

ATTO DI AUTORIZZAZIONE AL TRATTAMENTO

ICT Management

Ariston S.p.A. (di seguito, la “Società”), in qualità di Titolare del trattamento, con sede legale in Via **Viale Aristide Merloni n. 45, 60044, Fabriano (AN)**, CF **02853230429** e P.IVA **02853230429**, in persona del proprio legale rappresentate pro tempore,

PREMESSO CHE

- a. il Regolamento (UE) 2016/679 del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (di seguito, “**GDPR**” o “**Regolamento**”), prevede che le operazioni di trattamento di dati personali possono essere effettuate solo da persone fisiche che operano sotto la diretta autorità del Titolare o del Responsabile del trattamento che siano state espressamente “*autorizzate al trattamento dei dati personali*” e che siano state “*istruite in tal senso*” (art. 29 e art. 4, n. 10, del GDPR);
- b. il Garante per la protezione dei Dati Personali (di seguito, “Garante”), nella “Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali” del 28 aprile 2017, ritenendo le disposizioni previgenti in materia di “incaricati” del trattamento pienamente compatibili con la struttura e la filosofia del Regolamento, ha suggerito di mantenere in essere la struttura organizzativa e le modalità di designazione degli incaricati così come delineatesi negli anni anche attraverso gli interventi del Garante, come misura tecnica e organizzativa adeguata;
- c. il 19 settembre 2018 è entrato in vigore il d.lgs. 10 agosto 2018, n. 101 che ha adeguato la normativa nazionale ed in particolare il D. Lgs. 30 Giugno 2003, n. 196 (di seguito “Codice Privacy”) al GDPR (di seguito, “d.lgs. 101/2018”);
- d. l’art. 2-quaterdecies del Codice Privacy, così come modificato dal d. lgs. 101/2018, rubricato “Attribuzione di funzioni e compiti a soggetti designati”, prevede, al secondo comma, che “il titolare ed il responsabile individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta”;
- e. in applicazione del suddetto principio di accountability, la Società si è dotata di un proprio assetto organizzativo in ambito Privacy e Data Protection e ha pertanto deciso di procedere con la nomina dei soggetti autorizzati al trattamento, al fine di garantire il rispetto delle prescrizioni contenute nella normativa di riferimento;
- f. preso atto di quanto sopra, la Società con la presente autorizza al trattamento i propri dipendenti che, nell’espletamento delle loro mansioni, hanno necessità di trattare dati personali di cui la Società è Titolare e/o Responsabile.

AUTORIZZA

Il Sig./la Sig.ra **MALTONI LUIGI** nato/a a SAVIGNANO SUL RUBICONE il 17/01/1963,
al trattamento sia cartaceo che automatizzato dei dati specificati nell'**Allegato 1** (di seguito, "**Dati Personali**"), di competenza della Functional Area **ICT** fornendogli le istruzioni indicate nell'**Allegato 2**.

L'autorizzato si impegna a rispettare le istruzioni fornite dal Titolare.

Per tutto quanto non previsto dal presente atto si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

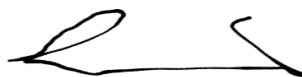
La presente nomina cessa con il venir meno per qualunque motivo del rapporto di lavoro in essere.



Il legale rappresentante
Maurizio Brusadelli

Per presa visione

Il soggetto autorizzato al
trattamento



Data: 24/05/2024 15:18:40

Firma elettronica con Sign4Top

MALTONI LUIGI

ALLEGATO 1

AMBITO del TRATTAMENTO

Il presente allegato specifica tipologia, ambito e natura del trattamento a cui l'Incaricato è autorizzato in base alle proprie mansioni.

TIPOLOGIA DI DATI PERSONALI OGGETTO DI TRATTAMENTO

- ☒ Dati comuni
- ☒ Dati particolari
- ☐ Dati relativi a condanne penali, reati o a connesse misure di sicurezza

CATEGORIE DI INTERESSATI

- ☒ Clienti
- ☒ Fornitori
- ☒ Utenti
- ☒ Candidati
- ☒ Dipendenti

NATURA E FINALITÀ DEL TRATTAMENTO

Gestione e sviluppo dei sistemi informativi; assistenza e supporto utenti; gestione delle misure tecniche e organizzative di sicurezza, gestione e erogazione dei servizi informativi aziendali, anche infrastrutturali; gestione attività di reportistica aziendale; garantire il funzionamento e la continuità del servizio, l'utilizzo e la sicurezza dei sistemi informativi, delle infrastrutture e delle reti.

I soggetti che operano all'interno della Functional Area ICT sono autorizzati dalla Società ad effettuare, in base alle mansioni assegnate, le operazioni di trattamento dei dati personali mappate all'interno del Registro dei Trattamenti tenuto dalla Società ai sensi dell'art. 30 del GDPR, tenuto conto delle istruzioni impartite dalle strutture preposte dal Titolare per la gestione della protezione dei dati.

ALLEGATO 2

ISTRUZIONI

Al fine della corretta gestione dei Dati Personali, è obbligatorio attenersi alle seguenti indicazioni, nonché alle successive eventuali istruzioni impartite dalla Società.

Le ricordiamo che, nello svolgimento delle operazioni di trattamento dei Dati Personali, Lei sarà tenuto/a ad osservare, in quanto applicabili e per quanto di Sua competenza, le norme vigenti in materia di protezione dei Dati Personali. In particolare:

1. In materia di principi generali, Lei dovrà:

- rispettare tutti i principi generali previsti in materia di protezione dei Dati Personali, tra i quali:
 - **Principio di stretta finalità:** i Dati Personali sono raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni di trattamento in termini compatibili con tali scopi;
 - **Principio di correttezza:** i Dati Personali sono esatti e, se necessario, aggiornati;
 - **Principio di pertinenza:** i Dati Personali sono pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
 - **Principio di limitazione temporale:** i Dati Personali sono conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati;
 - **Principio di cessazione del trattamento:** i Dati Personali trattati in violazione dei principi fin qui esposti non possono essere utilizzati e devono essere distrutti;
- trattare esclusivamente i Dati Personali necessari per l'espletamento delle proprie mansioni e/o per svolgere i compiti affidati;
- mantenere l'assoluta segretezza sulle informazioni di cui si venga a conoscenza nel corso delle operazioni del trattamento ed evitare qualunque diffusione delle informazioni stesse tenuto conto che l'eventuale violazione dell'obbligo ivi considerato può comportare l'applicazione di sanzioni di natura disciplinare ed una responsabilità civile e penale, secondo quanto previsto dal codice della privacy;
- astenersi dal trasmettere i Dati Personali a soggetti terzi esterni alla Società, salvo che ciò sia espressamente previsto e/o autorizzato dal Titolare e/o dalla legge;
- salvo espressa autorizzazione del Titolare, astenersi dall'effettuare copie dei Dati Personali, salvo che ciò non sia reso necessario in ragione dei compiti a Lei affidati, e comunque conservare tutte le copie autorizzate, così come gli eventuali originali cartacei dei documenti, in appositi armadi chiusi a chiave;
- astenersi dal costituire e/o duplicare qualsiasi banca dati per finalità che non siano strettamente pertinenti allo svolgimento dei compiti a Lei affidati e/o dal predisporre nuove procedure per la gestione dei Dati Personali;
- conservare i Dati Personali in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;

- ove possibile, accertarsi che la Società abbia messo a disposizione degli interessati l'Informativa Privacy;
- segnalare tempestivamente al Titolare del trattamento qualsiasi richiesta di esercizio dei diritti da parte degli interessati e, per quanto di competenza, fornire ogni necessario supporto nell'evadere in modo completo e tempestivo tali richieste;
- collaborare con gli altri Incaricati del medesimo trattamento stesso, nel rispetto delle indicazioni ricevute;
- attenersi alle istruzioni che Le sono state impartite con il presente atto di nomina e/o atti integrativi successivi, i quali La autorizzano a trattare esclusivamente i Dati Personali oggetto dei trattamenti correlati all'esercizio delle Sue funzioni e riportati nel Registro delle attività di trattamento ex art. 30 del GDPR e come specificato all'Allegato 1, che il Titolare si impegna a fornire all'Autorizzato nella versione più aggiornata al momento della richiesta;
- mantenere la massima riservatezza, anche al termine del rapporto di lavoro, sui Dati Personali delle quali sia venuto a conoscenza nell'adempimento dello svolgimento delle Sue attività.

2. **In materia di misure di sicurezza per i trattamenti effettuati con l'ausilio di strumenti elettronici, Lei dovrà osservare tutte le misure di sicurezza, già in atto o successivamente disposte dalla Società, atte ad evitare rischi di distruzione, perdita, accesso non autorizzato, o trattamento non consentito dei Dati Personali. Fra queste:**

- **Regola dello "Schermo Sicuro":** non lasciare incustodita e accessibile la propria postazione informatica. Anche nel caso di assenza temporanea, attivare il blocco con parola chiave dello strumento informatico utilizzato o, in alternativa, attivare permanentemente la funzione di blocco automatico con parola chiave dello strumento stesso.
- **Integrità e disponibilità dei Dati:** provvedere al salvataggio periodico dei Dati Personali, con frequenza possibilmente mensile, attraverso cartelle di rete, oltre che al loro ripristino nel caso di danneggiamento degli stessi o di danneggiamento degli strumenti elettronici impiegati nell'ambito del loro trattamento.
- **Dismissione e riuso degli strumenti elettronici e dei supporti di memorizzazione:** se non utilizzati, distruggere o rendere inutilizzabili i supporti di memorizzazione (compresi i supporti di memorizzazione contenuti negli strumenti elettronici, le copie di sicurezza utilizzate per le attività di salvataggio e ripristino contenenti Dati). Tali supporti di memorizzazione possono essere riutilizzati soltanto se le informazioni in essi precedentemente contenute non sono intellegibili e/o tecnicamente recuperabili.
- **Sistema di autenticazione:** adottare una password per l'accesso al proprio personal computer, nonché agli eventuali ulteriori dispositivi utilizzati per lo svolgimento del Trattamento in oggetto. Le password corte e facili da indovinare costituiscono un alto rischio. Si devono, dunque, utilizzare solamente le c.d. "*Quality Password*", che rispettino almeno le seguenti policy:
 - deve essere composta da almeno 8 caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
 - deve essere modificata al primo utilizzo;
 - deve essere modificata almeno ogni 3 mesi per il trattamento di Dati Personali, dati sensibili o giudiziari;

Ariston SpA
Viale Aristide Merloni 45 60044 Fabriano (AN) T: (+39) 0732 6011 F: (+39) 0732 602331
ariston@pec.ariston.com
aristongroup.com

- deve essere inoltre modificata al primo accesso successivo a quello di un soggetto terzo, espressamente autorizzato dalla Società;
- deve essere diversa dalle ultime 5 password utilizzate;
- deve essere mantenuta segreta.

Lei dovrà altresì:

- custodire con cautela le credenziali di autenticazione che Le sono state fornite per consentire l'accesso ai locali e ai sistemi aziendali contenenti i Dati Personali oggetto dei Suoi trattamenti e gli strumenti aziendali a Lei eventualmente forniti dal Titolare del trattamento per l'esercizio dei Suoi compiti (ad es.: personal computer, cellulare aziendale, badge, chiavi, password) e gestirne l'eventuale smarrimento o furto – informando tempestivamente il Titolare del trattamento;
 - spegnere i dispositivi informatici in dotazione al fine dello svolgimento delle attività di trattamento dei dati personali al termine della giornata lavorativa;
 - agire nel rispetto delle regole di comportamento imposte dall'azienda in materia di utilizzo in sicurezza di risorse e servizi informatici, con particolare riferimento a risorse e servizi che prevedono il trattamento di Dati Personali;
 - fornire supporto alle Funzioni del Titolare preposte all'esecuzione di controlli volti a verificare il livello di conformità delle misure tecniche da Lei implementate nell'ambito del trattamento di Dati Personali connesso allo svolgimento delle Sue funzioni;
 - segnalare, nelle modalità previste dalle procedure aziendali in vigore, gli incidenti relativi alla sicurezza dei Dati Personali o le eventuali anomalie nel funzionamento dei dispositivi informatici assegnati e dei sistemi informatici utilizzati per il trattamento dei dati;
 - osservare le procedure aziendali in materia di salvaguardia dei Dati Personali (es: conservazione di una copia negli archivi aziendali di rete, esecuzione di back-up settimanali, etc.);
 - utilizzare la casella di posta elettronica aziendale esclusivamente per scopi d'ufficio ed evitare la trasmissione, a mezzo di posta elettronica, di file o di messaggi contenenti dati personali, soprattutto se particolari. Qualora per ragioni di servizio sia necessario procedere alla trasmissioni di file o messaggi in tal senso, sarà necessario proteggere il contenuto del file dall'accesso e dalla visione di soggetti, non autorizzati o legittimati al trattamento, che siano diversi dai destinatari delle comunicazioni elettroniche considerate, tramite il ricorso all'uso di tecniche di crittazione o di cifratura dei messaggi, ovvero ricorrendo all'uso di codificazione dei dati contenuti nel testo delle comunicazioni;
 - non fornire dati e informazioni di carattere sanitario per telefono, qualora non si abbia la certezza assoluta sull'identità del soggetto chiamante; qualora giungano richieste telefoniche di dati sanitari da parte dell'Autorità Giudiziaria o degli organi di polizia e, in ogni caso, nell'ipotesi di richieste di comunicazione di dati presentate per telefono occorre verificare preliminarmente l'identità del soggetto richiedente.
- 3. In materia di misure di sicurezza per i trattamenti effettuati senza l'ausilio di strumenti elettronici, Lei dovrà adottare tutte le misure di sicurezza che siano indicate o saranno indicate dal Titolare, volte ad evitare rischi di distruzione, perdita, accesso non autorizzato o trattamento non consentito dei Dati Personali trattati con l'ausilio di strumenti cartacei. In particolare:**

- garantire che il trasferimento di documenti cartacei all'interno della Struttura, qualora la documentazione contenga dati personali, soprattutto se particolari, avvenga nel rispetto della riservatezza degli interessati e adottando misure che siano idonee a limitare la conoscenza dei dati medesimi da parte dei soli soggetti destinatari;
- creare, nell'ambito del trattamento di dati personali connesso allo svolgimento delle sue attività, un archivio cartaceo avente le seguenti caratteristiche:
 - esclusivamente dedicato al trattamento in oggetto;
 - contenente i soli documenti connessi al presente trattamento;
 - riservato al Suo accesso esclusivo o con possibilità di condivisione con altri soggetti autorizzati dal Titolare.
- archiviare negli armadi o in cassetti chiusi a chiave, al termine della giornata lavorativa e quando ci si allontana dalla propria postazione di lavoro, eventuali documenti cartacei contenenti Dati Personali;
- distruggere, qualora sia necessario, i documenti cartacei contenenti Dati Personali, ad esempio utilizzando apparecchi distruggi documenti, secondo modalità che non consentano di ricostruirne o intuirne il contenuto;
- controllare e custodire i documenti cartacei fino alla loro restituzione per evitare l'accesso da persone prive di autorizzazione e restituirli al termine delle operazioni affidate.

Fermo restando quanto sopra, si precisa che è fatto espressamente divieto all'Incaricato, salvo espressa e preventiva autorizzazione della Società, di:

- effettuare trattamenti di Dati Personali che non rientrano nei compiti lavorativi assegnati;
- iniziare, all'interno della Società, un nuovo trattamento di Dati Personali ovvero modificare un trattamento già in essere, se non dietro espressa richiesta di un referente aziendale autorizzato;
- comunicare o diffondere a terzi (inclusi altri dipendenti della Società), i Dati Personali di cui è venuto a conoscenza nello svolgimento delle proprie mansioni;
- comunicare a terzi le credenziali di autenticazione, salvo che nei casi di prolungata assenza dell'Incaricato o situazioni di emergenza o urgenza, per esclusive necessità di operatività o di sicurezza del sistema della Società;
- sottrarre supporti informatici e/o cartacei contenenti Dati Personali, ovvero portarli all'esterno delle aree e dei locali aziendali se non espressamente previsto nell'ambito delle mansioni assegnate.

Audit trail

Titolo del documento

24/05/2024 15:13:03	Creazione del documento
24/05/2024 15:17	Apertura del documento

Sezione di firma

24/05/2024 15:18	Documento firmato da
Campi sottoposti a firma	1bd0e3b6-92bf-41ab-92e4-336037a1ac37

Dati modificati

24/05/2024 15:18	Documento modificato da
Campi sottoposti a modifica:	
Nessun campo sottoposto a modifica	