CHECK LIST MISURE TECNICHE E ORGANIZZATIVE (ART. 28 REGOLAMENTO UE 2016/679)

Il presente allegato contiene la descrizione delle misure tecniche e organizzative messe in atto dal/dai Responsabile/i del trattamento (comprese le eventuali certificazioni pertinenti) per garantire un adeguato livello di sicurezza, tenuto conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche.

N°	Controlli	
1	**Riservatezza**	
1.1	**Controllo fisico degli accessi** - accesso ai locali e alle strutture in cui vengono trattati i dati. **Requisito:** *è necessario evitare l'accesso (fisico) di soggetti non autorizzati agli edifici e alle strutture in cui vengono trattati i dati personali del Titolare del trattamento. Il Responsabile del trattamento deve mettere in atto sistemi di controllo degli accessi efficienti (controllo degli accessi tecnologico o mediante personale).*	[Selezionare]
1.1.1	A tal fine vengono messe in atto le seguenti **misure tecniche**: ☐ Sistemi di allarme ☐ Sistemi antintrusione (barriere fotoelettriche/rilevatori di movimento) ☐ Sistemi automatici di controllo degli accessi ☐ Barriere di accesso biometriche ☐ Sistema di accesso mediante smart card/trasponder ☐ Sistemi di chiusura manuali ☐ Sistemi di chiusura con codice d'accesso ☐ Videosorveglianza dei punti di accesso ☐ *Altro: specificare o inserire spazi*	
1.1.2	A tal fine vengono messe in atto le seguenti **misure organizzative**. ☐ Controlli del personale tramite portineria/all'accoglienza ☐ Registrazione dei visitatori/libro dei visitatori ☐ Accompagnamento dei visitatori ☐ Registrazione delle chiavi/libro delle chiavi ☐ Obbligo di indossare badge identificativi per dipendenti ☐ Obbligo di indossare badge identificativi per ospiti ☐ Zone di sicurezza con diverse autorizzazioni di accesso ☐ Supervisione del personale esterno ad es. personale per la manutenzione e di servizio ecc. ☐ *Altro: specificare o inserire spazi*	

1.2	**Controllo logico degli accessi** - L'accesso logico ai sistemi di trattamento, alle applicazioni e ai dati deve essere riservato esclusivamente ai soggetti autorizzati. **Requisito**: *è necessario evitare l'accesso non autorizzato ai sistemi IT. Devono essere messe in atto misure tecniche e organizzative per l'identificazione e l'autenticazione degli utenti*. *L'accesso ai sistemi IT del Responsabile del trattamento deve essere limitato agli utenti autorizzati mediante un processo di autenticazione sicuro. Ogni utente deve avere un ID utente univoco. La condivisione degli account non è consentita. L'accesso ai sistemi IT e alle applicazioni del Responsabile del trattamento deve essere accessibile tramite sistemi di autenticazione che prevedono come requisito minimo l'utilizzo di credenziali composte da nome utente e password. Tale protezione deve includere, ma non essere limitata a una policy per la password sicura, una disconnessione automatica dopo un determinato periodo di tempo, il blocco in seguito a diversi tentativi di accesso falliti, una procedura di ripristino della password affidabile, una modifica periodica delle password. Le password devono essere sempre conservate e trasmesse in modo sicuro, ad es. mediante crittografia e funzione hash. Il Responsabile del trattamento ha definito i requisiti, le regole e gli standard delle linee guida per le password in una politica conosciuta dagli utenti e supportata a livello tecnico. Le password devono essere assegnate a una singola persona, conservate e trasmesse in modo sicuro, devono essere sufficientemente lunghe e complesse, modificate su base regolare, limitate in termini di validità, bloccate e successivamente eliminate se inattive per un lungo periodo di tempo e modificate immediatamente qualora compromesse. Ove possibile, in particolare per le utenze con privilegi elevati e per i sistemi e le applicazioni che ospitano dati particolari, si predilige l'utilizzazione di sistemi di autenticazione a più fattori*	. [Selezionare]
1.2.1	A tal fine vengono messe in atto le seguenti **misure tecniche**: ☐ Autenticazione con username e password ☐ Autenticazione a due fattori ☐ Autenticazione con dati biometrici ☐ Utilizzo di certificati digitali per l'autenticazione ☐ Identity and Access Management centralizzato ☐ Sistemi di Single Sign On ☐ Sistemi di controllo scadenza password ☐ Sistemi di controllo robustezza e complessità password ☐ Sistemi di blocco account dopo numero predefinito di tentativi falliti ☐ Sistemi di controllo dell'utilizzo contemporaneo dello stesso account sulle applicazioni ☐ Utilizzo di VPN autenticata crittografata per accesso da remoto ☐ Utilizzo password o pin per i dispositivi mobili ☐ Utilizzo di salvaschermi automatici ☐ Time-out sessione per le applicazioni ☐ *Altro: specificare o inserire spazi*	

1.2.2	A tal fine vengono messe in atto le seguenti **misure organizzative**. ☐ Procedure di assegnazione degli account ☐ Inventario aggiornato degli account assegnati ☐ Inventario aggiornato degli account di servizio utilizzati dalle applicazioni ☐ Cancellazione o disabilitazione degli account non utilizzati dopo un periodo di tempo definito ☐ Formazione del personale sull'uso degli account aziendali ☐ Regolamenti o politiche per gli account aziendali e la robustezza delle password ☐ Procedure di azzeramento o ripristino password ☐ *Altro: specificare o inserire spazi*	
1.3	**Profili di autorizzazione e controllo delle autorizzazioni** – Nessuna lettura, copia, modifica o rimozione non autorizzata all'interno del sistema informatico o per il trattamento di dati su supporti cartacei. **Requisito:** *Il Responsabile del trattamento deve definire specifici profili di autorizzazione per i soggetti che accedono ai dati e mettere in atto soluzioni per il controllo dei diritti di accesso e le necessarie autorizzazioni, che devono essere strettamente limitate a consentire l'attività delegata al soggetto autorizzato. Il controllo delle autorizzazioni prevede anche politiche e strumenti di monitoraggio e di registrazione degli accessi ai dati. Particolare attenzione deve essere posta all'assegnazione di privilegi elevati, che devono essere riservati ai tecnici che effettuano operazioni di amministrazione dei sistemi, delle banche dati e delle applicazioni (cd. Amministratori di sistema). Gli amministratori di sistema devono avere un account con privilegi elevati individuale per eseguire le loro attività di amministrazione diverso da quello utilizzato per le attività che non richiedono diritti particolari. I dischi e le memorie destinate allo smaltimento o riutilizzo devono essere distrutti o soggetti a cancellazione sicura*	[Selezionare]
1.3.1	A tal fine vengono messe in atto le seguenti **misure tecniche**. ☐ Profili utente con accesso limitato alla rete ed alle applicazioni ☐ Ruoli e autorizzazioni basati sul principio della necessità di accesso ai dati ☐ Configurazione dei file server con aree ad accesso limitato in base alle autorizzazioni assegnate ☐ Configurazione delle applicazioni per l'assegnazione di privilegi minimi per eseguire l'attività assegnata all'utente ☐ Sistema di registrazione (log) delle modifiche dei privilegi assegnati ☐ Sistema di alert delle modifiche dei privilegi assegnati ☐ Sistema di registrazione (log) dell'accesso ai sistemi da parte degli amministratori di sistema ☐ Sistema di registrazione (log) dell'accesso ai sistemi da parte degli utenti ☐ Sistema di registrazione (log) dell'accesso alle applicazioni o ai database da parte degli amministratori di sistema ☐ Sistema di registrazione (log) dell'accesso alle applicazioni da parte degli utenti ☐ Registrazione delle attività di inserimento, modifica o cancellazione di dati ☐ Profili di accesso a scanner, fotocopiatrici e stampanti di rete ☐ Meccanismi di cancellazione sicura dei dati (quali wiping program e formattazione a basso livello) per i dischi e le unità di memoria destinati a riutilizzo o smaltimento ☐ *Altro: specificare o inserire spazi*	

1.3.2	A tal fine vengono messe in atto le seguenti **misure organizzative**. ☐ Creazione di profili utente con autorizzazioni in base al ruolo e a compiti assegnati (Segregation of duty, need to know e least privilege) ☐ Procedure di autorizzazione documentate (richiesta, assegnazione, revoca delle autorizzazioni) ☐ Riesame regolare delle autorizzazioni ☐ Account con privilegi amministrativi individuali e utilizzati solo quando necessario ☐ Account individuali anche per i tecnici esterni che necessitano di credenziali amministrative ☐ Verifica delle caratteristiche soggettive di esperienza, capacità e affidabilità degli amministratori di sistema ☐ Elenco aggiornato degli amministratori di sistema, con il dettaglio dei compiti assegnati ☐ Verifica periodica delle attività degli amministratori di sistema ☐ Presidio, controllo e verifica delle attività degli interventi tecnici effettuati da personale esterno ☐ Distruzione dei supporti di memorizzazione destinati allo smaltimento ☐ Regole e policy su utilizzo di scanner, fotocopiatrici e stampanti di rete ☐ Utilizzo di tritadocumenti per la distruzione di documenti cartacei non più necessari ☐ Triturazione certificata dei documenti cartacei non più necessari ☐ *Altro: specificare o inserire spazi*	
1.**4**	**Pseudonimizzazione e cifratura** – Per i dati più critici è opportuno adottare ulteriori misure di sicurezza per evitare la comprensibilità e l'usabilità dei dati anche in caso di furto o accesso non autorizzato. **Requisito:** *Nei casi in cui il trattamento riguardi dati particolari o relativi a condanne penali o reati, nonché per i dispositivi a maggiore mobilità e quindi più soggetti a furti e smarrimenti, è opportuno applicare misure tecniche e organizzative per limitare la possibilità di utilizzo dai dati da parte di soggetti non autorizzati.*	[Selezionare]
1.4.1	A tal fine vengono messe in atto le seguenti **misure tecniche**. ☐ Sistemi di crittografia dei database ☐ Cifratura dei dischi dei server ☐ Cifratura dei dischi dei dispositivi ☐ Cifratura dei dati in cloud ☐ Cifratura dei supporti removibili ☐ Cifratura dei backup ☐ Cifratura delle memorie dei dispositivi mobili ☐ Nel caso di dati pseudonimizzati: separazione dei campi identificativi su sistemi separati protetti ☐ Abbreviazione dei record di dati per limitare le possibilità di identificazione (es. indirizzo IP) ☐ *Altro: specificare o inserire spazi*	
1.4.2	A tal fine vengono messe in atto le seguenti **misure organizzative**. ☐ Politiche di conservazione e gestione delle chiavi di cifratura ☐ Utilizzo di dati pseudonimizzati (codici) nelle fasi di trattamento in cui non è necessaria l'identificazione degli interessati ☐ Rimozione degli elementi identificativi degli interessati ove non necessari (fasi di sviluppo, rendicontazione, uso o comunicazione di dati aggregati) ☐ *Altro: specificare o inserire spazi*	

1.**5**	**Protezione dei dati durante la trasmissione** – È necessario garantire la sicurezza dei dati nella trasmissione tra sistemi, nel trasporto tra diverse sedi e nelle fasi di comunicazione. **Requisito:** *Nei casi di trasmissione di dati tra sistemi, di trasporto di dati tra diverse sedi e nei casi di comunicazione autorizzata a terze parti è necessario garantire la sicurezza dei canali di trasmissione. I canali di trasmissione elettronica devono essere sicuri, crittografati e garantiti. Va tutelata anche la sicurezza dei dati nel caso di trasporto e consegna di documenti cartacei.*	[Selezionare]
1.5.1	A tal fine vengono messe in atto le seguenti **misure tecniche**. ☐ Configurazione di tunnel VPN ☐ Crittografia delle e-mail ☐ Crittografia degli allegati ☐ Trasmissione di dati, documenti o allegati con password trasmessa su alto canale ☐ Utilizzo di https nei sistemi web based ☐ Protocolli TLS 1.2 o successivi su web server ☐ Crittografia delle reti WI-FI (almeno WPA2) ☐ Utilizzo di crittografia nei server ftp (FTPS o SFTP) ☐ Contenitori/involucri sicuri per la spedizione ☐ Istruzioni chiare riguardo ai destinatari autorizzati ☐ Altro: *Specificare misure previste*	
1.5.2	A tal fine vengono messe in atto le seguenti **misure organizzative**. ☐ Trasferimento dei dati in forma pseudonimizzata ☐ Elenchi dei destinatari autorizzati ☐ Regole e Istruzioni di trasferimento ai destinatari autorizzati ☐ Regole per il trasporto di documenti ☐ Verifica e controllo delle consegne ai destinatari autorizzati ☐ *Altro: specificare o inserire spazi*	
2	**Integrità**	
2.1	**Controllo delle modifiche –** Determinare se i dati personali sono stati inseriti, modificati o rimossi dai sistemi che trattano i dati e da chi. **Requisito:** *è necessario conservare la documentazione completa relativa alla gestione delle modifiche e alla manutenzione dei dati. Si devono garantire la tracciabilità e/o la documentazione del trattamento dei dati. Ove possibile è opportuno implementare misure tecniche che permettano la revisione successiva mediante sistemi di registrazione al fine di determinare i dettagli relativi all'immissione, alla modifica o alla rimozione di dati.*	[Selezionare]
2.1.1	A tal fine vengono messe in atto le seguenti **misure tecniche**. ☐ Registrazione (log) di inserimento, modifica, eliminazione dati dalle basi dati ☐ Sistemi di autorizzazione da parte di supervisori per la modifica o la cancellazione dei dati ☐ Avvisi di conferma(double-check) per la modifica o la cancellazione dei dati nelle applicazioni ☐ Altro: *Specificare misure previste*	

2.1.2	A tal fine vengono messe in atto le seguenti **misure organizzative**. ☐ Conservazione dei moduli cartacei da cui sono stati trasferiti i dati per il trattamento automatizzato ☐ Conservazione dei dati originali in caso di importazione da altre fonti ☐ Assegnazione di diritti separati per l'immissione, la modifica e la cancellazione di dati ☐ *Altro: specificare o inserire spazi*	
2.2	**Controllo dell'esattezza e dell'aggiornamento dei dati –** devono essere adottate tutte le misure ragionevoli per aggiornare, cancellare o rettificare tempestivamente i dati inesatti o obsoleti rispetto alle finalità per le quali sono trattati. **Requisito:** Il Responsabile è tenuto a monitorare per tutto il loro ciclo di vita i dati personali raccolti o gestiti, dal momento dell'acquisizione e fino alla loro cancellazione, mediante misure che limitino il più possibile la possibilità di errore	Not Applicable
2.2.1	A tal fine vengono messe in atto le seguenti **misure tecniche**. ☐ Applicazioni con campi predefiniti o sistemi di controllo nell'inserimento dei dati ☐ Sistemi di allineamento con altre banche dati / applicazioni ☐ Sistemi di aggiornamento automatico dei dati ☐ Sistemi di cancellazione automatica dei dati alla scadenza ☐ Altro: *Specificare misure previste*	
2.2.2	A tal fine vengono messe in atto le seguenti **misure organizzative**. ☐ Procedure di validazione dei dati ☐ Procedure di controllo periodico dell'esattezza dei dati inseriti nelle banche dati ☐ Procedure di controllo periodico dell'aggiornamento dei dati inseriti nelle banche dati ☐ Immediato aggiornamento / rettifica dei dati su tutti i sistemi in caso di segnalazione / rilevamento di errori o necessità di aggiornamento in uno specifico dataset ☐ Procedure – regole di data retention definite ☐ Cancellazione dei dati obsoleti ☐ *Altro: specificare o inserire spazi*	
3.	**Disponibilità e resilienza**	
3.1	**Sistemi di sicurezza nelle sale server -** Protezione da distruzione/perdita accidentale di dati e misure per la disponibilità dei servizi **Requisito:** *il Responsabile del trattamento è obbligato ad adottare le misure tecniche e organizzative per garantire la disponibilità dei dati. I dati devono essere protetti dalla distruzione o dalla perdita accidentale (ad esempio dovuta a blackout, incidenti o eventi naturali). In particolare le macchine e le sale server che le ospitano devono essere protette da influenze ambientali esterne e sabotaggi.*	[Selezionare]

3.1.1	A tal fine vengono messe in atto le seguenti **misure tecniche**. ☐ Estintori nelle sale server con estinguenti adatti ☐ Aria condizionata nelle sale server ☐ Dispositivi per il monitoraggio di temperatura e umidità nelle sale server ☐ Sistemi di rilevamento di fiamme e fumo ☐ Sistemi di controllo e alert per parametri server e dispostivi di rete (uptime, temperatura, carico, errori, anomalie ecc.) ☐ Sistemi automatic di spegnimento incendi ☐ Alimentazione elettrica ininterrotta (UPS e gruppi di continuità) ☐ Infrastruttura IT duale (ridondanza) ☐ Sistemi di protezione fisica per l'accesso alle sale server ☐ Sistemi di accesso alle sale server con smart card / pin / trasponder / identificatori biometrici ☐ Videosorveglianza delle sale server ☐ *Altro: specificare o inserire spazi*	
3.1.2	A tal fine vengono messe in atto le seguenti **misure organizzative**. ☐ Notifica di allarme in caso di accesso alle stanze server ☐ Notifica di allarme in caso di superamento dei parametri di temperatura/umidità/fumo ☐ Divieto di accesso al personale non autorizzato al perimetro fisico dell'infrastruttura del sistema IT ☐ Controllo dell'ubicazione delle sale server in relazione alle condutture idriche ☐ Le sale server si trovano ai piani rialzati se in una zona soggetta a inondazioni ☐ *Altro: specificare o inserire spazi*	
3.2	**Protezione della rete e dei dispositivi –** La rete, gli host e i dispostivi collegati in rete devono disporre di misure di protezione da attacchi di malintenzionati e da software malevolo. **Requisito:** *il Responsabile del trattamento è obbligato ad adottare le misure tecniche e organizzative per garantire la disponibilità (oltre alla riservatezza e l'integrità) dei dati trattati proteggendo la rete, i dispositivi e i dati conservati, elaborati o in transito, da effetti dovuti a software malevolo o attacchi di malintenzionati. I dati devono essere elaborati, trasmessi e conservati con strumenti la cui sicurezza è implementata secondo gli standard di settore*	[Selezionare]
3.2.1	A tal fine vengono messe in atto le seguenti **misure tecniche**. ☐ Protezione tramite sistemi firewall ☐ Appliance UTM (Unified Threat Management) ☐ Sistemi IDS, IPS o IDPS ☐ Sistemi NAC (Network Access Control) ☐ Sistemi DLP ☐ Sistemi SIEM ☐ DMZ per i servizi esposti ☐ WAF (Web Application Firewall) per i servizi esposti ☐ Software antimalware aggiornato a livello di rete ☐ Software antimalware aggiornato a livello di host ☐ Software antimalware aggiornato su tutti i dispostivi ☐ *Altro: specificare o inserire spazi*	

<table>
<tr><td>3.2.2</td><td colspan="2">A tal fine vengono messe in atto le seguenti misure organizzative.
<table>
<tr><td>☐</td><td>SOC (Security Operations Center)</td></tr>
<tr><td>☐</td><td>Servizi di MSS (Managed Security Services)</td></tr>
<tr><td>☐</td><td>Segmentazione delle reti</td></tr>
<tr><td>☐</td><td>Controllo e aggiornamento periodico delle policy dei firewall</td></tr>
<tr><td>☐</td><td>Analisi dei log e degli avvisi di sicurezza</td></tr>
<tr><td>☐</td><td>Test hardware su base regolare (ciclo di vita, prestazioni)</td></tr>
<tr><td>☐</td><td>Test di penetrazione su base regolare</td></tr>
<tr><td>☐</td><td>Regolamento / Disciplinare/ Policy sull’utilizzo della rete e degli strumenti informatici da parte degli utenti</td></tr>
<tr><td>☐</td><td>Formazione degli utenti in merito ad attacchi di phishing e social engineering</td></tr>
<tr><td>☐</td><td>Altro: specificare o inserire spazi</td></tr>
</table></td></tr>
<tr><td>3.3</td><td>Controllo delle disponibilità e controllo della recuperabilità – Salvataggio periodico dei dati e procedure per recuperare i dati il prima possibile.
Requisito: I dati devono essere conservati i più copie su reti/sistemi/sedi separate. Il Responsabile del trattamento deve mettere in atto una politica di backup e di ripristino che garantisce il recupero del sistema e dei dati.</td><td>[Selezionare]</td></tr>
<tr><td>3.3.1</td><td colspan="2">A tal fine vengono messe in atto le seguenti misure tecniche.
☐ Sistemi di backup automatizzato
☐ Sistemi di backup in cloud
☐ Sistemi di disaster recovery con infrastrutture proprie
☐ Sistemi di disaster recovery con piattaforme DRaaS in cloud
☐ Altro: specificare o inserire spazi</td></tr>
<tr><td>3.3.2</td><td colspan="2">A tal fine vengono messe in atto le seguenti misure organizzative.
☐ Contratti con i fornitori per la fornitura di hardware sostitutivo con tempi definiti (SLA)
☐ Piani di backup e di recovery del software, delle configurazioni e dei dati
☐ Procedure di continuità operativa
☐ Procedure di ripristino dei dati
☐ Test di ripristino periodici
☐ Esercitazioni di simulazione di crisi/emergenza su base regolare con prove di ripristino
☐ Altro: specificare o inserire spazi</td></tr>
<tr><td>3.4</td><td>Gestione e Controllo delle Risorse informatiche e del software: Il Responsabile del trattamento deve garantire la sicurezza dell’ambiente di trattamento e degli strumenti utilizzati.
Requisito: È necessaria una gestione globale e attiva (inventariare, abilitare, tracciare, aggiornare) di tutti gli strumenti utilizzati per il trattamento dei dati, compresi gli strumenti non direttamente attivi nel trattamento ma connessi alle reti o ai sistemi utilizzati per la conservazione, il transito o l’elaborazione dei dati. Questi comprendono i sistemi di rete, i sistemi di protezione, i sistemi server di elaborazione e archiviazione, i sistemi di comunicazione e trasmissione dei dati, i dispositivi dell’utente autorizzato, mobili e portatili inclusi, i dispositivi di rete, i dispositivi IoT connessi all’infrastruttura fisicamente, virtualmente, in remoto e quelli in ambienti cloud, per conoscere con precisione la totalità delle risorse che devono essere monitorate e protette.
Parimenti è necessario gestire attivamente (inventariare, tracciare e aggiornare) tutto il software (sistemi operativi e applicazioni) sulla rete in modo che solo il software autorizzato possa essere installato ed eseguito, adottando politiche o misure per impedire l’istallazione o l’esecuzione di software non autorizzato</td><td>[Selezionare]</td></tr>
</table>

3.4.1	A tal fine vengono messe in atto le seguenti **misure tecniche**. ☐ Strumenti di rilevamento attivo delle risorse connesse alla/e rete/i ☐ Strumenti di rilevamento passivo delle risorse connesse alla/e rete/i ☐ Strumenti di inventario dei dispositivi ad alimentazione manuale ☐ Strumenti automatici di rilevamento dei software utilizzati a livello di rete ☐ Strumenti di inventario dei software installati ad alimentazione manuale ☐ Sistemi di aggiornamento automatico del software ☐ Vulnerability assessment periodici ☐ Altro: *Specificare misure previste*	
3.4.2	A tal fine vengono messe in atto le seguenti **misure organizzative**. ☐ Inventario accurato, dettagliato e aggiornato di tutte le risorse aziendali con la possibilità di archiviazione o elaborazione dati ☐ Procedure per la gestione delle risorse non autorizzate (rimozione, blocco, quarantena) ☐ Inventario accurato, dettagliato e aggiornato di tutti software utilizzati a livello aziendale ☐ Registrazione e monitoraggio di tutte le modifiche alle configurazioni di risorse, apparati e sistemi IT ☐ Procedure per l'aggiornamento e l'applicazione delle correzioni di sicurezza nei software ☐ Verifica periodica dei bollettini di sicurezza per le vulnerabilità rilevate ☐ Altro: *Specificare misure previste*	
4	**Politiche e procedure per la gestione della tutela dei dati personali, per l'esame periodico del sistema di trattamento, per la valutazione e per la verifica su base regolare, nonché per l'assistenza al Titolare del trattamento**	
4.1	**Politiche di protezione dei dati personali** **Requisito:** *Il Responsabile del trattamento deve implementare un proprio sistema di tutela dei dati personali.* *Gli elementi includono:* – *Una struttura organizzativa vigente per la protezione dei dati con responsabilità definite (incluso la nomina di un responsabile della protezione dei dati, qualora richiesto a livello legale)* – *Conformità a tutti i requisiti legali per la protezione dei dati personali* – *Sistema di gestione dei contratti vigenti per la conservazione di tutti gli accordi relativi alla protezione dei dati (es. accordi per il trattamento dei dati, accordi con sub-responsabili del trattamento ecc.)* – *Formazione sulla tutela dei dati personali per i dipendenti del Responsabile del trattamento che trattano i dati personali del Titolare del trattamento* – *Accordi sulla riservatezza dei dati personali per i dipendenti del Responsabile del trattamento che trattano i dati personali del Titolare del trattamento* – *Una procedura che garantisce i diritti dei soggetti interessati (in cooperazione con il Titolare del trattamento)* – *L'adozione di certificazioni sulla sicurezza dei dati e l'adesione a codici di condotta possono essere validi strumenti di controllo delle politiche di protezione*	[Selezionare]

4.1.1	A tal fine vengono messe in atto le seguenti **misure organizzative**. ☐ Registro del trattamento in qualità di responsabile ☐ Analisi dei rischi che incombono sugli interessati in relazione ai trattamenti effettuati ☐ Nomina di un responsabile della protezione dei dati (se richiesto a livello legale) ☐ Adozione di un sistema di gestione o di un Modello Organizzativo per la tutala dei dati personali ☐ Adesione a codici di condotta in relazione al trattamento di dati personali ☐ Certificazioni relative alla sicurezza dei dati (es. ISO/IEC 27001 e 27701) ☐ Contratti con i fornitori che svolgono parte dei trattamenti affidati (sub-responsabili) che prevedono meccanismi di tutela dei dati personali e relativi accordi di riservatezza ☐ Piano di formazione del personale in relazione alla tutela dei dati personali ☐ Autorizzazione formale al personale incaricato del trattamento dei dati personali affidati ☐ Adozione di un accordo di riservatezza per il personale a cui è affidato il trattamento ☐ Procedura per la risposta alle richieste di esercizio dei diritti degli interessati ☐ Registrazione delle richieste di esercizio dei diritti degli interessati ☐ *Altro: specificare o inserire spazi*	
4.2	**Gestione delle risposte agli incidenti che possono comportare violazioni dei dati personali / data breach** **Requisito:** *Il Responsabile del trattamento deve implementare un proprio sistema di gestione degli incidenti e delle violazioni dei dati personali (cd. Data breach).* *Gli elementi includono:* – *Un processo per segnalare violazioni della protezione dei dati personali (in particolare in cooperazione con il Titolare del trattamento)* – *Una procedura per la gestione degli incidenti che possono comportare violazioni dei dati personali*	[Selezionare]
4.2.1	A tal fine vengono messe in atto le seguenti **misure organizzative**. ☐ Procedura per la risposta ad incidenti di sicurezza ☐ Procedura per la gestione e la notifica delle violazioni dei dati (data breach) ☐ Adozione di un registro dei data breach ☐ Assegnazione dei ruoli di valutazione degli incidenti di sicurezza ☐ Procedure o meccanismi di risposta agli incidenti di sicurezza, comprensivi dell'assegnazione di compiti e ruoli ☐ Regole o procedure di segnalazione delle anomalie o degli incidenti di sicurezza da parte degli utenti ☐ *Altro: specificare o inserire spazi*	
4.3	**Protezione dei dati by design e by default** **Requisito:** *il Responsabile del trattamento è obbligato a mettere in atto misure tecniche e organizzative nelle fasi iniziali della progettazione delle operazioni del trattamento, in modo da rispettare i principi della privacy e della protezione dei dati fin dall'inizio. Inoltre, il Responsabile del trattamento deve garantire che i dati personali vengano trattati con il massimo livello di protezione, in modo che i dati personali non siano accessibili a un numero indefinito di persone by default.*	[Selezionare]

4.3.1	A tal fine vengono messe in atto le seguenti **misure organizzative**. ☐ Procedura di privacy by design e by default ☐ Adozione di controlli preventivi per la minimizzazione dei dati in fase di raccolta ☐ Adozione di controlli preventivi per la minimizzazione dei dati in fase di elaborazione ☐ Adozione di controlli preventivi per la minimizzazione dei dati in fase di comunicazione ☐ Controllo delle caratteristiche di sicurezza e funzionalità nella tutela dei dati in fase di adozione di nuovi software ☐ Valutazione delle esigenze di tutela dei dati (comprese valutazioni su necessità, riduzione al minimo dei dati utilizzati, valutazione della necessità di pseudonimizzazione o di adozione di altre misure sicurezza) per ogni fase del flusso di dati necessaria all'attività delegata ☐ Altro: *Specificare misure previste*	
4.4	**Procedure di controllo** **Requisito:** *il Responsabile deve mettere in atto politiche e procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento*.	[Selezionare]
4.4.1	A tal fine vengono messe in atto le seguenti **misure organizzative**. ☐ Revisione periodica del sistema di trattamento dati e delle misure di sicurezza implementate ☐ Audit interni periodici documentati ☐ Audit del Responsabile della Protezione dei Dati (DPO) periodici documentati ☐ Audit di seconda parte documentati ☐ Audit di terza parte (es. come parte di procedure di certificazione o revisione di certificazioni) ☐ Altro: *Altro: specificare o inserire spazi*	
4.5	**Assistenza al Titolare del trattamento** **Requisito**: *Il Responsabile del trattamento ha l'obbligo di fornire assistenza al Titolare tenendo conto della natura del trattamento. Tale obbligo di assistenza riguarda anche gli eventuali sub-responsabili ove presenti e ove necessario.*	[Selezionare]
4.5.1	Se per l'assistenza vengono implementate specifiche misure tecniche e organizzative ulteriori rispetto a quelle indicate nel presente allegato, elencarle di seguito: ☐ ☐ ☐ ☐ ☐ ☐	

Qualora il fornitore si avvalga di (sub-)responsabili del trattamento specificare la ragione sociale, la sede legale e il servizio svolto:

RAGIONE SOCIALE	SEDE LEGALE	SERVIZIO SVOLTO