Misure tecniche e organizzative

1. Riservatezza (Art. 32 Par. 1 lett. b GDPR)

1. **Controllo degli accessi fisici**
   Nessun accesso non autorizzato ai sistemi di trattamento dei dati, ad esempio: carte magnetiche o chip, chiavi elettriche, dispositivi di sicurezza o gatekeeper, sistemi di allarme, sistemi video;

Domande relative al controllo degli accessi	**Presente**		**Documentato**		**Osservazioni**
	sì	**no**	**sì**	**no**	
Le vie di accesso sono protette?	✓			✓	
Quali misure tecniche e organizzative sono utilizzate per il controllo degli accessi e la legittimazione degli utenti autorizzati?					Chiavi con certificazione di sicurezza e gestione delle chiavi nel momento di restituzione.
• Carte o chip magnetici		✓			
• Chiavi	✓		✓		
• Dipositivi di sicurezza		✓			
• Dispositivi di sorveglianza		✓			
• Videosorveglianza		✓			
• Sistemi di allarme		✓			
• altri		✓			
I dipendenti autorizzati sono definiti? (sistema di controllo degli accessi)		✓			Avviene tramite la gestione delle chiavi.
Vengono redatti dei registri di presenza?		✓		✓	
È presente un servizio di portineria?		✓			

Sono previste delle disposizioni per il personale esterno, addetti alle pulizie, visitatori?	✓		✓		Restituzione delle chiavi con protocollo gestione chiavi.
Il controllo degli accessi è regolamentato per lavoratori da casa?		✓		✓	
L'accompagnamento di ospiti nell'edificio è regolato?		✓		✓	Ospiti vengono raramente e non hanno accesso libero.
Le aree/ zone di sicurezza sono definite? (ad es. per server, computer centrale, archivio)		✓		✓	Computer sono cifrati, server sono esterni.
Come viene protetto l'ingresso al centro server? ● Finestre speciali o con sbarre ● Serrature di sicurezza ● Aperture per ventilazione o luce ● Tapparelle a prova di spinta? ● Uscite d'emergenza					Non gestiamo centro server. Il fornitore della nostra infrastruttura server è la Wavecon GmbH.
I server sono posizionati in armadietti chiusi a chiave?	✓		✓		Server esterni.
I supporti di memorizzazione dati sono sotto chiave o in stanze chiuse?		✓			Non necessario perché cifrati e in cloud.
I computer portatili sono sotto chiave?		✓			Non necessario, perché cifrati.
L'archiviazione dei dati di backup è ben protetta?	✓		✓		Backup solo in cloud.

Ci sono delle disposizioni per la copia/distribuzione delle chiavi?	✓		✓		Gestione delle chiavi.

2. Controllo degli accessi autorizzati

Nessun utilizzo non autorizzato del sistema, ad esempio: password (sicure), meccanismi di blocco automatico, autenticazione a due fattori, crittografia del disco;

Domande relative al controllo degli accessi autorizzati	**Presente**		**Documentato**		**Osservazioni**
	sì	**no**	**sì**	**no**	
L'archiviazione dei supporti dati è protetta?		✓		✓	No, siccome cifrati / salvati in cloud.
Le persone autorizzate ad accedere ai supporti dati sono stabilite?	✓				Si, tramite nome utente e password.
Gli utenti non autorizzati vengono respinti?	✓		✓		Documentazione di tentativi login falliti.
Esiste una procedura garantita per la gestione dei supporti dati?					No supporti dati mobili, solo cloud.
• Identificazione					
• Sistema di inventariato					
• Monitoraggio delle risposte					
• Riscontro					
• Documenti di accompagnamento					
• Periodo di conservazione					
Si effettua la separazione dei supporti dati per i diversi committenti?		✓		✓	No supporti dati mobili, solo cloud.
La distruzione dei supporti dati di effettua conformemente alla		✓		✓	No, siccome cifrati / salvati in cloud.

protezione e alla sicurezza dei dati?					
Vengono utilizzati programmi di utilità appropriati per la cancellazione dei supporti dati (cancellazione fisica)?		✓		✓	No, siccome cifrati / salvati in cloud.
Esistono regole vincolanti per la procedura di creazione delle password descritta nei seguenti punti?					
• Combinazione di caratteri	✓		✓		
• Minimo 8 caratteri	✓		✓		
• Cambio periodico	✓		✓		
• Storico delle password	✓		✓		
• Nessuna password di gruppo	✓		✓		
• Blocco schermo durante le pause	✓		✓		
• Processo di reimpostazione della password	✓			✓	
• Password per l'amministrazione dello storage	✓		✓		
Esiste una procedura vincolante per il rilascio delle autorizzazioni?		✓		✓	
I dati sui supporti dati mobili (es. CD, chiavetta USB) vengono criptati?	✓		✓		
Esiste un firewall?	✓		✓		Dipende dal sistema.

3. Controllo degli accessi ai dati

Nessuna lettura, copia, modifica o rimozione non autorizzata all'interno del sistema, ad esempio: criteri per l'autorizzazione, diritti di accesso per necessità, registrazione degli accessi:

Domande relative al controllo degli accessi ai dati	Presente		Documentato		Osservazioni
	sì	no	sì	no	
Le autorizzazioni sono impostate nei sistemi IT?	✓		✓		
Esistono autorizzazioni differenziate (ad es. per leggere, cancellare, modificare?)	✓		✓		
Esistono autorizzazioni differenziate per dati, applicazioni e sistema operativo?	✓		✓		
Esiste una separazione tra autorizzazione organizzativa e autorizzazione tecnica?		✓			Parzialmente non possibile per dimensione dell'azienda.
Esiste un'impostazione di utilizzo e classificazione dei drive?					
Il recupero dei dati dal backup è regolato da una procedura obbligatoria?	✓		✓		Documentato dalla Wavecon GmbH.
L'utilizzo del programma e dei dati viene registrato e valutato (campionamento casuale)?					Dipende dal sistema.
Esiste un'eventuale separazione delle funzioni durante lo sviluppo di un programma (ambiente di test e produzione)?	✓		✓		

4. Controllo della separazione dei dati

Elaborazione separata dei dati raccolti per finalità diverse, ad es. funzionalità multi-client, sandboxing;

Domande relative al controllo della separazione dei dati	Presente		Documentato		Osservazioni
	sì	no	sì	no	
I dati del Titolare e di altri clienti sono trattati dal contraente su sistemi fisicamente separati?		✓			No separazione fisica perché sistema cloud.
I dati del Titolare e di altri clienti vengono trattati da diversi dipendenti presso il Responsabile?		✓			
I backup dei dati del Titolare si trovano su supporti dati separati (che non contengono dati di altri clienti)?		✓			No separazione fisica perché sistema cloud.
Esiste un tipo di autorizzazione che tenga conto del trattamento separato dei dati del Titolare dai dati di altri clienti?		✓			No separazione fisica perché sistema cloud.
Sandboxing (ambiente di test isolato)	✓				Per determinati casi di utilizzo.

5. Pseudonimizzazione (Art. 32 Par. 1 let. A GDPR; Art. 25 Par. 1 GDPR)

Il trattamento dei dati personali in modo tale che i dati non possano più essere attribuiti a un soggetto interessato specifico senza il ricorso a informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano mantenute separate e soggette ad adeguate misure tecniche e organizzative;

Domande relative alla pseudonimizzazione	Presente		Documentato		Osservazioni
	sì	no	sì	no	
Pseudonimizzazione secondo le specifiche disponibili?		✓			Lavori in corso.

2. Integrità (Art. 32 Par. 1 lett. B GDPR)

1. Controllo sulla divulgazione

Nessuna lettura, copia, modifica o cancellazione non autorizzate durante la trasmissione o il trasporto elettronico, ad esempio: crittografia, reti private virtuali (VPN), firme elettroniche;

Domande relative al controllo sulla divulgazione	Presente		Documentato		Osservazioni
	sì	no	sì	no	
I dati vengono inviati dal Responsabile al Titolare?	✓		✓		
Il Responsabile riceve dati dal Titolare?	✓		✓		Parzialmente documentato
Quale modalità di invio dei dati è in essere tra Titolare e Responsabile?					
• Trasporto dei supporti dati (ad esempio tramite poste, corriere affidabile)		✓			
• Indirizzo di imballaggio e spedizione		✓			

• Tracking della spedizione		✓			
• Contenitori sigillati		✓			
• Crittografia dei dati	✓				
• E-Mail (crittografia)		✓			
• Trasferimento dei file criptati (FTP-protocollo di trasferimento file)		✓			
• Connessione VPN criptata	✓				
Sono state stabilite ulteriori misure per la trasmissione / trasporto dei dati?					Protocollo di cifrazione assicura la completezza e correttezza dei dati.
• Tempistiche		✓			
• Risposta/feedback		✓			
• Test di completezza e accuratezza	✓				
• Registrazione (ad esempio, nota di accompagnamento del supporto dati trasportato)	✓				
Esiste una documentazione di rete per i percorsi di trasmissione?		✓			
Ci sono delle persone responsabili della trasmissione/ trasporto dei dati?	✓				
Il controllo di legittimità è effettuato dalle persone autorizzate?	✓				

2. Controllo dell'immissione dei dati

Determinare se e da chi i dati personali sono stati inseriti, modificati o rimossi nei sistemi di elaborazione dati, ad esempio, la registrazione, la gestione dei documenti;

Domande relative al controllo dell'immissione dei dati	Presente		Documentato		Osservazioni
	sì	no	sì	no	
Sono impostate delle autorizzazioni utente (rispetto ai vari profili)?	✓		✓		
Le autorizzazioni utente sono differenziate?					Nessun accesso diretto ai banca dati.
• Leggere, modificare, cancellare	✓				
• Accesso parziale a dati o funzioni	✓		✓		
• Accesso alle banche dati					
Viene registrato in modo automatico chi ha inserito cosa nell'applicazione tecnica e quando?	✓		✓		Dipende dalla funzionalità.
Le attività dell'amministratore vengono monitorate (creazione di utenti, modifica dei diritti dell'utente)?	✓		✓		
Sono definiti dei periodi di conservazione?	✓		✓		
Ci sono delle istruzioni per tenere un registro manuale per le procedure non automatizzabili?		✓		✓	
I requisiti per la reimpostazione delle password vengono archiviati?		✓		✓	

3. Disponibilità e resilienza dei sistemi (Art. 32 par. 1 lett. b GDPR)

3.1 Recupero rapido della disponibilità dei dati (Art. 32 Par. 1 lett. c GDPR);

Protezione da distruzione o perdita accidentali o intenzionali, quali: strategia di backup (online/ offline, on-site/ off-site), gruppi di continuità (UPS), antivirus, firewall, notifiche e piani di emergenza

Domande relative al controllo della disponibilità	**Presente**		**Documentato**		**Osservazioni**
	sì	**no**	**sì**	**no**	
Impostazione di backup e ripristino con backup giornaliero?	✓		✓		Documentato nella configurazione backup.
Accordo sul trasferimento dei backup (dati)?		✓		✓	Nessun trasferimento fisico.
Mirroring dei dischi rigidi?	✓				Dipende dal sistema.
Archiviazione a prova di calamità dei supporti dati?	✓				Avviene tramite la Wavecon GmbH.
Procedure di emergenza e recupero con test regolari?	✓				Avviene tramite la Wavecon GmbH.
Data center alternativo?		✓			
Sistemi gemelli alternativi?	✓				Dipende dal sistema.
Gruppo di continuità ininterrotto?	✓				Avviene tramite la Wavecon GmbH.
Viene utilizzato un software di sicurezza? • Scanner dei virus • Firewall • Filtro SPAM • Programmi di crittografia					Dipende dal sistema.

4. Procedure per revisione periodica e valutazione (Art. 32 Par. 1 lit. D GDPR; Art. 25 Par. 1 GDPR)

✓ Gestione delle attività di protezione dei dati presenti

✓ Gestione della risposta agli incidenti in essere

X Impostazioni predefinite compatibili con la privacy (Art. 25 Par. 2 GDPR)

✓ Condurre una valutazione d'impatto sulla protezione dei dati

Controllo relativo al contratto:

Non deve essere operato alcun trattamento dei dati senza le corrispondenti istruzioni del Titolare ai sensi dell'articolo 28 GDPR, ad esempio: chiara progettazione del contratto, gestione degli ordini formalizzata, selezione rigorosa del Responsabile di servizi, controlli di follow-up.

Domande relative a	**Presente**		**Documentato**		**Osservazioni**
	sì	**no**	**sì**	**no**	
I dipendenti del Responsabile sono soggetti all'obbligo di segretezza dei dati (art. 53 BDSG)?	✓				
Quali informazioni scritte sulla protezione dei dati vengono fornite ai dipendenti del Responsabile? (ad esempio, opuscoli, testi di legge)					Obbligo alla riservatezza.
I rapporti di subappalto del Responsabile sono definiti per iscritto?	✓		✓		
I subappaltatori del Responsabile sono regolarmente monitorati?	✓		✓		
Controllo regolare dell'affidabilità del subappaltatore	✓		✓		