamento (Ue) 2016/679 (GDPR). Vi sono contenute:

- Le regole comportamentali da seguire per evitare e prevenire condotte suscettibili di determinare l'insorgenza di rischi per i diritti e le libertà delle persone fisiche cui si riferiscono i dati personali oggetto dei trattamenti effettuati nello svolgimento delle attività lavorative ad opera degli individui designati quali incaricati al trattamento nell'organigramma aziendale (I dipendenti, i collaboratori, i consulenti, i volontari ed in generale tutte le persone autorizzate ad accedere ai dati personali e preposte allo svolgimento delle operazioni di trattamento relativa ai dati).
- La illustrazione del funzionamento delle misure di sicurezza adottate nelle attività di trattamento, di natura logica ed organizzativa, volte a scongiurare episodi di violazione dei dati personali trattati, nonché a tutelare la sicurezza del sistema informativo e del complesso delle risorse dell'Azienda.

1) DEFINIZIONI

Secondo la normativa in materia di privacy, anche di carattere tecnico, ed in particolare il Regolamento (Ue) 2016/679 (GDPR), e si definisce:

- "Dato personale": 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;
- "Trattamento": 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;

2) "Violazione dei dati personali": 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.

2) DOVERI GENERALI

In generale: Ciascun "Incaricato al trattamento" deve procedere alle operazioni prescritte in osservanza dei principi generali del Regolamento (Ue) 2016/679 (GDPR) ed effettuare i trattamenti di dati personali di attribuita competenza

attenendosi scrupolosamente alle presenti istruzioni, unitamente ad ogni ulteriore indicazione inequivocabile, anche verbale, che potrà essere fornita dal "Titolare del trattamento" o dal "Responsabile del trattamento", senza modificare i trattamenti esistenti o introdurre nuovi trattamenti in assenza di esplicita autorizzazione di questi ultimi.
In particolare l'incaricato deve osservare riferimento ai doveri di

- agire in modo lecito e secondo correttezza, procedendo alle operazioni di raccolta e registrazione dei dati per scopi determinati, espliciti e legittimi;
- utilizzare gli strumenti aziendali per accedere ai dati ai dati oggetto di trattamento unicamente nel rispetto del proprio profilo di autorizzazione, solamente per finalità compatibili all'esecuzione delle mansioni o dei compiti affidati;
- accedere ai soli dati strettamente necessari all'esercizio delle proprie funzioni e competenze;
- osservare criteri di riservatezza e l'obbligo di segretezza, ove imposto dal superiore gerarchico, e conseguentemente rispettare eventuali divieti di diffusione dei dati trattati nel corso dell'incarico svolto;
- procedere alla comunicazione dei dati solamente a soggetti legittimati quali destinatari individuati in conformità alle predeterminate operazioni dei trattamenti;
- custodire e controllare i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
- informare il responsabile in caso di incidente di sicurezza che coinvolga dati personali, e segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze che possano migliorare lo svolgimento delle operazioni affidate;
- rispettare le misure di sicurezza di natura logica, organizzativa e tecnica adottate dall'Azienda, le cui prescrizioni e specifici divieti sono illustrate nei paragrafi seguenti;

3) MODALITÀ OPERATIVE DEI TRATTAMENTI

Le principali operazioni degli incaricati del trattamento sono:

- identificazione dell'interessato:

al momento della raccolta dei dati personali, qualora sia necessario individuare l'identità del soggetto che fornisce le informazioni, è obbligatorio richiedere un documento di identità o di riconoscimento, al fine di verificare la identità e di procedere correttamente alla raccolta e alla registrazione delle informazioni;

- verifica del controllo dell'esattezza del dato e della corretta digitazione:

al momento della registrazione dei dati raccolti, occorre prestare attenzione alla digitazione e all'inserimento dei dati identificativi e degli altri dati riferiti all'interessato, al fine di evitare errori, che potrebbero generare problemi nella corretta gestione dell'anagrafica e nello svolgimento delle operazioni, che caratterizzano il processo di trattamento;

- comunicazione dei dati personali ai destinatari previamente individuati in conformità ai protocolli aziendali vigenti, ed alle istruzioni espressamente impartite dai superiori gerarchici rivestenti la qualità di responsabile del Trattamento.

4) ISTRUZIONI PER I TRATTAMENTI CON USO DI STRUMENTI INFORMATICI E PROCEDURE DI GESTIONE

Come principio generale, sia i dispositivi di memorizzazione del proprio PC sia le unità di rete, devono contenere informazioni strettamente professionali e non possono essere utilizzate per scopi diversi (immagini, video e documenti personali).
Di seguito in riferimento ai diversi strumenti informatici impiegati per il trattamento dati, sono riportate le procedure di:

a) GESTIONE DEGLI STRUMENTI ELETTRONICI (pc fissi e portatili)

Ciascun incaricato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card).
In nessun caso gli incaricati devono procedere alla installazione di hardware e software, né alla modifica dei parametri di configurazione, che sono riservate all'Amministratore di Sistema
Si devono adottare le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei all'organizzazione o non specificamente autorizzati.
Prescrizioni per la gestione della sessione di lavoro sul pc (fisso e portatile):

- al termine delle ore di servizio, l'Incaricato deve spegnere il PC a meno che non stia svolgendo elaborazioni particolari. In tal caso gli uffici debbono tassativamente essere chiusi a chiave;
- in caso di interruzione del lavoro, anche temporanea, che comporta l'allontanamento anche solo momentanea dalla propria postazione, l'Incaricato deve accertarsi che i dati trattati non siano accessibili a terzi non

autorizzati, e pertanto chiudere l'eventuale sessione di lavoro aperta sul PC facendo Logout, oppure in alternativa deve avere attivo un salvaschermo (screen- saver) protetto dalle credenziali di autenticazione;

- lo screen-saver deve essere utilizzato con le seguenti prescrizioni:
- Non deve mai essere disattivato;
- Il suo avvio automatico deve essere previsto non oltre i primi 10 minuti di inattività del PC;
- Deve essere messo in funzione manualmente ogni volta che si lascia il PC incustodito ed acceso;
- la stampa di un documento contenente dati personali, deve effettuarsi evitando l'accesso a soggetti non abilitati al trattamento, per cui occorre ritirare tempestivamente i documenti stampati, in particolare su una stampante condivisa.

Per l'utilizzo dei PC portatili valgono le regole elencate per i PC connessi alla rete, con le seguenti ulteriori raccomandazioni:

- prima della riconsegna, rimuovere eventuali file ivi elaborati;
- quando il PC portatile è nei locali dell'Azienda, non lasciarlo mai incustodito; in caso di brevi assenze assicurarlo alla scrivania o ad elementi "sicuri" dell'arredamento (maniglie, intelaiature…), oppure riporlo all'interno di elementi di arredo dotati di serratura (cassetti, armadi) e debitamente chiusi;
- quando il PC portatile è all'esterno dell'Azienda, evitare di lasciarlo incustodito;
- per assenze prolungate, anche qualora l'ambiente venga ritenuto "affidabile", è necessario custodire il portatile in modo opportuno es. cassaforte;
- in caso di furto di un portatile è necessario avvertire tempestivamente l'Amministratore di Sistema, onde prevenire possibili intrusioni ai sistemi aziendali;
- in caso di viaggio aereo trasportare tassativamente il portatile come bagaglio a mano;
- eseguire periodicamente salvataggi dei dati e non tenere tali backup insieme al PC portatile.

b) GESTIONE DELLE CREDENZIALI DI AUTENTICAZIONE

L'accesso alle applicazioni informatiche utilizzate dagli strumenti elettronici impiegati per le operazioni di trattamento dei dati personali è consentito solamente agli Incaricati in possesso di "credenziali di autenticazione", che permettano cioè il superamento di una procedura di autenticazione.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Incaricato (user-id) associato ad una parola chiave riservata (password), oppure in un dispositivo di autenticazione (es. smart card) o in una caratteristica biometrica. Gli Incaricati devono utilizzare e gestire le proprie credenziali di autenticazione attenendosi alle seguenti istruzioni.

Per scegliere le password l'incaricato deve adottare i seguenti criteri:

- Usare almeno 8 caratteri, o nel caso in cui lo strumento elettronico non lo permetta, usare un numero di caratteri pari al massimo consentito.
- Usare lettere, numeri e almeno un carattere tra . ; $! @ - > <;
- creare una combinazione di numeri e/o segni speciali, lettere, maiuscole e minuscole;
- evitare riferimenti ad informazioni agevolmente riconducibili ai soggetti utilizzatori o ai loro famigliari;

Per la corretta gestione e custodia della password l'Incaricato deve:

- modificare al primo utilizzo la password ricevuta;
- successivamente cambiare la password almeno ogni 3 mesi ;
- evitare la scelta di combinazioni uguali a password usate in precedenza
- conservare la password in un luogo sicuro; l'Incaricato deve inoltre osservare i seguenti DIVIETI:
- è vietato rivelare o condividere la password con i colleghi di lavoro, famigliari e amici, soprattutto attraverso il telefono;
- è vietato utilizzare la funzione, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni.
- è vietato condividere tra più utenti (anche se Incaricati del trattamento) gli strumenti di autenticazione (user-id individuali e password) per l'accesso alle applicazioni. Nel caso altri utenti debbano poter accedere ai dati è necessario richiedere l'autorizzazione al Responsabile del trattamento.

L'adozione e l'osservanza delle suindicate misure di sicurezza per il corretto utilizzo delle credenziali di autenticazione è fondamentale per la tutela dell'Azienda da accessi illeciti, atti di vandalismo e, in generale, violazioni e danneggiamenti del proprio patrimonio informativo; ma altresì per la tutela dell'Incaricato da falsi addebiti. Inoltre è a garanzia della identificabilità dell'operatore che ha svolto determinate azioni, e volta ad escludere la possibilità della apparenza di una "operatività sotto falso nome"

c) GESTIONE DELLA POSTA ELETTRONICA AZIENDALE E PROTEZIONE DAI VIRUS INFORMATICI

Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le

finalità della Azienda e in stretta connessione con l'effettiva attività e mansioni del lavoratore o del volontario che utilizza tale funzionalità.
A tutela della sicurezza delle operazioni di trattamento e del patrimonio Aziendale, l'incaricato deve osservare le seguenti prescrizioni comportamentali:

- procedere alla immediata eliminazione di comunicazioni e-mail eventualmente ricevute da destinatari sconosciuti contenenti file di qualsiasi tipo;
- è vietato scaricare file provenienti via e-mail da mittenti sconosciuti oppure da fonti non autorizzate;
- è vietato utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione;
- L'Account di posta elettronica assegnata deve essere mantenuto ordinato, ed i documenti inutili devono essere cancellati, specialmente se contengono allegati ingombranti come dimensione.
- Nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di dati particolari (ex dati sensibili), si raccomanda di verificare attentamente che:
  - l'indirizzo del destinatario sia stato correttamente digitato,
  - l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;
  - nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio;
- Il software antivirus aziendale installato su ogni elaboratore dell'Azienda non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito.
- Nel caso il programma antivirus installato sul proprio PC riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus è necessario darne immediatamente segnalazione all'Amministratore di Sistema.

d) GESTIONE DEL SALVATAGGIO DEI DATI E DEI SUPPORTI RIMOVIBILI

- L'Incaricato deve eseguire almeno una volta alla settimana la copia (salvataggio, o backup) dei dati ed i documenti che risiedono esclusivamente sul PC, allo scopo di garantire la disponibilità ed il ripristino dei Dati Personali nel caso di una generica compromissione delle risorse (cancellazioni accidentali, guasti, furti…).
- L'Incaricato deve verificare che i supporti informatici utilizzati per il backup, che normalmente sono dischi magnetici esterni, CD, DVD oppure flash disks (chiavette) siano funzionali e non corrotti.
- I supporti rimovibili, come ad esempio dischi magnetici esterni, penne USB o CD riscrivibili, quando contengono dati personali devono essere custoditi in luogo protetto e non accessibile (cassaforte, armadio chiuso a chiave, etc.).
- Quando i supporti rimovibili non sono più utilizzati devono essere distrutti o resi inutilizzabili.
- Il trasferimento di file contenenti dati personali, dati particolari (ex dati sensibili) e giudiziari su supporti rimovibili, è da eseguire unicamente in via transitoria, ponendo la massima attenzione alla destinazione di trasferimento e cancellando i file appena possibile.

5) ISTRUZIONI PER I TRATTAMENTI CON USO DI STRUMENTI "NON ELETTRONICI"

Per "non elettronici" si intendono sia documenti cartacei sia documenti di altro tipo come ad esempio microfilm, microfiches e lucidi.
I documenti di questo tipo contenenti dati particolari (ex dati sensibili) o giudiziari devono essere protetti in appositi armadi dotati di chiavi. Tutti i documenti contenenti dati particolari (ex dati sensibili) o giudiziari che si ritiene debbano essere eliminati devono essere distrutti e non gettati nei cestini.
Per proteggere i dati personali è opportuno evitare il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici (corridoi o sale riunioni), come pure l'abbandono in vista sulle scrivanie quando ci si debba assentare dal proprio posto di lavoro.
Nel caso di dati particolari (ex dati sensibili) e/o giudiziari, il rispetto di queste norme è obbligatorio.

a) Prescrizioni per gli incaricati

L'Incaricato deve attenersi alle seguenti prescrizioni:

- in nessun caso è concesso l'accesso a documentazione contenente Dati Personali per motivi non dettati da esigenze di lavoro strettamente connesse ai trattamenti dichiarati, autorizzati e tutelati dal Titolare;
- la documentazione contenente Dati Personali che, per ragioni di praticità operativa, risiede sulle scrivanie degli Incaricati, deve comunque essere rimossa al termine dell'orario di lavoro;
- l'accesso ai supporti deve essere limitato al tempo necessario a svolgere i Trattamenti previsti;

- i supporti devono essere archiviati in ambiente ad accesso controllato;
- i documenti contenenti dati personali, non devono essere lasciati incustoditi in un ambiente non controllato (ad es. a seguito della stampa dei documenti su stampante di rete);
- il numero di copie di documenti contenenti Dati Personali deve essere strettamente funzionale alle esigenze di lavoro;
- cassetti ed armadi contenenti documentazione riservata debbono tassativamente essere chiusi a chiave fuori dell'orario di lavoro;
- l'accesso fuori orario lavorativo a documenti contenti Dati particolari (ex dati sensibili) /giudiziari può avvenire da parte di personale Incaricato, o tramite autorizzazione di quest'ultimo, unicamente previa registrazione dell'accesso a tali documenti;
- la distruzione di documenti contenenti Dati Personali deve essere operata, ove possibile, direttamente dal personale Incaricato;
- ove non siano disponibili strumenti per la distruzione dei documenti (trita documenti), o il volume di questi sia tale da imporre il ricorso al servizio di macero, il personale Incaricato che avvia al macero la documentazione è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo e solido;
- quando gli atti e i documenti contenenti dati personali, dati particolari (ex dati sensibili) o giudiziari sono affidati agli Incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli Incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate; l'accesso agli archivi contenenti dati particolari (ex dati sensibili) o giudiziari deve essere controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.
- è severamente vietato utilizzare documenti contenenti Dati personali, dati particolari (ex dati sensibili) o giudiziari come carta da riciclo o da appunti.

b) distruzione delle copie cartacee

Coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzando strumenti per la riproduzione cartacea di documenti digitali, sono tenuti a procedere alla relativa distruzione del supporto, qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli, salva l'ipotesi di uso esclusivamente personale per eventuali appunti o brutte copie, da distruggere immediatamente quando non più necessarie;

6) VERIFICHE E SANZIONI PER OMESSA OSSERVANZA DELLA NORMATIVA AZIENDALE

Le presenti istruzioni sono impartite ai sensi delle normative vigenti in materia di privacy e la loro inosservanza da parte dell'Incaricato può comportare sanzioni anche di natura penale a suo carico.
Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.
Al fine di verificare la integrale osservanza dei doveri imposti, il rispetto dei divieti, l'effettiva applicazione delle misure di sicurezza illustrate, ed in generale l'ottemperanza alle prescrizioni impartite per l'esecuzione delle operazioni di trattamento dei dati personali ed il corretto utilizzo degli strumenti in dotazione potranno essere svolti controlli a campione mediante la raccolta e l'analisi di dati aggregati e anonimi. Inoltre, nel caso di provato o constatato uso illecito o non consentito degli strumenti elettronici, risultante dalla verifica delle informazioni in modalità aggregata e anonima, può essere necessario procedere alla verifica delle registrazioni delle sessioni di lavoro, al fine di sanzionare condotte illecite, anche su richiesta dell'autorità giudiziaria, cui le informazioni potranno essere comunicate, senza alcuna ulteriore informativa all'interessato.
In conformità ai più recenti arresti della Giurisprudenza Europea in materia di bilanciamento degli interessi, tra rispetto della vita privata ed esigenze di controllo datoriali, l'incaricato viene informato e prende atto che i contenuti delle comunicazioni inviate e ricevute sugli accounts di posta elettronica aziendale devono ritenersi non avere contenuti di natura personale, e sono suscettibili di essere conosciuti dal Responsabile del trattamento in occasione di controlli effettuati per verificare la rispondenza dell'operato degli Incaricati del trattamento alle direttive dei superiori gerarchici ed alle istruzioni di cui al presente documento.
In particolare i controlli potranno essere avviati e condotti sugli accounts di posta elettronica direttamente riconducibili all'Azienda M8 S.R.L., qualora siano raccolte o pervenute segnalazioni circa un indebito utilizzo di tali strumenti elettronici, che sia suscettibile di arrecare un nocumento al profitto e/o all'immagine dell'azienda, o che sia comunque realizzato in violazione dei doveri di correttezza, riservatezza e non concorrenza incombenti sugli Incaricati

al trattamento (siano essi lavoratori dipendenti o collaboratori esterni, comunque inquadrati) ai quali è attribuito una account di posta elettronica direttamente riconducibile all'azienda.
I controlli suddetti delle comunicazioni di posta elettronica, per qualsiasi ragione avviati, saranno limitati nel tempo e non potranno protrarsi oltre i 30 giorni lavorativi consecutivi senza che siano rilevate circostanze di rilievo disciplinare. In caso di rilievo di tali circostanze, sarà in facoltà dei superiori gerarchici l'avvio del procedimento disciplinare con la contestazione degli addebiti in ottemperanza alle modalità della normativa vigente.
È escluso il controllo sugli eventuali contenuti di natura personale che, in violazione delle vigenti istruzioni, l'Incaricato abbia riversato nei messaggi di posta elettronica inviati mediante gli accounts aziendali. Sono fatte salve le prerogative della società inerenti il suo diritto di difesa in sede giudiziaria

7) AGGIORNAMENTO E REVISIONE

Le presenti istruzioni per gli incaricati del trattamento sono aggiornate al 5 gennaio 2019, e sono soggette a revisione in occasione di sopravvenienze normative o giurisprudenziali di rilievo, e comunque con frequenza annuale.
Tutti gli Incaricati possono proporre, quando ritenuto necessario, integrazioni alle presenti Istruzioni.

La Direzione