MACFER s.r.l.

POLITICA AZIENDALE PER LA PROTEZIONE DEI DATI

Regolamento UE 2016/679 – GDPR

Politica aziendale per la protezione dei dati personali, al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche

INDICE

1. SCOPO

Scopo del presente documento è quello di descrivere i principi generali di sicurezza ed obblighi di riservatezza delle informazioni e dei dati personali definiti dal Titolare del trattamento, o del Responsabile che **Macfer S.r.l.** garantisce ed assicura a tutti i soggetti coinvolti nell'ambito del trattamento dei dati, al fine di sviluppare un efficiente e sicuro sistema di gestione delle procedure e dei processi per la sicurezza dei dati personali nel rispetto dei diritti e le libertà fondamentali delle persone, in ottemperanza al Regolamento Europeo 2016/679, d'ora in avanti GDPR.

2. DESCRIZIONE

Obiettivi perseguiti

Macfer S.r.l. intende perseguire obiettivi di sicurezza delle informazioni, dei dati personali, della struttura tecnologica, fisica, logica ed organizzativa e della loro gestione. Questo significa raggiungere e mantenere un sistema di gestione sicura delle informazioni attraverso il rispetto dei principi previsti dagli articoli 5 e 6 del GDPR;

- Liceità, correttezza, trasparenza;
- Garanzia rispetto alla gestione e raccolta dei dati per le sole finalità contrattuali, determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità. Tali garanzie sono applicate e verificate anche a cascata nei confronti degli eventuali subfornitori;
- Adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (principio di "minimizzazione dei dati");
- Esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
- Conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore alconseguimento delle finalità per le quali sono trattati;
- Trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche ed organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali "principio di integrità e riservatezza";
- Assicurare che i dati personali siano accessibili solamente ai soggetti e/o alle categorie degli stessi debitamente autorizzati;

- Salvaguardare la consistenza dell'informazione da modifiche non autorizzate;
- Assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati in riferimento ai ruoli e mansioni ricoperti;
- Assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
- Garantire l'affidabilità dei canali di provenienza delle informazioni;
- Garantire la protezione ed il controllo dei dati personali.

Formazione
Considerato che il GDPR all'articolo 29 prevede che tutte le persone, addetti, incaricati, sotto l'autorità del titolare o del responsabile debbano essere debitamente istruiti e quindi formati sui compiti, responsabilità e per l'effettuazione delle operazioni di trattamento dei dati, nonché si impegnino alla riservatezza, **Macfer S.r.l.** ha redatto un piano interaziendale di formazione sulla base dell'erogazione dei servizi, dei ruoli e mansioni interne, dell'attività esercitata, degli specifici trattamenti dati ed i rischi connessi.

La formazione è pensata e realizzata per le mansioni ed i ruoli ricoperti dal personale dipendente e ed ha le seguenti caratteristiche:

a) Specifica - corrispondente alla tipologia di mansione/ruolo svolto;
b) Appropriata - in relazione alla tipologia dei trattamenti dati realizzati;
c) Permanente - deve prevedere una programmazione temporale ed un aggiornamento periodico in particolare per eventuali nuovi assunti;
d) Documentata - il suo svolgimento ed i successivi aggiornamenti devono risultare da registri, attestati o altre forme che ne diano evidenza;
e) Efficace – deve essere verificata periodicamente la comprensione generale, specifica ed il recepimento delle procedure aziendali

Nei confronti dei nostri fornitori:
Tali principi e garanzie sono verificate al momento della scelta di ogni nostro fornitore. Viene inoltre monitorato sistematicamente lo stato di implementazione di tali garanzie.

3. AMBITO DI APPLICAZIONE

La politica per la protezione dei dati personali si applica a tutto il personale interno ed alle terze parti che collaborano alla gestione delle informazioni nonché a tutti i processi e risorse coinvolte nella progettazione, realizzazione, avviamento ed erogazione continuativa nell'ambito dei servizi.

Di seguito vengono descritti prodotti e servizi erogati ed illustrate le modalità di erogazione.

Attività realizzate:

- **COSTRUZIONI DI STRADE, AUTOSTRADE E PISTE AEROPORTUALI**

4. POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Adempimenti e procedure applicate alle aziende clienti:

- La verifica dei dati che saranno oggetto di trattamento con identificazione delle varie tipologie di dati e delle categorie di appartenenza. La verifica della finalità di ogni trattamento e della base giuridica sul quale ciascuno di essi si fonda, anche al fine di rendere adeguata informativa ai soggetti interessati, come previsto dagli artt. 13 e 14 del GDPR;

- La predisposizione della/delle informative (o il suo aggiornamento) che deve essere fornita agli interessati nel rispetto di tutti gli elementi indicati agli artt. 13 e 14 del GDPR. In particolare, gli

interessati dovranno essere messi a conoscenza dei diritti che il Regolamento riconosce loro (diritto di accesso, diritto all'oblio, diritto di rettifica, diritto di limitazione e di opposizione al trattamento, diritto alla portabilità dei dati); le informative per i soggetti interessati ai trattamenti dati di cui il cliente è titolare del trattamento sono fornite dal cliente se nei software o servizi sviluppati o configurati è prevista la raccolta di dati;

• La predisposizione del registro delle attività di trattamento dei dati personali, qualora esso risulti necessario in base al disposto dell'art. 30 del GDPR, ossia nel caso in cui l'impresa o l'organizzazione che effettua il trattamento dei dati abbia più di 250 dipendenti. Tale registro dovrà essere redatto anche nel caso in cui l'impresa od organizzazione abbia meno di 250 dipendenti, ma ponga in essere un trattamento dei dati che presenta un potenziale rischio per i diritti e libertà degli interessati il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

• L'instaurazione di una procedura da adottare in caso di eventuali violazioni dei dati (c.d. Data Breach di cui agli articoli 33 e 34 del GDPR), ad esempio al verificarsi di una divulgazione (intenzionale o meno), della distruzione, della perdita, della modifica o dell'accesso non autorizzato ai dati personali oggetto di trattamento. Il GDPR prevede infatti degli specifici adempimenti nel caso in cui si verifichi una violazione di tal genere, a causa di un attacco informatico, di un accesso abusivo o di un incidente. In questi casi il GDPR impone, come previsto dall'art. 33, in capo al Titolare del trattamento l'obbligo di comunicare all'autorità di controllo l'avvenuta violazione entro 72 ore (o comunque senza ritardo). Nel caso in cui la violazione verificatasi faccia presumere che vi sia anche un elevato e attuale pericolo per i diritti e le libertà degli interessati, anche questi ultimi dovranno essere direttamente informati senza ritardo di quanto successo;

• All'art. 35 del GDPR, si configura, in capo al Titolare del trattamento (e con la possibilità di consultare il Responsabile della protezione dei dati se nominato), l'obbligo di procedere ad una valutazione d'impatto sulla protezione dei dati nel caso in cui un tipo di trattamento, anche in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento stesso, presenti un rischio elevato per i diritti e le libertà delle persone fisiche. Si precisa che il GDPR non sancisce un vero e proprio obbligo di svolgimento della valutazione d'impatto, ma si ricorda che il Regolamento prevede un generale obbligo, in capo al Titolare del trattamento, di attuare le misure idonee al fine di gestire adeguatamente i rischi per i diritti e le libertà degli interessati che possono derivare dal trattamento dei loro dati. Sarà quindi opportuno procedere all'effettuazione della valutazione d'impatto anche quando sul Titolare non incombe l'obbligo normativo in tale senso.

• Agli articoli 37 – 38 e 39 viene introdotto un altro adempimento richiesto al Titolare del trattamento che consiste nella designazione del Responsabile della protezione dei dati definito altresì Data Protection Officer. Tale nomina, come previsto dall'art. 37 del GDPR, è obbligatoria soltanto in una serie di ipotesi, in particolare, nel caso in cui il trattamento dei dati sia effettuato da un'autorità pubblica o da un organismo pubblico (ad eccezione per le autorità giurisdizionali quando esercitano le loro funzioni); quando le attività principali svolte del titolare o del responsabile del trattamento consistono in operazioni che, per la loro natura, l'ambito di applicazione o le finalità, richiedono un monitoraggio regolare e sistematico degli interessati su larga scala;

e infine nel caso in cui le attività principali effettuate consistano nel trattamento, su larga scala, di dati sensibili o di dati relativi a condanne penali e a reati consistenti nell'illecito trattamento dei dati personali. Come suggerito anche dal Gruppo dei 29, l'organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro che ha predisposto le Linee guida dettando regolare sulla nomina del Responsabile per la protezione dei dati personali, quando il Regolamento non impone specificamente la nomina di un

DPO, questa figura potrà comunque essere designata dal titolare o dal responsabile del trattamento su base volontaria.

ISTRUZIONI PER I SOGGETTI INTERNI E/O ESTERNI CHE SI INTERFACCIANO CON LA NOSTRA ORGANIZZAZIONE

Particolare importanza viene attribuita alle procedure del Sistema di Gestione per la Protezione dei dati personali, indicate nelle istruzioni e formazione che dovranno essere fornite al personale ed alle quali vi è l'obbligo di attenersi scrupolosamente.

Vi è obbligo inoltre di prendere visione dei nominativi del personale autorizzato a trattare i dati relativi all'ambito assegnato, siano essi Titolari, responsabili o incaricati (Come definiti nell'organigramma).

Il personale è tenuto a prenderne visione ed a comunicare ai suoi referenti eventuali inesattezze. Se gli strumenti di lavoro consentissero la connessione con altre banche dati, l'autorizzazione comprenderà l'incarico di trattare anche i dati delle banche dati connesse, nei limiti in cui ciò sarà necessario all'efficiente e corretto svolgimento delle Sue mansioni e sempre in conformità al profilo di autorizzazione e alle possibilità e procedure indicate nelle istruzioni ricevute.

5. RESPONSABILITÀ DELLA POLITICA DI SICUREZZA DELLE INFORMAZIONI

Il "titolare del trattamento" e il "responsabile" sono responsabili del sistema di gestione sicura delle informazioni, in coerenza con l'evoluzione del contesto aziendale e di mercato, valutando eventuali azioni da intraprendere a fronte di eventi come:

- ✓ Evoluzioni significative del business;
- ✓ Nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio;
- ✓ Significativi incidenti di sicurezza;
- ✓ Evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni;

Periodicamente o all'occorrenza dovrà essere svolto un riesame per la verifica dell'efficienza e dell'efficacia, nonché dell'adeguatezza delle misure tecniche/organizzative applicate, nel rispetto ed al fine ultimo della protezione dei dati, diritti e libertà fondamentali delle persone.

Per approvazione Legale Rappresentante:

Luogo e Data documento:

Giugliano in Campania

27/02/2023

La Direzione

MACFER s.r.l.

ISTRUZIONI OPERATIVE UTILIZZO SISTEMI INFORMATICI

INDICE

PREMESSA

L'utilizzo delle risorse informatiche e telematiche della nostra Azienda deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro. Macfer s.r.l. ha adottato una procedura interna diretta ad evitare che comportamenti inconsapevoli possano innescareproblemi o minacce alla sicurezza nel trattamento dei dati.

UTILIZZO DEL PERSONAL COMPUTER

Il Personal Computer affidato al dipendente è uno **strumento di lavoro.** Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
Gli accessi logici sono regolamentati da procedura aziendale interna.
L'accesso all'elaboratore è protetto da password che deve essere custodita dall'autorizzato con la massima diligenza e non divulgata.
Il custode delle password, per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna.
Il custode delle password potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere alla stessa azienda, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dalla stessa azienda, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio, in caso di prolungata assenza o impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.
Non è consentito installare autonomamente programmi provenienti dall'esterno previa autorizzazione esplicita del *Titolare del Trattamento*, in quanto sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.
Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal *Titolare del Trattamento* della Macfer s.r.l. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche

penali in caso di violazione della normativa a tutela dei diritti d'autore sul software, che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.
Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo autorizzazione esplicita del *Titolare del Trattamento.*
Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso deve essere attivato lo screen saver e la relativa password.
Non è consentita l'installazione sul proprio PC di alcun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.), se non con l'autorizzazione espressa del *Titolare del Trattamento.*
Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il *Titolare del Trattamento* nel caso in cui vengano rilevati virus.

UTILIZZO DELLA RETE
Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup, così come previsto da procedura aziendale.
Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.
Il *Titolare del Trattamento* può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.
Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.
È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

GESTIONE DELLE PASSWORD
Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dal *Titolare del Trattamento.*
È necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati particolari (ex dati sensibili) e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi con contestuale comunicazione al *Titolare del Trattamento. (n.b.: in molti sistemi la comunicazione di variazione può essere "generata" dallo stesso sistema informatico all'atto della modifica, con invio di e-mail automatica al Titolare; molti sistemi permettono di "temporizzare" la validità delle password e, quindi, di bloccare l'accesso al personale computer e/o al sistema, qualora*

non venga autonomamente variata dall'incaricato entro i termini massimi: in questi casi vanno adattate le istruzioni contenute nel presenteregolamento)
Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.
La password deve essere immediatamente sostituita, dandone comunicazione al *Titolare del Trattamento*, nel caso si sospetti che la stessa abbia perso la segretezza.
Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla Direzione o al *Responsabile dei sistemi informatici aziendali*.

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

UTILIZZO DI PC PORTATILI
L'utente è responsabile del PC portatile assegnatogli dal *Titolare del Trattamento* e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Ai PC portatili si applicano le regole di utilizzo previste per i Pc connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
I PC portatili utilizzati all'esterno (convegni, visite in azienda, ecc...), in caso di allontanamento, devono essere custoditi in un luogo protetto.

USO DELLA POSTA ELETTRONICA
La casella di posta, assegnata dall'Azienda all'utente, è uno **strumento di lavoro.** Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
È fatto divieto di utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.
È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per Macfer s.r.l. deve essere visionata od autorizzatadalla Direzione, o in ogni modo è opportuno fare riferimento alle procedure in essereper la corrispondenza ordinaria.
La documentazione elettronica che costituisce per l'azienda "know how" aziendale tecnico o commerciale protetto, e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'impresa, non può essere comunicata all'esterno senza preventiva autorizzazione della Direzione.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta, ...).
Per la trasmissione di file all'interno di Macfer s.r.l. è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.
È obbligatorio controllare i file *attachements* di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al *Titolare del Trattamento*.
Non si devono in alcun caso attivare gli allegati di tali messaggi.

USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.
È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal *Titolare del Trattamento*.
È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto.
È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI

È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679 e della normativa nazionale in vigore.

NON OSSERVANZA DELLA NORMATIVA AZIENDALE

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.

AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione.

Il presente Regolamento è soggetto a revisione con frequenza annuale.

Data 27/02/2023

La Direzione