Mambu srl
P. Iva e C. Fisc: 02955720350
Sede Legale: Via Mameli 15 - 42123 Reggio Emilia
✉ commerciale@mambu.it ✆ 0522.1707140

AUTORIZZAZIONE E ISTRUZIONI PER IL TRATTAMENTO DATI PERSONALI (ADS)

Premesso che

- a decorrere dal 27 aprile 2016 è in vigore il Regolamento (UE) n. 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (d'ora innanzi anche "GDPR" o "Regolamento);
- in base a quanto previsto dall'artt. 29 e 32 comma 4 del Regolamento e all'art. 2 quaterdecies del D.Lgs. 196/2003, le operazioni di trattamento possono essere effettuate solo da persone autorizzate che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni da questi impartite;
- per "trattamento", ai sensi dell'art. 4 punto 2 del Regolamento, si intende "qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati";
- per "dati personali", ai sensi dell'art. 4 punto 1 del Regolamento, si intende "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»"); altresì 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";
- Tale autorizzazione non comporta alcuna modifica della qualifica professionale o delle mansioni assegnate.

Tutto quanto sopra premesso

Il Titolare con la presente autorizza _____
in qualità di ADS al trattamento dei dati personali conosciuti direttamente o anche solo incidentalmente nello svolgimento delle attività lavorative prestate all'interno della suddetta area e riportati nella tabella sottostante.

Ai fini della corretta applicazione del suddetto Regolamento, nonché per garantire una tutela adeguata dei diritti e delle libertà degli interessati, i soggetti autorizzati al trattamento dovranno attenersi scrupolosamente alle istruzioni impartite e riportate di seguito nella tabella:

Autorizzazione al trattamento delle seguenti categorie di dati trattati	• tutti i dati personali di cui è titolare la Società trattati direttamente o anche solo indirettamente per garantire la sicurezza informatica dei dati, delle reti e dei server e dei sistemi in generale, nonché le attività ad esse propedeutiche e/o consequenziali.
Validità e Revoca dell'autorizzazione	La presente autorizzazione ha validità per tutta la durata del rapporto giuridico intercorrente tra il soggetto autorizzato al trattamento ed il Titolare, restando ferma la facoltà di quest'ultimo di revocarla secondo sua discrezione e con le modalità da esso decise.

	L'esercizio del diritto o della facoltà di revoca, da parte del Titolare – senza obbligo di corresponsione di alcun risarcimento e/o indennità alla persona autorizzata – avverrà mediante invio di una comunicazione contenente la manifestazione di volontà di revoca.
Istruzioni generali; l'autorizzato deve:	**1.** trattare tutti i dati personali conosciuti nell'ambito dello svolgimento delle funzioni lavorative esercitate in modo lecito e secondo correttezza. **2.** trattare dati personali che siano esatti, pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono stati raccolti e successivamente trattati; **3.** trattare i dati personali esclusivamente per lo svolgimento delle proprie mansioni; **4.** provvedere a rilasciare idonea informativa agli interessati in caso di raccolta diretta dei dati, secondo le procedure predisposte dal Titolare del trattamento; **5.** seguire le istruzioni impartite in merito alle modalità di conservazione e di consultazione dei dati personali presenti su supporti cartacei; **6.** tenuto conto delle finalità di trattamento perseguite dal Titolare, mantenere assoluto riserbo in merito alle informazioni conosciute nello svolgimento delle proprie mansioni; **7.** evitare di asportare materiale contenente dati personali senza una preventiva autorizzazione del Titolare, restando fermo quando ciò sia strettamente necessario e indispensabile per l'esercizio delle mansioni lavorative preposte; **8.** non costituire banche dati ulteriori rispetto a quelle necessarie per lo svolgimento delle operazioni affidate, salvo espressa autorizzazione del Titolare; **9.** in caso di esercizio da parte dell'interessato dei diritti di cui all'artt. 15,16,17,18,20 e 21 del Regolamento (UE) n. 2016/679 seguire la relativa procedura/processo posta in essere dal Titolare; **10.** rispettare le policy/piani di data retention predisposti dal Titolare con riferimento ai dati autorizzati; **11.** rispettare le condizioni previste dalla legge per il trattamento, la comunicazione e la diffusione dei dati personali; **12.** comunicare i dati personali oggetto di trattamento solo a quei soggetti esterni (fornitori/consulenti) che presentino garanzie sufficienti secondo le procedure di selezione e autorizzazione disposte dal Titolare. Sono altresì consentite le comunicazioni richieste per legge nei confronti di soggetti pubblici; **13.** osservare scrupolosamente tutte le misure di sicurezza, tecniche e organizzative, predisposte a protezione dei dati personali oggetto di trattamento;

	14. nel caso dovessero sorgere dubbi in ordine alle operazioni di trattamento svolte per l'attività demandata, rivolgersi al Titolare; **15.** verificare periodicamente la corretta storicizzazione dei consensi, ove richiesti, prestati dagli interessati per il trattamento dati secondo le procedure anche tecniche implementate; **16.** verificare periodicamente o su indicazione del Titolare che i trattamenti posti in essere rispettino le condizioni di liceità previste dall'art. 6 Regolamento (UE) n. 2016/679; **17.** per quanto di propria conoscenza e rispetto alle proprie mansioni lavorative, è compito del soggetto autorizzato al trattamento fornire il necessario supporto per garantire una corretta tenuta ed aggiornamento del Registro delle attività di trattamento; anche rispetto ai trattamenti sottoposti a Data Protection Impact Assessment (c.d. DPIA) individuati dal Titolare è richiesto analogo supporto da parte del soggetto autorizzato; **18.** fornire assistenza per la gestione degli applicativi installati e/o installandi rispetto ai principi di privacy by design e privacy by default; **19.** coadiuvare il Titolare e/o il DPO nel monitoraggio di eventuali trasferimenti di dati al di fuori dei confini dell'UE, provvedendo a segnalarli al Titolare; **20.** segnalare tempestivamente, e comunque secondo le modalità previste dalle procedure, al Titolare e/o al DPO eventuali criticità, ivi inclusi i casi di data breach, che possono mettere a repentaglio la sicurezza dei dati, al fine di consentire idonei interventi.
Istruzioni ADS. **L'ADS deve:**	**21.** agire nell'ambito di operatività consentito in base al profilo di autorizzazione assegnato, nonché a quanto precisato nell file 'elenco ADS Interni' messo a disposizione; **22.** nello svolgimento delle funzioni tecniche preposte, l'autorizzato prende atto che, in qualità di 'amministratore di sistema, non svolgere attività di trattamento ulteriori rispetto a quelle necessarie per la messa in sicurezza e per la manutenzione dei sistemi del Titolare; **23.** accedere alle banche dati del Titolare, elettroniche, informatiche e telematiche, solo per ragioni di sicurezza e di manutenzione del sistema informativo con le quali vengono elaborate e utilizzate; **24.** accedere in qualità di amministratore di sistema solo quando ciò si renda necessario rispetto alle attività da compiere: non sono pertanto ammesse attività ultronee o non necessarie rispetto a quelle all'uopo svolte; **25.** rispettare tutte le misure di sicurezza già adottate o che verranno adottate in seguito dal titolare; **26.** aggiornare i sistemi operativi in uso dagli apparati elettronici presso i quali esercita le proprie mansioni, individuando anche quelli più confacenti ai tipi dati e alle operazioni di trattamento eseguibili con essi, secondo le indicazioni del Titolare, oltre che aggiornare i sistemi di

	protezione della rete, anche individuando quelli più confacenti all'esigenza per evitare accessi non consentiti ovvero trattamenti illeciti e la perdita dei dati; **27.** salvo quanto richiesto in base alle finalità perseguite dal Titolare, mantenere assoluto riserbo in merito alle informazioni conosciute nell'espletamento delle proprie mansioni; **28.** l'amministratore di sistema è consapevole che le attività svolte sono sottoposte a loggatura inalterabile e incancellabile, e che saranno oggetto di successivo controllo;
Il Responsabile della Sicurezza Informatica deve:	**29.** affinché sia sempre sotto monitoraggio un livello di rischio accettabile, esaminare periodicamente i livelli di rischio sui sistemi utilizzati dal Titolare secondo standard riconosciuti. In particolare, è compito del Responsabile identificare e definire i rischi nonché stimarne le criticità sulla base delle tipologie dei dati e delle peculiarità dei medesimi sistemi; **30.** sviluppare strategie di contrasto e di mitigazione dei rischi, atte a ridurre, eliminare o accettare i rischi individuati. Tali strategie devono tener conto del contesto ove opera il Titolare, delle categorie di dati e di interessati, nonché dei trattamenti effettuati ed al progresso tecnologico raggiunto; **31.** deve definire un piano di sicurezza informatico pluriennale atto a presidiare i dati ed i sistemi del Titolare, che tenga conto di misure organizzative (procedurali e documentali) e tecniche (sia fisiche che logiche); **32.** provvedere a riesaminare e perfezionare periodicamente il piano di sicurezza informatica ed in particolare in caso di incidenti di sicurezza, variazioni tecnologiche significative, modifiche all'architettura informatica, aggiornamenti delle prescrizioni normative o best practices, risultanze di audit; **33.** collaborare con altre funzioni aziendali in merito all'aggiornamento di ogni idoneo documento, anche di sintesi, capace di dare evidenza delle soluzioni tecniche ed organizzative, nonché delle politiche di sicurezza informatica adottate; **34.** per misurare l'efficacia sul medio e lungo termine le contromisure implementate, prevedere attività di monitoring a auditing con il precipuo fine di perfezionare o comunque migliorare tali contromisure; **35.** tenersi sempre aggiornato sulle novità che ineriscono la sicurezza informatica, e ciò sia in via autonoma che ricorrendo a fornitori qualificati; **36.** per ricorrere a fornitori/sub-fornitori qualificati, il Responsabile deve coadiuvare il Titolare nella predisposizione di misure di selezione preventiva, che tengano conto dell'adeguatezza delle caratteristiche del fornitori/sub-fornitore con riferimenti ai servizi ad esso richiesti; **37.** promuovere iniziative volte a sensibilizzare il tema della sicurezza informatica all'interno dell'azienda; **38.** gestire ed aggiornare un inventario degli asset hardware e software aziendali; **39.** sulla base delle vulnerabilità dei dati ed ai trattamenti effettuati, il Responsabile deve pianificare periodicamente vulnerability assessment

	e/o penetration test sui software e sui sistemi, ivi comprensivi dei successivi piani di remediation; **40.** definire ed applicare regole standard per l'installazione e la configurazione dei sistemi, e ciò anche quando sono coinvolti fornitori terzi; **41.** gestire adeguatamente eventi, problemi e incidenti, il Responsabile deve condurre regolarmente attività di monitoraggio sulle prestazioni dei sistemi; **42.** Rilevare, identificare e classificare gli incidenti di sicurezza e porre in essere tutte le attività di contenimento necessarie, di eliminazione e ripristino.
Istruzioni per il trattamento dati quando la Società agisce in qualità di Responsabile esterno del trattamento	In esecuzione dei servizi contrattualizzati con i propri Clienti, la Società Mambu S.r.l. (di seguito anche la "Società") compie i conseguenti trattamenti di dati personali, è stata pertanto nominata da taluni di essi responsabile esterno del trattamento. Al riguardo la Società è tenuta ad autorizzare ed istruire i propri dipendenti/collaboratori/lavoratori, in merito alle operazioni di trattamento dati effettuate per dar seguito ai rapporti contrattuali in essere con detti Clienti. Premesso ciò, i dipendenti/collaboratori/lavoratori sono autorizzati a trattare i dati indicati nelle nomine a responsabile del trattamento che la Società ha ricevuto e devono rispettare le seguenti istruzioni: • trattare solo i dati personali pertinenti, completi e non eccedenti rispetto alle finalità connesse all'esecuzione del contratto con il Cliente; • trattare i dati personali esclusivamente per lo svolgimento delle proprie mansioni; • tenuto conto delle finalità di trattamento, mantenere assoluto riserbo in merito alle informazioni conosciute nello svolgimento delle proprie mansioni in favore del Cliente -Titolare dei dati; • evitare di asportare materiale contenente dati personali senza una preventiva autorizzazione del Cliente -Titolare, restando fermo quando ciò sia strettamente necessario e indispensabile per l'esercizio delle mansioni lavorative preposte; • non costituire banche dati ulteriori rispetto a quelle necessarie per lo svolgimento delle operazioni affidate, salvo espressa autorizzazione del Cliente -Titolare; • in caso di esercizio da parte dell'interessato dei diritti di cui all'artt. 15,16,17,18,20 e 21 del Regolamento (UE) n. 2016/679, comunicarla senza ritardo al Responsabile di riferimento; • rispettare le policy/piani di data retention con riferimento ai dati autorizzati; • la comunicazione dei dati è possibile solo se il trattamento è indispensabile e funzionale a dare esecuzione agli obblighi contrattuali concordati. Non è in nessun modo ammessa la diffusione dei dati, salvo diversa disposizione;

	• osservare scrupolosamente tutte le misure di sicurezza, tecniche e organizzative a protezione dei dati personali oggetto di trattamento; • nel caso dovessero sorgere dubbi in ordine alle operazioni di trattamento svolte per l'attività demandata, rivolgersi al Responsabile; • segnalare al Titolare eventuali criticità ivi inclusi i casi di data breach che possono mettere a repentaglio la sicurezza dei dati, al fine di consentire idonei interventi da parte del Cliente-Titolare e/o della Società Mambu S.r.l.. **43.** La Società si riserva di integrare le istruzioni contenute nella presenta autorizzazione, comunicandole o mettendo a disposizione la nomina a responsabile esterno ricevuta dal Cliente. Tali ulteriori istruzioni eventualmente e successivamente comunicate costituiranno parte integrante e sostanziale della presenta autorizzazione.
Processi e procedure	La persona autorizzata al trattamento dati deve rispettare i processi e le procedure predisposte dal Titolare per la protezione dei dati personali sono reperibili presso www.mambu.it/privacy/interna
Regolamento informatico	Si chiarisce che il Regolamento Informatico aziendale costituisce parte integrante e sostanziale della presente autorizzazione.
DPO	La persona deve collaborare e coadiuvare il DPO nello svolgimento delle attività da questo effettuate. Il DPO è contattabile al seguente indirizzo: dpo@mambu.it
Sanzioni Disciplinari	Si precisa fin da ora che la violazione delle disposizioni contenute nella presente autorizzazione possono comportare l'applicazione di sanzioni disciplinari.

Reggio Emilia lì 15/01/2023