**NB. Le policy devono essere esposte nella bacheca,
ovvero inviata via mail ai dipendenti**

POLICY INTERNE

L'Ordine periti industriali e laureati delle province di Ascoli Piceno e di Fermo con sede in Via Sant'Alessandro, 3 - 63900 Fermo FM, (di seguito solo Ordine dei Periti) nella sua qualità di titolare del trattamento dei dati personali ai sensi dell'art. 4 lett. 7) del Regolamento Europeo 679/2016, al fine di porre in essere le misure tecniche ed organizzative di cui all'art. 32 del Regolamento Europeo 679/2016, ha istituito le seguenti policy interne:

1

POLICY PER L'ACCESSO ALLE BANCHE DATI CARTECEE

1. Individuazione delle Banche Dati e Regolamentazione dell'accesso:

Le banche dati cartacee sono ubicate presso la sede legale, tutti i documenti devono essere conservati negli appositi armadi dotati di serratura. Tutti i documenti, compresi quelli contenenti dati particolari dei lavoratori sono ivi ubicati, l'accesso è consentito al titolare e al personale autorizzato che si occupa della gestione amministrativa dell'ente e per cui è stata predisposta idonea nomina incaricati/autorizzati al trattamento. È fatto divieto di lasciare incustodita la banca dati, per cui all'interno degli uffici dove le stesse sono collocate, nel periodo di apertura dell'archivio dovrà essere sempre presente un dipendente. Nell'ipotesi di assenza di tutti i dipendenti, anche temporanea, la stanza dovrà essere chiusa a chiave.

2. Custodia delle chiavi d'accesso agli armadietti:

Le chiavi d'accesso al locale archivio sono custodite dagli Incaricati, i quale sono perciò responsabili di ogni accesso non autorizzato alla documentazione ivi contenuta. Dette chiavi non dovranno mai essere lasciate incustodite e/o posizionate sulla porta del locale stesso.

POLICY DATA BREACH

Le violazioni di dati personali sono gestite dal titolare del trattamento o da un suo delegato.

- *Segnalazione*

Nell'ipotesi in cui un incaricato si accorga di una concreta, potenziale o sospetta violazione dei dati personali deve immediatamente darne contezza al titolare.

- *Identificazione della violazione*

Il titolare procederà ad identificare, con il supporto degli incaricati, la natura dell'incidente verificatosi, coinvolgendo di volta il responsabile dell'ufficio competente per la violazione. In questa fase la valutazione deve tenere conto:

1. data della scoperta della violazione;
2. descrizione dell'incidente;
3. categorie degli interessati;
4. descrizioni di eventuali azioni poste in essere;

- *Recovery*

Il titolare, congiuntamente al responsabile dell'ufficio deve procedere, senza ritardo, a porre in essere tutte le azioni che possano limitare i danni derivanti dalla violazione (a puro titolo esemplificativo e non esaustivo: riparazione della strumentazione, utilizzo di file di backup, isolamento o chiusura del settore compromesso). Individuate tali azioni, il titolare vaglierà la possibilità di darne notizia al Garante e agli interessati.

- *Notifica al garante (se necessaria)*

Nelle caso in cui la notifica del data breach si rende necessaria, il Titolare procede comunica al garante quanto segue:

- a) il tipo di violazione subita;
- b) circostanza in cui la stessa si è verificata;
- c) conseguenza del data breach;
- d) provvedimenti adottati per porvi rimedio.

- *Comunicazione agli interessati (eventuale)*

Il titolare, qualora dalla violazione ne scaturisca un pericolo per la libertà e i diritti dell'interessato, provvede entro 72 ore a dargliene comunicazione. Il messaggio dovrà essere comunicato in maniera evidente e trasparente (valuta l'opportunità di fornire un modello al cliente).

- *Documentazione della violazione*

Anche fuori dei casi di comunicazione obbligatoria all'autorità garante ed agli interessati, è fatto obbligo di annotare il data breach nel registro della violazioni.

Tale registro deve essere costantemente aggiornato e messo a disposizione del garante qualora lo richieda.

POLICY DATA RETENTION

I dati personali sono conservati su supporto cartaceo e supporto informatico.

La conservazione del dato è connessa alla finalità del trattamento, per tali motivi la data retention segue le procedure di seguito elencate:

- Dati trattati con finalità fiscali: conservazione decennale al fine di garantire il diritto di difesa in eventuali contenziosi con l'autorità tributaria e/o penale;
- Dati trattati al fine di porre in essere la prestazione: i dati verranno cancellati entro 10 anni al fine di garantire il diritto di difesa in eventuali azioni di responsabilità contrattuale;

Il titolare, per quanto attiene al dato informatico, procede ad effettuare back up giornalieri dei dati contenuti sul server. Il titolare conserva i backup degli ultimi due giorni.

La distruzione dei supporti informatici è affidata alla Sig.ra Steca Fabrizia, la quale potrà di volta in volta nominare appositi incaricati, i quali opereranno sotto la loro supervisione, ovvero dei Responsabili del Trattamento ex art. 28 GDPR a tale esclusivo fine.

I dati contenuti negli archivi cartacei, decorsi i termini sopra riportati, verranno distrutti tramite trita carte, qualora i documenti contengano dati che possano andare ad incidere sui diritti o le libertà dell'interessato, il titolare dopo aver distrutto il documento con il trita carte procederà a bruciare la carta residua, ovvero procederà incaricando un Responsabile del Trattamento ex art. 28 GDPR appositamente per tali fini.

POLICY SULL'UTILIZZO DEGLI STRUMENTI ELETTRONICI

4. Utilizzo del Personal Computer

1.1. Il Personal Computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento. Il personal computer dato in affidamento all'utente permette l'accesso alla rete del Ordine dei Periti solo

attraverso specifiche **credenziali di autenticazione** come meglio descritto al successivo punto del presente Regolamento.

- 1.2. L'Ordine dei Periti rende noto che il personale è autorizzato a compiere interventi nel sistema informatico dell'ente diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.). Detti interventi potranno anche comportare l'accesso in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'ente, si applica anche in caso di assenza prolungata od impedimento dell'utente.
- 1.3. Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal titolare del trattamento e/o dietro sua autorizzazione, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone la stessa Ordine dei Periti a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.
- 1.4. Salvo preventiva espressa autorizzazione del titolare del trattamento non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, etc.).
- 1.5. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Titolare del Trattamento nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto 6. del presente Regolamento relativo alle procedure di protezione antivirus.
- 1.6. Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa

di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

2. Gestione ed assegnazione delle credenziali di autenticazione

- 2.1 Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal Titolare del Trattamento. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), associato ad una parola chiave (password) riservata che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Titolare.
- 2.2 La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.
- 2.3 È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni sei mesi (Ogni tre mesi nel caso invece di trattamento di dati sensibili attraverso l'ausilio di strumenti elettronici).
- 2.4 Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il Titolare del Trattamento.
- 2.5 Ogni utente è preposto alla custodia delle proprie credenziali di autenticazione.

3 Utilizzo della rete del Ordine dei Periti

- 3.1. Per l'accesso alla rete dell'Ordine dei Periti ciascun utente deve essere in possesso della specifica credenziale di autenticazione.
- 3.2. È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. La parola chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.
- 3.3. Le cartelle utenti presenti nei server dell'Ordine dei Periti sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.

3.4. Il Titolare del Trattamento può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

3.5. Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

4. Utilizzo e conservazione dei supporti rimovibili

4.1. Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il Titolare del Trattamento e seguire le istruzioni da questo impartite.

4.2. In ogni caso, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

4.3. E' vietato l'utilizzo di supporti rimovibili personali.

4.4. L'utente è responsabile della custodia dei supporti e dei dati dell'ente in essi contenuti.

5. Navigazione in Internet

5.1. Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento dell'ente utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

5.2. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare internet per:

- l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica

dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il Titolare del Trattamento);

-l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dal Titolare del Trattamento e comunque nel rispetto delle normali procedure di acquisto;

-ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;

-la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile d'ufficio;

- l'accesso, tramite internet, a caselle webmail di posta elettronica personale.

5.3. Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Ordine dei Periti rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black-list.

5.4. Gli eventuali controlli, compiuti dal Titolare del Trattamento, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'ente.

6. *Protezione antivirus*

6.1. Il sistema informatico dell'Ordine dei Periti è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico dell'ente mediante virus o mediante ogni altro software aggressivo.

6.2. Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al Titolare del Trattamento.

6.3. Ogni dispositivo magnetico di provenienza esterna all'ente dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso

venga rilevato un virus, dovrà essere prontamente consegnato al Titolare del Trattamento.

7. Utilizzo dei telefoni, fax e fotocopiatrici dell'ente

- 7.1. Il telefono dell'ente affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentito solo nel caso di comprovata necessità ed urgenza.
- 7.2. Qualora venisse assegnato un cellulare dell'ente all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare dell'ente si applicano le medesime regole sopra previste per l'utilizzo del telefono dell'ente: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare dell'ente è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite dal Titolare del Trattamento.
- 7.3. È vietato l'utilizzo dei fax dell'ente per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Responsabile di ufficio.
- 7.4. È vietato l'utilizzo delle fotocopiatrici dell'ente per fini personali, salvo preventiva ed esplicita autorizzazione da del Titolare del Trattamento.