

Roma li, 31/10/2022

La società GPA GRUPPO PROGETTI AVANZATI SRL (GPA od Organizzazione nel seguito del presente documento) al fine di fornire gli indirizzi ed il supporto a tutto il personale per la sicurezza delle informazioni trattate in conformità ai requisiti di business perseguiti ovvero a quelli del proprio Sistema di Gestione della Sicurezza delle Informazioni (SGSI) coerentemente alla norme della famiglia ISO/IEC 27000 ed in conformità alle leggi e regolamenti cogenti, dispone le seguenti regole aziendali a cui ogni lavoratore dovrà rigorosamente attenersi ed osservare all'interno dell'Organizzazione; tale regolamento costituisce parte integrante dell'Accordo di Riservatezza stabilito tra la GPA e il lavoratore.

IL LAVORATORE SI IMPEGNA AD OSSERVARE IL SEGUENTE REGOLAMENTO:

- Ogni ingresso/uscita alla/dalla sede dovrà sempre essere tracciato: all'uopo il lavoratore dovrà registrare ogni accesso/uscita (data, orario e firma) in/dalla sede della GPA nell'apposito registro disponibile presso la Reception/l'ingresso.
- Le informazioni trattate all'interno dell'Organizzazione (sia documentali che in formato elettronico) sono definite come "Non Classificate", "Riservate" e "Confidenziali". Per queste ultime 2 tipologie di informazioni, che comprendono tra l'altro dati personali/sensibili, quando stampate saranno evidenti etichette/filigrane identificative, quando in formato elettronico saranno accessibili solo con specifici profili autorizzativi. In relazione all'incarico/attività, il lavoratore sarà abilitato da parte del personale responsabile della GPA al trattamento di alcune di queste categorie: non è consentito per alcun motivo l'accesso a categorie di informazioni diverse da quelle abilitate. Eventuali accessi ad altre categorie saranno possibili solo previa formale autorizzazione del personale responsabile (Owner).
- Fermo restando le diverse modalità adottate per il trattamento delle informazioni classificate di cui al punto precedente, le postazioni di lavoro dei lavoratori devono garantire costantemente, ovvero il prima possibile, le massime condizioni di "scrivania pulita" (anche per brevi momenti di assenza) al fine di impedire l'accesso alle informazioni trattate a personale non autorizzato. In particolare tutti i documenti "Riservati" e "Confidenziali", dopo il loro trattamento, devono essere riposti negli archivi di origine e chiusi a chiave (o in cassettiere chiudibili a chiave nel caso di brevi assenze) ovvero riconsegnati all'Owner.
- I computer/laptop che espongono informazioni classificate non devono essere lasciati incustoditi anche per brevi momenti. Tutti i computer/laptop della GPA sono protetti da password di accesso: non è consentito per alcun motivo disabilitare tale impostazione.
- Le informazioni di proprietà della GPA (anche di tipo intellettuale), in particolare quelle classificate di cui al punto 2, non devono in nessun caso essere condivise all'esterno dell'Organizzazione, né oralmente né attraverso vie e supporti elettronici, ad eccezione dei casi autorizzati dalle funzioni responsabili.
- Il trasferimento all'esterno dell'Organizzazione delle informazioni classificate come "Riservate" e "Confidenziali" deve avvenire esclusivamente attraverso posta elettronica in modalità crittografata; l'acquisizione di qualsiasi tipo di documentazione proveniente dal cliente deve avvenire esclusivamente attraverso posta elettronica. Nel caso eccezionale in cui si renda necessario l'impiego dei supporti rimovibili, è richiesta l'autorizzazione preventiva dell'IT Manager. E' consentito il trasferimento delle informazioni dai server aziendali alla postazione locale per lo svolgimento dell'attività lavorativa; al termine della medesima è obbligatorio archiviare le informazioni elaborate sui server aziendali al fine di garantirne i backup programmati. Al termine delle attività le informazioni trattate sulla postazione locale devono essere cancellate.
- L'accesso fisico alla sala server è consentito solo a IT Manager ovvero al personale da lui autorizzato: ogni accesso dovrà essere tracciato nell'apposito registro disponibile nella sala server. L'accesso agli archivi

cartacei disponibili presso le varie aree aziendali, allocati in armadi chiusi a chiave, è consentito solo agli Owners ovvero al personale da loro autorizzato.

- I computer/laptop assegnati al personale devono essere preservati da danneggiamenti e/o manomissioni ovvero dall'installazione/utilizzo di SW non autorizzato, ovvero garantire l'efficacia dell'antivirus ivi installato, in conformità agli "Accordi di comodato d'uso" sottoscritti; in particolare non devono contenere informazioni che non abbiano attinenza con la propria prestazione lavorativa.
- È consentito il trattamento di informazioni di cui al punto 2, pervenute attraverso posta elettronica aziendale, anche al di fuori dell'Organizzazione garantendone la riservatezza in conformità con gli "Accordi di Riservatezza" stipulati.
- Eventuali minacce o potenziali vulnerabilità fisiche e/o tecniche, rilevate da qualsiasi lavoratore, devono essere tempestivamente segnalate a IT Manager e/o IT Operator.
- Tutti i clienti/fornitori che accedono all'interno dell'Organizzazione devono essere registrati nell'apposito registro disponibile presso la Reception e sempre accompagnati nella loro attività dal personale della GPA; in particolare l'accesso alle informazioni e agli Asset dell'Organizzazione, quando necessario, deve essere costantemente monitorato evidenziando eventuali comportamenti sospetti al RSGSI ovvero al personale da lui delegato.
- Nel caso di attività presso il Cliente, sarà cura del lavoratore assicurare che i dati e le informazioni ivi acquisiti siano utilizzati esclusivamente per le finalità inerenti all'esecuzione dell'incarico assegnato e comunque garantire che nessuna di tali informazioni sia diffusa verso soggetti terzi estranei all'incarico ovvero al di fuori del perimetro del Cliente, per alcun motivo, salvo che in caso di preventiva autorizzazione del personale responsabile del Cliente e/o della GPA. Sarà cura del lavoratore, inoltre, adottare tutte le cautele e le misure necessarie, per garantire la riservatezza delle eventuali informazioni appartenenti alla GPA ovvero della documentazione in suo possesso, classificata come "Riservata".
Tutta la documentazione e/o i supporti del Cliente, trattati e/o in possesso del lavoratore al termine del suo incarico dovrà essere riconsegnata senza indugio; eventuale documentazione appartenente alla GPA dovrà essere riconsegnata alle funzioni responsabili in sede.

Eventuali richieste di deroga al rispetto delle disposizioni riportate nel presente regolamento saranno valutate, relativamente all'aspetto tecnico e di sicurezza logica/fisica delle informazioni, da parte del RSGSI e dell'IT Manager ed eventualmente autorizzate dalla Direzione.

Le richieste devono essere motivate e formalmente avanzate dalla funzione responsabile.

Il Presidente del CdA

(Giuseppe PETRINI)