Allegato 1

Regolamento aziendale per la Privacy e conferimento dell'incarico al Trattamento dati

PRIMA PARTE: REGOLAMENTO AZIENDALE PER LA PROTEZIONE DEI DATI PERSONALI

1. I dirigenti, i componenti degli organi, i dipendenti, i collaboratori, i consulenti, i volontari ed in generale tutte le persone autorizzate ad accedere ai dati personali e preposte allo svolgimento delle operazioni di Trattamento relativa ai dati, devono ispirarsi a un principio generale di diligenza e correttezza.
2. Ogni utilizzo dei dati personali diverso da finalità strettamente professionali è espressamente vietato.
3. Ciascun incaricato del Trattamento deve:
   - rispettare i principi generali del GDPR 679/16, con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi;
   - rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;
   - utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti aziendali;
   - rispettare le misure di sicurezza idonee adottate dalla società, atte a salvaguardare la riservatezza e l'integrità dei dati;
   - segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;
   - accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze;
   - in caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;
   - mantenere riservate le proprie credenziali di autenticazione;
   - svolgere le attività previste dai trattamenti secondo le direttive del responsabile del Trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del Trattamento dei dati;
   - rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
   - informare il responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;
   - raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
   - eseguire qualsiasi altra operazione di Trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.
4. Al momento della raccolta dei dati personali, qualora sia necessario individuare l'identità del soggetto che fornisce le informazioni, è obbligatorio richiedere un documento di identità o di riconoscimento, al fine di verificare l'identità e di procedere correttamente alla raccolta e alla registrazione delle informazioni.
5. I locali, in cui sono custoditi i dati personali (ed in particolare quelli di natura sensibile), devono essere soggetti a controllo e a verifica, al fine di evitare che durante l'orario di lavoro possano essere conosciuti o accessibili da parte di soggetti non autorizzati. Si raccomanda, in caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, di adottare tutte le

accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'organizzazione di appartenenza. Laddove si esegue il Trattamento di Dati Personali, deve essere possibile ricoverare in luogo sicuro i documenti cartacei ed i supporti rimovibili contenenti tali dati. Pertanto le porte degli uffici ed almeno un armadio per ufficio devono essere dotati di serratura con chiave. Al termine dell'orario lavorativo, ove la dinamica delle attività ed il numero di occupanti lo consentano, è necessario chiudere sempre a chiave gli uffici nei quali vengono svolti trattamenti di Dati Personali.

6. Ciascun incaricato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card). Si devono adottare le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei all'organizzazione o non specificamente autorizzati. Al fine di verificare il corretto utilizzo degli strumenti in dotazione potranno essere svolti controlli a campione mediante la raccolta e l'analisi di dati aggregati e anonimi.
7. Per la gestione della sessione di lavoro sul pc (fisso e portatile), si applicano le seguenti regole:
   - al termine delle ore di servizio, il PC deve essere spento, a meno che non stia svolgendo elaborazioni particolari. In tal caso gli uffici debbono tassativamente essere chiusi a chiave;
   - se l'incaricato si assenta momentaneamente dalla propria postazione deve accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone;
   - relativamente all'utilizzo dello screen-saver, occorre osservare le seguenti norme:
   - non deve mai essere disattivato;
   - il suo avvio automatico deve essere previsto non oltre i primi 10 minuti di inattività del PC;
   - deve essere messo in funzione manualmente ogni volta che si lascia il PC incustodito ed acceso;
   - quando si esegue la stampa di un documento contenente dati personali, in particolare su una stampante condivisa, occorre ritirare tempestivamente i documenti stampati per evitare l'accesso a soggetti non abilitati al Trattamento;
   - per l'utilizzo dei PC portatili valgono le regole elencate per i PC connessi alla rete, con le seguenti ulteriori raccomandazioni:
     - prima della riconsegna, rimuovere eventuali file ivi elaborati;
     - quando il PC portatile è nei locali dell'Azienda, non lasciarlo mai incustodito;
     - quando il PC portatile è all'esterno dell'Azienda, evitare di lasciarlo incustodito;
     - per assenze prolungate, anche qualora l'ambiente venga ritenuto "affidabile", è necessario custodire il portatile in modo opportuno es. cassaforte o armadio dotato di serratura;
     - in caso di furto di un portatile è necessario avvertire tempestivamente il responsabile del Servizio Informatico, onde prevenire possibili intrusioni ai sistemi aziendali;
     - in caso di viaggio aereo trasportare tassativamente il portatile come bagaglio a mano;
     - eseguire periodicamente salvataggi dei dati e non tenere tali backup insieme al PC portatile.
8. L'accesso al PC, sia esso collegato in rete o meno, è protetto da un sistema di autenticazione che richiede all'Incaricato di inserire sulla videata di accesso all'elaboratore un codice utente (username) ed una parola chiave (password). L'adozione ed il corretto utilizzo della combinazione username / password è fondamentale per il corretto utilizzo del PC, in quanto:
   - tutela l'utilizzatore ed in generale l'Azienda da accessi illeciti, atti di vandalismo e, in generale, violazioni e danneggiamenti del proprio patrimonio informativo;
   - tutela l'incaricato da false imputazioni, garantendo che nessuno possa operare a suo nome e che, con il suo profilo (ossia con le sue user id e password) solo lui possa svolgere determinate azioni;
   - è necessario per gestire correttamente gli accessi a risorse condivise.
   - ciascun incaricato deve scegliere le password in base ai seguenti criteri:
   - devono essere lunghe almeno otto caratteri;
     - non devono fare riferimento ad informazioni agevolmente riconducibili ai soggetti

utilizzatori o ai loro famigliari;
- devono contenere una combinazione di numeri e/o segni speciali, lettere, maiuscole e minuscole;
- non deve essere uguali alle precedenti.

Per la corretta gestione della password è necessario:
- almeno ogni 3 mesi è obbligatorio cambiare la password;
- ogni password ricevuta va modificata al primo utilizzo;
- la password venga conservata in un luogo sicuro;
- non rivelare o condividere la password con i colleghi di lavoro, famigliari e amici, soprattutto attraverso il telefono;
- non utilizzare la funzione, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni.

9. L'installazione di hardware e software, nonché la modifica dei parametri di configurazione, possono essere eseguiti solamente dalle persone incaricate dall'Associazione, sicché l'incaricato deve rispettare le seguenti regole di comportamento:
   - non installare sistemi per connessione esterne (es: modem, wifi); tali connessioni, aggirando i sistemi preposti alla sicurezza della rete aziendale, aumentano sensibilmente i rischi di intrusioni e di attacchi dall'esterno;
   - non installare programmi, anche in versione demo. In particolare, è vietata l'installazione di giochi, programmi in prova (shareware), programmi gratuiti (freeware), programmi pirata, e in generale tutti i software non autorizzati dal Servizio Informatico;
   - non modificare i parametri di configurazione del proprio PC senza espressa autorizzazione e senza il supporto di personale tecnico qualificato;
   - si ricorda che normalmente la condivisione di aree e di risorse del proprio PC è vietata. Può essere autorizzata dal Servizio Informatico, solo in casi eccezionali e solo per il tempo strettamente necessario allo svolgimento delle attività di lavoro. In questi casi devono essere adottate password di lettura e scrittura e la condivisione deve operare solo su singole directory del PC, e non sull'intero disco rigido.
10. Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità dell'Associazione e in stretta connessione con l'effettiva attività e mansioni del lavoratore o del volontario che utilizza tale funzionalità.
    Nell'uso della posta elettronica occorre rispettare le seguenti regole di comportamento:
    - se si ricevono mail da destinatari sconosciuti contenenti file di qualsiasi tipo, procedere alla loro immediata eliminazione;
    - è fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione;
    - la casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione;
    - nell'ipotesi in cui la mail debba essere utilizzata per la trasmissione di dati particolari (ex dati sensibili), si raccomanda di prestare attenzione a che:
      - l'indirizzo del destinatario sia stato correttamente digitato;
      - l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;
      - nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio.
11. In merito alle operazioni di salvataggio, occorre rispettare le seguenti regole di comportamento:
    - per i dati ed i documenti che risiedono sui server gestiti centralmente, come ad esempio cartelle di rete e database, il Servizio Informatico esegue i salvataggi con la possibilità di ripristinare in toto oppure selettivamente eventuali files distrutti, ad esempio per guasti hardware oppure per cancellazioni involontarie;
    - per i dati ed i documenti che risiedono esclusivamente sul PC, ogni Incaricato deve eseguire almeno una volta alla settimana la copia (salvataggio, o backup). Questo allo scopo di garantire la disponibilità ed il ripristino dei Dati Personali nel caso di una generica compromissione delle risorse (cancellazioni accidentali, guasti, furti…).

12. I supporti rimovibili, come ad esempio dischi magnetici o hard disk esterni, penne/chiavette USB o CD riscrivibili, quando contengono dati personali devono essere custoditi in luogo protetto e non accessibile (armadio chiuso a chiave, etc.). Quando non sono più utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri Incaricati non autorizzati al Trattamento degli stessi dati, soltanto dopo essere stati formattati. Tali operazioni vengono effettuate a cura del servizio Sistemi. Il trasferimento di file contenenti dati personali, dati particolari (ex dati sensibili) e giudiziari su supporti rimovibili, è da eseguire unicamente in via transitoria, ponendo la massima attenzione alla destinazione di trasferimento e cancellando i file appena possibile. I dati particolari (ex dati sensibili)/giudiziari devono essere crittografati.
13. Per prevenire eventuali danneggiamenti al software causati dalla presenza o dall'azione di programmi virus informatici, su ogni elaboratore dell'Associazione è stato installato un software antivirus aziendale che si aggiorna automaticamente all'ultima versione disponibile.
    L'antivirus aziendale non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito. Nel caso il programma antivirus installato sul proprio PC riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus è necessario darne immediatamente segnalazione al responsabile del Servizio Informatico. Si raccomanda di non scaricare e né tantomeno aprire file provenienti via e-mail da mittenti sconosciuti. Tali file, possono essere portatori di virus e compromettere la funzionalità del PC, l'integrità dei dati in essa contenuti e soprattutto l'integrità dei sistemi collegati al PC stesso.
14. In merito alla gestione degli strumenti "non elettronici" (vale a dire sia documenti cartacei sia documenti di altro tipo) i documenti contenenti dati particolari o giudiziari devono essere protetti in appositi armadi dotati di chiavi. Tutti i documenti contenenti dati particolari o giudiziari che si ritiene debbano essere eliminati devono essere distrutti e non gettati nei cestini.
    Per proteggere i dati personali è opportuno evitare il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici (corridoi o sale riunioni), come pure l'abbandono in vista sulle scrivanie quando ci si debba assentare dal proprio posto di lavoro. Nel caso di dati particolari (ex dati sensibili) e/o giudiziari, il rispetto di queste norme è obbligatorio.
15. In merito alla distruzione delle copie cartacee, coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzando strumenti per la riproduzione cartacea di documenti digitali, sono tenuti a procedere alla relativa distruzione del supporto, qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli, salva l'ipotesi di uso esclusivamente personale per eventuali appunti o brutte copie, da distruggere immediatamente quando non più necessarie.
16. Il Trattamento sicuro di documenti contenenti Dati Personali richiede la presenza di misure di sicurezza con le quali l'Incaricato possa interagire ed una serie di accorgimenti direttamente gestibili dall'Incaricato stesso. In particolare, si richiede:
    - la presenza e l'uso tassativo di armadi e cassetti dotati di serratura adeguata;
    - la presenza e l'uso tassativo, ove si richieda la distruzione di documenti contenenti dati particolari (ex dati sensibili) e giudiziari, di un trita documenti.
17. L'Incaricato deve attenersi alle seguenti prescrizioni:
    - in nessun caso è concesso l'accesso a documentazione contenente Dati Personali per motivi non dettati da esigenze di lavoro strettamente connesse ai trattamenti dichiarati, autorizzati e tutelati dal Titolare;
    - la documentazione contenente Dati Personali che, per ragioni di praticità operativa, risiede sulle scrivanie degli Incaricati, deve comunque essere rimossa al termine dell'orario di lavoro;
    - l'accesso ai supporti deve essere limitato al tempo necessario a svolgere i Trattamenti previsti;
    - i supporti devono essere archiviati in ambiente ad accesso controllato;
    - i documenti contenenti dati personali, non devono essere lasciati incustoditi in un ambiente non controllato (ad es. a seguito della stampa dei documenti su stampante di rete);

- il numero di copie di documenti contenenti Dati Personali deve essere strettamente funzionale alle esigenze di lavoro;
- cassetti ed armadi contenenti documentazione riservata debbono tassativamente essere chiusi a chiave fuori dell'orario di lavoro;
- l'accesso fuori orario lavorativo a documenti contenenti Dati particolari (ex dati sensibili) /giudiziari può avvenire da parte di personale Incaricato, o tramite autorizzazione di quest'ultimo da parte del Responsabile al trattamento, previa registrazione dell'accesso ai documenti su supporto;
- la distruzione di documenti contenenti Dati Personali deve essere operata, ove possibile, direttamente dal personale Incaricato;
- ove non siano disponibili strumenti per la distruzione dei documenti (trita documenti), o il volume di questi sia tale da imporre il ricorso al servizio di macero, il personale Incaricato che avvia al macero la documentazione è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo e solido;
- quando gli atti e i documenti contenenti dati personali, dati particolari (ex dati sensibili) o giudiziari sono affidati agli Incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli Incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate;
- l'accesso agli archivi contenenti dati particolari (ex dati sensibili) o giudiziari deve essere controllato. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.
- è severamente vietato utilizzare documenti contenenti dati personali, dati particolari (ex dati sensibili) o giudiziari come carta da riciclo o da appunti.

Regolamento aziendale per la Privacy e conferimento dell'incarico al Trattamento dati

SECONDA PARTE: INCARICO AL TRATTAMENTO DATI

Il sottoscritto _____, in qualità di Direttore della Sede di _____, Responsabile Interno del Trattamento, conferisce l'incarico al Trattamento dei dati, con le modalità a seguire definite.

Cognome e nome dell'incaricato: _____

Mansioni svolte: _____

categoria di soggetti interessati	dati che l'incaricato è autorizzato a trattare

L'incaricato, nel firmare il presente incarico per accettazione, s'impegna a rispettare il Regolamento Aziendale per la Protezione dei Dati Personali, **relativamente alle clausole compatibili con le mansioni svolte** ed i dati personali oggetto dell'incarico, consapevole che in caso di violazione potrà incorrere in provvedimenti sanzionatori.

Data _____

firma del Responsabile Interno _____

firma dell'Incaricato per accettazione _____