AUTORIZZAZIONE AL TRATTAMENTO DI DATI PERSONALI

IN QUALITÀ DI AMMINISTRATORE DI SISTEMA

[Ai sensi del Regolamento (UE) 2016/679, del D.lgs. 196/2003 come novellato per effetto del D.lgs. 101/2018 e del Provvedimento del Garante per la protezione dei dati personali “Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”, del 27 novembre 2008 e successive modifiche]

Egr. Sig. [NOME AMMINISTRATORE DI SISTEMA]

Ufficio/area di appartenenza: [INSERIRE UFFICIO/AREA DI APPARTENENTE, ES. CESI REGIONALE, CESI CDL DI ….]

Svolgerà le mansioni specificamente indicate nel presente documento presso:

la **[NOME STRUTTURA, ES. Camera del Lavoro di \_\_\_\_\_\_\_, CGIL Regionale \_\_\_\_\_]**con sede in [indirizzo] PEC [PEC] (di seguito “**CGIL**” e/o “**Organizzazione**”)

**PREMESSO CHE**

* il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati (“**Regolamento**”) fissa le modalità da adottare per il Trattamento ed individua i soggetti che, in relazione all'attività svolta, sono tenuti agli adempimenti previsti dal Regolamento;
* l’Autorità di Controllo italiana (“**Garante per la protezione dei dati personali**”) ha introdotto con Provvedimento del 27 novembre 2008, come successivamente modificato con Provvedimento del 25 giugno 2009 (“**Provvedimento sugli Amministratori di Sistema**” o “**Provvedimento**”), una serie di obblighi per il Titolare del Trattamento (ciascuna singola Struttura verticale e/o Orizzontale del Sindacato Confederale) concernenti l'individuazione e la designazione di Persone Autorizzate che svolgono all'interno della CGIL il ruolo di Amministratore di Sistema, così come definito nel richiamato Provvedimento;
* la CGIL ritiene che la conformità alle disposizioni contenute nel citato Provvedimento costituiscano una misura di sicurezza adeguata e compatibile con le disposizioni del Regolamento;
* deve essere considerato “Amministratore di Sistema” (di seguito anche ADS) chiunque, in maniera non occasionale, si occupa della gestione e manutenzione di impianti di elaborazione con cui vengono effettuati Trattamenti di Dati Personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (*Enterprise resource planning*) utilizzati in grandi organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire, anche accidentalmente, sui Dati Personali;
* l’art. 2-*quaterdecies* del D.lgs. 196/03 (“**Codice Privacy**”), come novellato per effetto del D.lgs. 101/2018, prevede che l’Organizzazione, sia che questa rivesta il ruolo di Titolare del trattamento che di Responsabile del trattamento: (i) possa prevedere, sotto la propria responsabilità e nell’ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al Trattamento di Dati Personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la sua autorità; (ii) individui le modalità più opportune per autorizzare al Trattamento dei Dati Personali le persone che operano sotto la propria autorità diretta;
* peraltro, la figura dell’ADS è individuata anche nel Regolamento Confederale sul Trattamento dei Dati che prevede:

1. Ciascun Centro Regolatore procede alla nomina di uno o più Amministratori di Sistema, a mezzo atto scritto che contenga le specifiche funzioni attribuitegli, nel rispetto della normativa nazionale in materia e delle indicazioni del DPO. I Centri Regolatori Regionali possono attribuire ad uno o più ADS competenze sui sistemi informatici e informativi delle altre strutture orizzontali e verticali della CGIL Regionale, o alcune di esse.

2. La Categorie o Federazioni o SPI regionali i cui sistemi informatici e informatici siano autonomi rispetto a quelli della CGIL Regionale possono designare un proprio ADS.

3. Laddove il Centro Regolatore Regionale non abbia provveduto ai sensi del comma 1, secondo periodo, l’ADS deve essere designato dalla singola Camera del Lavoro, con competenza anche per i sistemi informatici e informativi delle strutture verticali e orizzontali territoriali, o per alcune di esse.

4. Le Categorie o Federazioni o SPI territoriali i cui sistemi informatici e informatici siano autonomi rispetto a quelli della Camera del Lavoro possono designare un proprio ADS.

[…]

* la persona in intestazione è stata autorizzata al Trattamento (“**Persona Autorizzata**”) ai sensi degli artt. 28(3)(b), 29, 32(4) del Regolamento e dell’art. 2-*quaterdecies* del Codice Privacy, attraverso la sottoscrizione dell’Autorizzazione al Trattamento di Dati Personali per le sole finalità riferibili ai Trattamenti indicati nel presente atto;
* le mansioni della Persona Autorizzata in intestazione svolte all'interno della CGIL richiedono la Sua ulteriore designazione ad amministratore di sistema (“**Amministratore di Sistema**” e/o **ADS**) e la raccolta - in conformità a quanto indicato al paragrafo 4.5. del Provvedimento - dei Suoi Dati Personali inerenti allo svolgimento dell'attività di Amministratore di Sistema;
* la CGIL ha in essere con Lei un rapporto giuridico dal quale discende la Sua documentata preposizione e qualificata assegnazione allo svolgimento di attività di gestione e manutenzione di sistemi informatici presso la CGIL (di seguito anche “**Incarico”**) e che nell'ambito dell’Incarico sono state assegnate mansioni riconducibili a quelle tipiche dell’Amministratori di Sistema ovvero a quelle di altre figure ad essi equiparabili quali, ad esempio, gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza, gli amministratori di sistemi software complessi, etc.;
* ai fini dello svolgimento dell’Incarico affidatole è stato preventivamente valutato l’adeguato grado di capacità, esperienza ed affidabilità, ed in relazione a tale valutazione si ritiene che le prestazioni da Lei effettuate forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di protezione dei Dati Personali, ivi compreso il profilo relativo alla sicurezza;
* nell’ambito dello svolgimento delle sue funzioni, Lei effettua il Trattamento dei Dati Personali sia direttamente sia come implicita e indiretta conseguenza delle mansioni assegnate e svolte;
* per l’esecuzione dell’Incarico, Lei potrà procedere al Trattamento dei Dati Personali che sono stati e/o le verranno messi a disposizione dalla CGIL, la quale agisce in qualità di Titolare del Trattamento e/o, eventualmente, di Responsabile del Trattamento;
* il presente documento sostituisce eventuali precedenti lettere di designazione ad ADS che Lei abbia ricevuto dalla CGIL e che Le siano state conferite ai sensi del Codice Privacy, del Provvedimento o del Regolamento; pertanto, il presente documento è da intendersi come aggiornamento dell’ambito di operatività consentito nel caso in cui Lei sia stato designato in precedenza quale Amministratore di Sistema;
* ogni parola con lettera iniziale maiuscola non espressamente definita nel presente documento, ha il significato espresso all’interno del Regolamento;

**TUTTO CIÒ PREMESSO**

l’intestata organizzazione La individua e designa quale Persona Autorizzata al Trattamento con mansione di “**Amministratore di Sistema”** in relazione agli ambiti di operatività indicati nel seguito.

Dal momento che con il Provvedimento sugli ADS, il Garante per la Protezione dei Dati Personali ha previsto che la designazione debba essere in ogni caso individuale e recare l’elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato, specificatamente e limitatamente a tale contesto, a Lei vengono assegnati gli ambiti di operatività e i profili indicati nel seguito:

|  |  |
| --- | --- |
| **AMBITO DI OPERATIVITÀ** | **ATTIVITÀ SISTEMISTICHE DI MANUTENZIONE E AMMINISTRAZIONE DEGLI STRUMENTI INFORMATICI DELL’ORGANIZZAZIONE** |
| **PROFILI** | **1) Predisporre e manutenere le postazioni informatiche degli utenti (*hardware* e *software*), i servizi, gli apparati e i dispositivi di rete interni all’Organizzazione, verificando che siano opportunamente aggiornati e protetti (*antivirus*, *firewall*, permessi di accesso, ecc.);****2) Gestire e amministrare gli *account* di rete (creazione, dismissione, *password* *policy*) e le autorizzazioni di accesso a servizi/applicazioni in uso ai dipendenti e collaboratori dell’Organizzazione;****3) Gestire e amministrare i piani di *backup*, *restore*, *disaster recovery* e di *business continuity* relativi ai dati e alle applicazioni in uso presso la sede dell’Organizzazione e non già gestite centralmente dal fornitore di servizi/*cloud provider*;****4) Gestire amministrare e manutenere i sistemi di posta elettronica e di archiviazione dei dati (es. *cloud*) avvalendosi, quando prevista, della collaborazione dei fornitori esterni;****5) Coordinare le attività tecnico-informatiche interne e svolgere il ruolo di referente tecnico verso i fornitori esterni di servizi informatici (es. gestione *ticket* di assistenza verso *service provider*);****6) Fornire assistenza sistemistica e di sicurezza informatica a tutto il personale dell’Organizzazione attraverso le modalità concordate;** |
| **AMBITO DI OPERATIVITÀ** | **SICUREZZA INFORMATICA E PROTEZIONE DEI DATI PERSONALI – ATTIVITÀ DI SUPPORTO** |
| **PROFILI** | **1) Coadiuvare l’Organizzazione nell’adozione delle misure tecniche e organizzative opportune al fine di rispettare il Provvedimento sugli Amministratori di Sistema;****2) Coadiuvare l’Organizzazione sia in fase di valutazione dei rischi sulla sicurezza dei sistemi informatici, in termini di riservatezza, integrità e disponibilità di dati e servizi, sia nella successiva fase di implementazione delle misure di sicurezza necessarie per mitigare i rischi, nonché nell’adempimento delle Valutazioni di Impatto (DPIA) ex art. 35 del Regolamento che dovessero rendersi necessarie in relazione alla tipologia dei trattamenti dati svolti;****3) Segnalare all’Organizzazione eventuali problematiche concernenti la sicurezza dei dati e dei sistemi, indicando tutti gli aspetti necessari a circoscrivere la vulnerabilità;****4) Gestire gli aspetti tecnici di eventuali possibili violazioni dei sistemi informatici e i connessi profili relativi alla segnalazione dei Data Breach;****5) Verificare che il riutilizzo e/o la dismissione dei dispositivi o supporti informatici siano effettuati nel rispetto del Provvedimento del Garante privacy del 13 ottobre 2008.** |

Nel rammentarLe la delicatezza e l’importanza del ruolo ricoperto e dei compiti assegnati, vengono riportate di seguito le modalità di comportamento – integrative dell’ambito di operatività precedentemente riportato - che Lei sarà tenuto ad osservare per un corretto esercizio delle funzioni associate al Suo Incarico:

* con riferimento ai Dati Personali di cui potrà venire a conoscenza, Lei avrà facoltà di eseguire le operazioni e/o il complesso di operazioni che si renderanno strettamente necessarie per l’esecuzione dell’Incarico Professionale ricevuto;
* il Trattamento di eventuali Dati Personali (qualunque sia il soggetto Interessato a cui i dati si riferiscono ed anche qualora i dati non siano consultati “in chiaro”) dovrà essere svolto unicamente ai fini dell’esecuzione dell’Incarico Professionale affidato e, in particolare, per lo svolgimento dei compiti associati al profilo di autorizzazione di cui sopra;
* non potrà perseguire, nel Trattamento dei Dati Personali, finalità ulteriori rispetto a quelle sopra indicate;
* non dovrà comunicare a terzi e/o diffondere i Dati Personali oggetto di Trattamento, né utilizzarli autonomamente per finalità diverse da quelle sopra indicate per tutta la vigenza dell’Incarico Professionale ricevuto, durante il rapporto di lavoro in essere con l’Organizzazione, nonché, anche successivamente, senza limiti di tempo;
* nello svolgimento dell’incarico e delle operazioni di Trattamento, Lei dovrà rispettare le disposizioni e le specifiche istruzioni impartite dall’Organizzazione e dovrà compiere tutto quanto si renderà necessario ai fini del rispetto e della corretta applicazione della normativa applicabile in materia di protezione dei Dati Personali;
* qualora fra gli ambiti di operatività consentiti sia prevista la possibilità di effettuare verifiche sugli strumenti di comunicazione elettronica utilizzati dai lavoratori, Lei dovrà operare nel rigoroso rispetto dei limiti imposti dalle disposizioni legislative e regolamentari vigenti (e, in particolare, di quelli previsti dalle *Linee Guida del Garante per posta elettronica ed internet,* rif. deliberazione n.13del 1.3.2007 - Gazzetta Ufficiale n. 58 del 10 marzo 2007), oltre che nel rispetto dei principi e delle regole indicate all’interno dei regolamenti per l’utilizzo degli strumenti informatici formalmente applicati dall’Organizzazione e delle istruzioni di volta in volta impartite dalla stessa. È fatto comunque espresso divieto svolgere qualsiasi tipo di operazione che realizzi e/o si possa concretizzare in un’attività di illecito controllo a distanza dell’attività dei lavoratori;
* il Trattamento dei dati dovrà essere svolto mediante gli strumenti cartacei, elettronici e/o telematici messi a disposizione dall’Organizzazione, con logiche strettamente correlate alle finalità di cui sopra e, comunque, in modo tale da garantire la sicurezza e riservatezza dei dati stessi. In ogni caso in cui Lei ritenga che gli strumenti o le istruzioni messe a disposizione dall’Organizzazione per lo svolgimento dell’incarico ricevuto possano compromettere la sicurezza e/o la riservatezza dei sistemi, è tenuto a darne immediato avviso al Responsabile dei sistemi informativi dell’Organizzazione;
* le credenziali amministrative di autenticazione sui sistemi informatici gestiti per effetto dell’Incarico e assegnate univocamente, devono essere custodite con cura ed attenzione e non devono essere rivelate a nessuno. Tali credenziali devono essere conservate in luoghi e/o forme non accessibili ad altri. La responsabilità della segretezza delle credenziali è dell’assegnatario il quale deve astenersi dal trascriverla in qualsiasi forma. Qualora sussista il dubbio di violazione della segretezza, deve provvedere al cambiamento della password;
* le credenziali amministrative sui sistemi devono essere utilizzate esclusivamente in relazione alle sessioni ed ai processi inerenti la gestione e manutenzione dei sistemi stessi; è vietato l’utilizzo di tali credenziali per attività che per il loro svolgimento non necessitino di un privilegio amministrativo ma possono essere svolte attraverso le credenziali di utente standard (es. consultazione della casella di posta elettronica assegnata, utilizzo degli strumenti di produttività individuali, *office automation*, navigazione Internet, etc.);
* le utenze generiche di servizio predisposte esclusivamente per l’avvio di servizi pianificati non devono essere utilizzate per effettuare accessi interattivi ai sistemi amministrati; tali accessi sono consentiti esclusivamente con autenticazione attraverso le credenziali che Le sono assegnate in via univoca in qualità di Amministratore di Sistema;
* applicare le regole di gestione dei sistemi e le misure di sicurezza idonee e adeguate adottate dall’Organizzazione;
* evitare, ove non strettamente indispensabile per lo svolgimento delle operazioni tecniche connesse al proprio ruolo, di visualizzare, leggere, copiare, stampare ed effettuare qualsiasi altra operazione di Trattamento di Dati Personali non consentita rispetto all’Incarico assegnatoLe;
* segnalare all’Organizzazione l’eventuale necessità di un Suo aggiornamento professionale per garantire uno svolgimento del proprio ruolo in linea con il progresso tecnologico e normativo in materia di Trattamento dei Dati Personali.

Le è richiesta la più scrupolosa osservanza delle disposizioni che Le vengono impartite in ordine alle misure di sicurezza adottate dall’Organizzazione, per la protezione degli elaboratori e dei dati, sia da intrusioni che da eventi accidentali.

La CGIL, sulla base di quanto previsto alla regola 2 lettera *e)* del Provvedimento, La informa che potrà procedere alla verifica almeno annuale delle attività da Lei svolte in modo da controllare la loro rispondenza alle misure organizzative, tecniche e di sicurezza adottate. A tal fine si specifica, inoltre, che l’Organizzazione effettuerà, tramite sistemi adottati sulla base della regola 2 lettera *f)* del Provvedimento, la registrazione degli accessi logici da Lei effettuati, in qualità di Amministratore di Sistema, ai sistemi di elaborazione e agli archivi elettronici. Tali registrazioni (*access log*) comprenderanno i riferimenti temporali e la descrizione dell’evento che le ha generate e saranno conservate per un congruo periodo, non inferiore a sei mesi.

Sulla base di quanto previsto alla regola 2 lettera *c)* del Provvedimento, l’Organizzazione la informa, altresì, che i suoi estremi identificativi, in caso di Trattamento di informazioni a carattere personale riferite ai prestatori di lavoro appartenenti all’Organizzazione potranno essere a questi ultimi comunicati.

La presente designazione cesserà di produrre i propri effetti a decorrere dalla data di tale cessazione, cioè nei seguenti casi: (i) in caso di revoca espressa da parte della CGIL a suo insindacabile giudizio; (ii) cessazione per qualunque causa dell’Incarico; (iii) cessazione del rapporto di lavoro tra l’Organizzazione e Lei in qualità di ADS.

La persona fisica indicata in intestazione e nel campo firma in calce al presente documento prende atto ed accetta quanto previsto dalla presente designazione, dalla normativa applicabile in materia di protezione dei Dati Personali ed assume la qualifica di ADS.

Data e Luogo: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Per la CGIL

Firma: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Per presa visione e accettazione, l’Amministratore di Sistema

Firma: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_