INFORMATIVA PRIVACY DIPENDENTI

Resa ai sensi degli artt. 12, 13 e 14 del Regolamento (EU) 2016/679

ESA-Com S.p.A.
Sede legale e operativa: Via Labriola n. 1 – 37054 Nogara (VR)
P.IVA C: IT03062710235 - Cod. REA: VR – 306558
PEC: esacomspapec@esacom.eu
Telefono +39 0442511045
e-mail: info@esacom.it

ELENCO DEI CONTENUTI

1 DESTINATARI

Questo documento è destinato ai dipendenti e collaboratori (*)[1] della società **ESA-Com S.p.A.** (di seguito semplicemente "**Società**", "Azienda", "**Organizzazione**" o "**ESA-Com**") e ai soggetti che svolgono, presso **ESA-Com**, stage o tirocini formativi.

È vietata la comunicazione delle informazioni contenute all'interno di questo documento a soggetti diversi dai destinatari.

2 NOTE PER LA LETTURA

Al fine di rendere questo documento più comprensibile e trasparente al lavoratore, abbiamo ritenuto necessario utilizzare un linguaggio semplice e colloquiale. Pertanto, l'utilizzo di un tono meno formale non deve essere interpretato come una mancanza di rispetto o cortesia nei confronti del lavoratore ma semplicemente un modo per agevolare la comunicazione.

3 SCOPO DEL DOCUMENTO

In ottemperanza alle indicazioni previste dal **Regolamento (UE) 2016/679** (in seguito, "**Regolamento**" o "**GDPR**") in materia di trattamento e libera circolazione dei dati personali, del **D.lgs. n. 104/2022** (c.d. "*Decreto Trasparenza*") e del **D.lgs. 24/2023** (c.d. Whistleblowing") per cui è stata rilasciata informativa specifica, Tu hai il diritto di conoscere tutte le informazioni in merito al trattamento dei Tuoi dati personali nell'ambito dell'esecuzione della Tua prestazione lavorativa in modo chiaro e trasparente. Tutti i trattamenti saranno improntati ai principi di correttezza, liceità e trasparenza, tutelando la riservatezza e i diritti di tutti i soggetti interessati.
Questa informativa Ti viene fornita preventivamente al momento dell'acquisizione delle informazioni durante l'instaurazione del rapporto di lavoro e, successivamente, ogni qual volta ne venga effettuato un aggiornamento. Tutte le ulteriori informazioni riferite alla Tua persona acquisite successivamente e necessarie all'esecuzione del contratto di lavoro, saranno trattate esclusivamente per le finalità dichiarate nel presente documento.

4 DEFINIZIONI

Le definizioni dei termini utilizzati nel presente documento, sono da intendersi come da art. 4 del Regolamento UE 2016/679.

5 TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI E DATA PROTECTION OFFICER

ESA-Com in qualità di persona giuridica che determina le finalità e i mezzi per la gestione del rapporto di lavoro, è considerata Titolare del Trattamento dei Tuoi dati personali ai sensi dell'art. 4.7 del Regolamento.

5.1 COME CONTATTARE IL TITOLARE DEL TRATTAMENTO

Fatta salva la possibilità di rivolgerti sempre al Tuo diretto superiore e referente aziendale per la protezione dei dati personali, di seguito ti sono fornite le informazioni di contatto che puoi utilizzare per richiedere informazioni o esercitare i diritti che Ti sono riconosciuti dal Regolamento:

ESA-Com S.p.A.
Sede legale e operativa: Via Labriola n. 1 – 37054 Nogara (VR)
P.IVA IT 03062710235 - Cod. REA: VR – 306558
PEC: esacomspapec@esacom.eu
Telefono +39 0442511045
e-mail: info@esacom.it

5.2 Data Protection Officer – DPO

ESA-Com, dopo aver analizzato le condizioni di obbligatorietà di nomina previste dall' art.37 del GDPR, ha nominato il Responsabile della Protezione dei dai personali.
Puoi contattare il Data Protection Officer (DPO) al seguente indirizzo e- mail: privacy@esacom.it.

(*) [1] Soggetti che operano con un contratto di collaborazione coordinata e continuativa e, dunque, lavoratori parasubordinati.

6 ATTIVITÀ DI TRATTAMENTO

6.1 PER COSA VENGONO UTILIZZATI I TUOI DATI E PERCHÉ LI POSSIAMO TRATTARE

ESA-Com utilizzerà i Tuoi dati personali esclusivamente per il raggiungimento delle seguenti finalità:

ID	Finalità e descrizione
F1	**Amministrare e gestire le risorse umane** Descrizione: *La gestione delle risorse umane comprende tutti i compiti amministrativi e di routine dell'area del personale, dall'assunzione alle dimissioni di un dipendente nel rispetto delle norme di legge, della contrattazione collettiva, dei contratti aziendali, dei contratti di lavoro dei dipendenti e degli accordi individuali.*

Elenco dei principali trattamenti eseguiti:

- Curare l'iscrizione dei dipendenti agli Istituti previdenziali di competenza;
- Gestire la redazione e stipula dei rapporti di lavoro aziendali di carattere obbligatorio, tipico ed atipico: assunzioni, cessazioni, trasferimenti, contratti, convenzioni, appalti, ecc.;
- Gestire le relazioni con DTL, INAIL, INPS, ecc.;
- Assolvere agli adempimenti previdenziali e assicurativi come ad esempio gi adempimenti previdenziali e assicurativi mensili ed annuali / denuncia di infortunio / malattia professionale / maternità e cassa integrazione;
- Gestione del rapporto di lavoro;
- Gestione delle presenze;
- Elaborazione buste paga;
- Elaborazione contributi;
- Elaborazioni Certificazione Unica CU;
- Pagamento degli stipendi;
- Applicare i contratti di lavoro, collettivi ed individuali;
- Direzione del personale;
- Valutazione idoneità salariale, crescita e impegno del personale;
- Gestione operativa del personale, rilevamento delle presenze, gestione dei turni e organizzazione del lavoro;
- Gestione Amministrativa SIM TEL/Dati Aziendali;
- Gestione Amministrativa dei Fringe Benefits, delle Carte di credito, carte carburante, telepass, ecc.;
- Gestione e selezione dei candidati per l'inserimento in organico;
- Gestione del percorso di carriera;
- Attrarre, trattenere e far crescere la forza lavoro (c.d. *Talent Management*");
- Gestione delle performance aziendali e delle valutazioni;
- Gestione delle procedure disciplinari;
- Previsione degli interventi di gestione e pianificazione di modifiche nella struttura societaria;
- Gestione risarcimenti danni;
- Gestione delle riserve;
- Gestione dei viaggi di lavoro;
- Attuare i suggerimenti degli impiegati;
- Gestione della formazione professionale obbligatoria e facoltativa;
- Contattare te, la tua famiglia o chi vorrai indicarci in caso di emergenza.

Ulteriori finalità connesse all'amministrazione e gestione delle risorse umane:

a. affrontare controversie e sinistri, commissionando consulenze legali od altre consulenze professionali; prevenire truffe; gestire qualsivoglia contenzioso effettivo e/o potenziale o di indagine giudiziale concernente l'azienda (es. prevenzione e risoluzione di controversie relative ai rapporti di lavoro, gestione di eventuali contenziosi e cause di lavoro, nonché di tutti gli aspetti eventualmente connessi);
b. realizzare adeguati controlli, nei casi previsti dalla legge, del casellario giudiziale e dei precedenti giudiziari;
c. assicurare un'amministrazione ed una gestione efficace del Tuo rapporto di lavoro o di collaborazione, i benefit, nonché la gestione del business e la sua continuità;
d. controllare che Tu possa legittimamente lavorare;

e. gestire il processo di valutazione delle performance e di valutazione per le promozioni;
f. gestire i requisiti di training e sviluppo.

ID	Finalità e descrizione
F2	**Gestione della sicurezza e dell'igiene sui luoghi di lavoro** (D.lgs. 81/2008) Descrizione: *L'attività di gestione consiste nell' attuare le misure di carattere tecnico, organizzativo o procedurale volte a garantire la salute e la sicurezza del lavoratore nell'ambiente di lavoro.*

Elenco dei principali trattamenti eseguiti:

- Gestione e sviluppo della formazione del personale;
- Gestione salute e sicurezza sul lavoro - D.lgs. 81/2008;
- Gestione del personale in relazione ai giudizi di idoneità/non idoneità alle mansioni, sicurezza dei cantieri;
- Gestione e distribuzione dei dispositivi di protezione individuale (DPI);
- Verifica dell'idoneità fisica in relazione allo stato di salute.

In via eccezionale, se necessario, tutelare gli interessi vitali Tuoi o di un terzo soggetto (per esempio, evitare seri rischi di danno a te stesso o agli altri).

ID	Finalità e descrizione
F3	**Garantire la sicurezza fisica dei locali aziendali e tutelare il patrimonio in essi contenuto** Descrizione: *La gestione consiste nell'attuare misure tecniche ed organizzative per scoraggiare l'accesso fisico ai locali e/o ad altre risorse aziendali da parte di soggetti estranei o comunque non autorizzati.*

Elenco dei principali trattamenti eseguiti:

- Monitorare e gestire gli accessi fisici allo stabilimento aziendale e ai locali critici ubicati all'interno dello stesso;
- Effettuare la Videosorveglianza delle aree critiche.

ID	Finalità e descrizione
F4	**Garantire la sicurezza delle risorse informatiche aziendali** Descrizione: *La gestione consiste nel proteggere l'insieme delle informazioni utilizzate, prodotte e trasformate dall'azienda durante l'esecuzione dei processi operativi e curare le modalità in cui esse sono gestite dalle risorse umane e dalle tecnologie utilizzate, anche al fine di garantire la disponibilità di risorse tecnologiche funzionali ai servizi aziendali e verificare che siano adeguatamente dimensionate, protette e correttamente utilizzate.*

Elenco dei principali trattamenti eseguiti:

- consentire l'accesso al patrimonio informativo e assicurare che i sistemi informatici dell'azienda vengano utilizzati per scopi lavorativi pertinenti e siano protetti dalle minacce di cybersecurity come, ad esempio, i malware;
- gestione dell'infrastruttura di rete informatica aziendale;
- gestione del traffico di rete e delle regole di instradamento delle informazioni attraverso la rete (c.d. "instradamento");
- gestione dei servizi per la trasmissione delle informazioni attraverso la rete informatica aziendale (es. IP, DNS, FTP, DHCP, DNS, WINS, ecc.);
- gestione del dominio di Active Directory;
- gestione dei servizi di connettività ad internet;
- gestione della sicurezza perimetrale (c.d. "firewall");
- gestione della sicurezza degli accessi logici;
- gestione delle credenziali di autenticazione degli utenti;
- gestione dei profili di autorizzazione degli utenti;
- gestione dei sistemi di autenticazione multifattore (Multi Factor Authentication - MFA) e dei sistemi di autenticazione unica (Sigle Sign On - SSO);
- gestione delle chiavi di cifratura;

- fornire agli utenti servizi software gestionali (es. Enterprise Resource Planning -ERP e Customer Relationship Management - CRM), applicativi di produzione (Microsoft 365) e progettazione (es. CAD / CAE);
- fornire agli utenti aziendali servizi di comunicazione elettronica sicuri ed efficienti;
- gestione della posta elettronica (es. Microsoft 365 Exchange);
- gestione delle comunicazioni vocali (Centralino telefonico) e del Voice Over IP (VoIP);
- gestione dei sistemi di videoconferenza (es. Microsoft Teams);
- gestione dei dispositivi elettronici assegnati in dotazione ai dipendenti e collaboratori per svolgere la propria mansione lavorativa (Dispositivi USB, Endpoint come, ad esempio, Notebook, PC, Tablet, Smartphone, ecc.);
- gestione dei dispositivi di tipo mobile (es. smartphone, tablet) e delle relative SIM Dati/Voce;
- gestione delle vulnerabilità dei dispositivi;
- monitoraggio dei LOG dei sistemi e gestione degli eventi correlati attraverso azioni anche in Real time (c.d. "SIEM"). Vedere *paragrafo 10* Sistemi decisionali e monitoraggi automatizzati;
- gestione e monitoraggio degli eventi prodotti dai sistemi e potenzialmente correlabili agli utenti che li stanno utilizzando in quel momento (c.d. *Event LOG)*;
- gestione e monitoraggio degli eventi generati dal sistema di autenticazione informatica all'atto dell'accesso o tentativo di accesso da parte di un utente di sistema o all'atto della sua disconnessione (c.d. *Access LOG*);
- gestione e monitoraggio delle operazioni eseguite dai software di sistema o dagli utenti del sistema (c.d. *Operational LOG*");
- gestione e monitoraggio delle operazioni sensibili per la sicurezza informatica (c.d. *Security LOG*);
- gestione delle procedure di Disaster Recovery e di Business Continuity.

Quali dati personali sono trattati e da dove provengono:

Oltre ai dati identificativi e di contatto già raccolti per la finalità **F1**, saranno trattati dati quali: credenziali di accesso, dati impliciti nei protocolli di comunicazione, indirizzi (es. IP e MAC), data e ora di un evento, tipologia di evento (es. accessi effettuati, tentativi falliti, operazioni compiute su cartelle, file, dati o sistemi) e altri dati che possono essere ricavati dai software forniti in dotazione ai lavoratori.

I dati sono automaticamente generati dai sistemi informatici della Società, durante il loro utilizzo da parte del lavoratore (es. dati impliciti nel protocollo di rete, Time-Stamp e dati di LOG).

6.2 BASI GIURIDICHE DEL TRATTAMENTO

Devi sapere che l'azienda può trattare i Tuoi dati personali solamente se sussiste almeno una delle seguenti condizioni:

 **Consenso** art. 6.1 lettera **a**) GDPR	Questa base di liceità non è normalmente utilizzabile nell'ambito di un rapporto lavorativo subordinato. Tuttavia, in assenza di altre basi giuridiche e nelle sole circostanze in cui il datore di lavoro può dimostrare la libertà del consenso espresso dal lavoratore, è possibile individuare il consenso quale base giuridica del trattamento. Nei limitati casi in cui Tu debba fornire il consenso hai il diritto di revocarlo in qualsiasi momento senza pregiudicare la liceità dei trattamenti effettuati fino a quel momento.
 **Contratto** art. 6.1 lettera **b**) GDPR	Quando il trattamento è necessario per la corretta esecuzione del contratto di lavoro o del contratto di collaborazione e per il rispetto dei termini degli stessi, oppure allo scopo di effettuare delle trattative volte alla conclusione di detti accordi; Questa base di liceità è applicata principalmente ai Trattamenti eseguiti per le finalità: **F1, F2**.
 **Obbligo Legale** art. 6.1 lettera **c**) GDPR	Quando dobbiamo trattare i Tuoi dati personali allo scopo di rispettare obblighi imposti da leggi o regolamenti come, ad esempio, rispettare gli obblighi previsti dalla legislazione italiana in materia di lavoro, previdenza sociale, ordine pubblico, imposte e tasse, quali, a titolo esemplificativo, gli obblighi previsti dal D.lgs. n.81/2008 (Sicurezza ed igiene dei luoghi di lavoro), dal D.lgs. 198/2006 (Codice delle pari opportunità) o relativi alle previsioni in tema di indennità per malattia o infortuni o di indennità di maternità; Questa base di liceità è applicata principalmente ai Trattamenti eseguiti per le finalità: **F1, F2**.

Legittimo Interesse
art. 6.1 lettera **f**) GDPR

Quando il trattamento si rende necessario per tutelare un interesse legittimo dell'azienda (o di un soggetto terzo) bilanciando l'interesse perseguito con i diritti e le libertà del lavoratore; Ad esempio, quando è necessario intraprendere, esperire ovvero difendersi da un'azione legale.
Questa base di liceità è applicata principalmente ai Trattamenti eseguiti per le finalità: **F3, F4**.

Puoi ottenere ulteriori informazioni sulla base di liceità applicata ad ogni specifico trattamento dichiarato in questa informativa o l'eventuale interesse aziendale perseguito, contattando il **Coordinatore Protezione Dati aziendale**.

6.3 ULTERIORI TRATTAMENTI

Ti informiamo che l'azienda potrà effettuare il trattamento dei Tuoi dati personali senza che Tu ne sia a conoscenza in conformità alle previsioni sopra elencate e quando ciò sia richiesto o consentito dalla legge.
Inoltre, qualora durante il rapporto di lavoro dovessero rendersi necessari ulteriori e specifici trattamenti, non indicati nella presente informativa, sarà cura della Società fornirti preventivamente una specifica informativa e, se del caso, procedere ad acquisire il Tuo necessario consenso. Questo principio verrà applicato anche qualora fosse necessario e lecito il trattamento di categorie particolari di dati (ex art. 9 del GDPR) o il trattamento dei dati personali relativi a condanne penali e reati (ex 10 del GDPR) se ciò è previsto dalla legge.

7 INFORMAZIONI SUI DATI PERSONALI

7.1 QUALI DATI PERSONALI TRATTIAMO

Dati comuni

La Società registra, archivia e utilizza le informazioni necessarie e pertinenti alla gestione del Tuo rapporto di lavoro o di collaborazione con la Società elencate nell'**Allegato A** alla presente Informativa.

Categorie particolari

Alcuni dati personali trattati potrebbero appartenere alle categorie particolari di dati personali ("*dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale ovvero dati genetici o relativi alla salute*" - art. 9 GDPR).
Ad esempio, in modo graduale rispetto al processo di selezione, potremmo, trattare dati relativi a condizioni di disabilità (eventuale iscrizione al collocamento mirato) per valutare la Tua idoneità al lavoro e per garantire il rispetto delle previsioni di cui alla Legge 12 marzo 1999, n. 68 (lavoro disabili).
Il trattamento di tali dati avverrà nel rispetto delle prescrizioni contenute nell'Autorizzazione al trattamento dei dati sensibili nel rapporto di lavoro (n. 1/2016) aggiornata al Provvedimento dell'Autorità Garante del 13 dicembre 2018 ("Provvedimento che individua le prescrizioni contenute nelle Autorizzazioni generali che risultano compatibili con il Regolamento e con il D.lgs. n. 101/2018 di adeguamento del Codice" – Doc. web n. 9068972).
Inoltre, le informazioni relative alla Tua salute saranno trattate dal nostro medico competente al fine di valutare la Tua idoneità a svolgere le mansioni a te affidate.

Informazioni relative a condanne penali

Raccoglieremo informazioni relative alle condanne penali e reati solo qualora ciò sia necessario e appropriato data la natura del ruolo e sempre che tale indagine sia consentita o richiesta dalla Legge.
In questi casi, la Società registrerà tali informazioni durante il processo di assunzione o nel caso sia messa al corrente direttamente da Te. Inoltre, sempre se previsto dalla legge e necessario, in relazione a determinati ruoli, effettueremo un controllo periodico delle condanne penali e reati che potrà avvenire anche mediante autocertificazione.

Utilizzeremo tali informazioni per le seguenti ragioni:

- valutazione dell'adeguatezza a ricoprire un determinato ruolo;
- qualora sia necessario per proteggere un Tuo interesse, gli interessi di altri lavoratori ovvero per proteggere i clienti, fornitori ed i terzi da furti, truffe e rischi similari;
- qualora sia necessario in relazione ad un procedimento legale.

La Società è autorizzata ad utilizzare i Tuoi dati personali in questi termini qualora sia necessario per rispettare i propri diritti ed i propri obblighi quale datore di lavoro.
Sarà cura della Società avvisarti qualora si renda necessario il trattamento di informazioni relative alle condanne penali e reati.

7.2 DA DOVE PROVENGONO I DATI TRATTATI E COME LI RACCOGLIAMO

I dati personali necessari e funzionali ai trattamenti dichiarati in questa informativa, possono essere:

a) forniti da Te stesso;
b) ottenuti da terze parti (generalmente nel corso del processo di selezione ed assunzione del personale). In particolare, alcuni dati possono essere ottenuti da pubbliche amministrazioni, agenzie per l'impiego, assicurazioni, banche, clienti, fornitori, altri nostri dipendenti o collaboratori, agenzie di servizi;
c) generati dalla Società nel corso di attività correlate e svolte durante il rapporto di lavoro / collaborazione;
d) generati automaticamente o ricavati durante il Tuo utilizzo dei sistemi informatici aziendali.

7.3 COSA SUCCEDE SE NON CI FORNISCI I DATI RICHIESTI O CI FORNISCI DATI ERRATI

Per le finalità **F1** ed **F2**, il conferimento dei Tuoi dati personali è un requisito necessario e un Tuo eventuale rifiuto a conferire le informazioni richieste potrebbe non consentire alla Società di rispettare tutti gli adempimenti imposti dalla legge o dagli obblighi contrattuali, ovvero, di effettuare tutti gli adempimenti relativi al Tuo rapporto di lavoro o di collaborazione come, a titolo esemplificativo, quelli relativi alle buste paga, la gestione dei benefit, il pagamento delle imposte, gli adempimenti assicurativi nonché quelli volti ad assicurare la Tua salute e la Tua sicurezza sul lavoro.
Inoltre, è molto importante che i dati personali da Te forniti siano precisi ed aggiornati, per questo motivo sei invitato ad informare tempestivamente il dipartimento delle risorse umane della Società nel caso di eventuali modifiche intervenute nel corso del rapporto lavorativo.

8 CONSERVAZIONE

Generalmente, conserveremo i Tuoi dati personali solo per il tempo necessario a raggiungere gli scopi per i quali i medesimi dati sono stati raccolti, anche al fine di soddisfare eventuali requisiti legali, contabili o di segnalazione alle autorità competenti.
In generale, ciò significa che conserveremo i Tuoi dati personali per tutta la durata del nostro rapporto di lavoro e, successivamente, per un periodo di **10 anni** dal momento della cessazione o, in caso di contestazioni, per il termine prescrizionale previsto dalla normativa per la tutela dei diritti connessi, fatti salvi in ogni caso periodi di conservazione maggiori previsti da specifiche normative di settore.
In alcune circostanze potremmo rendere anonimi i Tuoi dati personali cosicché non potranno più essere associati a Te, in tali casi potremmo utilizzare detti dati senza ulteriore avviso nei Tuoi confronti.
Per ulteriori dettagli circa il periodo di conservazione dei Tuoi dati personali puoi contattare le risorse umane o il Coordinatore Protezione Dati Aziendale.

9 MODALITÀ DEL TRATTAMENTO

9.1 COME TRATTIAMO I TUOI DATI PERSONALI

A partire dalla loro acquisizione, la Società tratterà i Tuoi dati personali mediante strumenti cartacei, informatici e telematici. In ogni caso, allo scopo di prevenire ogni accesso da parte di persone non autorizzate, anche attraverso il nostro sistema di gestione DPMS, adottiamo ed osserviamo severe procedure per conservare, utilizzare e permettere di visionare i Tuoi dati personali. Il trattamento dei Tuoi dati avviene con logiche strettamente correlate alle finalità dichiarate e, comunque, in modo da garantire sempre la riservatezza, l'integrità e la disponibilità dei dati stessi.
A tal proposito, i Tuoi dati saranno raccolti e trattati per le finalità dichiarate e se necessario, aggiornati, cancellati e rettificati anche in base alle Tue indicazioni.

9.2 COME GARANTIAMO LA SICUREZZA DEI TUOI DATI PERSONALI

Il sistema di gestione DPMS prevede idonee misure di sicurezza al fine di prevenire la perdita dei dati, usi illeciti o non corretti degli stessi ovvero accessi non autorizzati, a tal proposito, la Società ha provveduto a censire tutti i rischi per i diritti e libertà dei soggetti interessati coinvolti nei trattamenti dichiarati in questa informativa, identificando i rischi incombenti sugli asset informatici utilizzati per tali trattamenti. Tutti i rischi sono stati successivamente valutati (analizzando le fonti di rischio) e mitigati (mitigando le minacce in grado di concretizzarli), mediante l'adozione di misure tecniche e organizzative ritenute adeguate.

9.3 UTILIZZO DI DISPOSITIVI PERSONALI PRIVATI DEL DIPENDENTE

In alcune limitate circostanze e previa autorizzazione scritta, l'azienda adotta un insieme di criteri per consentire ai dipendenti di utilizzare i propri dispositivi personali privati (telefono, laptop, tablet o altro) per accedere alle applicazioni e/o ai dati aziendali in alternativa all'utilizzo di dispositivi forniti dall'azienda (es. APP timbrature, Token virtuali per autenticazione, WEB mail, ecc.).
In questo caso l'azienda, anche indirettamente, può acquisire le informazioni del dispositivo personale del lavoratore rilasciate implicitamente attraverso il protocollo di comunicazione di rete.

9.4 VIDEOCONFERENZA

I sistemi di videoconferenza aziendale consentono la registrazione della Tua immagine e della Tua voce. In molte circostanze l'attivazione della webcam e del microfono sono requisiti essenziali al fine di svolgere la Tua mansione lavorativa. La società farà di tutto per proteggere i Tuoi dati personali raccolti attraverso i sistemi di videoconferenza.
In qualità di lavoratore sei tenuto a rispettare la politica aziendale sull'utilizzo accettabile dei sistemi di videoconferenza e sei reso consapevole che l'azienda si riserva il diritto di effettuare i necessari controlli.

9.5 LAVORO DA REMOTO O FUORI SEDE

In relazione alla Tua prestazione lavorativa in modalità remota (es. *smart working) o fuori sede (es. trasferta),* **ESA-Com** effettuerà trattamenti dei Tuoi dati personali con la finalità di consentire lo svolgimento della Tua attività lavorativa al di fuori dei locali aziendali. Più in dettaglio, i trattamenti perseguiranno finalità connesse e strumentali alla gestione del rapporto di lavoro, anche allo scopo di consentire la cooperazione, la supervisione e la comunicazione tra colleghi e con i Tuoi superiori gerarchici. I trattamenti sono, altresì, volti a consentire le opportune sinergie lavorative, oltre che la Tua necessaria partecipazione alla vita sociale aziendale (come ad es. la normale interazione con i colleghi).
Questa modalità di lavoro comporta il rispetto di specifiche norme di sicurezza che la società si impegna a far rispettare ai propri dipendenti/collaboratori anche mediante controlli.

10 SISTEMI DECISIONALI E MONITORAGGI AUTOMATIZZATI

Non prevediamo di sottoporti a nessuna decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che possa produrre effetti in grado di incidere in modo significativo sulla Tua persona o possa influire sulla Tua crescita professionale all'interno della nostra azienda.

Tuttavia, per trasparenza, Ti informiamo che l'azienda utilizza software e sistemi di sicurezza in grado di eseguire monitoraggi automatici che possono dare origine a decisioni automatizzate che, pur non incidendo in modo significativo sulla tua persona, possono impattare temporaneamente sui Tuoi processi lavorativi (es. blocco temporaneo dell'accesso al sistema).

Tali sistemi sono in grado di evidenziare e segnalare possibili violazioni delle policy di sicurezza ICT e fornire informazioni che consentono all'azienda la prevenzione degli incidenti e l'accertamento di eventuali violazioni di sicurezza commesse durante lo svolgimento della Tua prestazione lavorativa. In particolare, i monitoraggi di sicurezza comprendono:

10.1 MONITORAGGIO ATTRAVERSO I SISTEMI DI CYBERSECURITY

ESA-Com adotta severe politiche di sicurezza sulla gestione e l'utilizzo delle risorse ICT aziendali, tali politiche prevedono l'applicazione di specifici controlli di sicurezza al fine di verificarne la corretta applicazione.
I controlli sono effettuati esclusivamente per finalità di Cybersecurity e possono avvenire mediante monitoraggi automatici che possono generare processi decisionali automatizzati in grado di registrare, segnalare o bloccare le attività dell'utente.
In particolare, sono attivi i seguenti monitoraggi:

a. **sistema di Asset Management** in grado di controllare eventuali modifiche alle configurazioni hardware e software dei sistemi ICT in dotazione al lavoratore;
b. **sistema di Vulnerability Assessment** in grado di identificare e classificare le vulnerabilità degli asset aziendali e definire le priorità di correzione e mitigazione delle vulnerabilità del software;
c. **sistema di Endpoint Protection** (c.d. "*Antivirus*") in grado di rilevare codici malevoli anche attraverso il monitoraggio dei comportamenti anomali del sistema;
d. **sistema Firewall** in grado di monitorare e bloccare il traffico di rete pericoloso generato dai sistemi in dotazione all'utente lavoratore;

e. **sistema di Log Management (c.d. "SIEM")** in grado di raccogliere, registrare, analizzare e correlare i Log generati dai sistemi ICT aziendali al fine di rilevare comportamenti anomali dei sistemi o violazioni delle politiche aziendali di cybersecurity;
f. **sistemi di gestione e controllo degli accessi logici** in grado di assicurare l'accesso sicuro alle risorse informative aziendali in funzione delle credenziali di autenticazione e autorizzazione rilasciate al lavoratore, anche mediante tecniche c.d. "di *Multi Factor Authentication*" (MFA);
g. **sistemi o servizi di Penetration Test** in grado di simulare attacchi cibernetici ai sistemi ICT aziendali anche attraverso tecniche c.d. di "*Social Engineering*" rivolte agli utenti lavoratori a cui sono assegnati in dotazione gli strumenti.

Tutti i sistemi di Cybersecurity sopra elencati, pur essendo destinati al monitoraggio dei sistemi ICT, possono consentire di rilevare indirettamente comportamenti errati o anomali dell'utilizzatore del sistema. Tali comportamenti possono comportare la violazione di regolamenti aziendali e l'applicazione delle relative sanzioni.

I sistemi di Cybersecurity aziendali sono implementati nel rispetto della normativa sulla protezione dei dati personali e di quanto stabilito dall' art. 4 della Legge n. 300/1970 - c.d. "*Statuto dei Lavoratori*".

10.2 MONITORAGGIO ATTRAVERSO I SISTEMI DI GESTIONE DELL'ACCESSO FISICO ALLE AREE AZIENDALI

Per esigenze organizzative e di tutela del patrimonio, **ESA-Com** è dotata di un sistema di controllo degli accessi fisici alle aree aziendali mediante dispositivo Badge.
Il sistema viene utilizzato per la registrazione delle timbrature delle presenze e l'accesso allo stabilimento.

10.3 MONITORAGGIO IN AMBITO EROGAZIONE DELLA FORMAZIONE

L'azienda aggiorna costantemente i propri piani di formazione. In particolare, oltre ai corsi di aggiornamento professionale, vengono effettuati corsi di formazione e consapevolezza in ambito Cybersecurity, Data Protection, Information Security e sicurezza del lavoro.
I corsi di formazione possono essere erogati nelle seguenti modalità:
a. Formazione sincrona in presenza fisica o a distanza (on-line) o mista;
b. Formazione asincrona on-line (es. mediante piattaforma dedicata FAD).
La partecipazione ad un corso on-line può comportare il monitoraggio automatico della presenza del lavoratore al corso e possono essere utilizzati sistemi di decisione automatizzata del raggiungimento degli obiettivi (superamento di test di valutazione).
In alcuni casi, l'azienda potrebbe effettuare campagne di valutazione della resilienza dell'utente agli attacchi di Cybersecurity c.d. "Penetration Test" mediante l'utilizzo di software automatizzati (es. campagne di Phishing). In caso di esito positivo (attacco andato a buon fine) tali software invitano il lavoratore ad effettuare corsi obbligatori di aggiornamento e a superare specifici test di valutazione dell'apprendimento. Il mancato superamento di tali Test potrebbe comportare in alcuni casi la sospensione dell'account del lavoratore per ragioni di sicurezza. Tutti gli automatismi saranno sempre gestiti sotto la supervisione dell'ICT Manager aziendale a cui il lavoratore potrà sempre far ricorso in caso di difficoltà o necessità di chiarimento.

11 CHI PUÒ VENIRE A CONOSCENZA DEI TUOI DATI PERSONALI

Potremmo condividere i Tuoi dati personali con società, organizzazioni ed individui interni ed esterni alla nostra Azienda nei seguenti termini:

a) con **dipendenti e collaboratori** aziendali per scopi organizzativi, produttivi e amministrativi e di gestione dei servizi informatici aziendali;

b) a condizione di poter adottare, da parte nostra, misure ragionevoli volte a garantire, su base permanente, la sicurezza dei Tuoi dati personali:
- **fornitori, distributori e terzi contraenti** che effettuano servizi per la nostra azienda e trattano i Tuoi dati personali per nostro conto, per gli scopi suddetti, sulla base di nostre istruzioni, inclusi:
  - coloro che svolgono indagini di preassunzione;
  - il nostro consulente del lavoro, il medico competente, RSPP esterno;
  - gli studi di consulenza che provvedono all'elaborazione delle buste paga;
  - gli enti pensionistici;

- fornitori di benefit ai dipendenti (es. società erogazione buoni pasto, sanità privata, compagnie assicurative, società di noleggio auto, leasing);
- servizi per la formazione, finanziata e no;
- consulenti, anche legali, ed altri professionisti;
- fornitori di servizi informatici e cybersecurity.

c) **autorità competenti** (ad es. Agenzia delle Entrate), Autorità Giudiziale e le altre Autorità previste dalla legge, organi di vigilanza, auditor di terze parti;

d) **società, organizzazioni od individui interni o esterni alla nostra azienda** qualora la comunicazione dei dati personali sia ragionevolmente necessaria a:
- rispettare ogni legge o regolamento applicabile, procedimento giudiziario, o provvedimento amministrativo o richiesta proveniente da Autorità amministrative, ad esempio, Autorità amministrative indipendenti od enti pubblici (per l'amministrazione degli adempimenti fiscali e previdenziali);
- far rispettare il Tuo contratto di lavoro, inclusa l'indagine di potenziali violazioni;
- rilevare, prevenire o comunque contrastare truffe, problemi di sicurezza o tecnici;
- fornire a potenziali acquirenti od investitori informazioni relative all'impiego di qualsiasi *asset* od attività dell'azienda;
- proteggere da danni ai diritti, alle proprietà od alla sicurezza della nostra azienda, dei nostri dipendenti, contraenti, clienti o del pubblico, come richiesto dalla, e nei limiti di, legge.

Ti informiamo che potremo comunicare i Tuoi dati identificativi e di contatto aziendali (es. indirizzo mail o numero di telefono aziendale, la Tua presenza in azienda, il Tuo titolo di studio, il Tuo ruolo in azienda) e ogni altra informazione ritenuta ragionevolmente pertinente a clienti, fornitori o altri soggetti attinenti alla Tua mansione lavorativa, qualora ciò fosse opportuno e necessario al fine del raggiungimento degli obiettivi di business in conformità con il Tuo contratto di assunzione.

12 TRASFERIMENTO ALL'ESTERO

Normalmente **ESA-Com** non trasferisce i dati personali all'esterno dello Spazio Economico Europeo (SEE). Tuttavia, qualora i Tuoi dati personali dovessero essere trasferiti verso Paesi situati fuori dallo spazio economico europeo (SEE), in assenza di decisioni di adeguatezza della Commissione dell'Unione Europea, **ESA-Com** farà in modo di garantire tutele appropriate per proteggere i dati personali dei propri dipendenti in questi Paesi. Alcune delle tutele che potrebbero essere adottate, ove appropriato, includono l'utilizzo di clausole contrattuali standard approvate dalla Commissione Europea, la pseudonimizzazione e, se possibile, la cifratura dei dati stessi.
A titolo esemplificativo ma non esaustivo, Ti comunichiamo che il trasferimento all'estero dei Tuoi dati personali è spesso legato all'utilizzo di tecnologie cloud, sistemi di comunicazione digitale, software di sicurezza e protezione dei servizi informatici. I questi casi la nostra Società si impegna ad utilizzare servizi scelti tra gli operatori che garantiscono maggiori standard di sicurezza e attenzione alla protezione dei dati personali.
A tal proposito, Ti informiamo che **ESA-Com** utilizza alcuni servizi ICT forniti da società USA come ad esempio Microsoft, Google e Apple che operano in qualità di nostri Responsabili del Trattamento ai sensi dell'art 28 del GDPR.
Per questa ragione, sottoscriviamo con tali società contratti di servizio e "*Data Processing Agreement* "(DPA) che includono anche le "*Standard Contractual Clauses*" (SCCs) stabilite dalla Commissione Europea ai sensi dell'art. 46, par. 1, GDPR.
Tuttavia, pur selezionando dove possibile l'erogazione di tali servizi attraverso Data Center ubicati all'interno dello SEE, il Responsabile del Trattamento potrebbe dover consentire l'accesso ai nostri dati alle autorità americane per effetto del c.d. "Cloud ACT".

13 DIRITTI DELL'INTERESSATO

In qualità di soggetto interessato, potrai esercitare in qualunque momento i diritti che Ti sono riconosciuti dagli articoli da 15 a 22 del Regolamento. In particolare, nelle modalità e nei limiti di legge, Ti sono garantiti i seguenti diritti:

- **Accesso**: hai il diritto di chiederci se stiamo trattando dei Tuoi dati personali, nel caso, potrai accedere ai Tuoi dati personali (comunemente indicati come "dati soggetti a richiesta di accesso"). Questo Ti permette di ricevere una copia dei dati personali che conserviamo su di Te e di controllare che il trattamento stia avvenendo in modo legittimo.
- **Correzione o rettifica**: hai il diritto di richiedere che ogni Tuo dato personale incompleto od impreciso in nostro possesso venga corretto.

- **Cancellazione od Anonimizzazione**: in alcune circostanze hai il diritto di chiederci di cancellare o rimuovere i Tuoi dati personali, ovvero di renderli anonimi. Vi sono alcune ipotesi nelle quali potremo rifiutarci di dar seguito ad una Tua richiesta di cancellazione, ad esempio qualora i Tuoi dati personali siano necessari per rispettare la legge ovvero in relazione a procedimenti legali.
- **Limitazione**: hai il diritto di chiedere di sospendere il trattamento di determinati Tuoi dati personali, ad esempio qualora Tu voglia accertarti della loro precisione ovvero della ragione che ne ha determinato il trattamento da parte nostra.
- **Portabilità**: potrai richiedere la portabilità dei Tuoi dati personali ad un terzo.
- **Opposizione**: qualora stessimo trattando i Tuoi dati personali sulla base di un Interesse Legittimo nostro (o di un terzo) avrai il diritto di opporti in qualunque momento al trattamento dei dati. Ad ogni modo potremmo essere legittimati a proseguire nel trattamento dei Tuoi dati sulla base del nostro Interesse Legittimo.

Per l'esercizio dei Tuoi diritti puoi utilizzare i canali di contatto che Ti abbiamo comunicato in questo documento.

13.1 MODULISTICA PER L'ESERCIZIO DEI DIRITTI

Per esercitare i Tuoi diritti verso la nostra Società, puoi utilizzare il modulo messo a disposizione dall' Autorità Garante.
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1089924

13.2 ESERCIZIO DEI DIRITTI MEDIANTE SOGGETTO DELEGATO

Se eserciti i Tuoi diritti attraverso un soggetto delegato, tale soggetto dovrà fornirci una copia della delega e i necessari documenti per l'identificazione.

14 RECLAMO ALL'AUTORITÀ DI CONTROLLO (art. 77 GDPR)

Fatta salva la possibilità di rivolgerti alla Società per ottenere qualunque informazione in merito al trattamento dei Tuoi dati personali o per esercitare i diritti che Ti sono riconosciuti dal Regolamento, Ti informiamo che puoi proporre reclamo dinnanzi all' Autorità amministrativa indipendente competente nello Stato Membro dell'Unione Europea dove risiedi abitualmente, dove lavori, ovvero dove ritieni si sia verificata un'asserita violazione della legge sulla protezione dei Tuoi dati personali.
Nel territorio italiano puoi presentare un reclamo al Garante per la Protezione dei Dati Personali (GPDP).
Per informazioni su come presentare il tuo reclamo puoi contattare il GPDP ai seguenti recapiti:

Garante per la protezione dei dati personali

Centralino:	+39 06.696771
Indirizzo e-mail:	garante@gpdp.it
Indirizzo PEC:	protocollo@pec.gpdp.it
Sito Web:	https://www.garanteprivacy.it

15 AGGIORNAMENTO DELL'INFORMATIVA

Il documento viene revisionato periodicamente in funzione di cambiamenti normativi e/o aziendali.
In caso di modifica nelle sue parti fondamentali (come ad esempio le finalità, modalità, a chi comunichiamo i dati, dove li trasferiamo, ecc.) sarà cura della nostra Società informarti del cambiamento.
Inoltre, Ti informiamo che la versione aggiornata di questa informativa è sempre disponibile presso le risorse umane, sulla intranet aziendale e nelle apposite bacheche.

ALLEGATO A – ELENCO DELLE CATEGORIE DI DATI PERSONALI TRATATTATI

Dati personali

- *Identificatori Personali* come titolo, nome, data di nascita, età, genere, residenza, *e-mail* personale, numero di telefono, numero di patente, passaporto, nonché, se applicabile, codice fiscale, numero di previdenza sociale, numero di carta d'identità.
- *CV* che includerà informazioni sulla tua formazione scolastica e dettagli come qualifiche, dati accademici, scuole, formazione e competenze professionali.
- *Dati sul personale* che includono offerte di lavoro, lettere di presentazioni, conoscenza politica aziendale, contratti di lavoro, promozioni e trasferimenti, licenze e certificazioni dei dipendenti, lettere di dimissioni o di conclusione del contratto di lavoro, dati sulle *exit interview* ed eventuali accordi, valutazioni e revisioni delle prestazioni, registro richieste di permessi e assenze, registro sulle procedure disciplinari e relativo alla formazione, appartenenza ad associazioni professionali.
- *Informazioni fornite nell'ambito del procedimento di assunzione* (vedi Informativa per i Candidati).
- *Dati relativi all'impiego* come inquadramento, qualifica, descrizione delle mansioni, ID impiegato, tipo di impiego e se full oppure part-time, luogo di lavoro, data inizio impiego, data cessazione rapporto di lavoro, foto riconoscimento e dettagli organizzativi come il nome della società, recapito, telefono aziendale ed e-mail, credenziali intranet aziendale, dettagli sul dipartimento e sul supervisore.
- *Informazioni finanziarie* come lo storico dei compensi, i benefit (inclusi moduli di iscrizione e richiesta, report sugli accantonamenti e gli anni di servizio, documentazione riassuntiva di iscrizione e partecipazione alla programmazione benefit, comunicazioni generali agli impiegati sui benefit), titolarità di azioni, paghe, spese di trasferta, dati sugli assegni, dati sul conto corrente bancario, obiettivi bonus, dati sulla pensione.
- *Registri generati da o in occasione di indagini* in caso di presunte violazioni o al fine generale di raccogliere fatti o altre informazioni.

Informazioni relative alla famiglia

- Recapiti di emergenza.
- Stato civile, numero ed identità di moglie e persone a carico (se presenti) allo scopo di assegnare i benefit.
- Dati dei beneficiari, per quanto concerne l'assicurazione sanitaria ed altri benefit per i dipendenti e le loro famiglie.

Dati relativi all'utilizzo da parte tua del nostro sistema informatico e di comunicazione

- Registri relativi all'utilizzo da parte Tua dei nostri sistemi IT, incluse e-mail, internet, computer, lap-top (acceso da remoto incluso) telefono e dispositivi mobili.
- Registrazioni immagini dal sistema di video-sorveglianza ed altre informazioni ottenute attraverso mezzi elettronici quali i Badge magnetici.

Dati relativi alle condanne penali

- Dati del casellario giudiziale, sanzioni amministrative e reati.

Categorie particolari di dati personali

Potremmo occasionalmente raccogliere, archiviare ed utilizzare le seguenti "categorie particolari" di dati personali:

- Origine razziale ed etnica ed informazioni relative a disabilità, credenze religiose, orientamento sessuale per il controllo del rispetto delle pari opportunità (nei casi previsti dalla legge).
- Condizioni di salute fisica e mentale (ad es., registro accesso alle cure sanitarie, registro esiti alcool test e test antidroga, esami medici e registro assenze per malattia ed infortuni sul lavoro e sinistri così come registri sulla salute dei dipendenti richiesti dalla legge o dalle autorità amministrative indipendenti.
- Dati biometrici.
- Registro dati su immigrazione e naturalizzazione per gli impiegati e gli operai rispetto ai quali tali dati possono rivelare informazioni sulla razza e/o l'origine etnica.
- Informazioni relative all'appartenenza ad un'associazione sindacale.

DICHIARAZIONE DEL DIPENDENTE

Questa dichiarazione è richiesta dal Titolare del trattamento ai sensi dell'art. 24 Regolamento UE 2016/679
"Responsabilità del Titolare del trattamento"
(Principio di Accountability)

Io sottoscritto/a _____,

con riferimento al rapporto di lavoro in corso con la società **ESA-Com S.p.A.** con sede in Via Labriola n. 1 – 37054 Nogara (VR)

Dichiaro

di aver ricevuto le informazioni contenute nell'informativa privacy dipendenti in merito al trattamento dei miei dati personali relativamente alla gestione del rapporto di lavoro e segnatamente relative:

- alle finalità a cui sono destinati i miei dati personali (ed eventualmente dei miei familiari), comprese le categorie particolari di dati personali nonché gli eventuali dati relativi a condanne penali e reati, e alle modalità del relativo trattamento;
- alla natura obbligatoria o facoltativa del conferimento dei dati richiesti e alle conseguenze di un mio eventuale rifiuto a fornire tali dati;
- ai soggetti ai quali i dati personali possono essere comunicati;
- al periodo di conservazione dei dati;
- ai diritti riconosciuti dal GDPR e alle relative modalità di esercizio.

Luogo e data,_____

Firma: _____