OGGETTO: CODICE DELLE ISTRUZIONI GENERALI PER IL TRATTAMENTO DEI DATI PERSONALI
REVISIONE: 01
PROTOCOLLO:22L271
DATA: 07/10/2022

***

1. DEFINIZIONI.

1.1. CODICE: Il presente CODICE DELLE ISTRUZIONI GENERALI PER IL TRATTAMENTO DEI DATI PERSONALI AI SENSI DEL REGOLAMENTO EUROPEO PER LA PROTEZIONE DEI DATI (GDPR).
1.2. CONSORZIO: Il CONSORZIO BLUE LINE GROUP e le società dello stesso consorziate
1.3. DIPENDENTE: Tutti i dipendenti, gli amministratori, i collaboratori a qualsiasi titolo, soggetti in formazione del CONSORZIO BLUE LINE GROUP e delle società dello stesso consorziate.
1.4. DATO PERSONALE: Qualsiasi informazione riguardante una persona fisica identificata o identificabile mediante riferimento a qualsiasi altra informazione disponibile.
1.5. DATO PARTICOLARE: I dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
1.6. TRATTAMENTO: Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali.
1.7. TITOLARE DEL TRATTAMENTO: La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
1.8. INCARICATO AL TRATTAMENTO: Le persone fisiche autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, a prescindere dalla funzione svolta all'interno dell'Ateneo.
1.9. POSTAZIONE DI LAVORO: L'insieme degli strumenti informatici e non messi a disposizione dal CONSORZIO per rendere la prestazione lavorativa, sia in sede sia in mobilità (ad esempio: archivi, armadi, scrivanie, computer, stampanti, telefoni cellulari).

2. AMBITO DI APPLICAZIONE.

2.1. Il CODICE è la formalizzazione dell'insieme dei valori, norme e delle regole comportamentali fatte proprie ed aventi valore vincolante per il CONSORZIO BLUE LINE GROUP e per tutte le società dello stesso consorziate.
2.2. Il CODICE si applica, deve essere conosciuto, compreso e tassativamente rispettato da ogni DIPENDENTE.
2.3. Il CODICE è parte integrante del Modello di Organizzazione e Gestione di cui al D.lgs. n. 231/01 (abbreviato "M.O.G.") adottato dal CONSORZIO.
2.4. L'ottemperanza delle prescrizioni del CODICE costituisce parte integrante delle obbligazioni contrattuali di ogni DIPENDENTE.
2.5. La violazione del CODICE da parte del DIPENDENTE può costituire, a seconda dei casi, un illecito disciplinare, sanzionabile nel rispetto della normativa di riferimento, e/o un inadempimento contrattuale e può comportare il risarcimento dei danni eventualmente derivanti da tale violazione.
2.6. Il CONSORZIO dispone quanto segue: Chiunque abbia accesso a dati personali, li consulti, li archivi, li diffonda, li modifichi, li raccolga o, comunque, effettui qualsiasi operazione su informazioni, sia in formato elettronico che cartaceo, riferite a persone, deve trattare tali dati personali con le modalità contenute nel presente CODICE.

3. ACCESSO AI DATI DA PARTE DI SOGGETTI NON AUTORIZZATI AL TRATTAMENTO.

3.1. Occorre sempre controllare che l'accesso ai dati personali trattati in qualsiasi contesto (segreterie, uffici, cantieri, divisioni/direzioni, dipartimenti, attività didattica e di ricerca, eventi) avvenga esclusivamente da parte di persone autorizzate al trattamento, siano essi interni o esterni al CONSORZIO.
3.2. Il dato personale deve, innanzitutto, essere protetto da accessi non autorizzati, che possono avvenire di persona (si pensi a un soggetto non autorizzato che entra fisicamente in un ufficio e prova a conoscere o sottrarre dati) o tramite contatti telematici che possono rivelarsi truffaldini (ad esempio un'e-mail o altra forma di presa di contatto mediante la quale si provino a raccogliere determinati dati o informazioni).
3.3. I documenti cartacei contenenti dati personali e tutta la documentazione amministrativa devono essere custoditi per evitare l'accesso agli stessi da parte di soggetti non autorizzati.

4. SICUREZZA DELLA POSTAZIONE DI LAVORO.

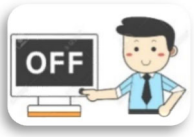
4.1. È fatto divieto di lasciare il computer acceso incustodito. Qualora ci si allontani dal computer è obbligatorio bloccarne l'accesso utilizzando la propria password.
4.2. Lasciare il proprio computer accessibile quando ci si allontana dalla propria scrivania genera una vulnerabilità molto pericolosa, e incontrollabile, al proprio lavoro e al patrimonio dei dati.
4.3. In caso di assenza momentanea dal proprio posto di lavoro, ci si deve accertare che la sessione di lavoro non sia accessibile a terzi, facendo logout o attivando il salvaschermo (screensaver) con blocco della sessione protetta da credenziali di autenticazione.
4.4. Tutti i soggetti incaricati al trattamento devono assicurarsi che i computer di cui fanno uso, sia desktop che portatili, devono avere installato e attivo il software antivirus, con firewall attivato e devono essere mantenuti costantemente aggiornati con le patch di sicurezza del sistema operativo e degli applicativi utilizzati. Tali aggiornamenti sono, nella maggior parte dei casi, automatici e non richiedono l'intervento dell'utente. Non bisogna però, salvo casi eccezionali, bloccare o ritardare un aggiornamento dei software o dei sistemi. Le ulteriori misure di sicurezza richieste sono specificate nei regolamenti, atti, disposizioni in materia di strumenti informatici adottati dal CONSORZIO.
4.5. Il DIPENDENTE è tenuto in particolare all'osservanza del REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI - PROTOCOLLO 22H198 e s.m.i.

Consorzio Blue Line Group-Via dei Boschetti 57 Monfalcone 34074- P.iva 01087760318-Tel 0481 482626-Fax 0481 269805– info@cblg.it–www.bluelinegroup.it

4.6. **La postazione di lavoro deve essere configurata in modo che sia impostato l'avvio automatico dello screensaver ("salvaschermo") dopo al massimo 3 (TRE) minuti di inattività del computer.**

4.7. È facoltà degli incaricati, qualora lo ritengano necessario od opportuno in ragione dei dati che stanno trattando, stabilire un intervallo temporale minore.

5. SPEGNIMENTO OBBLIGATORIO DEL COMPUTER.



5.1. Tutti i computer (desktop e portatili) che vengono usati nei luoghi dove opera il CONSORZIO, al termine delle ore di servizio, devono essere spenti, a meno che per particolari ragioni tecniche o di servizio debbano rimanere in funzione (in tal caso, il computer acceso deve risiedere in un ufficio o in un locale chiuso a chiave o protetto e con salvaschermo attivo e protetto da credenziali).

6. SUPPORTI ESTERNI.

6.1. Particolare attenzione alla custodia deve riguardare anche i supporti esterni (es. chiavette USB, dischi esterni, tablet, smartphone,) evitando di lasciarli in luoghi non protetti.

6.2. **Salvo espressa autorizzazione del CONSORZIO è vietato l'uso di supporti di archiviazione removibili per la memorizzazione dei dati. In particolare, salvo espressa autorizzazione del CONSORZIO è fatto divieto di collegare al PC chiavi USB, dispositivi bluetooth, hard disk o altri device idonei al trasferimento dei dati.**

6.3. È vietato utilizzare servizi di archiviazione e condivisione file per backup offerti da operatori commerciali (ad esempio: Google Drive, Dropbox, iCloud, OneDrive), se non espressamente previsti da una lista autorizzata dal CONSORZIO.

7. GESTIONE DEL COMPUTER PORTATILE.

7.1. Non lasciare mai incustodito il computer portatile.

7.2. Lo smarrimento, il furto, l'accesso non autorizzato o la sospetta manomissione di un computer che contenga dati personali comporta un cosiddetto data breach, ossia una violazione del patrimonio di dati, che deve essere segnalato immediatamente, e comunque al massimo entro 24 ore, all'indirizzo dell'ORGANISMO DI VIGILANZA del CONSORZIO e al proprio responsabile affinché vengano svolti in tempo utile gli adempimenti di legge.

8. STAMPA DI DOCUMENTI.

8.1. **Occorre prestare attenzione alla stampa di documenti o alla ricezione di fax su stampanti condivise o fotocopiatrici di rete, avendo cura di recuperare tempestivamente la stampa e di non lasciare i documenti incustoditi.**

8.2. La protezione dei dati si applica anche a documenti cartacei, cui va garantita custodia e controllo. Non riutilizzare per appunti il retro di fogli stampati o fotocopiati se contengono dati personali.

8.3. Qualora sia fornito, è sempre necessario utilizzare il "distruggi-documenti" per rendere non leggibili i documenti contenenti dati personali o informazioni rilevanti.

9. PASSWORD.

9.1. La password utilizzate per l'accesso alla propria postazione deve essere sicura, non nota ad altri e mai comunicata a terzi, né a voce, né per e-mail, su siti non istituzionali o in chat.

9.2. In particolare, la password deve essere univoca (non usata per più servizi, sistemi o siti), robusta (lunghezza idonea, formata da lettere maiuscole e minuscole, numeri e/o caratteri speciali, senza riferimenti riconducibili all'utente), cambiata frequentemente (almeno ogni 6 mesi) e regolarmente, e sempre diversa da quelle utilizzate in precedenza.

9.3. Le password non devono essere mai scritte e conservate in luoghi e modi che non garantiscano adeguata protezione.

10. CAUTELA NEI CONFRONTI DI QUALSIASI RICHIESTA DI DATI.

10.1. Il DIPENDENTE deve mantenere sempre un atteggiamento prudenziale e di cautela davanti a richieste di fornire dati personali.

10.2. Le richieste di dati personali devo provenire da soggetti autorizzati, e la cui identità, in caso di dubbio, deve essere accuratamente verificata.

10.3. È vietato, altresì, fornire o rendere disponibili informazioni tecniche, riferite alla rete e ai sistemi del CONSORZIO, alle policies e alle credenziali usate, ai software e alle applicazioni utilizzate, a soggetti esterni al CONSORZIO. Tali informazioni sono solitamente domandate per cercare di violare i sistemi.

11. MINIMIZZARE L'UTILIZZO DEI DATI PERSONALI.

11.1. I dati personali degli interessati devono essere utilizzati il meno possibile, non diffusi a soggetti terzi, cancellati non appena la politica del CONSORZIO lo consente, e particolare attenzione va portata nei confronti di dati classificati come particolari (già dati sensibili).

11.2. Nel momento in cui il dipendente venga a conoscenza di un trattamento non corretto, eccedente le finalità, inutile o pericoloso, deve anche per il tramite del proprio responsabile, segnalarlo all'ORGANISMO DI VIGILANZA.

12. RIFERIMENTI.

12.1. Per gli approfondimenti e aggiornamenti di quanto descritto nel presente CODICE, per le modalità di implementazione delle misure di sicurezza richieste, fare riferimento all'ORGANISMO DI VIGILANZA.

Consorzio Blue Line Group

Consorzio Blue Line Group-Via dei Boschetti 57 Monfalcone 34074- P.iva 01087760318-Tel 0481 482626-Fax 0481 269805– info@cblg.it–www.bluelinegroup.it