Regolamento Aziendale BmpEurope Srl per la tutela della privacy ai sensi del D.Lgs n.196 del 30.06.2003 e del Regolamento UE n.679/2016 (GDPR)

Lo scopo del presente documento è definire le procedure per adempiere ai dettami del D.Lgs. n. 196 del 30.06.2003 (codice per la protezione dei dati personali – c.d. Codice della Privacy) e del Regolamento UE n. 679 del 2016 (General Data Protection Regulation – c.d. GDPR), in materia di privacy aziendale, ovvero individuare le disposizioni operative interne volte a disciplinare il trattamento dei dati personali effettuato dalla Società. In essa sono quindi disciplinati i ruoli e le responsabilità nonché gli adempimenti da seguire in materia di protezione dei dati personali anche con riferimento alle decisioni e ai provvedimenti emessi dall'Autorità Garante per la protezione dei dati personali.

I fini del presente documento si applicano le seguenti definizioni:

- **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;
– limitazione di trattamento: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- **profilazione**: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
– pseudonimizzazione: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
– archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
– titolare del trattamento: 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;
– responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

- **destinatario**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.

– **terzo:** 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;
- **consenso dell'interessato**: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- **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;
– **dati genetici**: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
– **dati relativi alla salute**: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
– **rappresentante:** la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;
- **impresa**: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

– **norme vincolanti d'impresa:** le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;
- **autorità di controllo:** l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR;

Principi, ambito di applicazione e destinatari del regolamento
Il presente documento si applica a tutti i trattamenti dei dati personali, automatizzati o svolti manualmente, effettuati dalla BmpEurope Srl in qualità di titolare.
Il presente regolamento interno.
La Società si impegna a garantire e dimostrare che il trattamento dei dati avviene in maniera conforme a quanto previsto dalla normativa e secondo principi di liceità di trattamento.

Condizioni per il consenso
Le condizioni per il consenso che devono sussistere sono:

- qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

Oggetto e modalità di applicazione
Oggetto del presente regolamento è il trattamento dei dati personali effettuato da BmpEurope Srl
Sono esclusi dall'ambito di applicazione i trattamenti dei dati personali effettuati dai lavoratori per fini esclusivamente personali e nei casi in cui i dati non sono destinati ad una comunicazione sistematica o alla diffusione anche se utilizzati ai fini di esigenze di lavoro (ad esempio, rubrica personale su telefono fisso o mobile ed utilizzata solo ed esclusivamente dall'utente)

Titolare del trattamento
Conformemente a quanto previsto dalla normativa, è titolare del trattamento la BmpEurope Srl, nella persona del suo legale rappresentante, e si impegna a:

- adeguare il proprio assetto organizzativo nel rispetto della normativa vigente in materia di protezione dei dati;
- adottare le modalità operative connesse con la gestione degli adempimenti ed il trattamento dei dati;
- assumere le decisioni in ordine alle finalità, alle modalità del trattamento dei dati e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Incaricati/referenti interni del trattamento
L'incaricato/referente interno del trattamento dei dati è la persona nominata dal titolare al fine di garantire l'attuazione delle misure di sicurezza previste in materia di trattamento dei dati. La persona preposta allo svolgimento della funzione viene individuata in quanto dotata di adeguate garanzie.

Amministratore di sistema
La figura professionale che, in ambito informatico, mantiene, configura e gestisce reti e apparati di telecomunicazione di sicurezza è nominata amministratore di sistema. L'attribuzione delle funzioni di amministratore di sistema avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
La nomina ad amministratore di sistema deve essere individuale, formalizzata, con l'indicazione analitica degli ambiti di applicazione di operatività consentiti in base al profilo di autorizzazione assegnato.
Impegno alla riservatezza
La Società, in qualità di titolare del trattamento dei dati, si impegna a garantire la riservatezza, conformemente alle procedure interne e la confidenzialità delle informazioni e dei dati degli interessati acquisiti nel corso della propria attività. A tal scopo, i dati e le informazioni raccolte durante lo svolgimento dell'incarico sono trattati per:

– finalità strettamente connesse alla propria attività lavorativa;
– finalità connesse agli obblighi previsti da leggi, regolamenti e normativa comunitaria nonché da disposizioni impartite da autorità a ciò legittimate dalla legge.

In relazione alle indicate finalità il trattamento dei dati avverrà in modo da garantire la sicurezza e la riservatezza e potrà essere effettuato attraverso strumenti manuali, informatici e telematici atti a

memorizzare, gestire e trasmettere i dati stessi nel rispetto delle misure di sicurezza previste dal D.Lgs 196/2003 e dal GDPR.

Tutti i dati e le informazioni acquisite, in aggiunta alle comunicazioni previste nei confronti di soggetti e organi che hanno responsabilità di direzione, supervisione e controllo potranno essere comunicati esclusivamente a:

- autorità di vigilanza, italiane o estere, nei casi e con le limitazioni previste dalla legge;
- autorità amministrativa, giudiziaria e fiscale, nei casi e con le limitazioni previsti dalla legge.

Registro delle attività di trattamento dei dati personali
In attuazione del presente regolamento il titolare del trattamento ha deciso di adottare un registro delle attività di trattamento svolte sotto la propria responsabilità.

Ogni referente/incaricato interno del trattamento tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento. I registri sono tenuti in forma scritta Su richiesta, il titolare del trattamento o il responsabile esterno del trattamento mettono il registro a disposizione dell'autorità di controllo.

Dati dei fornitori
BmpEurope Srl per mezzo dei propri referenti o autorizzati, può raccogliere i dati personali dei fornitori, al fine di perfezionare accordi contrattuali. I dati personali dei fornitori potranno essere trattati nell'ambito della normale attività per fornire i servizi richiesti e gestire i rapporti con i fornitori; e adempiere ad obblighi previsti da un regolamento o dalla normativa comunitaria nonché per osservare disposizioni impartite dalle pubbliche autorità ed organi di vigilanza e controllo a ciò legittimati dalla legge. In tal caso il conferimento dei dati personali è necessario e obbligatorio e per il trattamento di tali dati non è richiesto il consenso.

Misure di sicurezza e relativi controlli
La gestione della sicurezza: ruoli e responsabilità
La responsabilità dell'attività di impostazione e coordinamento dei sistemi che garantiscono la sicurezza e la tutela di tutti i dati oggetto di trattamento aziendale sono in carico all'amministratore di sistema.

Misure per garantire l'integrità a protezione dell'accesso ai dati
Sono le misure di sicurezza volte a minimizzare i rischi che le informazioni siano rivelate o modificate senza autorizzazione, ovvero perse o alterate accidentalmente o intenzionalmente. Il sistema in atto prevede un sistema di autenticazione, basato su codice identificativo e password individuale segreta, per assicurare che la persona che accede al sistema sia identificata con certezza, nonché un sistema di autorizzazione, che prevede che a ciascuna persona che accede al sistema sia assegnato un profilo di accesso che definisce i dati ai quali l'utente è autorizzato ad accedere e, ove applicabile, le operazioni che per ciascun dato o gruppo di dati è autorizzato ad eseguire (consultazione, inserimento, modifica, cancellazione).

Sicurezza della postazione di lavoro
Lo scopo di questa politica è di stabilire i requisiti minimi per prevenire eventi di data breach e responsabilizzare i dipendenti aziendali.

Dismissione dei dispositivi utilizzati dagli utenti di BmpEurope Srl
Tutti i dispositivi di BmpEurope Srl, eventualmente rilasciati in dotazione ai dipendenti, vengono formattati a seguito delle dimissioni degli stessi al fine di rimuovere tutti i dati personali contenuti al loro interno. I sistemi informatici dismessi quali: pc, tablet e telefoni cellulari non potranno essere ceduti anche gratuitamente a terzi .

Informazione e formazione dei destinatari
L'obiettivo di garantire un corretto trattamento dei dati, conforme ai requisiti previsti dalla normativa fin dal momento di ingresso di una nuova risorsa, BmpEurope Srl presenta a quest'ultima il regolamento aziendale sul trattamento dei dati. Questo regolamento viene affisso nella bacheca aziendale.

Notifica di una violazione dei dati personali all'autorità di controllo (Data Breach)
In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 del GDPR senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Disposizioni interne per il corretto utilizzo degli strumenti informatici e telematici
La Società, con il seguente regolamento, si è dotata di procedure specifiche per l'uso dei sistemi informatici nonché l'accesso ad internet. Tali procedure, che vengono diffuse tra i dipendenti della Società con il seguente regolamento interno, hanno lo scopo di ridurre i rischi di natura patrimoniale, di danneggiamento di immagine della Società nonché di incorrere in responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge.

Le regole che disciplinano l'utilizzo delle risorse informatiche e telematiche si ispirano al principio della diligenza e correttezza, principi che normalmente si adottano nell'ambito dei rapporti di lavoro. Per quanto non espressamente indicato, si rimanda alla normativa specifica in materia.

La mancata adozione delle misure indicate in questo regolamento da parte dei dipendenti espone gli stessi a provvedimenti disciplinari e risarcitori previsti dal vigente CCNL, nonché a tutte le azioni civili e penali consentite.

Utilizzo del personal computer e internet
Il Personal Computer affidato/utilizzato dall'utente è uno strumento di lavoro, pertanto ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. È quindi assolutamente proibita la navigazione in Internet per motivi personali e diversi da quelli strettamente legati all'attività lavorativa.
Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

L’amministratore di sistema, sotto indicazione del DPO, ha la facoltà di collegarsi, in presenza dell’utente, alle singole postazioni PC al fine di garantire l’assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc.

Salvo autorizzazione del DPO, non è consentito all’utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem ecc.).

Gestione delle credenziali di accesso
Le credenziali di autenticazione per l’accesso alla rete vengono assegnate dall’amministratore di sistema previa formale richiesta del responsabile d’area nell’ambito del quale verrà inserito ed andrà ad operare il nuovo utente. Nel caso di tirocinanti, stagisti e collaboratori esterni, la preventiva richiesta, se necessaria, verrà inoltrata direttamente dal responsabile dell’unità operativa con il quale il collaboratore si coordina nell’espletamento del proprio incarico.

Il soggetto preposto alla custodia delle credenziali di autenticazione è l’amministratore di sistema.