VERIFICA DELLE MISURE DI SICUREZZA ADEGUATE DI CUI ALL'ART.32 DEL REGOLAMENTO UE 2016/679 (GDPR) E DELL'ULTERIORE NORMATIVA APPLICABILE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

.

Informazioni sulla data protection quanto riguarda l'utilizzo della piattaforma RADAC-NPH-Park gestito da "Fondazione LIMPE per il Parkinson onlus" come database per lo studio "Studio clinico osservazionale, prospettico, multicentrico, non interventistico, no profit "RAccolta DAti Clinici (RADAC) NPH-Park"

Quesito	Possibili risposte	Risposta
Responsabile esterno (Fornitore/Sponsor)		Rapsodoo Italia srl
Nome del Software		Odoo 9
Referente Software Fornitore	cognome, nome, telefono, indirizzo email	Francesca Tucci, tel. 06-4503673 francesca.tucci@rapsodoo.com
Informazioni generali		
Dove viene registrato e conservato il dato	in locale sul PC dell'utente, su un server aziendale, su server remoto del fornitore	su server remoto del fornitore
Data Base utilizzato	(Oracle, Access, MsSql, ecc)	PostgreSQL10
Il software memorizza dati personali (anagrafica)?	SI, NO	NO
Il software memorizza dati sensibili (sanitari)?	SI, NO	SI
Sistema di Autenticazione		
Esiste una gestione di login e password per l'accesso la programma?	SI, NO	SI
Esistono funzioni apposite per la gestione di login e password utilizzabili solo dall'amministratore?	SI, NO	SI
Esiste la possibilità di disattivare il login?	SI, NO	SI
Esiste la possibilità di disattivare in automatico il login dopo 6 mesi dall'ultimo utilizzo?	SI, NO	NO
E' prevista l'impossibilità di usare lo stesso login contemporaneamente da più postazioni?	SI, NO	NO
La Password deve essere cambiata al 1° accesso?	SI, NO	SI
La Password è lunga almeno 8 caratteri	SI, NO	SI
La Password contiene almeno 3 delle seguenti caratteristiche: un carattere minuscolo; un carattere maiuscolo; un numero; un carattere speciale?	SI, NO	SI
La password ha una scadenza? Se sì ogni quanto?	SI, NO, mesi	NO
La password è definita dall'amministratore?	SI, NO	NO
Sistema di Autorizzazione, Sicurezza e Tracciabilità		
Esiste un sistema di autorizzazione in base al quale ogni login è assegnato ad un ruolo o profilo che regola l'accesso ai dati?	SI, NO	SI
Esistono funzioni apposite per la gestione dei ruoli e dei profili utilizzabili solo dall'amministratore?	SI, NO	SI
Esistono utenti diversi dall'Amministratore che possono accedere al DataBase?	SI, NO	SI
I dati sono crittografati?	SI, NO	SI
Le operazioni di modifica dei dati effettuate dall'applicativo sono marcate con il codice	SI, NO	NO

VERIFICA DELLE MISURE DI SICUREZZA ADEGUATE DI CUI ALL'ART.32 DEL REGOLAMENTO UE 2016/679 (GDPR) E DELL'ULTERIORE NORMATIVA APPLICABILE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Quesito	Possibili risposte	Risposta
identificativo del login e con un timestamp?		
Sono previsti i backup dei dati: come e con quale periodicità?	es. Full settimanale e differenziale giornaliero	Full giornaliero
Trasmissione dati		
Modalità di trasmissione dei dati	Internet, pec, ecc	Internet
Frequenza di trasmissione	in tempo reale, periodicità mensile, ecc,.	In tempo reale
Protocollo di comunicazione (porte utilizzate)	HTTPS, VPN, ecc	https
Collocazione geografica dei server in cui sono conservati i dati	es. Italia, Stati Uniti	EU (regione Francoforte)

Si riporta il testo dell'art. 32 del GDPR:

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 a 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."*