ULTIMO AGGIORNAMENTO: 23/3/2016
In un'ottica di agevolazione dei Colleghi nell'adempimento degli obblighi derivanti dall'applicazione del D.Lgs. n. 196/2003 la Commissione Informatica dell'Ordine degli Avvocati di Rovereto propone il seguente modello di documento di descrizione delle misure minime di sicurezza presenti nello studio professionale completo dei fac simile di informativa e lettere d'incarico. Non è un documento obbligatorio, ma risulta utile per controllare di aver correttamente adempiuto gli obblighi derivanti dalla normativa relativa al trattamento dei dati personali.

L'intento è quello di fornire un valido aiuto per l'adempimento degli obblighi normativi e la Commissione Informatica ha compiuto ogni ragionevole sforzo per assicurare che questo materiale sia il più possibile preciso. Tuttavia errori, inesattezze ed omissioni sono possibili e si declina ogni responsabilità per eventuali errori, inesattezze ed omissioni eventualmente presenti.
Vi preghiamo di segnalare eventuali errori alla mail dell'Ordine.

Scopo di questo documento è descrivere le

MISURE MINIME DI SICUREZZA

adottate nel trattamento dei dati personali, a norma degli artt. 33 e ss. del Codice Privacy (D.Lgs. n. 196/2003 e ss. mm.) e dell'all. B) dello stesso D.Lgs. 196/2003 e ss.mm..

TITOLARE DEI DATI

_____

Via _____, città _____.

AGGIORNAMENTI

anno	2016	2017	2018	2019	2020	2021	2022
data							

1. NORME DI RIFERIMENTO

D.LGS. 196/2003, Codice in materia di protezione dei dati personali

[…]

Titolo V - Sicurezza dei dati e dei sistemi

Capo I - Misure di sicurezza

0. Art. 31. Obblighi di sicurezza: "1*. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta*".

[…]

Capo II - Misure minime di sicurezza

Art. 33. Misure minime: "*1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali"*.

Art. 34. Trattamenti con strumenti elettronici: "*1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:*

a) autenticazione informatica;
b) adozione di procedure di gestione delle credenziali di autenticazione;
c) utilizzazione di un sistema di autorizzazione;
d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
g) [soppressa] (1);
h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari".

1-bis. [abrogato] (2)

1-ter. Ai fini dell'applicazione delle disposizioni in materia di protezione dei dati personali, i trattamenti effettuati per finalità amministrativo-contabili sono quelli connessi allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile, a prescindere dalla natura dei dati trattati. In particolare, perseguono tali finalità le attività organizzative interne, quelle funzionali all'adempimento di obblighi contrattuali e precontrattuali, alla gestione del rapporto di lavoro in tutte le sue fasi, alla tenuta della contabilità e all'applicazione delle norme in materia fiscale, sindacale, previdenziale-assistenziale, di salute, igiene e sicurezza sul lavoro".

Art. 35. Trattamenti senza l'ausilio di strumenti elettronici: "1*. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:*

a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;

b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;

c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati".

[…]

ALLEGATO B. Disciplinare tecnico in materia di misure minime di sicurezza

Trattamenti con strumenti elettronici
Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica
1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione
12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.
18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Documento programmatico sulla sicurezza
19. [soppresso] (1)

19.1. [soppresso](1)
19.2. [soppresso](1)
19.3. [soppresso](1)
19.4. [soppresso](1)
19.5. [soppresso](1)
19.6. [soppresso](1)
19.7. [soppresso](1)
19.8. [soppresso](1)

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari
20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.
21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.
24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia
25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.
26. [soppresso] (1)

Trattamenti senza l'ausilio di strumenti elettronici
Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:
27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli

incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

2. MISURE MINIME DI SICUREZZA:ORGANIZZATIVE, FISICHE, LOGICHE

Compiti, responsabilità e profili di autorizzazione

Nello Studio […] operano n. […] professionisti iscritti in un albo, e precisamente:
1. […];
2. […];
3. […]
4. […].

Titolare del trattamento dati: [*ripetere quanto indicato nella prima pagina*]

Incaricato/i e relativo ambito del trattamento: *[per ciascuno, nome cognome, compiti/mansioni e relative tipologie di dati trattati],* come da atto di nomina archiviato;

(eventuale) **responsabile/i Interno/i**: [*indicare nome cognome e ruolo*], come da atto di nomina archiviato;

(eventuale) **responsabile/i Esterno/i**: [*per ciascuno, indicare nome cognome/denominazione/ragione sociale, data di nomina*], come da atto di nomina archiviato;

(eventuale) **Amministratore di sistema** (come da Provvedimento Generale del Garante dd. 27 novembre 2008 “Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”): [*nome cognome, data di nomina*]; per i compiti attribuiti e gli adempimenti connessi si veda l’atto di nomina archiviato;

(alternativo al precedente) **Soggetto cui è affidata l’assistenza informatica**: [*nome cognome / denominazione / ragione sociale, sede, C.F. o P.IVA*],

(eventuale) **Custode delle password**: [*nome cognome*].

Descrizione della Struttura informatica
La struttura informatica [non è] / è condivisa, ed è così composta:
[*indicare (per ogni professionista qualora la struttura informatica non sia condivisa):*
- *numero server, pc fissi e portatili;*
- *se sono state create delle partizioni su di essi;*
- *se sono disposti in rete e quale, se stand alone;*
- *(per ogni computer) il sistema operativo utilizzato, la data dell’ultimo aggiornamento; l’antivirus e come si aggiorna;*
- *se esiste un collegamento internet, se esiste un router, se esiste un firewall (hardware o software), se esiste un proxy*].

Descrizione sistema di autorizzazione e autenticazione informatica
[*indicare esistenza di credenziali / dispositivo di autenticazione, descrizione della procedura di autenticazione, modalità di individuazione e caratteristiche delle eventuali credenziali, modalità e periodicità nel cambiamento delle stesse*].

Descrizione delle modalità di aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative

[*possibile esempio: annualmente il Titolare verifica l'elenco dei soggetti dei quali si avvale, i loro compiti, l'esistenza e il contenuto di eventuali nomine, e registra l'esito di tale attività in questo documento, alle pagine …*]

Descrizione delle procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti

[*quantomeno, richiamare le istruzioni assegnate assieme all'incarico al trattamento; poi possono variare a seconda delle scelte del Titolare*].

Descrizione delle procedure per il controllo dell'accesso agli archivi contenenti dati sensibili o giudiziari

[*variano da studio a studio; quantomeno, descrivere le misure fisiche per la sicurezza dello studio (allarme, porta blindata, etc) chi ha la custodia delle chiavi, o se è sempre presente qualcuno in studio che possa controllare visivamente l'accesso; l'esistenza di autorizzazioni inserite nell'incarico al trattamento*].

Misure adottate e da adottare per garantire l'integrità e la disponibilità dei dati e la protezione delle aree e dei locali

Lo Scopo di questa parte è tener traccia delle misure adottate per la protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici come richiesto dall'art. 34 lettera e), D.Lgs. 196/2003.

rischio di danneggiamento, perdita, alterazione dei dati, contenuti su supporti di memorizzazione o durante operazioni di trattamento, a causa di	**misura adottata**	**misura da adottare**
Incendio Allagamento		
mancanza di energia elettrica		
Intrusione Ingresso non controllato o non autorizzato		
Accesso ai dati non controllato o non autorizzato		
Intercettazione durante l'invio		
Non conoscenza da parte degli incaricati delle procedure informatiche, delle misure di sicurezza, dei rischi		
Errore da parte degli incaricati nell'utilizzo delle procedure informatiche, delle misure di sicurezza, dei rischi		

[*compilare secondo le caratteristiche dello studio*]

Descrizione procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi

[*descrivere se e come viene effettuato back up dei dati, e più in generale il sistema di disaster recovery predisposto*]

3. ALLEGATI

ALLEGATO 1: Informativa ai sensi dell'art. 13 d. lgs. 196/2003

Gentile Cliente,

ai sensi dell'art. 13 d. lgs. 196/2003 (di seguito T.U.), ed in relazione ai dati personali di cui questo Studio Legale entrerà in possesso, il Titolare del trattamento dati Le fornisce le seguenti informazioni.

1. **Finalità del trattamento.** Il trattamento dei Suoi dati verrà effettuato ai seguenti fini: i) la corretta e completa instaurazione e esecuzione dell'incarico professionale conferito; ii) la corretta e completa gestione amministrativo-contabile del rapporto contrattuale con Lei in via di instaurazione o instaurato; iii) l'adempimento di obblighi previsto dalla legge, da un regolamento o dalla normativa comunitaria, quale, in particolare, vi) l'adempimento degli obblighi previsti dal D.Lgs. 231/2007 e normative collegate.
2. **Natura obbligatoria del conferimento.** Il conferimento di tutti i dati personali che Le verranno richiesti è necessario per il raggiungimento delle finalità di cui al punto 1., e un conferimento parziale o inesatto può comportare l'impossibilità di raggiungere dette finalità e/o di proseguire nel rapporto professionale. Per le finalità di cui al punto iv) la reticenza o il mendacio nel conferimento dei dati richiesti comporteranno la rinuncia al mandato e la risoluzione del rapporto professionale.
3. **Modalità e durata del trattamento.** Il trattamento viene effettuato con modalità manuali e/o informatizzate.
4. **Comunicazione e diffusione dei dati.** Ove necessario per il raggiungimento delle finalità di cui al punto 1., dei dati conferiti potranno venire a conoscenza, soggetti stabilmente inseriti nell'organizzazione del Titolare, nominati Incaricati o Responsabili del trattamento; i dati potranno altresì essere comunicati a soggetti operanti nel settore giudiziario, alle controparti e ai relativi difensori, ad altri soggetti privati (quali Commercialisti, Banche, Istituti di Credito, consulenti, etc.) a Pubbliche Amministrazioni o Autorità. I dati non sono oggetto di diffusione.
5. **Trasferimento dei dati all'estero.** Nell'ambito delle finalità di cui al punto 1., i dati personali potranno essere trasferiti verso Paesi dell'Unione Europea e/o verso Paesi esterni all'Unione Europea nel rispetto degli artt. 43 e 44 del T.U.. (*FARE ATTENZIONE SE SI USANO SERVIZI CLOUD)*
6. **Titolare del Trattamento.** [*ripetere quanto indicato nella prima pagina*], con studio/sede in via [—], cui potrà rivolgersi ai seguenti recapiti - tel. [—], email [—], fax [—] - per esercitare i Diritti previsti dall'art. 7 T.U., per Sua comodità qui di seguito riprodotto:

   Art. 7 - (Diritto di accesso ai dati personali ed altri diritti) 1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

   2. L'interessato ha diritto di ottenere l'indicazione: a) dell'origine dei dati personali; b) delle finalità e modalità del trattamento; c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2; e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati. 3. L'interessato ha diritto di ottenere: a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati; b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati; c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato. 4. L'interessato ha diritto di opporsi, in tutto o in parte: a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta; b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Per ricevuta informativa

Data, Luogo, Cognome e Nome e Firma leggibile

ALLEGATO 2: Lettera di incarico al trattamento dei dati con istruzioni

Egregio Signore / Gentile Signora

[nome cognome]

a mani

Il sottofirmato [*nome cognome*], in qualità di Titolare del Trattamento / legale rappresentante del Titolare del Trattamento / Responsabile del Trattamento [*scegliere l'opzione corretta*],

considerato che Lei si occupa di / effettua le attività collegate al ruolo di …… (*specificare*) e che in tale contesto Lei tratta necessariamente dati personali riferiti alle seguenti categorie d soggetti [*cancellare le voci non pertinenti*]: clienti; fornitori; dipendenti,

ai sensi dell'art. 30 del D.Lgs. 196/2003 **La incarica**

- del trattamento dei dati comuni, sia con modalità elettronica che cartacea riguardanti le seguenti categorie di soggetti: clienti; fornitori; dipendenti [*cancellare le voci non pertinenti*];
- del trattamento dei dati sensibili, sia con modalità elettronica che cartacea riguardanti: clienti; dipendenti [*cancellare le voci non pertinenti*];

Lei è autorizzato a compiere le seguenti operazioni [*cancellare le voci non pertinenti, spuntare solo le voci pertinenti*]:

☐ Operazioni "standard": raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, utilizzo.
☐ modificazione;
☐ comunicazione;
☐ cancellazione e distruzione;
☐ blocco;
☐ operazioni diverse quali selezione, estrazione, raffronto, interconnessione.
☐ Lei inoltre è autorizzato ad accedere agli archivi cartacei contenenti dati sensibili e giudiziari.

Nell'adempimento dell'incarico conferito, con la firma in calce al presente documento Lei si impegna a:

- rispettare tutte le misure di sicurezza già operanti, nonché ad osservare scrupolosamente tutte le misure di sicurezza che saranno adottate dal titolare, nonché ogni ulteriore istruzione che sarà impartita in relazione a determinati trattamenti, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- trattare in modo lecito e secondo correttezza tutti i dati personali di cui verrà a conoscenza nell'ambito dello svolgimento delle sue attività sopra descritte;
- qualora debba portare fuori dal contesto operativo supporti informatici o cartacei contenenti dati personali, essi non dovranno mai essere lasciati incustoditi e/o nella disponibilità di terzi non autorizzati ad accedervi;
- comunicare dati personali a soggetti esterni solo ove ciò sia strettamente necessario alla miglior esecuzione dei compiti ricevuti;
- verificare, all'atto della raccolta o dell'utilizzo dei dati personali, la loro esattezza, pertinenza, e non eccedenza, ed a raccogliere e registrare i soli dati personali attinenti agli scopi e alle finalità perseguite dal titolare;
- evitare di comunicare per telefono informazioni relative a dati sensibili o giudiziari, ove non sia certo dell'identità della persona all'altro capo del telefono e che la stessa sia legittimata a ricevere dette

informazioni;

- accedere ai dati e agli strumenti elettronici con l'inserimento dei codici identificativi personali e password i- l cui uso è strettamente personale - individuati con le modalità che le saranno indicate dal Titolare; in ogni caso la password da lei scelta dovrà essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; a password non dovrà contenere riferimenti agevolmente riconducibili all'incaricato;
- custodire con diligenza tali informazioni, evitando di comunicarle ad altri incaricati od a soggetti estranei, ed a modificarli ogni volta che venga richiesto dal Titolare del Trattamento / dal sistema informatico;
- consegnare le nuove credenziali, ogni qualvolta le cambi, in busta chiusa controfirmata al Titolare / Responsabile della loro custodia, ove nominato;
- mantenere assoluto riserbo sui dati personali di cui si viene a conoscenza nell'esercizio delle proprie funzioni;
- controllare e custodire gli atti e i documenti contenenti dati personali per l'intero svolgimento delle operazioni di trattamento, facendo in modo che ad essi non accedano persone non autorizzate;
- non lasciare incustoditi o accessibili da terzi durante una sessione di trattamento gli strumenti elettronici ricevuti in uso; in caso di allontanamento durante una sessione del trattamento, il computer/tablet deve - a seconda dei casi - essere bloccato (premere i tasti Ctrl + Alt + Canc – blocca computer) oppure deve essere attivata la procedura di screen saver con password o deve essere chiusa a chiave la porta di accesso all'ufficio;
- effettuare un back up, con frequenza almeno settimanale, di eventuali dati personali elaborati che non fossero coperti dal salvataggio centralizzato (ad esempio quelli contenuti nel disco fisso del PC in dotazione) I supporti utilizzati per il salvataggio dovranno essere custoditi a sua cura in modo da impedire l'accesso da parte di terzino autorizzati;
- distruggere o rendere inutilizzabili tutti i supporti rimovibili che non vengono più utilizzati; tali supporti possono comunque essere riutilizzati, anche da altri incaricati, se le informazioni precedentemente in essi contenute non sono intelligibili o tecnicamente in alcun modo ricostruibili. Si raccomanda quindi la totale formattazione dei supporti utilizzati. Se non fosse possibile formattare completamente i supporti utilizzati, gli stessi devono essere distrutti;
- utilizzare il sistema informatico - l'account mail, eventuali device, il collegamento ad internet, etc. - assegnatole in uso dal Titolare solamente per i fini strettamente necessari allo svolgimento del suo lavoro;
- evitare di utilizzare fax o posta elettronica per l'invio di documenti in chiaro contenenti dati sensibili, speciose relativismo stato di salute, e giudiziari; se necessario, procedere alla trasmissione in due tempi diversi, comunicando in un primo tempo i documenti coperti da password e in un secondo momento, magari a voce o via sms, la password;
- evitare l'installazione di software sugli hardware in uso in assenza di una preventiva autorizzazione del Titolare;
- qualora si dovessero riscontrare malfunzionamenti o non conformità, comunicare l'accaduto al più presto al titolare;
- modificare le credenziali di autenticazione - nel caso in cui l'hardware in uso sia stato trasferito presso il Centro Assistenza e comunicate al tecnico per permettere l'accesso - al termine della manutenzione ed al primo utilizzo dell'hardware al suo rientro in Studio;
- qualora sia effettuato un intervento manutentivo attraverso la tele-assistenza, a consentire il controllo dell'hardware all'assistenza tecnica mantenendo rimanendo comunque presso la postazione e sorvegliando visivamente le operazioni eseguite dall'assistenza tecnica;
- strappare, sminuzzare utilizzando i distruggi documenti se esistenti o altrimenti, i documenti cartacei che non sono più utilizzati, onde renderli illeggibili prima di essere cestinati.

Il Titolare del Trattamento/legale rappresentante del Titolare del Trattamento/Responsabile del Trattamento

_____

Luogo e data

_____

L'incaricato

_____

ALLEGATO 3: Lettera di incarico della custodia delle parole chiave

(da utilizzarsi qualora non esista un amministratore di sistema o il Titolare - la persona fisica non preferisca custodire le password direttamente)

Egregio Signore / Gentile Signora

[nome cognome]

a mani

Il sottofirmato [*nome cognome*], in qualità di Titolare del Trattamento / legale rappresentante del Titolare del Trattamento / Responsabile del Trattamento [*scegliere l'opzione corretta*],

considerato che
- Lei si occupa di / effettua le attività collegate al ruolo di …… [*specificare*];

- l'allegato B al D.Lgs. 196/2003, prevede che - laddove l'accesso ai dati e agli strumenti elettronici sia consentito esclusivamente mediante la componente riservata della credenziale per l'autenticazione - siano impartite idonee e preventive disposizioni scritte volte ad individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici, in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile ed indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema e che in tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato;

ciò premesso,

La incarica

della custodia delle parole chiave per l'accesso ai dati personali o agli strumenti del sistema informatico del Titolare.

Nell'adempimento del presente incarico, Lei dovrà aver cura di:
- ricordare agli incaricati di consegnarle, ad ogni sostituzione, in busta chiusa controfirmata la propria nuova parola chiave;
- conservare le buste contenenti le password in un posto sicuro non accessibile a soggetti non autorizzati;
- aprire la busta e utilizzare la parola chiave in essa contenuta, nel caso in cui, in assenza o impedimento dell'incaricato, sia necessario utilizzare il profilo di autorizzazione dell'incaricato assente per intervenire sul sistema informatico per necessità operative o di sicurezza;
- informare l'incaricato, al suo rientro, dell'intervento effettuato e della necessità di cambiare la parola chiave.

Titolare del Trattamento / legale rappresentante del Titolare del Trattamento / Responsabile del Trattamento

_____

Luogo e data

_____

Il custode delle parole chiave

ALLEGATO 4: Ambito del trattamento per il personale tecnico informatico

(*clausole da far sottoscrivere alla società che effettua la manutenzione del sistema informatico, anche quale parte del contratto, se non la si è nominata responsabile del trattamento)*

- L'accesso ai dati da parte del personale tecnico è improntato ai principi di correttezza, liceità e riservatezza e il personale tecnico non diffonderà eventuali informazioni di qualunque genere di cui sia anche accidentalmente venuto a conoscenza in occasione di un intervento di manutenzione;
- I tecnici per l'assistenza software o hardware che interverranno sul sistema informatico del Titolare accederanno ai dati ivi contenuti per il tempo strettamente necessario all'esecuzione delle operazioni di manutenzione e nei limiti di quanto strettamente necessario alla loro esecuzione
- In particolare è vietata la modifica, l'elaborazione, la cancellazione dei dati se non richiesta da Titolare.
- E' concessa una eventuale procedura di back up dei dati, previa autorizzazione del Titolare nel caso in cui sia possibile una perdita dei dati durante le operazioni di manutenzione.
- Accederanno ad un hardware *client* esclusivamente sotto il controllo del soggetto che lo ha in uso, il quale digiterà le credenziali di autenticazione (nome utente e password) evitando di comunicarle ai tecnici;
- per accedere al Server è necessario rivolgersi al Titolare o all'incaricato preposto alla sezione informatica;
- eventuali prove sul funzionamento di stampanti o sulla comunicazione dei dati fra hardware o attraverso il web dovranno essere effettuate esclusivamente creando dei file di prova e non attingendo ai dati personali archiviati dal Titolare o comunque presenti nello Studio;
- qualora si intervenga attraverso la teleassistenza, l'accesso è consentito solo previa richiesta telefonica di intervento da parte del Titolare o dell'incaricato, che attiveranno le procedure previste per consentire l'accesso al sistema.

ALLEGATO 5: Promemoria Verifiche

) A) OGNI 6 MESI

a. Verificare aggiornamento programmi anti intrusione e antivirus, nonché l'installazione degli aggiornamenti volti alla sicurezza dei *software* in uso (patch/service pack/hotfix)

2016/I	2016/II	2017/I	2017/II	2018/I	2018/II	2019/I	2019/II

.

Nella parte bianca della tabella: visto per eseguito.

) B) OGNI ANNO

a. Verificare la conservazione dell'ambito di trattamento precedentemente assegnato ai singoli incaricati, e la sua corrispondenza con il loro profilo di autorizzazione

2016	2017	2018	2019	2020	2021	2022

.

Nella parte bianca della tabella: visto per eseguito in assenza di modiche

Modifiche eventualmente intervenute:

_____
_____
_____
_____
_____

b. formazione agli incaricati [*opportuno un refresh annuale, ma non c'è un termine: si dice "alla bisogna*]

2016	2017	2018	2019	2020	2021	2022

Nella parte bianca della tabella: data e modalità di esecuzione

1

c. Verifica sull'organizzazione nel trattamento dati del responsabili esterni (*ove presenti)*

2016	2017	2018	2019	2020	2021	2022

Nella parte bianca della tabella: data e modalità di esecuzione