Elenco delle misure tecniche e organizzative generali ai sensi dell'art. 32 del Regolamento generale sulla protezione dei dati di BIOTRONIK SE & CO. KG e delle misure speciali relative al funzionamento dell'Home Monitoring Service Center.

Le organizzazioni che raccolgono, trattano o utilizzano dati personali per loro conto o per conto terzi sono tenute ad adottare le misure tecniche e organizzative necessarie per garantire l'applicazione delle norme relative alle Leggi sulla protezione dei dati. Le misure sono necessarie solo se proporzionate all'obiettivo di protezione perseguito.

La suddetta organizzazione soddisfa questo requisito mediante le misure seguenti:

1. Riservatezza conformemente all'art. 32 par. 1 lett. b Regolamento generale sulla protezione dei dati (GDPR)

1.1. Controllo d'accesso della persona fisica

I seguenti provvedimenti si applicano per proteggere le sale con impianti di trattamento dei dati dall'accesso di persone non autorizzate.

Misure tecniche	**Misure organizzative**
☒ Impianto di allarme	☒ Regolamento chiavi / elenco
☒ Sistema di controllo degli accessi automatico	☒ Controllo d'identità alla reception
☒ Barriere di sicurezza biometriche	☒ Tesserino collaboratori / visitatori
☒ Carte con chip / sistemi a transponder	☒ Accompagnamento dei visitatori da parte dei collaboratori
☒ Sistema di chiusura manuale	☒ Particolare cura e attenzione nella selezione del personale di vigilanza
☒ Serrature di sicurezza	☒ Particolare cura e attenzione nella selezione del personale addetto alla pulizia
☒ Sistema di chiusura a blocco con codice	☒ Registrazione dei visitatori
☒ Messa in sicurezza dei pozzi dell'edificio	
☒ Porte con pomello esterno	
☒ Campanello con videocamera	
☒ Videosorveglianza degli accessi	
☒ Fotocellule / sensori di movimento	

I servizi ReportShare e Home Monitoring vengono erogati in sale sistemi protette e non accessibili a tutti. Queste sale sono protette da porte in acciaio. L'accesso viene regolato tramite un sistema di controllo elettronico con autenticazione a 3 fattori (biometrico, conoscenza, possesso).

1.2. Controllo dei diritti d'accesso software e hardware

Si applicano le seguenti misure per proteggere i sistemi di trattamento dei dati dall'utilizzo di persone non autorizzate.

Misure tecniche	Misure organizzative
☒ Login con nome utente + password	☒ Gestione delle autorizzazioni utente
☒ Software antivirus per i server	☒ Creazione di profili utente
☒ Software antivirus per i clienti	☒ Direttiva "Password sicura"
☒ Intrusion Detection Systems	☒ Istruzioni "Blocco manuale del desktop"
☒ Gestione dei dispositivi mobili (Mobile Device Management)	
☒ Impiego VPN per accesso remoto	
☒ Crittografia dei supporti di dati	
☒ Blocco automatico del desktop	
☒ Crittografia dei dispositivi notebook / tablet	
☒ Procedura di autenticazione biometrica	
☒ Impiego di un firewall hardware	

I servizi ReportShare e Home Monitoring vengono erogati in un ambiente chiuso; questo ambiente è separato da altri sistemi e applicazioni e viene utilizzato esclusivamente per fornire servizi in remoto (Home Monitoring e ReportShare). Tutte le connessioni da o verso questa scatola nera sono protette tramite firewall. Le connessioni nelle reti pubbliche sono protette da almeno due diversi tipi di firewall. L'accesso amministrativo è possibile solo localmente mediante accesso fisico diretto oppure in remoto dalla Intranet, dalle postazioni di lavoro dell'amministratore definite. L'accesso remoto dalle postazioni di lavoro dell'amministratore è crittografato con tecnologia IPSec tramite VPN e utilizza accessi separati. Per l'accesso amministrativo ai server e / o ad altri nodi di rete, viene utilizzato un login personalizzato (nome utente e password).

1.3. Controllo dell'accesso ai dati

Si applicano le seguenti misure per proteggere i dati dall'accesso di persone non autorizzate.

Misure tecniche	Misure organizzative
☒ Distruggidocumenti (min. livello 3, taglio a croce)	☒ Impiego di sistemi di autorizzazione
☒ Distruggidocumenti esterno (DIN 32757)	☒ Numero di amministratori ridotto all'essenziale
☒ Cancellazione fisica dei supporti di dati	☒ Gestione dei diritti utente da parte degli amministratori
☒ Registrazione degli accessi alle applicazioni, in particolare per ciò che concerne immissione, modifica e cancellazione dei dati	☒ Direttiva password incl. lunghezza e modifica della password
☒ Corretta distruzione dei supporti di dati (DIN 66399)	☒ Conservazione sicura dei supporti di dati

L’accesso ai dati ReportShare e Home Monitoring è protetto da un sistema di diritti di accesso. In questo modo, agli utenti viene consentito l’accesso solo ai dati per i quali hanno ottenuto l’apposita autorizzazione. Attraverso un servizio di directory, gli amministratori possono accedere solo alle aree necessarie per eseguire i propri compiti. Ulteriori accessi non sono possibili.

1.4. Controllo di separazione

Misure da adottare per garantire che i dati raccolti per diversi scopi possono essere trattati separatamente. Ad esempio, questo può essere garantito tramite una separazione logica e fisica dei dati.

Misure tecniche	**Misure organizzative**
☒ Separazione dell’ambiente di prova dall’ambiente di produzione	☒ Gestione della logica di autorizzazione
☒ Separazione fisica (sistemi / banche dati / supporti informatici) per il trattamento dei dati raccolti per diversi scopi	☒ Definizione dei privilegi relativi alle basi di dati
☒ Conservazione separata di specifici dati sensibili	
☒ Separazione logica dei clienti (basata su software)	

Il trattamento dei dati personali avviene esclusivamente nel sistema produttivo. Altri sistemi non possiedono alcuna informazione sui dati personali o in merito all’accesso a questi ultimi. Il servizio di controllo Home Monitoring Service viene effettuato tramite server virtuali dedicati, all’interno di zone protette per mezzo di firewall. Non vi sono collegamenti di alcun genere ad altri sistemi/servizi che raccolgono i dati per altri scopi.
I dati di carattere medico o privato dei pazienti vengono conservati in banche dati separate.

1.5. Pseudonimizzazione (art. 32 par. 1 lett. a del GDPR; art. 25 par. 1 del GDPR)

Trattare i dati personali affinché questi non possano più essere attribuiti a un interessato specifico senza l’utilizzo di informazioni aggiuntive, a condizione che queste ulteriori informazioni vengano conservate separatamente e siano soggette a misure organizzative;

Misure tecniche	**Misure organizzative**
☒ L’associazione degli pseudonimi ai dati ottenibili degli utenti viene separata dalle altre informazioni, conservate in modalità criptata	☒ Istruzioni interne per garantire l’anonimato dei dati personali in caso di trasferimento o dopo la cancellazione per scadenza legale

2. Integrità (art. 32 par. 1 lett. b del GDPR)

2.1. Controllo del trasferimento

Misure da adottare per garantire che alla trasmissione elettronica o durante il trasporto o la memorizzazione su un supporto informatico i dati personali non possano più essere letti, copiati, alterati o rimossi da persone non autorizzate. Inoltre devono essere garantiti la verifica e l'accertamento degli enti ai quali è previsto il trasferimento di dati personali tramite i dispositivi di trasmissione.

Misure tecniche	**Misure organizzative**
☒ Cifratura delle e-mail all'interno di BIOTRONIK	☒ Documentazione del destinatario dei dati così come della durata prevista della cessione, ovvero della cancellazione
☒ Impiego di VPN	☒ Regolamento per una disattivazione sicura e riservata degli apparecchi con i supporti informatici (ad esempio i server)
☒ Disponibilità di un collegamento criptato come sftp, https	
☒ Impiego di procedure per la firma	

BIOTRONIK non inoltra a terzi i dati conservati via ReportShare o Home Monitoring che non soddisfano l'uso previsto dai sistemi. In caso di trasferimento di dati a terzi, richiesto dal contesto d'uso, i fornitori di servizi si impegnano ad agire ai sensi del Regolamento del GDPR e della Legge tedesca sulle telecomunicazioni.

In caso di trasmissione di dati e conservazione vengono utilizzate le seguenti misure:

- La trasmissione di dati tra HMSC e medico avviene solo in modalità criptata (via TLS)
- La conservazione dei dati personali dei pazienti avviene in modalità criptata nella banca dati. L'accesso a tali dati è consentito solo agli utenti che hanno la relativa autorizzazione.

2.2. Controllo di inserimento

Misure da adottare per garantire che sia possibile verificare e accertare a posteriori se e da chi i dati personali siano stati inseriti nei sistemi di trattamento dei dati e se siano stati alterati o rimossi.

Misure tecniche	**Misure organizzative**
☒ Registrazione tecnica delle operazioni di immissione, modifica e cancellazione dei dati	☒ Tracciabilità dell'inserimento, modifica e cancellazione dei dati attraverso i nomi utente individuali (non gruppi di utenti)
☒ Attuazione di un concetto di utilizzo basato sul ruolo	☒ Concessioni dei diritti per l'inserimento, la modifica e la cancellazione dei dati sulla base di una logica di autorizzazione

	☒ Conservazione dei moduli utilizzati per la raccolta dei dati nel trattamento automatico

L'accesso al sistema produttivo e ai relativi dati è protetto dalla citata logica di diritto e dalla registrazione in un log di ciascun accesso degli amministratori. Per garantire un controllo delle informazioni dei pazienti inserite dal medico nei ReportShare o Home Monitoring System, ogni variazione richiede sempre la conferma attraverso una specifica finestra di dialogo.

3. Accessibilità e resilienza (art. 32 par. 1 lett. b del GDPR)

3.1. Controllo di accessibilità

Misure da adottare per garantire che i dati personali siano tutelati da danneggiamenti accidentali o perdite.

Misure tecniche	**Misure organizzative**
☒ Sistemi di allarme antincendio e rilevatori di fumo	☒ Piano di backup e di recupero (elaborato)
☒ Estintori nel locale dei server	☒ Controllo della procedura di sicurezza
☒ Monitoraggio di temperatura e della presenza di acqua nel locale dei server	☒ Test periodici per recupero dati e registrazione dei risultati
☒ Locale dei server climatizzato	☒ Backup archiviati in luoghi sicuri, in altra sede
☒ UPS	☒ Locali dei server non situati al di sotto di impianti di servizi igienici
☒ Allarme in caso di accesso non autorizzato al locale dei server	
☒ Prese multiple protette da sovratensione nei locali dei server	

L'hardware utilizzato per i servizi ReportShare e Home Monitoring è situato in un proprio locale dei server separato. Questo locale è protetto da interruzioni di corrente grazie a sistemi di alimentazione continua e di alimentazione di riserva, nonché a misure di sicurezza analoghe (che si applicano a BIOTRONIK). Regolarmente vengono effettuati dei backup e viene effettuato un training per il ripristino dei dati. La disponibilità e la performance dei servizi e di tutti i componenti principali vengono controllate da un sistema di monitoraggio. Controlli di sicurezza interni ed esterni vengono eseguiti regolarmente. I backup vengono archiviati in un compartimento antincendio differente e ulteriormente copiati in un altro sito.

4. Procedura per il controllo, la verifica e la valutazione regolari (art. 32 par. 1 lett. d del GDPR; art. 25 par. 1 del GDPR)

4.1. Gestione della protezione dei dati personali

Misure tecniche	Misure organizzative
☒ Soluzioni software per la gestione della protezione dei dati personali in uso	☒ Incaricato della protezione dei dati personali (IPDP) interno: Alfred Maus, BIOTRONIK SE & Co. KG, alfred.maus@biotronik.com
☒ Documentazione centrale di tutte le modalità procedurali e i regolamenti per la protezione dei dati con possibilità di accesso per i collaboratori in base alle esigenze / autorizzazioni (ad es. Wiki, Intranet…)	☒ Collaboratori formati e vincolati alla riservatezza/confidenzialità dei dati
☒ Sistema di gestione della sicurezza delle informazioni certificato secondo ISO 27001	☒ Sensibilizzazione periodica dei collaboratori. Almeno ogni anno.
	☒ Incaricato alla protezione delle informazioni (IPI) interno: Martin Noll, BIOTRONIK SE & Co. KG, martin.noll@biotronik.com
	☒ La valutazione d'impatto sulla protezione dei dati viene eseguita in caso di necessità
	☒ L'organizzazione adempie agli obblighi di informazione secondo l'art. 13 e 14 GDPR
	☒ È presente un processo formalizzato per l'elaborazione di richieste di informazioni da parte dell'interessato

4.2. Gestione della reazione agli incidenti

Supporto nella reazione alle violazioni della sicurezza

Misure tecniche	Misure organizzative
☒ Impiego di firewall e aggiornamenti regolari	☒ Processo documentato per il riconoscimento e la segnalazione di incidenti di sicurezza e relativi ai dati (anche in considerazione dell'obbligo di segnalazione alle autorità di sorveglianza)
☒ Impiego di antivirus e aggiornamenti regolari	☒ Modalità procedurali documentate per affrontare incidenti di sicurezza
☒ Intrusion Detection Systems	☒ Collegamento delle ☒ IPDP e ☒ IPI in incidenti di sicurezza e relativi ai dati

	☒ Documentazione di incidenti di sicurezza e relativi ai dati, ad es. tramite sistema di ticketing
	☒ Processo formale e responsabilità per l'elaborazione successiva di incidenti di sicurezza e relativi ai dati

4.3. Impostazioni predefinite per la protezione dei dati (art. 25 par. 2 GDPR);

Privacy by design / Privacy by default

Misure tecniche	**Misure organizzative**
☒ Non verranno più raccolti altri dati personali oltre a quelli necessari per la relativa finalità	☒ La revoca può essere eseguita dalla clinica
☒ L'utente può disattivare la registrazione dell'uso del sito Web tramite il browser (opt-out)	

4.4. Controllo sull'incarico (outsourcing a terzi)

Misure tecniche	**Misure organizzative**
☒ Soluzioni software per la gestione della protezione dei dati personali in uso	☒ Attribuendo l'incarico a parti esterne, il fornitore deve dimostrare di rispettare il GDPR.

Tutti i dati nel sistema Home Monitoring (incl. ReportShare) sono elaborati e salvati da BIOTRONIK SE & Co. KG. In caso di trasferimento di dati a terzi, richiesto dal contesto d'uso, i fornitori di servizi si impegnano ad agire ai sensi del Regolamento del GDPR e della Legge tedesca sulle telecomunicazioni.