# Policy sugli strumenti IT

**SOMMARIO**

# I. INTRODUZIONE

## A. SCOPO

La presente Policy sugli strumenti IT ha lo scopo di regolamentare l'utilizzo degli Strumenti Aziendali dello Studio STUDIO DENTISTICO ASS.TO DOTT.BOSCARINI-DOTT.SSA CORDIOLI (infra solo **"Studio"**), nonché degli Strumenti Personali autorizzati per uso lavorativo.

Salvo diversamente previsto all'interno di questo documento, tutti i termini riportati con lettera iniziale maiuscola si riferiscono alle definizioni riportate nel GDPR e riportate per comodità nella sezione "Glossario e Acronimi".

## B. ENTRATA IN VIGORE, PUBBLICITÀ E CAMPO DI APPLICAZIONE

La presente Policy sostituisce integralmente tutte le disposizioni in precedenza adottate dallo Studio in materia, in qualsiasi forma comunicate. La stessa Policy:

- è stata allegata all'Autorizzazione al Trattamento dei Dati Personali;
- è disponibile previa richiesta;
- si applica a tutte le Persone Autorizzate, siano esse interne od esterne allo Studio.

## C. NORMATIVA DI RIFERIMENTO

Articolo 29

**Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento**

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Articolo 32

**Sicurezza del trattamento**

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.
4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

## D. DOCUMENTI DI RIFERIMENTO

1. Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679
2. Procedura per la gestione dei Data Breach
3. Procedura sull'esercizio dei diritti dell'Interessato
4. Registro dei Trattamenti ex art. 30 GDPR

## E. GLOSSARIO E ACRONIMI

**Aree Sensibili:** sono quei luoghi fisici o della Rete Aziendale in cui vengono Trattati Dati Particolari e/o Dati Giudiziari relativi a persone fisiche; e/o luoghi in cui vengono gestiti e consultati documenti riservati a cui è assolutamente vietato accedere se non per motivi di servizio;
**Autorità di Controllo:** l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 GDPR;
**Consenso dell'Interessato** o **Consenso**: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i Dati Personali che lo riguardano siano oggetto di Trattamento;
**Dati Biometrici:** i Dati Personali ottenuti da un Trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
**Dati Comuni:** sono tutti i Dati Personali che non appartengono alle categorie dei Dati Particolari e Dati Giudiziari;
**Dati Genetici:** i Dati Personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
**Dati Giudiziari:** Dati Personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;
**Dati Particolari:** Dati Personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
**Dati relativi alla Salute:** i Dati Personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
**Dato Personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("**Interessato**"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
**Destinatario/i**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di Dati Personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di Dati Personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli

Stati membri non sono considerate Destinatari; il Trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del Trattamento;

**Device Fissi**: si intendono gli strumenti informatici non facilmente removibili dal perimetro dello Studio quali personal computer, server locali, stampanti affidati alle Persone Autorizzate per uso professionale;

**Device Mobili**: in generale si intendono quegli strumenti informatici che per loro natura sono facilmente asportabili dal perimetro aziendale quali chiavette USB, SD cards, hard disk esterni, tablet e smartphone utilizzati dalla Persone Autorizzate per uso professionale;

**DPO** o **Data Protection Officer**: è una persona fisica, nominata obbligatoriamente nei casi di cui all'art. 37.1 GDPR dal Titolare o dal Responsabile del Trattamento e deve possedere una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati per assisterli nel rispetto a livello interno del GDPR;

**GDPR** o **Regolamento:** Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679;

**Incaricato/i o Persona/e Autorizzata/e:** si tratta dei Collaboratori autorizzati al Trattamento dei Dati Personali sotto la diretta autorità del Titolare e/o del Responsabile ex artt. 4(10) e 29 del GDPR. Stante la definizione fornita dal Gruppo di Lavoro Articolo 29 dell'Opinione 2/2017 questa definizione ricomprende: dipendenti ed ex dipendenti, dirigenti, sindaci, collaboratori e lavoratori a partita IVA, lavoratori a chiamata, part-time, *job-sharing*, contratti a termine, stage, senza distinzione di ruolo, funzione e/o livello, e, più in generale, tutti coloro che utilizzino od abbiano utilizzato Strumenti Aziendali o Strumenti Personali, operino sulla Rete Aziendale ovvero siano a conoscenza di informazioni aziendali rilevanti quali, a titolo esemplificativo e non esaustivo: (a) i Dati Personali di pazienti, dipendenti e fornitori, compresi gli indirizzi di posta elettronica; (b) tutte le informazioni aventi ad oggetto informazioni confidenziali di natura commerciale, finanziaria o di strategia di business; nonché (c) i dati e le informazioni relative ai processi aziendali, inclusa la realizzazione di marchi, brevetti e diritti di proprietà industriale, la cui tutela prescinde dagli effetti pregiudizievoli che potrebbe comportare la diffusione delle medesime.

**Pseudonimizzazione:** il Trattamento dei Dati Personali in modo tale che i Dati Personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali Dati Personali non siano attribuiti a una persona fisica identificata o identificabile;

**Responsabile del Trattamento** o **Responsabile**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta Dati Personali per conto del Titolare del Trattamento; deve presentare garanzie sufficienti di attuare misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato;

**Rete Aziendale:** rappresenta il perimetro digitale dello Studio, possibilmente contenente Dati Personali e/o informazioni riservate, comprensivo dei dispositivi hardware/software sia per la gestione dei servizi interni (es. switch, LAN, Wi-Fi) che dei collegamenti da o verso l'esterno (es. boundary router, SSH, VPN);

**Strumenti Aziendali**: l'insieme di Device Fissi e Device Mobili concessi in comodato d'uso dallo Studio alle Persone Autorizzate al fine di svolgere le proprie mansioni, comprensivi altresì di eventuali strumenti di diagnostica necessari per l'erogazione della prestazione medica (es. radiografo);

**Strumenti Personali**: i Device Mobili di proprietà delle Persone Autorizzate autorizzati ad essere impiegati per uso professionale;

**Titolare del Trattamento** o **Titolare:** 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; quando le finalità e i mezzi di tale Trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

**Trattamento** o **Trattato/Trattati:** 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, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

**Violazione Dei Dati Personali** ovvero **Data Breach:** è la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque Trattati.

## II. LA POLICY SUGLI STRUMENTI IT

Lo Studio ritiene fondamentale la comprensione, il rispetto e la corretta applicazione di quanto indicato nella presente Policy al fine di arginare il più possibile i rischi connessi ad un eventuale utilizzo illecito (o, comunque, non corretto) delle risorse informatiche del medesimo, proteggendo le Persone Autorizzate da azioni illegali e/o pericolose e salvaguardando il patrimonio intellettuale dello Studio. L'utilizzo degli Strumenti Aziendali e Strumenti Personali da parte della Persone Autorizzate, pertanto, deve sempre ispirarsi ai principi di massima diligenza, buona fede e correttezza.

Si ricorda come un uso improprio e/o non conforme ai suddetti principi degli Strumenti Aziendali e Strumenti Personali ovvero della Rete Aziendale e della posta elettronica, potrebbe esporre lo Studio a serie conseguenze pregiudizievoli, quali, a titolo meramente esemplificativo, accessi non autorizzati al suo sistema informatico o al suo patrimonio di dati e notizie, introduzione di virus, o ancora furti o divulgazioni di informazioni segrete, confidenziali e/o riservate, sottrazione o Trattamenti Illeciti di Dati Personali.

In ragione pertanto di primarie esigenze organizzative, produttive e di sicurezza, lo Studio ha adottato la presente Policy, che ha la finalità ed utilità di:

- fornire precise indicazioni alle Persone Autorizzate circa le modalità di funzionamento degli Strumenti Aziendali e Strumenti Personali, della Rete Aziendale e della posta elettronica aziendale;
- codificare chiare regole di comportamento da rispettare nell'uso di detti strumenti, onde evitare problemi, disservizi e maggiori costi (di manutenzione o di altro tipo) ovvero minacce alla Rete Aziendale o alla sicurezza dei sistemi e dei dati in essi contenuti;
- istituire idonei strumenti di controllo che - nel rispetto delle previsioni di cui agli artt. 4 e 8 della Legge 20 maggio 1970 n. 300 ("**Statuto Lavoratori**"), nonché dei principi di correttezza, pertinenza e non eccedenza di cui all'art. 5 del Regolamento - consentano di evitare e prevenire condotte improprie nell'utilizzo degli Strumenti Aziendali e Strumenti Personali, in modo da salvaguardare le Informazioni aziendali, gli standard qualitativi dei servizi resi ai pazienti ed il *know how* dello Studio.

La presente Policy intende anche informare i suoi destinatari circa l'esercizio dell'eventuale potere disciplinare dello Studio nei confronti delle Persone Autorizzate ad essa soggette, qualora si verificasse ed accertasse - secondo le procedure e nel rispetto delle garanzie e tutele oggetto delle previsioni che seguono - un uso improprio e/o non autorizzato degli Strumenti Aziendali e Strumenti Personali.

Lo Studio garantisce, quindi, che con la presente Policy:

- non si intende adottare e/o autorizzare e/o istituire, in alcun modo, sistemi e/o strumenti di controllo a distanza e/o in forma occulta delle opinioni, abitudini e/o dell'attività delle Persone Autorizzate della medesima, che rimangono strettamente vietati e non consentiti;
- si intende unicamente, come detto, istituire forme di verifica del corretto uso delle degli Strumenti Aziendali e Strumenti Personali, esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro,

per la tutela del patrimonio aziendale e della sicurezza del sistema e della Rete Aziendale dello Studio, al fine di tutelare quest'ultima da eventuali danni che possano essere generati e che siano riconducibili ad una condotta posta in essere dalla Persona Autorizzata, in violazione della presente policy e/o in violazione di norme di legge, inadempimenti contrattuali e/o dalla commissione di fatti illeciti e/o aventi rilevanza penale e/o disciplinare.

Al fine di agevolare la lettura della presente Policy, lo Studio ha predisposto un riassunto nella "**To do List**" allegata in calce alla presente.

## A. UTILIZZO DEGLI STRUMENTI AZIENDALI

Tutti gli Strumenti Aziendali nonché la Rete Aziendale devono essere utilizzati e gestiti dalla singola Persona Autorizzata nel rispetto dei principi di diligenza e correttezza in modo conforme alla presente Policy ed all'Autorizzazione al Trattamento dei Dati Personali.

In ogni caso di revoca dell'Autorizzazione al trattamento dei Dati Personali, gli Strumenti Aziendali dovranno essere prontamente restituiti secondo la procedura indicata alla sezione *Ricognizione, riconsegna e ripristino di strumenti aziendali, strumenti personali, supporti cartacei e oggetti personali*.

Lo Studio si riserva di verificare, nel rispetto della tutela dei Dati Personali e del diritto alla riservatezza di ogni Persona Autorizzata (nonché, più in generale, nel rispetto di quanto previsto dalla vigente normativa in materia di controllo a distanza dei lavoratori), che l'utilizzo degli Strumenti Aziendali avvenga in maniera conforme alla presente Policy e che, in particolare, non venga scaricato/installato/utilizzato alcun software non autorizzato o che, comunque, possa compromettere gli Strumenti Aziendali o la Rete Aziendale. Maggiori dettagli in merito sono contenuti nella sezione *Attività di controllo della Rete Aziendale, Strumenti Aziendali e Strumenti Personali*.

### 1. Regole comuni per Device Fissi e Device Mobili

I Device Fissi e Device Mobili, intesi nell'accezione di Strumenti Aziendali, sono uno strumento di lavoro che pertanto deve essere utilizzato esclusivamente per l'attività lavorativa.

Gli Strumenti Aziendali devono essere custoditi con cura, evitando ogni possibile forma di danneggiamento ed essere bloccati (cd. *log-out* di sessione) quando se ne interrompe l'uso, in modo che utenti non autorizzati non abbiano accesso ai dati in esso contenuti salvo che con l'inserimento delle credenziali di sblocco.

Anche al fine di evitare di compromettere la stabilità degli Strumenti Aziendali, è espressamente vietato:

- salvo non sia già impedito by default, installare ed utilizzare programmi non espressamente autorizzati dallo Studio;
- la conservazione e la trasmissione di programmi, file, contenuti multimediali ed altro in violazione delle rispettive licenze di utilizzo (v., in proposito, gli obblighi imposti dalla l. 22 aprile 1941, n. 633 e ss. mm. ii. sulla protezione del diritto d'autore e altri diritti connessi al suo esercizio);
- installare ed utilizzare mezzi di comunicazione propri (ad es. modem, VPN, access point/apparati wi-fi), tantomeno per consentire l'accesso a persone non autorizzate alla Rete Aziendale;
- fare copia, in qualunque forma e su qualunque tipo di Device Mobile, di Dati Personali e/o informazioni riservate e/o file dello Studio nella disponibilità della Persona Autorizzata al fine di farne un uso personale o per trasferirle a terzi, salvo quanto espressamente previsto di volta in volta per le ipotesi di trasferimento dei dati relativi alla salute dei pazienti a colleghi, collaboratori e/o odontotecnici per le attività necessarie all'erogazione della prestazione medica;
- utilizzare programmi informatici o strumenti per intercettare, falsificare, alterare o cancellare per finalità illecite il contenuto di comunicazioni e/o documenti informatici;

- modificare le configurazioni aziendali impostate sugli Strumenti Aziendali, salvo autorizzazione preventiva dello Studio e/o delle competenti funzioni tecniche espressamente indicate dal medesimo;
- collocare, anche temporaneamente, sugli Strumenti Aziendali o nella Rete Aziendale qualsiasi file che non sia attinente allo svolgimento dell'attività lavorativa;
- utilizzare, per la propria attività lavorativa, Strumenti Personali non previamente autorizzati. Salvo quanto precede, la Persona Autorizzata si impegna comunque a prendere ogni accorgimento di sicurezza idoneo per la salvaguardia delle informazioni aziendali.
- ascoltare e/o visionare e/o scaricare programmi, film, file audio/musicali su Strumenti Aziendali, salvo autorizzazione preventiva dello Studio e/o delle competenti funzioni tecniche espressamente indicate dal medesimo.

L'inosservanza delle suddette previsioni può esporre lo Studio a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software e su tutte le opere di ingegno (es: film, file musicali, ecc.) - che impone la presenza nel sistema di software regolarmente licenziati o comunque liberi e quindi non protetti dal diritto d'autore - vengono sanzionate anche penalmente.

Sul punto, lo Studio ha installato, sulla Rete Aziendale, sistemi, meglio descritti nella sezione *Utilizzo della Rete Aziendale*, in grado di impedire, nel rispetto del principio di data protection *by design e by default*, l'accesso a siti non pertinenti con l'attività lavorativa o che offrono contenuti palesemente violativi del diritto d'autore.

Nel caso si rilevino continue attività anomale da parte di uno Strumento Aziendale (traffico eccessivo, trasmissione di virus, attività comunque in grado di causare danno alla normale operatività aziendale o a soggetti terzi), lo Studio si riserva di intervenire prontamente e di bloccare l'utilizzo dello Strumento Aziendale, al fine di risolvere successivamente il problema/disservizio in presenza della Persona Autorizzata. In caso di prolungata assenza o impedimento dell'Utente che renda indispensabile e indifferibile per lo Studio intervenire per esclusive necessità di operatività e di sicurezza dello Strumento Aziendale, questi potrà accedere, tramite l'intervento di amministratori di sistema (ove presenti), ai dati e ai sistemi cui la Persona Autorizzata ha accesso riservato nell'ambito delle sue mansioni lavorative. In tali casi, la Persona Autorizzata sarà tempestivamente informata dell'intervento effettuato.

La Persona Autorizzata che rilevi attività anomale da parte di uno Strumento Aziendale è tenuta ad informare prontamente lo Studio e/o le competenti funzioni tecniche espressamente indicate dal medesimo tramite la **Procedura di gestione dei Data Breach**.

Ove possibile ed anche in ragione delle esigenze di tutela di informazioni aziendali rilevanti, è suggerito alla Persona Autorizzata l'utilizzo di *share* aziendali nella Rete Aziendale (e non in locale) per il salvataggio di file. Nel caso di memorizzazione dei dati su Device Mobili, la Persona Autorizzata dovrà accertarsi che questi siano Strumenti Aziendali che dovranno essere restituiti in caso di revoca dell'Autorizzazione al trattamento dei Dati Personali (vale a dire, al momento della cessazione del rapporto di lavoro/collaborazione con lo Studio), secondo la procedura indicata alla sezione *Ricognizione, riconsegna e ripristino di strumenti aziendali, strumenti personali, supporti cartacei e oggetti personali*.

Si elencano di seguito le misure specifiche - ove applicabili - adottate dallo Studio che la Persona Autorizzata è tenuta a non modificare e, ove applicabile, a verificarne il corretto funzionamento:

- *Antivirus*: sui sistemi in cui ciò sia tecnicamente possibile (eccezioni da approvare a cura dello Studio e/o delle competenti funzioni tecniche espressamente indicate dal medesimo) deve essere installato un antivirus aggiornato alla versione più recente e con aggiornamento delle firme con la frequenza massima consentita dal *tool* o comunque non inferiore ad una volta al giorno. L'antivirus deve essere configurato per controllare tutti i file introdotti sul sistema, provengano essi da Device Fissi o Device Mobili;

- *Firewall*: sui sistemi deve essere attivato il firewall, secondo le modalità stabilite dallo Studio e/o dalle competenti funzioni tecniche espressamente indicate dal medesimo;
- *Aggiornamenti software*: sugli Strumenti Aziendali deve essere attivato l'aggiornamento automatico del software installato (sistema operativo e applicazioni), con frequenza del controllo almeno quotidiana. Nel caso non fosse possibile automatizzare l'aggiornamento, esso dovrà essere effettuato manualmente dalla Persona Autorizzata con le stesse modalità;
- *Cifratura supporti*: le corrette modalità tecniche di cifratura degli Strumenti Aziendali sono indicate a cura dello Studio e/o delle competenti funzioni tecniche espressamente indicate dal medesimo nelle *Istruzioni per la cifratura degli Strumenti Aziendali e degli allegati contenenti Dati Particolari*;
- *Installazione software*: l'installazione di software oltre a quello di dotazione iniziale deve essere autorizzata esplicitamente dallo Studio e/o dalle competenti funzioni tecniche espressamente indicate dal medesimo, ivi compresi plugin ed estensioni di software già installato;
- *Backup*: l'operatore è tenuto ad effettuare frequenti backup, secondo le modalità specifiche fornite dallo Studio e/o dalle competenti funzioni tecniche espressamente indicate dal medesimo, dei dati e file di rilevanza aziendale. La frequenza del backup deve essere almeno settimanale.

Ogni eccezione a quanto riportato sopra deve essere approvata per iscritto dallo Studio e/o dalle competenti funzioni tecniche espressamente indicate dal medesimo.

## 2. Regole particolari per i Device Mobili

Rispetto al Device Fissi, i Device Mobili devono essere gestiti dalla Persona Autorizzata con più cura e diligenza, adottando tutti i ragionevoli provvedimenti per evitare eventuali danni e/o sottrazioni sia durante gli spostamenti sia durante l'utilizzo nei locali aziendali.

Si ricorda che i Device Mobili:

- non possono essere impostati dalla Persona Autorizzata in modo tale da abbassare i livelli di sicurezza rispetto a quanto previsto dallo Studio per gli Strumenti Aziendali e/o da eventuali aggiornamenti dei livelli di sicurezza comunicati dalla medesima. Pertanto, la Persona Autorizzata dovrà tutelare le informazioni aziendali presenti sul Device Mobile mediante un sistema di blocco tra quelli ritenuti adeguati e comunicati dallo Studio;
- possono essere facilmente rubati o smarriti e, quindi, comportare la perdita – oltre che dello strumento in sé - di informazioni importanti per lo Studio, ivi compresi Dati Personali;
- in caso di furto o smarrimento, la Persona Autorizzata deve denunciare, senza indugio, l'accaduto: i) alle funzioni competenti indicate nella **Procedura per la gestione dei Data Breach** in modo che possano essere prese misure per ridurre i rischi; ii) alle competenti autorità di Pubblica Sicurezza, consegnando copia della denuncia entro tre giorni dall'evento allo Studio e/o alle competenti funzioni tecniche espressamente indicate dal medesimo;
- in caso di revoca dell'Autorizzazione al trattamento dei Dati Personali (vale a dire al momento della cessazione del rapporto di lavoro/collaborazione con lo Studio), e in tutti gli altri casi in cui ciò sia richiesto dallo Studio (quali ad esempio il venir meno delle ragioni lavorative e/o professionali che avevano determinato l'assegnazione, la sua sostituzione con altro Strumento Aziendale), verrà seguita la procedura indicata alla sezione *Ricognizione, riconsegna e ripristino di strumenti aziendali, strumenti personali, supporti cartacei e oggetti personali* che consente alla Persona Autorizzata di partecipare alla ricognizione e alla consegna nella loro interezza dei Device Mobili allo Studio e/o alle competenti funzioni tecniche espressamente indicate dal medesimo;

- possono essere revocati/disabilitati dallo Studio in caso di uso improprio e/o in ogni altro caso ritenuto opportuno, previa comunque l'applicazione della procedura indicata alla sezione *Ricognizione, riconsegna e ripristino di strumenti aziendali, strumenti personali, supporti cartacei e oggetti personali* che consente alla Persona Autorizzata di partecipare alla ricognizione e alla consegna dei medesimi nella loro interezza.

Gli Strumenti Aziendali, e soprattutto i Device Mobili, se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altre Persone Autorizzate, per altri usi, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
Nel caso di Device Mobili usati per trattare dati aziendali, contenenti credenziali di accesso, Dati Personali, tra cui Dati Particolari (quali dati relativi alla salute dei pazienti) o comunque riservati, è dunque necessario adottare le opportune tecniche per impedire che, in caso di furto o smarrimento, i dati possano essere acceduti indebitamente secondo le modalità indicate nelle *Istruzioni per la cifratura degli Strumenti Aziendali e degli allegati contenenti Dati Particolari*. Lo Studio e/o le competenti funzioni tecniche espressamente indicate dal medesimo potranno supportare la Persona Autorizzata, qualora fosse necessario, dando ulteriori istruzioni.

Premesso il generale divieto di conservare informazioni aziendali rilevanti fuori dagli share aziendali nella Rete Aziendale, qualora ciò si rendesse necessario, la Persona Autorizzata dovrà accertarsi che questi siano Strumenti Aziendali che possono essere concessi in uso temporaneo, esclusivo o condiviso; in ogni caso, essi sono affidati alla piena responsabilità della Persona Autorizzata, anche in termini di custodia del supporto e dei dati ivi contenuti.
Per quanto concerne l'utilizzo dei Device Mobili sui quali vengano immesse informazioni aziendali rilevanti, fermo restando quanto sopra, la Persona Autorizzata, ove applicabile:

a) deve sempre salvare i dati sugli share aziendali nella Rete Aziendale, ove possibile;

b) non può concedere in uso il Device Mobile a soggetti terzi;

c) al momento della restituzione del supporto, deve cancellare o comunque rimuovere i Dati Personali o le informazioni aziendali rilevanti in esso presenti con tecniche crittograficamente sicure, così da impedire casi di Data Breach (cfr. **Procedura per la gestione dei Data Breach**).

In generale, la Persona Autorizzata è responsabile dei Device portatili e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nei locali aziendali.

Per quanto riguarda, invece, l'utilizzo di Device Mobili fuori dai locali dello Studio (es. presso un paziente, in treno ecc.), si ricorda che l'accesso alla Rete Aziendale è impedito per definizione.
Ove possibile, la Persona Autorizzata può richiedere l'abilitazione ad una Virtual Private Network (VPN) per l'accesso alla Rete Aziendale. Si ricorda che una volta attivata, tutta la navigazione verrà filtrata da sistemi, meglio descritti nella sezione *Utilizzo della Rete Aziendale*, in grado di impedire, nel rispetto del principio di data protection *by design e by default*, l'accesso a siti non pertinenti con l'attività lavorativa o che offrono contenuti palesemente violativi del diritto d'autore.

## B. UTILIZZO DEGLI STRUMENTI PERSONALI

La presente sezione disciplina l'uso degli Strumenti Personali, ossia le modalità con le quali la Persona Autorizzata può utilizzare Device Mobili personali anche a fini lavorativi.
Riassunta spesso come "Bring Your Own Device" (BYOD), questa policy può portare a una serie di vantaggi per le Persone Autorizzate, tra cui una migliore soddisfazione dei dipendenti circa il loro lavoro, un aumento generale del morale, una maggiore efficienza lavorativa e una maggiore flessibilità. Tuttavia, l'uso di Strumenti Personali a fini

lavorativi può favorire delle inferenze nella vita privata della Persona Autorizzata perché quegli strumenti potrebbero essere utilizzati, per definizione, dalla Persona Autorizzata per uso personale o dai propri familiari (ad es., alla sera o nel fine settimana). Se gli Strumenti Personali non sono correttamente impostati, è dunque possibile che lo Studio Tratti Dati Personali di eventuali familiari della Persona Autorizzata che utilizzano i dispositivi in questione.
Per evitare tale inferenze, ma permettere alle Persone Autorizzate di poter utilizzare i propri Strumenti Personali, lo Studio ha creato una serie di misure, elencate di seguito, che permettono l'uso di questi strumenti senza pregiudizio degli interessi dello Studio o delle Persone Autorizzate.

### 1. Autorizzazione degli Strumenti Personali

Ad esclusione dell'uso della posta elettronica, per il quale si richiama quanto indicato più sotto nella sezione *Utilizzo della posta elettronica*, lo Studio e/o le competenti funzioni tecniche espressamente indicate dal medesimo procedono, a seconda del tipo di Strumento Personale, ad impostare le configurazioni necessarie per arginare i rischi potenzialmente derivanti dall'utilizzo dello Strumento Personale a fini lavorativi, ovvero rischi di cybersecurity e privacy sia ad opera dello Studio a discapito della Persona Autorizzata, che viceversa.
Tra queste configurazioni è possibile che sullo Strumento Personale venga installato:

- un software di Mobile Application Management (MAM), che permetterebbe a un amministratore di sistema (sia esso interno o esterno allo Studio) di configurare i flussi di dati permessi su o mediante specifiche applicazioni professionali, ovvero l'estrazione o la copia di dati che la Persona Autorizzata può operare attraverso un'applicazione professionale utilizzata sul proprio Strumento Personale, e/o
- una Virtual Private Network (VPN) per l'accesso alle Rete Aziendale, meglio descritta nella sezione *Utilizzo della Rete Aziendale*, in grado di impedire, nel rispetto del principio di data protection by design e by default, l'accesso a siti non pertinenti con l'attività lavorativa o che offrano contenuti palesemente violativi del diritto d'autore. Per quest'ultima, si ricorda che sarà onere della Persona Autorizzata, al fine di evitare che la navigazione venga filtrata, disconnettere la VPN nel momento in cui intenda utilizzare il Device Mobile per la navigazione ad uso personale, e/o
- *strong authentication* (es. codice di sblocco) e cifratura di tutto o parte del Device Mobile, in modo che i Dati Personali ivi contenuti non siano accessibili in casi di smarrimento/furto.

Una volta che lo Strumento Personale è configurato, la Persona Autorizzata è tenuta a ricordare che:

- gli Strumenti Personali non possono essere impostati dalla Persona Autorizzata in modo tale da abbassare i livelli di sicurezza rispetto a quanto previsto dallo Studio per gli Strumenti Aziendali e/o da eventuali aggiornamenti dei livelli di sicurezza. Pertanto, la Persona Autorizzata dovrà tutelare le informazioni aziendali e gli eventuali Dati Particolari (quali i dati relativi alla salute dei pazienti) presenti sul Device Mobile mediante un sistema di blocco tra quelli ritenuti adeguati e/o consigliati dallo Studio;
- gli Strumenti Personali possono essere facilmente rubati o smarriti e, quindi, comportare la perdita – oltre che dello strumento in sé - di informazioni importanti per lo Studio, ivi compresi i Dati Personali e i Dati Particolari quali i dati relativi alla salute dei pazienti;
- in caso di furto o smarrimento, la Persona Autorizzata deve denunciare, senza indugio, l'accaduto alle funzioni competenti interne allo Studio indicate nella **Procedura per la gestione dei Data Breach**, in modo che possano essere prese misure per mitigare i rischi;
- in caso di revoca dell'Autorizzazione al trattamento dei Dati Personali (vale a dire al momento della cessazione del rapporto di lavoro/collaborazione con lo Studio) e in tutti gli altri casi in cui ciò sia richiesto dallo Studio (quali ad esempio il venir meno delle ragioni lavorative e/o professionali che avevano determinato l'autorizzazione all'uso dello Strumento Personale) verrà seguita la procedura indicata alla

sezione *Ricognizione, riconsegna e ripristino di strumenti aziendali, strumenti personali, supporti cartacei e oggetti personali* che consente alla Persona Autorizzata di partecipare alla ricognizione e rimozione delle configurazioni apportate;

- gli Strumenti Personali possono essere disabilitati all'uso lavorativo dallo Studio in caso di uso improprio e/o in ogni altro caso ritenuto opportuno, previa comunque l'applicazione della procedura indicata alla sezione *Ricognizione, riconsegna e ripristino di strumenti aziendali, strumenti personali, supporti cartacei e oggetti personali* che consente alla Persona Autorizzata di partecipare alla ricognizione e rimozione delle configurazioni apportate.

Lo Studio declina ogni responsabilità in caso di guasti o anomalie negli Strumenti Personali, se non contestati entro 2 giorni dalla riconsegna.

## C. RICOGNIZIONE, RICONSEGNA E RIPRISTINO DI STRUMENTI AZIENDALI, STRUMENTI PERSONALI, SUPPORTI CARTACEI E OGGETTI PERSONALI

In caso di modifica, revoca dell'Autorizzazione al trattamento dei Dati Personali (si legga al momento della cessazione del rapporto di lavoro/collaborazione con lo Studio) o trasferimento della Persona Autorizzata presso altra postazione fisica o sede, lo Studio, in applicazione del principio di correttezza dei Trattamenti e a tutela della dignità della persona, tenuto conto delle circostanze del caso concreto, adotta procedure che consentano alla Persona Autorizzata di partecipare alla ricognizione di Strumenti Aziendali, Strumenti Personali, supporti cartacei ed oggetti collocati all'interno degli uffici e delle altre aree dello Studio, in modo da distinguere ciò che appartiene allo Studio da ciò che appartiene alla Persona Autorizzata.

Alla fase di ricognizione segue una sempre una *Riconsegna degli Strumenti Aziendali e di supporti cartacei dello Studio* e/o un *Ripristino degli Strumenti Personali e restituzione degli oggetti personali*.

### 1. Riconsegna degli Strumenti Aziendali e di supporti cartacei dello Studio

Gli Strumenti Aziendali devono essere considerati in tutto il loro ciclo di vita e, dunque, regole di comportamento devono essere seguite anche quando diventano inservibili o, per qualsiasi causa, devono essere dismessi.

Nel seguito, come prescritto nel Provvedimento del Garante per la Protezione dei Dati Personali "*Rifiuti di apparecchiature elettriche ed elettroniche (RAAE) e misure di sicurezza dei dati personali*" del 13 ottobre 2008, si elencano le regole da rispettare per rottamare Strumenti Aziendali, quando non sono più utilizzabili poiché non funzionanti o, per qualsiasi motivo, non si intende più utilizzarli, nonché quando gli Strumenti Aziendali vengono smarriti o illecitamente sottratti. In tutti questi casi, la Persona Autorizzata dovrà dare informazione e ottenere autorizzazione dallo Studio e/o dalle competenti funzioni tecniche espressamente indicate dal medesimo.

Una volta effettuata la ricognizione dei dati contenuti nello Strumento Aziendale (che per definizione possono essere utilizzati solo per scopi lavorativi) in presenza dello Studio e/o delle competenti funzioni tecniche espressamente indicate dal medesimo e della Persona Autorizzata, lo Studio e/o le competenti funzioni tecniche espressamente indicate dal medesimo provvedono ad applicare misure tecniche per la cancellazione sicura dei dati tramite programmi (es. *wiping program*) che provvedono a distruggere i dati ivi contenuti in modo crittograficamente sicuro o comunque a renderli totalmente irrecuperabili. L'effettiva cancellazione dei Dati Personali dai supporti contenuti negli strumenti elettronici può anche risultare dai seguenti metodi, anche secondo il tipo di Strumento Aziendale da dismettere:

- sistemi di punzonatura o deformazione meccanica;
- distruzione fisica;
- demagnetizzazione ad alta intensità.

Le tecniche usate dallo Studio e/o dalle competenti funzioni tecniche espressamente indicate dal medesimo sono in ogni caso adeguate agli standard internazionali. La stessa procedura si applica ai supporti cartacei - contenenti Dati Personali o informazioni aziendali dello Studio - per i quali viene utilizzato, se del caso, un distruggi-documenti.
Qualora i dati non siano stati cancellati prima della consegna dello Strumento Aziendale a un rottamatore, lo Studio e/o le competenti funzioni tecniche espressamente indicate dal medesimo richiedono al rottamatore una dichiarazione scritta di garanzia di avere distrutto lo Strumento Aziendale consegnato e di non avere acceduto ai dati in esso contenuti o ceduti a terzi, né di averne tratto copie, né cartacee né informatiche, né totali né parziali.

### 2. Ripristino degli Strumenti Personali e restituzione degli oggetti personali.

Qualora la Persona Autorizzata sia (anche) stata autorizzata all'uso di Strumenti Personali e, per una qualunque delle ragioni sopra elencate (es. furto, sottrazione, revoca dell'autorizzazione), venga meno la necessità di utilizzare quello Strumento Personale per scopi lavorativi, la Persona Autorizzata deve darne comunicazione allo Studio e/o alle competenti funzioni tecniche espressamente indicate dal medesimo.
Salvo i casi di furto e sottrazione, una volta effettuata la ricognizione dei dati contenuti nello Strumento Personale in presenza dello Studio e/o delle competenti funzioni tecniche espressamente indicate dal medesimo e della Persona Autorizzata, lo Studio e/o le competenti funzioni tecniche espressamente indicate dal medesimo provvedono ad applicare misure tecniche per il ripristino delle configurazioni apportate in fase di approvazione in modo che i Dati Personali o informazioni aziendali dello Studio non siano più presenti o accessibili dallo Strumento Personale.
Per quanto concerne la gestione della casella della posta elettronica dell'Utente in caso di cessazione del rapporto di lavoro, si veda la sezione *Utilizzo della posta elettronica*.

## D. UTILIZZO DELLA RETE AZIENDALE

Lo Studio fornisce l'accesso alla Rete Aziendale a tutte le Persone Autorizzate al fine di supportarle nell'espletamento delle loro mansioni e per evitare che i benefici derivanti dall'impiego di questo strumento (divenuto oramai essenziale anche per l'attività lavorativa) possano essere parzialmente o totalmente annullati da un utilizzo erroneo e/o non regolamentato da parte della Persona Autorizzata.
L'accesso alla Rete Aziendale è permesso e registrato da tutti gli Strumenti Aziendali e, previa autorizzazione, dagli Strumenti Personali, attraverso credenziali di autenticazione specifiche per ciascuna Persona Autorizzata e, ove possibile, di un accesso VPN nel caso di Device Mobili che accedono da fuori il perimetro aziendale (cfr. sezione *Gestione delle credenziali*).
Trattandosi di uno strumento funzionale allo svolgimento della sola attività lavorativa, lo Studio vanta un interesse legittimo a che la Rete Aziendale sia sottoposta a tecniche di filtraggio e monitoraggio che ne garantiscano la sicurezza. Sul punto, si ricorda che lo Studio ha installato sulla Rete Aziendale sistemi di registrazione degli accessi, proxy e sistemi di content filtering in grado di impedire, l'accesso a siti non pertinenti con l'attività lavorativa o che offrono contenuti palesemente violativi del diritto d'autore.
Questa precauzione è stata adottata nel rispetto del principio di *data protection by design e by default*, in modo che le navigazioni delle Persone Autorizzate non vengano monitorate.
In ogni caso, alla Persona Autorizzata non è consentito accedere a siti Internet:

a) (i) superando o tentando di superare o disabilitando i sistemi di protezione e/o filtro eventualmente adottati dallo Studio per bloccare l'accesso ai medesimi ed in ogni caso utilizzare siti o altri strumenti che realizzino tale fine; (ii) che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che sia in qualche modo discriminatorio sulla base della razza, del colore della pelle, della fede religiosa, del sesso, della cittadinanza, dello stato civile,

degli handicap, ovvero degli altri principi e valori statuiti al riguardo dalla legislazione nazionale ed europea, salvo quanto espressamente autorizzato di volta in volta dallo Studio o per assolvere a richieste dell'autorità competente od ad obblighi di legge;

b) per trasmettere messaggi o accedere a siti Internet che non siano compatibili o che violino i regolamenti adottati dallo Studio, salvo quanto espressamente autorizzato di volta in volta dallo Studio o per assolvere a richieste dell'autorità competente o ad obblighi di legge;

c) per promuovere utile o guadagno personale nell'orario di lavoro e all'interno dei locali aziendali o tramite Strumenti Aziendali;

d) per utilizzare l'accesso alla Rete Aziendale in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore;

e) per visionare e/o effettuare il *download* di file di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, salvo quanto espressamente autorizzato di volta in volta dallo Studio o per assolvere a richieste dell'autorità competente o ad obblighi di legge.

Nel caso in cui la Rete Aziendale impedisca l'accesso a contenuti rilevanti per l'attività lavorativa (cd. falsi positivi), la Persona Autorizzata può informare lo Studio e/o le competenti funzioni tecniche espressamente indicate dal medesimo affinché crei un'eccezione temporanea o permanente per quel contenuto.

Resta inteso che pur non essendo monitorati, gli accessi alla Rete Aziendale sono comunque registrati, pertanto lo Studio si riserva di tutelarsi in giudizio contro la Persona Autorizzata qualora la sua navigazione sulla Rete Aziendale abbia recato danno alla medesima (si veda di seguito la sezione *Attività di controllo della Rete Aziendale, Strumenti Aziendali e Strumenti Personali*).

### 1. Wi-Fi guest e VPN

In considerazione del fatto che la Rete Aziendale può essere utilizzata solo per l'attività lavorativa, lo Studio - ove possibile - potrebbe prevedere un accesso Wi-Fi libero per tutte le Persone Autorizzate e per i pazienti dello Studio (cd. Wi-Fi guest).

Salvo il filtraggio di contenuti palesemente violativi del diritto d'autore e/o di natura oltraggiosa che non appartengano ai valori dello Studio, il Wi-Fi guest dovrebbe essere utilizzato dalle Persone Autorizzate per un moderato uso personale di Internet (es. gmail, home banking, social media ecc.) se tale uso:

- non interferisce con uno svolgimento responsabile della singola attività professionale;
- non espone lo Studio all'acquisto di beni e/o servizi estranei al servizio offerto dallo Studio e connessi al profitto personale della Persona Autorizzata (i.e. transazioni finanziarie, acquisti online, gioco d'azzardo e simili) e, comunque, non autorizzati;
- non infrange le regole della proprietà intellettuale dello Studio e/o di terzi;
- non arreca un danno di qualsiasi natura allo Studio, ai sistemi, alle Persone Autorizzate, ai pazienti o, più in generale, all'attività dello Studio.

Si precisa che dal Wi-Fi guest non sarebbe possibile accedere alla Rete Aziendale, pertanto la Persona Autorizzata dovrebbe scollegarsi dal Wi-Fi guest per poter accedere alla medesima.

La stessa limitazione si applica all'utilizzo di Device Mobili fuori dai locali dello Studio (es. presso un paziente, in treno, a casa ecc.), per i quali l'accesso alla Rete Aziendale è impedito per definizione.

La Persona Autorizzata - ove possibile - potrà richiedere l'abilitazione ad una Virtual Private Network (VPN) per l'accesso alla Rete Aziendale. Si ricorda che una volta attivata la VPN, tutta la navigazione verrà filtrata da sistemi

più sopra descritti, in grado di impedire, nel rispetto del principio di *data protection by design e by default*, l'accesso a siti non pertinenti con l'attività lavorativa o che offrono contenuti palesemente violativi del diritto d'autore.

## E. UTILIZZO DELLA POSTA ELETTRONICA

L'eventuale casella di posta elettronica aziendale assegnata alla Persona Autorizzata è uno strumento di lavoro e deve essere utilizzata in via prevalente per motivi attinenti e conferenti con l'attività lavorativa.
A tal fine, si suggerisce alla Persona Autorizzata di inserire alla fine di ogni messaggio il testo di seguito riportato nel **Footer** con il quale i destinatari vengono avvisati del contenuto professionale e riservato della comunicazione.
Utilizzando l'indirizzo di posta elettronica aziendale, l'Utente è a conoscenza e consapevole che:

- tutti i messaggi in entrata e in uscita dagli indirizzi di posta elettronica aziendale sono di proprietà dello Studio;
- l'uso dell'indirizzo di posta elettronica aziendale è in linea di principio ammesso in via prevalente per motivi attinenti all'attività professionale; l'uso della casella di posta elettronica aziendale per motivi personali è da ritenersi residuale ed eccezionale e l'Utente dovrà periodicamente cancellare i messaggi di natura personale eventualmente presenti nella propria casella di posta elettronica aziendale;
- il messaggio di posta elettronica potrebbe essere letto da destinatari diversi da quelli cui era diretto e ciò potrebbe determinare danni e conseguenze pregiudizievoli anche gravi per lo Studio;
- messaggi di posta elettronica spediti dalla casella di posta elettronica aziendale potrebbero non essere recapitati, essere distrutti o subire ritardi.

Alla Persona Autorizzata non è consentito:

a) utilizzare l'indirizzo aziendale di posta elettronica per inviare e/o ricevere: (i) allegati contenenti filmati o brani musicali (es.mp3) non correlati all'attività lavorativa; (ii) messaggi a carattere personale, se non nei limiti della normalità e cioè per un limitato numero di messaggi di cortesia o inerenti a rapporti parentali o amicali, sempre nel rispetto delle norme di comportamento di cui alla presente Policy e tenuto conto dell'interesse aziendale ed a condizione che tale utilizzo sia moderato e non intralci in alcun modo l'attività lavorativa;
b) salvo quanto espressamente autorizzato di volta in volta dallo Studio o per assolvere a richieste dell'autorità competente o ad obblighi di legge, inviare, tramite la posta elettronica aziendale, anche all'interno della Rete Aziendale, materiale a contenuto violento, sessuale o comunque offensivo dei principi di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico;
c) inviare a soggetti esterni allo Studio, tramite posta elettronica aziendale, messaggi con in allegato file eseguibili (.exe), salvo espressa autorizzazione dallo Studio;
d) utilizzare la posta elettronica aziendale in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore.

Non è consentito parimenti utilizzare la propria casella di posta elettronica personale a fini lavorativi, salvo espressa autorizzazione in caso di impossibilità della Persona Autorizzata di poter utilizzare l'account aziendale, ad esempio per inviare a soggetti terzi documenti aziendali tramite la propria casella di posta elettronica personale.
È obbligatorio porre la massima attenzione nell'aprire i *file attachment* di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o FTP non conosciuti).
In considerazione dell'ambito di attività dello Studio, particolare cautela deve essere prestata dalla Persona Autorizzata in caso di ricezione e trasmissione all'esterno di file contenenti Dati Particolari o informazioni riservate, quali ad esempio i dati relativi alla salute dei pazienti e/o dei dipendenti o collaboratori. A tal fine, tali documenti

e file trasmessi devono essere sempre protetti con adeguate tecniche di cifratura, secondo le indicazioni delle *Istruzioni per la cifratura degli Strumenti Aziendali e degli allegati contenenti Dati Particolari*.

### 1. Procedure per l'*auto-reply*, assenze e accesso alla posta elettronica da parte dello Studio

Al fine di garantire la funzionalità del servizio di posta elettronica aziendale, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella, sospensione dal servizio, ecc.), invierà automaticamente messaggi di risposta contenenti le coordinate di posta elettronica di un altro soggetto o altre utili modalità di contatto dello Studio (cd. *out of office*). In tal caso, la funzionalità deve essere attivata dalla stessa Persona Autorizzata.

In caso di assenza non programmata da parte della Persona Autorizzata (ad es. per malattia, infortunio, altra causa di assenza, ecc.), al fine di procedere all'attivazione del messaggio di cui al precedente punto, qualora detta funzionalità non possa essere attivata dalla Persona Autorizzata medesima avvalendosi del servizio *webmail*, essa sarà attivata - ove possibile - da un amministratore di sistema (sia esso interno o esterno allo Studio) in presenza di un collaboratore di fiducia della Persona Autorizzata ("**Fiduciario**") - qualora individuato nell'Autorizzazione al trattamento dei Dati Personali o anche tramite e-mail, che verrà ritenuto valido fino a rettifica della stessa Persona Autorizzata e/o fino alla revoca dell'Autorizzazione al trattamento dei Dati Personali - o, in mancanza, del titolare dello Studio o del responsabile gerarchico della Persona Autorizzata.

Nell'ipotesi in cui, per assenza improvvisa o prolungata della Persona Autorizzata e per improrogabili necessità legate all'attività lavorativa, lo Studio debba conoscere il contenuto dei messaggi di posta elettronica del medesimo, uno dei Fiduciari verifica il contenuto dei messaggi con l'ausilio di un amministratore di sistema, ove presente (sia esso interno o esterno allo Studio), che lo coadiuvi nell'accesso all'account di posta e che effettui l'accesso mediante le password di amministratore di sistema, ed inoltra alla persona delegata dal Titolare nell'ambito della propria funzione, ad es. il responsabile gerarchico o il titolare dello Studio, quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. L'accesso avviene secondo le finalità di cui alla sezione *Attività di controllo della Rete Aziendale, Strumenti Aziendali e Strumenti Personali*. A cura dello Studio, tale attività sarà, di volta in volta, documentata e ne verrà informata la Persona Autorizzata alla prima occasione utile.

In caso di assenza dei Fiduciari, sarà comunque consentito al responsabile gerarchico della Persona Autorizzata (o al titolare dello Studio), con l'ausilio di un amministratore di sistema, ove presente, accedere alla casella di posta elettronica della medesima in ogni ipotesi in cui - durante l'assenza - si renda necessario procedere in tal senso per improrogabili necessità legate all'attività lavorativa, sempre nel rispetto delle modalità e tutele oggetto della presente Policy. Anche in tale ipotesi, tale attività sarà documentata e ne verrà informata la Persona Autorizzata alla prima occasione utile. Al suo rientro, la password di posta elettronica utilizzata in sua assenza dovrà essere dal medesimo modificata.

Infine, in caso di revoca dell'Autorizzazione al trattamento dei Dati Personali la Persona Autorizzata dovrà procedere alla verifica nella casella di posta elettronica aziendale (ed alla conseguente cancellazione) di eventuali messaggi aventi contenuto personale o comunque non connessi all'attività aziendale.

Lo Studio, all'atto di risoluzione del rapporto, seguirà la seguente procedura:

1) le credenziali dell'account di posta della Persona Autorizzata verranno "resettate" da un amministratore di sistema, disattivando così l'accesso alle mail in ingresso (inbox) ed in uscita (sentbox) e prevedendo per 30 giorni (di seguito solo **"Periodo"**) un risponditore automatico in cui verrà indicato:
   a) che la Persona Autorizzata non è più dipendente/collaboratore dello Studio;
   b) un indirizzo aziendale alternativo a cui il mittente deve re-inoltrare il messaggio di posta;
   c) che alla data DD.MM.YYYY (scadenza del Periodo) l'indirizzo di posta dell'Utente non sarà più esistente;

2) durante il Periodo, lo Studio non potrà accedere all'account per la lettura di messaggi in entrata e uscita;
3) scaduto il Periodo, o prima in caso di accordo con la Persona Autorizzata per un'interruzione anticipata del rapporto professionale, lo Studio:
   a) rimuoverà definitivamente il risponditore automatico e l'account di posta elettronica in modo da inibire in modo definitivo la ricezione in entrata ed uscita dei messaggi;
   b) concorderà con l'ex Persona Autorizzata una data per permettergli/le di visionare (ed eventualmente estrarre) ulteriori messaggi di natura personale (o comunque non connessi all'attività lavorativa, che, si ricorda, non dovrebbero essere presenti) pervenuti presso il predetto account di posta elettronica, in presenza dell'amministratore di sistema e/o di una persona delegata dallo Studio;
4) una volta estratti (in forma digitale o cartacea) gli eventuali messaggi personali di cui al punto 3.b sopra, lo Studio eliminerà la copia presente sui propri server.

Resta inteso che i restanti messaggi relativi a vicende professionali dello Studio verranno conservati solo per il tempo necessario a perseguire la finalità di cui alla sezione H.1.e) di seguito (tutela dei diritti in sede giudiziaria nei limiti del GDPR, meglio descritti nel Registro dei Trattamenti ex art. 30).

## F. UTILIZZO DEI SOCIAL MEDIA

Fermo restando il generale divieto di partecipazione a chat-line e newsgroup o social network non attinenti all'attività professionale, in qualsiasi caso, se si partecipa a blog, forum di discussione e social network, devono essere rispettare determinate regole di comportamento:

- non effettuare comunicazioni che arrechino danni o turbative in rete o a terzi utenti o che violino le leggi ed i regolamenti vigenti;
- non immettere in rete materiale o comunicazioni con contenuti potenzialmente offensivi o che arrechino danni allo sviluppo armonico della personalità del minore,
- rispettare i principi che regolano l'ordine pubblico e la sicurezza sociale, evitando la diffusione di messaggi, immagini o altro materiale che possa istigare al compimento di reati, all'uso di violenza o ad atti violenti, a qualsiasi forma di partecipazione o collaborazione ad attività illecite;
- non diffondere alcunché di lesivo al decoro, alla dignità umana, o che abbia contenuto pornografico o contrario al buon costume o che favorisca la prostituzione o la pedopornofilia;
- non immettere in rete materiale in violazione della legge sul diritto d'autore, o altri diritti di proprietà intellettuale o industriale; in particolare software pirata, file musicali, immagini, video, testi protetti da copyright;
- non usare un linguaggio irrispettoso, tanto meno termini turpi ed evitare flame (non ingiuriare);
- non immettere materiale pornografico e a sfondo sessuale e comunque di natura oscena;
- non immettere materiale offensivo o diffamatorio nei confronti di chicchessia, incluse espressioni di fanatismo, razzismo, odio, irriverenza o minaccia;
- non inviare materiale che contenga dati giudiziari propri o di terzi;
- non immettere materiale che promuove o fornisce informazioni che istruiscano su attività illegali o che siano comunque ad esse in qualsiasi modo correlate o che possano causare pregiudizio a terzi;
- non eseguire upload di software, informazioni o altro materiale contenente virus o componenti dannosi;
- non immettere materiale contenente iniziative legate al gioco d'azzardo, concorsi, giochi che richiedono una partecipazione a titolo oneroso;
- non inviare materiale non adatto ai minori di 18 (diciotto) anni;
- non immettere materiale contenente pubblicità o sponsorizzazioni, anche a pagamento;

- non inserire materiale o attività che, in generale, violi o induca a violare una qualsiasi disposizione di legge o di regolamento posta a tutela anche solo di privati od una disposizione legittimamente impartita dalla Pubblica Autorità;
- non immettere materiale che ritragga minori – o riferimenti di minori – senza che vi sia una espressa autorizzazione del genitore/i o esercente la potestà sul/i minore/i;
- non inserire materiale che ritragga immagini di terzi o loro riferimenti personali che non abbiano dato il consenso alla pubblicazione;
- non inserire materiale che contenga dati inerenti alla salute, alle opinioni politiche o religiose, alle origini razziali o alle abitudini sessuali di terzi.

## G. GESTIONE DELLE CREDENZIALI

Le credenziali di autenticazione per l'accesso alla Rete Aziendale e agli applicativi aziendali a cui la Persona Autorizzata ha accesso in base alla sua funzione, vengono assegnate dallo Studio e consistono in un codice per l'identificazione (user id), associato ad una parola chiave riservata (password), che dovrà essere modificata al primo accesso e in seguito custodita dalla Persona Autorizzata medesima con la massima diligenza e prudenza.
In particolare, è vietata la comunicazione e/o divulgazione, in qualsiasi modo essa avvenga, della password, così come è vietato lasciare incustodita la propria password.
La Persona Autorizzata non può condividere la propria password con altri e deve procedere alla modifica della password almeno ogni tre mesi. La password deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili alla Persona Autorizzata; lo Studio raccomanda che la password contenga almeno un carattere maiuscolo, uno minuscolo ed un carattere numerico (es. "Abdde1yz"). Tali caratteristiche devono essere applicate anche quando non impostate e/o richieste automaticamente dal sistema.
La Persona Autorizzata è responsabile di qualunque accesso alla Rete Aziendale che sia effettuato, anche da terzi, utilizzando le sue credenziali di autenticazione.
In caso la Persona Autorizzata dimentichi ovvero smarrisca le proprie credenziali di autenticazione, sarà dovere della stessa fare immediata segnalazione e richiesta di inizializzazione allo Studio e/o alle competenti funzioni tecniche interne o esterne allo Studio e, allo stesso modo, sarà suo dovere avvisare il suddetto servizio, nonché modificare immediatamente la password, nel caso in cui sospetti un'effrazione, incidente, abuso o violazione della sicurezza e segretezza delle proprie credenziali di autenticazione, segnalando se del caso l'accaduto alle funzioni competenti tramite la **Procedura per la gestione dei Data Breach**.

Nell'ipotesi di sospensione e/o revoca delle credenziali di autenticazione, le stesse verranno automaticamente disattivate dallo Studio. Inoltre, come regola generale, le credenziali di autenticazione non utilizzate fino a un massimo di sei mesi, o minor durata coincidente con la durata delle credenziali di autenticazione, saranno disattivate dallo Studio, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
È buona pratica, e costituisce una misura di sicurezza da tenere presente, NON utilizzare la medesima password per accedere a diversi sistemi, applicazioni, e/o sistemi esterni.
Si ricorda, inoltre, che non è possibile in nessun caso inserire password all'hard disk ovvero al BIOS degli Strumenti Aziendali diverse da quelle permesse nelle *Istruzioni per la cifratura degli strumenti aziendali e degli allegati contenenti dati particolari*.

## H. ATTIVITÀ DI CONTROLLO DELLA RETE AZIENDALE, STRUMENTI AZIENDALI E STRUMENTI PERSONALI

Obiettivo primario delle attività di presidio e controllo dei sistemi informatici è quello di proteggere il patrimonio aziendale e salvaguardare le informazioni aziendali rilevanti.

## 1. Tipologie di controllo

Ove presenti, gli incaricati delle competenti funzioni tecniche interne o esterne allo Studio, debitamente nominati amministratori di sistema, sono autorizzati a compiere interventi nella Rete Aziendale e sugli applicativi aziendali:

a) diretti a garantire la sicurezza degli stessi sistemi, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.),
b) per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.),
c) per finalità di salvaguardia del patrimonio, del *know how* e dei beni/strumenti dello Studio in dotazione alle Persone Autorizzate;
d) per evitare che la continuità della normale attività operativa possa essere pregiudicata da azioni od omissioni delle Persone Autorizzate;
e) per prevenire/accertare e di conseguenza potersi tutelare in giudizio in caso di fatti illeciti e/o condotte/eventi aventi rilevanza penale e/o inadempimenti contrattuali e/o fatti/eventi e/o condotte aventi rilevanza disciplinare, commessi dalle Persone Autorizzate e che possano arrecare danno allo Studio.

I suddetti controlli non potranno, comunque, mai avere la finalità di verificare le abitudini e/o le opinioni delle Persone Autorizzate, né finalità di controllo a distanza dei lavoratori.

I controlli posti in essere dallo Studio e/o dalle competenti funzioni tecniche espressamente indicate dal medesimo potranno avere ad oggetto anche il rispetto delle corrette modalità di utilizzo da parte delle Persone Autorizzate degli Strumenti Aziendali e degli Strumenti Personali in loro dotazione, nonché della Rete Aziendale e della posta elettronica aziendale, sempre e solo per le suddette precipue finalità organizzative e/o di sicurezza, ossia senza alcuna finalità di controllo delle abitudini e/o opinioni delle medesime.

La stessa facoltà di controllo da parte dello Studio e/o delle competenti funzioni tecniche espressamente indicate dal medesimo - sempre ai fini della sicurezza del sistema informatico aziendale e del patrimonio dello Studio nonché per garantire la normale operatività - si estende anche in caso di assenza prolungata o impedimento della Persona Autorizzata, ovvero nel caso di revoca dell'Autorizzazione al trattamento dei Dati Personali.

Il personale incaricato dello Studio e/o delle competenti funzioni tecniche espressamente indicate dal medesimo può collegarsi e visualizzare in remoto il desktop dei singoli Strumenti Aziendali e Strumenti Personali al fine di garantire l'assistenza tecnica e la normale attività operativa, nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata della Persona Autorizzata o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico o della Rete Aziendale. In quest'ultimo caso, sempre che non si pregiudichi la tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

## 2. Modalità di controllo

### *a) Controllo ordinario (ove applicabile)*

Salve le cautele di *data protection by design e by default* indicate più sopra nella sezione *Utilizzo della Rete Aziendale*, in casi di ripetuti tentativi di accesso a contenuti non autorizzati dai filtri della Rete Aziendale, non preceduti da una richiesta di accesso, lo Studio si riserva, per mezzo delle competenti funzioni incaricate, il diritto di accedere ai server aziendali - ove presenti - per svolgere un'attività di controllo ordinario, in forma anonima, circa l'uso della Rete Aziendale, in conformità a quanto stabilito nella presente policy e alle disposizioni del Regolamento.

Secondo un criterio graduale ed alla luce dei principi di pertinenza e non eccedenza, in caso di necessità gli addetti dello Studio e/o delle competenti funzioni tecniche espressamente indicate dal medesimo effettueranno in via ordinaria un controllo preliminare su dati aggregati, riferiti all'intera Rete Aziendale. Il controllo anonimo può

concludersi con un avviso generalizzato alle Persone Autorizzate relativo ad un rilevato utilizzo anomalo della Rete Aziendale, con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.
Gli eventuali controlli, con specifico riferimento all'utilizzo della Rete Aziendale, compiuti dal personale incaricato dello Studio e/o delle competenti funzioni tecniche espressamente indicate dal medesimo, potranno avvenire mediante "file di log" della navigazione svolta. Con riferimento ai file di log riferiti al traffico web, il trattamento dei dati verrà effettuato su base anonima o comunque su base collettiva o per gruppi sufficientemente ampi di Persone Autorizzate. I file di log vengono conservati non oltre sei mesi, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dello Studio e/o di pubblica sicurezza e non includono la registrazione delle pagine web visitate dalla Persona Autorizzata, ma solo quella dell'indirizzo IP di connessione, senza alcuna investigazione successiva dell'identità di quell'indirizzo.

*b) Controllo straordinario (ove applicabile)*

Al fine di assicurare il rispetto della presente Policy, nonché della normativa vigente, in chiave di accertamento e repressione di comportamenti illeciti delle Persone Autorizzate – sempre nel rispetto del sopracitato criterio graduale ed alla luce dei principi di pertinenza e non eccedenza – ove anche nel corso del Controllo ordinario che precede dovessero riscontrarsi anomalie ovvero dovesse emergere, dai dati e dalle informazioni rilevate, il sospetto del verificarsi, anche potenziale, di fatti illeciti e/o condotte/eventi aventi rilevanza penale e/o inadempimenti contrattuali e/o fatti/eventi e/o condotte aventi rilevanza disciplinare, lo Studio potrà in qualsiasi momento, per mezzo delle competenti funzioni incaricate in qualità di amministratori di sistema, ove presenti, accedere sia al server che alla memoria di massa degli Strumenti Aziendali e/o Strumenti Personali in dotazione alla Persona Autorizzata. In tale eventualità, lo Studio potrà effettuare il backup ed eventualmente la stampa della directory o, anche, di tutto il contenuto della memoria di massa di detti strumenti affidato in dotazione Persona Autorizzata, compresi tutti i messaggi di posta elettronica in entrata e in uscita. Con specifico riferimento ai contenuti dei messaggi di posta elettronica in entrata e uscita, tale analisi riguarderà la sola ipotesi in cui le informazioni esteriori dei suddetti messaggi (quali l'oggetto dell'e-mail, l'orario di ricezione o di invio della stessa ecc.) non siano sufficienti ad individuare e/o accertare il contenuto e/o la portata dei predetti fatti illeciti e/o delle citate condotte/eventi.
Si precisa, altresì, che una volta effettuato il backup, ivi inclusa eventualmente la stampa, di tutto il contenuto della memoria di massa degli Strumenti Aziendali e/o Strumenti Personali in dotazione alla Persona Autorizzata ritenuti indispensabili per la finalità di cui alla sezione H.1 e), tale documentazione verrà conservata per un periodo di tempo non superiore a quello necessario agli scopi per i quali la stessa è stata raccolta e successivamente trattata (tutela dei diritti in sede giudiziaria nei limiti del GDPR).
In ogni caso, non verrà svolta alcuna delle seguenti attività:

a) lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
b) riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dalla Persona Autorizzata;
c) lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
d) analisi occulta di Strumenti Aziendali e/o Strumenti Personali affidati in uso.

Resta inoltre fermo il divieto per lo Studio di utilizzare, in alcun modo, i dati ricavati attraverso i controlli suddetti per finalità diverse da quelle esplicitate e codificate nella presente Policy.

## I. PROPRIETÀ INTELLETTUALE DELLE INFORMAZIONI

Tutte le informazioni, dati e/o file contenuti nella Rete Aziendale e sistemi informativi dello Studio sono, e rimangono, di esclusiva proprietà del medesimo che ne vieta espressamente la copia e/o la riproduzione e/o l'utilizzo per fini estranei all'attività professionale.

Sono vietate, altresì, la copia e/o la riproduzione di materiale protetto dal diritto d'autore, nonché la diffusione e la trasmissione a terzi di informazioni e dati contenuti nei sistemi informativi dello Studio e/o di terzi in genere e, comunque, protetti da copyright e/o da segreto professionale, nonché i Dati Particolari quali i dati relativi alla salute dei pazienti. Tutti gli strumenti informatici dello Studio sono dotati di software coperti da licenza e, fermo restando che è comunque vietato alla singola Persona Autorizzata installare e/o distribuire software o prodotti "pirata". Sarà responsabilità dello Studio e/o delle competenti funzioni tecniche espressamente indicate dal medesimo, attraverso il Controllo Ordinario, verificare e controllare periodicamente tutta la Rete Aziendale al fine di garantire il completo adeguamento alle leggi sul copyright, procedendo, se necessario, anche alla rimozione immediata di eventuali software installati senza licenza (cfr. Controllo Straordinario).

## J. ACCESSO AI LOCALI SERVER (OVE APPLICABILE)

Si ricorda che - ove possibile - l'accesso a tutti i locali in cui sono custoditi i server dello Studio, nonché a tutte le altre Aree Sensibili, è strettamente riservato alle Persone Autorizzate e debitamente approvate.

## K. SANZIONI

È fatto obbligo a tutte le Persone Autorizzate di osservare le disposizioni e regole di condotta portate a conoscenza con la presente Policy che, laddove applicabile in base alla tipologia di rapporto professionale, integrano quelle previste nei relativi contratti di lavoro, ovvero quelle contenute nei CCNL applicati ai medesimi rapporti di lavoro.

In particolare, la violazione delle previsioni della presente Policy da parte delle Persone Autorizzate potrà quindi determinare l'applicazione:

- di sanzioni disciplinari di natura conservativa e/o espulsive, il tutto nel rispetto dei limiti di cui all'art. 2106, 2118 e 2119 codice civile, dell'art. 7 Statuto Lavoratori ovvero delle specifiche previsioni, anche procedurali, contemplate dalla contrattazione collettiva in essere presso lo Studio, ove applicabili; ovvero
- risoluzione espressa ex art. 1456 del contratto di servizio in essere per violazione degli obblighi di riservatezza delle Persone Autorizzate,

a seconda della gravità, intenzionalità e della relativa categoria, nonché sulla base dei dati e delle informazioni rilevate nel corso dei controlli di cui alla sezione *Attività di controllo della Rete Aziendale, Strumenti Aziendali e Strumenti Personali* che precede (utilizzabili, ai sensi dell'art. 4 Statuto Lavoratori, a tutti i fini connessi al rapporto di lavoro). Nel primo caso, l'eventuale applicazione di misure disciplinari nei confronti della Persona Autorizzata non precluderà il diritto dello Studio di intraprendere, ove ne ricorrano i presupposti, iniziative ed azioni (anche cautelari) finalizzate ad ottenere l'inibitoria degli eventuali comportamenti posti in essere dalla Persona Autorizzata in violazione delle regole oggetto della presente Policy, così come non precluderà di agire per ottenere il ristoro di eventuali danni verificatisi in conseguenza di condotte negligenti e/o inadempienti alle medesime previsioni.

Nel secondo caso, l'eventuale risoluzione espressa non pregiudica la possibilità dello Studio di agire per il risarcimento del danno causato.

## L. DIRITTI DEGLI INTERESSATI

Le Persona Autorizzate in qualità di Interessati hanno il diritto di chiedere allo Studio, in qualunque momento, l'accesso ai loro Dati Personali, la rettifica o la cancellazione degli stessi o di opporsi al loro Trattamento, hanno

diritto di richiedere la limitazione del Trattamento nei casi previsti dall'art. 18 del Regolamento, nonché di ottenere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati che le riguardano, nei casi previsti dall'art. 20 del Regolamento.

Le richieste vanno rivolte per iscritto allo Studio al seguente indirizzo:

via messedaglia 116 - 37069 - Villafranca di Verona (VR) (Posta Cartacea) - amministrazione@dentistacordioliboscarini.it (Email).

In ogni caso esse hanno sempre diritto di proporre reclamo all'Autorità di Controllo competente (Garante per la Protezione dei Dati Personali), ai sensi dell'art. 77 del Regolamento, qualora ritengano che il Trattamento dei loro Dati Personali sia contrario alla normativa in vigore.

# III. ALLEGATI

## A. "TO DO LIST"

- ✓ Leggere approfonditamente la Policy Strumenti IT
- ✓ In caso di concessione di account di posta elettronica aziendale, nominare due Fiduciari per l'accesso alla casella nei casi previsti (in assenza dei Fiduciari accede il rispettivo responsabile gerarchico). La delega viene inserita direttamente nell'Autorizzazione al Trattamento di Dati Personali o inviata via mail
- ✓ Utilizzare solo gli Strumenti Aziendali forniti dallo Studio
- ✓ Implementare ed attenersi sempre alle *Istruzioni per la cifratura degli Strumenti aziendali e degli allegati contenenti Dati Particolari*
- ✓ Utilizzare la Rete Aziendale dello Studio solo per fini lavorativi; per fini personali verificare se è presente la rete Wi-Fi guest o, in alternativa (e solo ove effettivamente necessario), richiedere preventivamente allo Studio l'autorizzazione ad utilizzare la Rete Aziendale anche per fini personali
- ✓ Non tentare di superare i filtri della Rete Aziendale. In caso di necessità, chiedere l'autorizzazione allo Studio e/o alle competenti funzioni tecniche (interno o esterne) espressamente indicate dal medesimo per l'accesso temporaneo a contenuti bloccati dalla Rete Aziendale
- ✓ Utilizzare la posta elettronica aziendale solo per fini lavorativi, inserendo il Footer in ogni messaggio
- ✓ In caso di assenza programmate (ferie) e non (malattia) attivare - anche via webmail - un risponditore automatico contenente le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto dello Studio.

## B. FOOTER

"*L'uso di questa casella di posta è a scopo professionale; non si garantisce che la corrispondenza verso questa casella venga letta dal solo destinatario, potendo essere necessario, in determinate circostanze, l'accesso alla casella da parte di terzi, appartenenti allo Studio* STUDIO DENTISTICO ASS.TO DOTT.BOSCARINI-DOTT.SSA CORDIOLI. *Si prega di non inviare messaggi di natura personale a questo indirizzo*"

## C. ISTRUZIONI PER LA CIFRATURA DEGLI STRUMENTI AZIENDALI E DEGLI ALLEGATI CONTENENTI DATI PARTICOLARI

Pagina da sostituire con il word che trovi in piattaforma opportunamente compilato.