

FISIO 10 srl

via Guasti 12H - int.3 35124 Padova

Tel. 049.680080

Website: www.fisio10.it

E-Mail: info@fisio10.it

Policy generale per il rispetto delle prescrizioni del Regolamento (UE) 2016/679

ai sensi ex art. 24 e dei considerando 74-75-76-77-83 del Regolamento (UE) 2016/679

Documentazione redatta in ottemperanza a quanto disposto dal GDPR 2016/679 "Regolamento generale sulla protezione dei dati".
al D. lgs. 196/2003 "Codice in materia di protezione dei dati" e s.m.i. e ai Provvedimenti del Garante per la protezione dei dati personali



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

X

dott. Daniele Maggiolo
Data Protection Officer



Sommario

Premessa.....	3
1. Elenco dei trattamenti dei dati personali.....	3
1.1 Tipologie di dati trattati.....	3
1.2 Caratteristiche di aree, locali e strumenti con cui si effettuano i trattamenti.....	4
2. Organigramma privacy.....	4
3. Autorizzati al trattamento: responsabilità e formazione.....	4
4. Analisi dei rischi che incombono sui dati.....	5
5. Misure atte a garantire l'integrità e la disponibilità dei dati.....	6
5.1 La protezione di aree e locali.....	6
5.2 La custodia e l'archiviazione di atti, documenti e supporti.....	7
5.3 Le misure logiche di sicurezza.....	8
5.3.1 Il sistema di autenticazione informatica.....	8
5.3.2 Credenziali di autorizzazione.....	8
5.3.3 Protezione di strumenti e dati.....	8
5.3.4 Supporti rimovibili.....	9
6. Criteri e modalità di ripristino dei dati.....	9
7. L'affidamento di dati personali all'esterno.....	10
8. Controllo generale sullo stato della sicurezza.....	10
9. Considerazioni conclusive e conseguenze applicative.....	10



Premessa

Scopo di questo documento è di delineare il quadro complessivo delle misure di sicurezza, organizzative, fisiche e logiche, adottate per il trattamento dei dati personali, identificativi, sensibili e giudiziari effettuato da parte di FISIO 10 srl (di seguito anche solo FISIO10) nell'ambito della propria attività professionale in applicazione delle prescrizioni contenute nel Regolamento (UE) 2016/679 General Data Protection Regulation (di seguito anche solo "GDPR").

Nel presente documento si forniscono idonee informazioni riguardanti:

1. l'elenco dei trattamenti di dati personali (*Art. 30 par. 1 lett. c*), mediante:
 - la individuazione dei tipi di dati personali trattati
 - la descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti
 - l'indicazione delle finalità per cui vengono trattati i dati
2. il nominativo e i dati di contatto del titolare del trattamento, nonché la distribuzione dei compiti e delle responsabilità, nell'ambito delle strutture preposte al trattamento dei dati e previsione di interventi formativi degli autorizzati del trattamento
3. l'analisi dei rischi che incombono sui dati, nonché le misure, già adottate e da adottare, per garantire la riservatezza, l'integrità e la disponibilità dei dati; i criteri e le modalità di ripristino dei dati, in seguito a distruzione o danneggiamento i criteri da adottare, per garantire l'adozione delle misure adeguate di sicurezza, in caso di trattamenti di dati personali affidati all'esterno
4. considerazioni conclusive e conseguenze applicative

1. Elenco dei trattamenti dei dati personali

1.1 Tipologie di dati trattati

I dati trattati dal Titolare e forniti per iscritto o verbalmente e liberamente comunicati dai pazienti in qualità di "interessati" (*considerando 14 GDPR*), risultano essere esclusivamente necessari al fine di prestare cure, terapie e diagnosi, ovvero quelli trattati nell'ambito del rapporto di lavoro con personale dipendente all'interno dello stesso studio, ovvero con collaboratori o consulenti esterni.

L'insieme della tipologia dei dati trattati ricomprende pertanto i seguenti dati personali (*art. 4 def. 1 GDPR*) e particolari (*art. 9 GDPR*) relativi a pazienti / fornitori / consulenti / personale amministrativo / collaboratori:

- dati personali dei pazienti dagli stessi forniti, dei fornitori e di terzi;
- dati personali del personale dipendente, collaboratori necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi, dati richiesti ai fini fiscali, previdenziali, e di natura bancaria e postale;
- dati personali dei fornitori concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai fini fiscali e dati di natura bancaria e postale;
- dati personali di altri professionisti ai quali lo studio si affida per consulenze, quali quelli concernenti la reperibilità e la corrispondenza con gli stessi, inerenti a finalità fiscali, di natura bancaria e postale;
- dati particolari del personale dipendente, conseguenti al rapporto di lavoro, e inerenti i rapporti con gli enti previdenziali ed assistenziali;
- dati particolari dei pazienti, dagli stessi forniti idonei a rivelare l'origine razziale ed etnica, le convinzioni e l'adesione ad organizzazioni a carattere religioso, politico, sindacale e filosofico, lo stato di salute e la vita sessuale;
- dati particolari di terzi, forniti dai pazienti idonei a rivelare lo stato di salute o la vita sessuale.



1.2 Caratteristiche di aree, locali e strumenti con cui si effettuano i trattamenti

Il trattamento dei dati personali e particolari avviene esclusivamente all'interno di FISIO 10 srl, sita in via Guasti 12H - int.3 35124 Padova.

L'accesso a FISIO 10 srl è regolato da un servizio di reception e segreteria, sempre presidiato. I pazienti vengono accolti negli ambulatori solo su appuntamento.

Quando FISIO10 è chiuso al pubblico, la sicurezza passiva è assicurata dal sistema di allarme.

Il locale destinato all'archivio dei documenti storici e cartacei dei pazienti è la reception e gli spazi disponibili nella sala server e i documenti vengono conservati ambiente chiuso a chiave ed accessibili solo al personale autorizzato.

Il trattamento dei dati personali avviene con i seguenti strumenti:

- schedari ed altri supporti cartacei;
- PC fissi e portatili, collegati alla rete interna ed esterna (vedi SS-01-Inventario-asset-sistema-informatico);
- Macchinari e attrezzature diagnostiche collegate alla rete interna ed esterna.

2. Organigramma privacy

Titolare del trattamento

- FISIO 10 srl nella figura del legale rappresentante legale protempore

Responsabile Protezione Dati / Data Protection Officer

- Dott. Daniele Maggiolo – dpo@maggioloconsulting.it – cell. 328.6241003

Autorizzati del trattamento

- vedi MPA-02

Consulente esterno responsabile degli asset informatici e ADS

- vedi EFE-01

Responsabili del trattamento esterni

- vedi EFE-01

3. Autorizzati al trattamento: responsabilità e formazione

I dati degli interessati, così come schematizzati nel paragrafo 1.1, sono trattati dal titolare e da tutti gli autorizzati che hanno ricevuto un formale incarico, mediante specifica designazione scritta.

Oltre alle istruzioni generali su come devono essere trattati i dati personali, agli autorizzati vengono fornite esplicite istruzioni in merito ai seguenti punti, ciò al fine di garantire la sicurezza del trattamento medesimo:

- procedure da seguire per la classificazione dei dati, per garantire la sicurezza dei quali occorrono maggiori cautele, rispetto a quanto è previsto per i dati di natura comune
- modalità di reperimento dei documenti, contenenti dati personali, e modalità da osservare per la custodia degli stessi e la loro archiviazione, al termine dello svolgimento del lavoro per il quale è stato necessario utilizzare i documenti
- modalità per elaborare e custodire le *password*, necessarie per accedere agli elaboratori elettronici ed ai dati in essi contenuti
- prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro
- procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi
- procedure per il salvataggio dei dati



- modalità di custodia ed utilizzo dei supporti rimovibili, contenenti dati personali
- dovere di aggiornarsi, utilizzando il materiale e gli strumenti forniti dal Titolare, sulle misure di sicurezza.

Le lettere di incarico o di designazione degli autorizzati vengono raccolte in modo ordinato e periodicamente, con cadenza almeno annuale, si procede ad aggiornare la definizione dei dati cui gli autorizzati sono autorizzati ad accedere, e dei trattamenti che sono autorizzati ad attuare, ciò al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni.

Sono previsti periodici interventi formativi degli autorizzati del trattamento (*art. 29 GDPR*), finalizzati a renderli edotti dei seguenti aspetti:

- profili della disciplina sulla protezione dei dati personali, che appaiono più rilevanti per l'attività svolta dagli autorizzati, e delle conseguenti responsabilità che ne derivano;
- rischi che incombono sui dati;
- misure disponibili per prevenire eventi dannosi;
- modalità per aggiornarsi sulle misure di sicurezza, adottate dal titolare.

Tali interventi formativi sono programmati in modo tale da avere luogo al verificarsi di una delle seguenti circostanze:

- già al momento dell'ingresso in servizio;
- in occasione di cambiamenti di mansioni, che implicino modifiche rilevanti rispetto al trattamento di dati personali;
- in occasione della introduzione di nuovi significativi strumenti, che implicino modifiche rilevanti nel trattamento di dati personali.

Gli interventi formativi possono avvenire sia all'interno, a cura del Titolare, del DPO o di altri soggetti esperti nella materia, che all'esterno presso soggetti specializzati.

Essi tendono a sensibilizzare gli autorizzati sulle tematiche di sicurezza, facendo comprendere i rischi e le responsabilità (con specificazione delle connesse sanzioni penali e disciplinari) che riguardano il trattamento dei dati personali.

Gli interventi formativi pongono altresì come obiettivo la compiuta spiegazione del concetto di quale sia la natura ed il contenuto dei dati particolari, con l'invito a segnalare eventuali disfunzioni dei sistemi operativi e, nel dubbio, di richiedere al Titolare o al DPO se un dato possa avere o meno natura particolare (*art. 9 GDPR*).

4. Analisi dei rischi che incombono sui dati

È stata compiuta l'analisi dei rischi che si può così sintetizzare.

Per i dati personali del personale dipendente, dei pazienti, di terzi, dei fornitori, degli altri professionisti cui lo FISIO10 affida incarichi, dagli stessi forniti o comunque acquisiti: il rischio legato alla loro gestione può definirsi basso.

Per i dati particolari del personale dipendente, dei pazienti, di terzi, dagli stessi forniti o comunque acquisiti: il rischio legato alla loro gestione è da definirsi basso poiché il trattamento dei dati avviene esclusivamente all'interno dei locali dello FISIO10. Si definisce altrettanto basso anche il rischio dei trattamenti effettuati dai fornitori di servizi di cui all'allegato EFE-01 poiché si sono scelti professionisti che evidenziano delle ottime e verificate caratteristiche organizzative e procedurali tali da assicurare il trattamento dei dati in sicurezza.

Il rischio di accesso all'interno del centro fisioterapico da parte di soggetti non autorizzati può essere definito basso perché l'ingresso alla struttura in orario di apertura è controllato da personale dipendente addetto all'accoglienza dei pazienti ed al loro indirizzamento presso i diversi ambulatori.



Il rischio di accesso all'interno degli ambulatori e delle singole stanze della struttura può essere definito basso perché l'ingresso dei pazienti avviene solo previa accettazione in reception, controllo dei flussi e indirizzamento diretto all'interno di FISIO10.

Il rischio di accesso alle singole postazioni di lavoro da parte di persone non autorizzate può essere definito basso perché viene controllato l'accesso di terzi alle diverse aree di lavoro, la zona di attesa è distanziata dalle singole postazioni di lavoro oltre che protetta da strutture mobili (banconi, tavoli, etc). In caso di inutilizzo temporaneo i computer sono messi in stand-by o comunque spenti e non accessibili a terzi.

Avendo adottato le disposizioni di sicurezza stabilite dal D.lgs. 81/2008 ed essendo presente il dispositivo "salvavita", il rischio elettrico e di incendi conseguenti può comunque definirsi basso.

Non può tuttavia escludersi che le aree ed i locali potrebbero essere interessati da eventi imprevedibili, quali incendi e corto circuiti, o possa verificarsi la possibilità che terzi malintenzionati accedano nei locali dove si svolge il trattamento (rapine, furti, danneggiamenti da atti vandalici).

Per quanto riguarda gli strumenti elettronici, il rischio di accesso ai dati in essi contenuti può essere definito basso per le misure di sicurezza volte a ridurre il rischio di perdita e di accesso non autorizzato dei dati (credenziali di accesso composte da user e password per accedere al computer ed ai programmi gestionali). Non sono consentite duplicazioni di dati per finalità differenti da quelle stabilite per il trattamento.

Per quanto riguarda la documentazione cartacea, il rischio può essere definito basso perché gli armadi contenenti gli archivi sono dotati serratura e chiusi a chiave anche durante l'apertura al pubblico.

Per quanto riguarda i supporti di memorizzazione, il rischio di deterioramento dei dati in essi contenuti può essere ritenuto basso poiché i supporti vengono controllati periodicamente ed eventualmente sostituiti in caso di non corretto funzionamento.

Gli elaboratori presenti all'interno dello studio non sono tra loro connessi in rete ma accedono al sistema di cartelle contenente dati personali e particolari unicamente mediante digitazione di password personale e il loro impiego è condiviso tra i medici che operano all'interno di FISIO10 ed il personale autorizzato.

Atteso – infine – che gli autorizzati al trattamento dei dati sono qualificati ed affidabili e dimostrano riservatezza ed attenzione nella gestione dei dati stessi, il rischio legato ad atti di sabotaggio e ad errori umani, da parte del personale appartenente all'organizzazione di FISIO10 e di persone che con esso hanno stretti contatti, può essere definito basso.

Per quanto riguarda i software contenuti negli strumenti elettronici, possono verificarsi errori e disfunzioni da virus, in relazione ai quali sono state applicate da parte del responsabile della gestione del sistema informativo e amministratore di sistema opportune ed idonee contromisure, più avanti meglio specificate.

Si dà atto che FISIO10 non utilizza processi automatizzati, essendo sempre previsto l'intervento umano, ai sensi dell'art. 22 GDPR.

5. Misure atte a garantire l'integrità e la disponibilità dei dati

5.1 La protezione di aree e locali

I locali in cui sono conservati i dati personali trattati sono accessibili ai soggetti che vi svolgono stabilmente o saltuariamente l'attività lavorativa.

Tutti i soggetti sono nominati autorizzati del trattamento dei dati personali con atto separato, revisionato almeno una volta l'anno.



Occasionalmente e solo su richiesta, è concesso l'accesso di terzi (fornitori, personale che svolge interventi di manutenzione di interni e di impianti elettrici, idraulici, informatici ecc.), e solo in presenza di personale di FIO10.

FIO10 è aperto al pubblico dal lunedì al venerdì negli orari 08.00 – 13.00 / 14.30 – 20.00, i pazienti accedono ai locali previo appuntamento a orari concordati preventivamente oppure dopo l'accettazione in reception. All'accettazione i pazienti vengono fatti accomodare nell'area collocata nell'atrio della reception e questo consente di controllare e percepire i movimenti delle persone che passano dalla porta di ingresso e di quelle che si trovano in attesa di essere ricevute, per impedire l'accesso non autorizzato di estranei all'interno dei locali di FIO10.

FIO10 è dotato di più estintori regolarmente controllati, al fine di contrastare inizi di incendi.

Gli impianti ed i sistemi di cui è dotata FIO10 appaiono pertanto soddisfacenti al fine di garantire le opportune misure di sicurezza al trattamento di dati personali da esso svolti.

5.2 La custodia e l'archiviazione di atti, documenti e supporti

Per quanto concerne il reperimento, la custodia e l'archiviazione di atti, documenti e supporti diversi (ad esempio, CD, chiavette, fotografie, fotocopie, radiografie, certificazione medico-sanitaria), si è provveduto ad istruire gli autorizzati, affinché adottino precise procedure atte a salvaguardare la riservatezza dei dati contenuti.

Agli autorizzati vengono date disposizioni, per iscritto, di accedere ai soli dati personali, la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati: in caso di dubbi, è stato loro prescritto di rivolgersi direttamente al titolare.

Di conseguenza, agli autorizzati è prescritto di prelevare dagli archivi i soli atti e documenti che vengono loro affidati per lo svolgimento delle mansioni lavorative, che devono controllare e custodire, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi restituirli all'archivio, al termine di tale ciclo.

Gli autorizzati devono custodire in modo appropriato gli atti, i documenti ed i supporti contenenti dati personali, loro affidati per lo svolgimento delle mansioni lavorative.

Cautele particolari sono previste per gli atti, documenti e supporti contenenti dati particolari: agli autorizzati viene in questi casi prescritto di provvedere al controllo ed alla custodia in modo tale che ai dati non possano accedere persone prive di autorizzazione. A tale fine, gli autorizzati sono stati dotati di:

- casseti con serratura
- armadi chiudibili a chiave

nei quali devono riporre i documenti, contenenti dati particolari, prima di assentarsi dal posto di lavoro, anche temporaneamente. All'interno di tali dispositivi i documenti devono essere riposti anche al termine della giornata di lavoro, qualora l'incaricato debba continuare ad utilizzarli, nei giorni successivi.

Al termine del trattamento, l'incaricato dovrà restituire all'archivio gli atti, i documenti ed i supporti, non più necessari per lo svolgimento delle proprie mansioni lavorative.

Dopo l'orario di chiusura di FIO10, l'accesso all'archivio è consentito unicamente ai Titolari. Si dà atto che i dati non più utilizzati verranno eliminati entro il termine di dieci anni con modalità sicure. In qualunque momento, in conformità agli artt. 16 e 17 GDPR, l'interessato potrà chiederne la cancellazione o la rettifica.

Gli impianti e le attrezzature di cui sono dotati i Titolari per la custodia e l'archiviazione di atti, documenti e supporti, con particolare riferimento a quelli contenenti dati particolari, oggetto di trattamento da parte di FIO10 appaiono soddisfacenti al fine di garantire la necessaria sicurezza ai dati personali contenuti in tali atti, documenti e supporti.



5.3 Le misure logiche di sicurezza

Per i trattamenti effettuati con **strumenti elettronici** (elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato), si adottano le seguenti misure:

5.3.1 Il sistema di autenticazione informatica

Viene adottato una specifica policy per disciplinare gli accessi a tutti gli strumenti elettronici presenti all'interno di FISIO10.

Per realizzare le credenziali di autenticazione, si associa un codice per l'identificazione dell'incaricato (username), ad una parola chiave riservata (password), conosciuta solamente dall'incaricato, che provvederà ad elaborarla, mantenerla riservata e modificarla periodicamente.

Al verificarsi dei seguenti casi, è prevista la disattivazione delle credenziali di autenticazione:

- immediatamente, nel caso in cui l'incaricato perda la qualità che gli consentiva di accedere allo strumento
- in ogni caso, entro sei mesi di mancato utilizzo, con l'unica eccezione delle credenziali che sono state preventivamente autorizzate per soli scopi di gestione tecnica, il cui utilizzo è quindi sporadico.

Relativamente al sistema di autenticazione informatica sopra descritto, agli **autorizzati vengono impartite precise istruzioni** in merito ai seguenti punti:

- obbligo di non lasciare incustodito e accessibile lo strumento elettronico, durante una sessione di trattamento, neppure in ipotesi di breve assenza
- dovere di elaborare in modo appropriato la password, e di conservare la segretezza sulla stessa, nonché sulle altre componenti riservate della credenziale di autenticazione (username). Agli autorizzati è imposto l'obbligo di provvedere a modificare la password, con la seguente tempistica:
 - immediatamente, non appena viene consegnata loro da chi amministra il sistema
 - successivamente, almeno ogni sei mesi. Tale termine scende a tre mesi, se la password dà accesso ad aree in cui sono contenuti dati particolari.

Le password sono composte da almeno dieci caratteri oppure, nel caso in cui lo strumento elettronico non permetta una tale lunghezza, da un numero di caratteri pari al massimo consentito dallo strumento stesso.

Agli autorizzati è prescritto di utilizzare alcuni accorgimenti nell'elaborazione delle password:

- esse non devono contenere riferimenti agevolmente riconducibili all'interessato (non solo nomi, cognomi, soprannomi, ma neppure date di nascita proprie, dei figli o degli amici), né consistere in nomi noti, anche di fantasia (pippo, pluto, paperino, pippobaudò...)
- buona norma è che, dei caratteri che costituiscono la password, da un quarto alla metà siano di natura numerica.

5.3.2 Credenziali di autorizzazione

Per le ridotte dimensioni logistiche di FISIO10 e per assicurare la necessaria continuità operativa tra i vari autorizzati al trattamento, le credenziali di accesso sono conosciute e condivise.

5.3.3 Protezione di strumenti e dati

Per quanto riguarda la **protezione di strumenti e dati** da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus), vengono adottate le misure sotto descritte.

Il primo aspetto è l'applicazione di **software antivirus** di ultima generazione ed installato sia lato server che lato client per assicurare la **protezione dei dati personali dal rischio di intrusione e dall'azione di programmi di cui all'articolo 615-quinquies del Codice penale**, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso



pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento (comunemente conosciuti come virus). L'adozione del software antivirus risponde anche alle prescrizioni ex art. 32 del GDPR. A tale fine, si è dotati di idonei strumenti elettronici e programmi, che si aggiornano i protocolli di sicurezza più volte al giorno in automatico.

Tutti gli autorizzati sono stati istruiti, in merito all'utilizzo dei programmi antivirus e, più in generale, sulle norme di comportamento da tenere, per minimizzare il rischio di essere contagiati.

Il secondo aspetto (applicazione di **firewall** adeguato e di ultima generazione) riguarda la **protezione degli elaboratori dall'accesso abusivo, di cui all'articolo 615-ter del Codice penale**, ai sensi del quale compie tale reato chi si introduce abusivamente in un sistema informatico o telematico, protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo. L'adozione del firewall risponde anche alle prescrizioni ex art. 32 del GDPR.

La protezione da tali accessi avviene mediante l'impiego di idonei strumenti elettronici, comunemente conosciuti come firewall, obbligatori nei casi in cui si trattino dati particolari.

A tale riguardo la nostra organizzazione si è da tempo dotata di tali strumenti, per la protezione degli elaboratori

5.3.4 Supporti rimovibili

Per quanto concerne i **supporti rimovibili** (es. chiavette USB, CD, DVD, hard disk esterni...), contenenti dati personali e particolari, la norma impone particolari cautele ai sensi e per gli effetti delle prescrizioni di cui all'art. 32 del GDPR.

FISIO10 ha ritenuto di estendere tali precetti a tutti i supporti contenenti dati personali e particolari di qualsiasi natura prescrivendo agli autorizzati del trattamento quanto segue:

- i supporti devono essere custoditi ed utilizzati in modo tale da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: in particolare, essi devono essere conservati in cassette chiuse a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi
- una volta cessate le ragioni per la conservazione dei dati, si devono in ogni caso attuare gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati contenuti nei supporti. Tali dati devono quindi essere cancellati, se possibile, e si deve arrivare addirittura a distruggere il supporto, se necessario per i fini in esame.

Le misure logiche di sicurezza, di cui è dotato il Titolare per la protezione dei trattamenti che avvengono con strumenti elettronici appaiono nel loro complesso soddisfacenti, al fine di garantire la necessaria sicurezza ai dati personali trattati.

6. Criteri e modalità di ripristino dei dati

Per fronteggiare le ipotesi in cui i dati siano colpiti da eventi che possano danneggiarli, o addirittura distruggerli, vengono previsti criteri e modalità tali da garantire il loro ripristino in termini ragionevoli, e comunque entro massimo 5 ore per i dati particolari.

Per i dati trattati con strumenti elettronici, sono previste particolari procedure di **backup** attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema, su dispositivi opportuni (CD, backup online...).

Il salvataggio dei dati trattati avviene come descritto nel modello GBU-02-POLITICA_DI_BACKUP_E_RIPRISTINO_DATI.

Ai sensi dell'art. 33 GDPR, nel caso in cui vi sia una violazione dei dati personali, il titolare del trattamento, senza indugi – e in ogni caso entro 72 ore - notificherà la violazione all'autorità di controllo competente a norma dell'art. 55 GDPR.



7. L'affidamento di dati personali all'esterno

Nei casi in cui i trattamenti di dati personali vengano affidati all'esterno della struttura del Titolare, si adottano i seguenti criteri, atti a garantire che il soggetto destinatario adotti misure di sicurezza conformi a quelle minime.

Per la generalità dei casi in cui il trattamento di dati personali, **di qualsiasi natura**, venga affidato all'esterno della struttura del titolare, sono impartite istruzioni per iscritto al terzo destinatario, di rispettare quanto prescritto per il trattamento dei dati personali.

8. Controllo generale sullo stato della sicurezza

Al Titolare, affiancato dal DPO, è affidato il compito di aggiornare le misure di sicurezza, al fine di adottare gli strumenti e le conoscenze, resi disponibili dal progresso tecnico, che consentano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito.

Al fine di verificare l'efficacia delle misure di sicurezza adottate, i Titolari, con l'ausilio del responsabile della gestione del sistema informativo e amministratore di sistema, provvedono con frequenza semestrale, anche tramite controlli a campione, ad effettuare una o più delle seguenti attività:

- verificare l'accesso fisico ai locali dove si svolge il trattamento
- verificare la correttezza delle procedure di archiviazione e custodia di atti, documenti e supporti contenenti dati personali
- monitorare l'efficacia ed il corretto utilizzo delle misure di sicurezza adottate per gli strumenti elettronici
- verificare l'integrità dei dati e delle loro copie di backup
- verificare la sicurezza delle trasmissioni in rete
- verificare che i supporti magnetici, che non possono più essere riutilizzati, vengano distrutti
- verificare il livello di formazione degli autorizzati.

9. Considerazioni conclusive e conseguenze applicative

Il presente documento scaturisce dall'analisi dei problemi conseguenti all'entrata in vigore del Regolamento UE 2016/679 citato in premessa.

In esecuzione di ciò si è provveduto con atto separato (che costituisce parte integrante del presente documento e per tale motivo anche a questo allegato) all'individuazione e nomina dei soggetti autorizzati del trattamento dei dati personali ed alla specificazione scritta ed analitica dei compiti loro affidati ed i termini dell'autorizzazione al trattamento dei dati comuni, sensibili e giudiziari che non siano già contemplati dal presente documento.

Le nomine, le comunicazioni, l'autorizzazione, unitamente al presente documento che viene allegato, sono consegnate ai destinatari che sottoscrivono per ricevuta.

Il presente documento viene sottoscritto dal Titolare e conservato in originale presso lo FISIO10, unitamente alle nomine con istruzioni firmate per accettazione dai destinatari. Copia del presente documento sarà pubblicata anche nel sito web istituzionale.

Ad esso saranno uniti i documenti che in futuro costituiranno integrazione ed aggiornamento del presente atto, necessari per adeguarsi a successive disposizioni di leggi o regolamenti, ovvero a diversa organizzazione dello FISIO10 per la parte che attiene all'organigramma, ai locali ed agli strumenti informatici o comunque automatizzati.