Allegato 1	**ELENCO SUB-RESPONSABILI** **MD14_PGT01_0_Allegato_Elenco_SubResponsabili**
Trattamento Dati	Servizi Tributari Prodotto: **TRIBOX** Erogazione: **SaaS**

Sezione Valida per l'erogazione delle soluzioni Municipia
Ad integrazione di quanto specificato nell'offerta e/o nel contratto principale relativamente ai fornitori che tratteranno dati per conto di Titolare/Responsabile/Sub-Responsabile come ulteriori sub-responsabili del trattamento, e che si intendono dal Titolare/Responsabile già autorizzati conl'accettazione dell'offerta, il Titolare/Responsabile autorizza il Sub-Responsabile ad affidare parte delle operazioni di trattamento ai seguenti ulteriori sub-responsabili:

Di seguito è riportato l'elenco dei sub-responsabili per le varie soluzioni Municipia.

Il trattamento oggetto del contratto è riferito al prodotto indicato sopra nella fascia arancione.

Paese cui è stabilito Sub-Responsabile	**Sub-Responsabili**	**Dati di contatto**	**Attività di trattamento affidata**	**Per il sub-responsabile indicato nella colonna sotto sono indicati i prodotti interessati.**
Italia	D-HUB Gruppo Engineering	info.dhub@eng.it	Service Provider (CSP qualificato AGID)	TRIBOX – GEIS – MERCURIO – GERI / STARS ARGO - GNOSIS
Lussemburgo	Amazon Web Services EMEA SARL	https://aws.amazon.com/it/contact-us/	Service Provider (CSP qualificato AGID)	MUNIPAY

Qualora Municipia intenda affidare ad un ulteriore sub-responsabile trattamenti 'diversi' rispetto a quelli indicati in tabella e/o nell'offerta e/o nel contratto principale, o ingaggiare altri sub-responsabili diversi da quelli comunicati, dovrà provvedere a comunicare tali variazioni.

Allegato Z	CARATTERISTICHE DEL TRATTAMENTO E MISURE TECNICHE E ORGANIZZATIVE MD15_PG101_0_Allegato_CaratteristicheTrattamento_Dati
Trattamento Dati	Servizi Tributari Prodotto: TRIBOX Erogazione: SaaS

Di seguito è riportato l'elenco delle varie soluzioni Municipia con l'indicazione delle caratteristiche del trattamento e le misure tecniche organizzative.

Il trattamento oggetto del contratto è riferito al prodotto indicato sopra nella fascia arancione.

ARGO è un Citizen Relation Management System, composto dai seguenti moduli:
- Front-End Cittadino: permette al cittadino la consultazione della propria situazione debitoria nei confronti dell'ente;
- Agenda: permette la gestione degli appuntamenti tra Cittadino ed Operatori preposti;
- Gestione Ticket: supporto al cittadino;

GEIS offre un supporto al comune per la riscossione e la gestione dell'imposta di soggiorno. Lato operatore fornisce un sistema per gestire le strutture, i gestori/rappresentanti legali, inserire dichiarazioni e versamenti, generazione di report. Lato gestore permette l'inserimento delle dichiarazioni e la gestione del bollettario elettronico.

TRIBOX è un Gestionale Tributi. È alimentato da fonti esterne eterogenee (catasto, demografici, SIATEL, 290, ecc), offre funzionalità puntuali e massive sulla situazione contributiva dei soggetti censiti nella banca dati dell'ente, relativamente ai tributi trattati.

GERI per il servizio di riscossione

STARS per il servizio starlight che supporta l'Ente nell'esame dei crediti affidati in riscossione all'Agente Nazionale

GNOSIS è lo strumento software realizzato da Municipia a supporto del servizio di ricerca evasione TARI/IMU.

MERCURIO è uno strumento con funzione di spedizioniere. È in grado di recepire documenti da inviare attraverso diversi canali (export SIN, PEC, e-mail e notifiche AppIO. All'atto della spedizione è in grado di reperire informazioni PEC da Registro Imprese.

MUNIPAY è la soluzione di Municipia completa e modulare che supporta l'Ente nell'interazione con il mondo PagoPA.

DETTAGLI DEL TRATTAMENTO

- Application Maintenance Management
- Customer Support
- Sviluppo Prodotto

CATEGORIE DI INTERESSATI

Categoria interessati	Prodotti
Cittadini e contribuenti	TUTTI I PRODOTTI

TIPOLOGIA DI DATI PERSONALI TRATTATI DA MUNICIPA

Dati Personali	Prodotti

Dati Personali Comuni (es. dati anagrafici, di contatto, relativi all'istruzione, stato civile/familiare, esperienza professionale)	TUTTI I PRODOTTI
Dati Finanziari (es. reddito, transazioni finanziarie, investimenti, carte di credito, fatture, ecc.)	TUTTI I PRODOTTI

CARATTERISTICHE DEL TRATTAMENTO

1. Full Outsourcing
   (per l'erogazione SaaS)

2. Traditional On-Premises IT - trattamento on site presso il Titolare con devices (laptop, desktop, ecc.) forniti dal Titolare/Cliente
   (per erogazione On-Premises)

MISURE DI SICUREZZA

Municipia e i suoi ulteriori Sub-Responsabili adotteranno le seguenti misure di sicurezza al fine di garantire un livello di sicurezza adeguato al rischio relativo alle attività che ricadono nella loro diretta responsabilità.

Il Cliente, in considerazione dei rischi associati al Trattamento dei Dati Personali, conferma che le Misure di Sicurezza adottate da Municipia e i suoi ulteriori Sub-Responsabili sono idonee a fornire un adeguato livello di protezione dei Dati Personali trattati per conto dello stesso.

Nel caso in cui il Cliente operasse per conto di un Titolare terzo, il Cliente si riserverà di integrare e/o modificare le misuredi sicurezza come richiesto dallo stesso Titolare.

Municipia potrà modificare le misure di sicurezza, anche integrandole, con le istruzioni previste nell'accordo per il trattamento dei dati sottoscritto con il Cliente.

Risk Level	Categoria	ID	Descrizione	Geis ARGO MuniPay	Tribox Gnosis Mercurio	GERI STARS
B	**Security Policy e procedure per la protezione dei dati personali**	**A.1**	L'organizzazione documenta la propria politica in merito all'elaborazione dei dati personali come parte della sua politica di sicurezza delle informazioni.	X	X	X
B	**Security Policy e procedure per la protezione dei dati personali**	**A.2**	La politica di sicurezza è riesaminata e aggiornata, se necessario, su base annuale.	X	X	X
M	**Security Policy e procedure per la protezione dei dati personali**	**A.3**	L'organizzazione documenta una politica di sicurezza dedicata separata per quanto riguarda il trattamento dei dati personali. La politica approvata dalla Direzione e comunicata a tutti i dipendenti e alle parti esterne interessate.	N/A	X	X
M	**Security Policy e procedure per la protezione dei dati personali**	**A.4**	La politica di sicurezza fa riferimento a: i ruoli e le responsabilità del personale, le misure tecniche e organizzative di base adottate per la sicurezza dei dati personali, per i responsabili del trattamento dei dati o per le altre terze parti coinvolte nel trattamento dei dati personali.	N/A	X	X
M	**Security Policy e procedure per la protezione dei dati personali**	**A.5**	È creato e mantenuto un inventario di politiche / procedure specifiche relative alla sicurezza dei dati personali, basato sulla politica generale di sicurezza.	N/A	X	X
B	**Ruoli e responsabilità**	**B.1**	I ruoli e le responsabilità relativi al trattamento dei dati personali sono chiaramente definiti e assegnati in conformità con la politica di sicurezza.	X	X	X
B	**Ruoli e responsabilità**	**B.2**	Durante le riorganizzazioni interne o le cessazioni e il cambio di impiego, sono chiaramente definite le modalità di revoca dei diritti e delle responsabilità con le rispettive procedure di passaggio di consegne.	X	X	X

Risk Level	Categoria	ID	Descrizione	Geis ARGO MuniPay	Tribox Gnosis Mercurio	GERI STARS
M	**Ruoli e responsabilità**	**B.3**	È effettuata una chiara individuazione e designazione delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.	N/A	X	X
A	**Ruoli e responsabilità**	**B.4**	Il responsabile della sicurezza nominato formalmente (in modo documentato). Anche i compiti e le responsabilità del responsabile della sicurezza sono chiaramente definiti e documentati.	N/A	N/A	
A	**Ruoli e responsabilità**	**B.5**	Doveri e aree di responsabilità che possono essere in conflitto, ad esempio i ruoli di responsabile della sicurezza, auditor e DPO, sono considerati separati per ridurre le opportunità di modifiche non autorizzate o non intenzionali o di uso improprio di dati personali.	N/A	N/A	
B	**Policy per il controllo degli accessi**	**C.1**	I diritti specifici di controllo dell'accesso sono assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio di necessità e di pertinenza.	X	X	X
M	**Policy per il controllo degli accessi**	**C.2**	Una politica di controllo degli accessi dettagliata e documentata. L'organizzazione dovrebbe determinare in questo documento le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti nel contesto dei processi e delle procedure relative ai dati personali.	N/A	X	X
M	**Policy per il controllo degli accessi**	**C.3**	La segregazione dei ruoli per gestire il controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, gestione degli accessi) è chiaramente definita e documentata.	N/A	X	X
A	**Policy per il controllo degli accessi**	**C.4**	I ruoli con diritti di accesso privilegiato sono chiaramente definiti e assegnati limitatamente a membri specifici dello staff.	N/A	N/A	
B	**Gestione degli asset/risorse**	**D.1**	L'organizzazione dispone di un registro delle risorse IT utilizzate per il trattamento dei dati personali (hardware, software e rete). Il registro potrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. server, workstation), posizione (fisica o elettronica). Ad una persona specifica è assegnato il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).	X	X	X
B	**Gestione degli asset/risorse**	**D.2**	Le risorse IT sono riesaminate e aggiornate regolarmente.	X	X	X
M	**Gestione degli asset/risorse**	**D.3**	I ruoli che hanno accesso a determinate risorse sono definiti e documentati.	N/A	X	X
A	**Gestione degli asset/risorse**	**D.4**	Le risorse IT sono riesaminate e aggiornate su base annuale.	N/A	N/A	
B	**Gestione del cambiamento**	**E.1**	L'organizzazione deve assicurarsi che tutte le modifiche al sistema IT siano registrate e monitorate da una persona specifica (ad esempio, responsabile IT o sicurezza). Questo processo è monitorato regolarmente.	X	X	
B	**Gestione del cambiamento**	**E.2**	Lo sviluppo del software è eseguito in un ambiente speciale, non collegato al sistema IT utilizzato per il trattamento dei dati personali.	X	X	X

Risk Level	Categoria	ID	Descrizione	Geis ARGO MuniPay	Tribox Gnosis Mercurio	GERI STARS
			Quando è necessario eseguire I test, sono utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non è possibile, sono previste procedure specifiche per la protezione dei dati personali utilizzati nei test.			
M	**Gestione del cambiamento**	**E.3**	È presente una politica dettagliata e documentata di gestione dei cambiamenti. Dovrebbe includere: un processo per l'introduzione dei cambiamenti, i ruoli / utenti che hanno i diritti di cambiamento, le tempistiche per l'introduzione dei cambiamenti. La politica di gestione dei cambiamenti regolarmente aggiornata.	N/A	X	X
B	**Gestione degli incidenti / Data Breaches**	**G.2**	Le violazioni dei dati personali sono segnalate immediatamente alla Direzione. Sono in atto procedure di notifica per la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi dell'art. 33 e 34 GDPR.	X	X	
A	**Gestione degli incidenti / Data Breaches**	**G.4**	Gli incidenti e le violazioni dei dati personali sono registrati insieme ai dettagli riguardanti l'evento e le successive azioni di mitigazione eseguite.	N/A	N/A	
B	**Business Continuity**	**H.1**	L'organizzazione dovrebbe stabilire le procedure e i controlli principali da seguire al fine di garantire il livello richiesto di continuità e disponibilità del sistema informatico che elabora i dati personali (in caso di incidente / violazione dei dati personali).	X	X	
M	**Business Continuity**	**H.2**	Un BCP dettagliato e documentato (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.	N/A	X	
M	**Business Continuity**	**H.3**	Un livello di qualità del servizio garantito definito nel BCP per i processi aziendali fondamentali che prevedono la sicurezza dei dati personali.	N/A	X	
A	**Business Continuity**	**H.5**	Si prende in considerazione una struttura alternativa, a seconda dell'organizzazione e dei tempi di inattività accettabili del sistema IT.		N/A	
B	**Riservatezza del personale**	**I.1**	L'organizzazione garantisce che tutto il personale comprenda le proprie responsabilità e gli obblighi relativi al trattamento dei dati personali. I ruoli e le responsabilità sono chiaramente comunicati durante il processo di pre-assunzione e / o inserimento.	X	X	X
M	**Riservatezza del personale**	**I.2**	Prima di assumere i propri compiti, il personale è invitato a riesaminare e concordare la politica di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e di non divulgazione.	N/A	X	X
B	**Formazione**	**J.1**	L'organizzazione garantisce che tutto il personale sia adeguatamente informato sui controlli di sicurezza del sistema informatico relativi al suo lavoro quotidiano. Il personale coinvolto nel trattamento dei dati personali dovrebbe inoltre essere adeguatamente informato in merito ai requisiti in materia di protezione dei dati e agli obblighi legali attraverso regolari campagne di sensibilizzazione.	X	X	X

Risk Level	Categoria	ID	Descrizione	Geis ARGO MuniPay	Tribox Gnosis Mercurio	GERI STARS
M	**Formazione**	**J.2**	L'organizzazione dispone di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici (relativi alla protezione dei dati personali) per l'inserimento dei nuovi arrivati.	N/A	X	X
B	**Controllo degli accessi ed autenticazione**	**K.1**	È attuato un sistema di controllo accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, il riesame e l'eliminazione degli account degli utenti.	X	X	X
B	**Controllo degli accessi ed autenticazione**	**K.2**	L'uso di account generici (non personali) è evitato. Nei casi in cui ciò è necessario, è necessario garantire che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità.	X	X	X
B	**Controllo degli accessi ed autenticazione**	**K.3**	È presente un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sul sistema di controllo degli accessi). Come minimo è utilizzata una combinazione di user-id e password. Le password dovrebbero rispettare un certo livello (configurabile) di complessità.	X	X	X
B	**Controllo degli accessi ed autenticazione**	**K.4**	Il sistema di controllo degli accessi è in grado di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile).	X	X	X
M	**Controllo degli accessi ed autenticazione**	**K.5**	Una politica specifica per la password è definita e documentata. La politica deve includere almeno la lunghezza della password, la complessità, il periodo di validità e il numero di tentativi di accesso non riusciti accettabili.	N/A	X	X
M	**Controllo degli accessi ed autenticazione**	**K.6**	Le password degli utenti sono archiviate in formato "hash".	N/A	X	X
B	**Logging e monitoraggio**	**L.1**	I log sono attivati per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).	X	X	X
B	**Logging e monitoraggio**	**L.2**	I log sono registrati con marcatura temporale (timestamp) e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi sono sincronizzati con un'unica fonte temporale di riferimento.	X	X	
M	**Logging e monitoraggio**	**L.3**	È necessario registrare le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / eliminazione / modifica dei diritti di accesso degli utenti.	N/A	X	X
M	**Logging e monitoraggio**	**L.4**	Non c'è alcuna possibilità di cancellazione o modifica del contenuto dei log. Anche l'accesso ai log è registrato oltre al monitoraggio per rilevare attività insolite.	N/A	X	
M	**Logging e monitoraggio**	**L.5**	Un sistema di monitoraggio elabora i log e produce rapporti sullo stato del sistema e notificare potenziali allarmi.			X
B	**Server/Database security**	**M.1**	I database e application server sono configurati affinché lavorino con un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.	X	X	

Risk Level	Categoria	ID	Descrizione	Geis ARGO MuniPay	Tribox Gnosis Mercurio	GERI STARS
B	**Sicurezza desktop/laptop/mobile**	**N.1**	Gli utenti non sono in grado di disattivare o aggirare le impostazioni di sicurezza.			X
B	**Sicurezza desktop/laptop/mobile**	**N.2**	Le applicazioni anti-virus e le relative signatures sono configurate su base settimanale.	X	X	X
B	**Sicurezza desktop/laptop/mobile**	**N.3**	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.			X
B	**Sicurezza desktop/laptop/mobile**	**N.4**	Il sistema dovrebbe avere timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.	X	X	X
B	**Sicurezza desktop/laptop/mobile**	**N.5**	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema sono installati regolarmente.	X	X	X
M	**Sicurezza desktop/laptop/mobile**	**N.6**	Le applicazioni antivirus e le signature sono configurate su base giornaliera.	N/A	X	X
B	**Network/Communication security**	**O.1**	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione è crittografata tramite protocolli crittografici (TLS / SSL).	X	X	
M	**Network/Communication security**	**O.2**	L'accesso wireless al sistema IT è consentito solo a utenti e processi specifici. È protetto da meccanismi di crittografia.	N/A	X	
M	**Network/Communication security**	**O.4**	Il traffico da e verso il sistema IT è monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni.			X
B	**Back-ups**	**P.1**	Le procedure di backup e ripristino dei dati sono definite, documentate e chiaramente collegate a ruoli e responsabilità.	X	X	X
B	**Back-ups**	**P.2**	Ai backup assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.	X	X	X
B	**Back-ups**	**P.3**	L'esecuzione dei backup monitorata per garantire la completezza.	X	X	X
B	**Back-ups**	**P.4**	I backup completi sono eseguiti regolarmente.	X	X	X
M	**Back-ups**	**P.5**	I supporti di backup sono testati regolarmente per assicurarsi che possano essere utilizzati.	N/A	X	X
M	**Back-ups**	**P.6**	I backup incrementali programmati sono eseguiti almeno su base giornaliera.	N/A	X	X
M	**Back-ups**	**P.7**	Le copie del backup sono conservate in modo sicuro in luoghi diversi dai dati di origine.	N/A	X	X
B	**Sicurezza del ciclo di vita del software**	**R.1**	Durante il ciclo di vita dello sviluppo si seguono le migliori pratiche, lo stato dell'arte e pratiche, framework o standard di sicurezza ben noti.			X
B	**Sicurezza del ciclo di vita del software**	**R.2**	Specifici requisiti di sicurezza sono definiti durante le prime fasi del ciclo di vita dello sviluppo.			X

Risk Level	Categoria	ID	Descrizione	Geis ARGO MuniPay	Tribox Gnosis Mercurio	GERI STARS
B	**Sicurezza del ciclo di vita del software**	**R.3**	Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET Privacy Enhancer Technologies)) sono adottate in analogia con i requisiti di sicurezza.			X
B	**Sicurezza del ciclo di vita del software**	**R.4**	Sono seguiti standard e pratiche di codifica sicure.	X	X	X
B	**Sicurezza del ciclo di vita del software**	**R.5**	Durante lo sviluppo, sono eseguiti test e convalida rispetto all'implementazione dei requisiti di sicurezza iniziali.			X
M	**Sicurezza del ciclo di vita del software**	**R.6**	I vulnerability assessment, i penetration test applicativi e dell'infrastruttura sono eseguiti da una terza parte fidata prima del passaggio in ambiente di produzione. Il passaggio non può avvenire a meno che non sia raggiunto il livello di sicurezza richiesto.	N/A	X	X
M	**Sicurezza del ciclo di vita del software**	**R.7**	Sono eseguiti penetration test periodici.	N/A	X	X
M	**Sicurezza del ciclo di vita del software**	**R.8**	Si ottengono informazioni sulle vulnerabilità tecniche dei sistemi IT utilizzati.	N/A	X	X
M	**Sicurezza del ciclo di vita del software**	**R.9**	Le patch software sono testate e valutate prima di essere installate in ambiente di produzione.	N/A	X	X
B	**Sicurezza fisica**	**T.1**	Il perimetro fisico dell'infrastruttura IT non accessibile da personale non autorizzato.	X	X	X
M	**Sicurezza fisica** (solo per Cloud SaaS)	**T.2**	L'identificazione chiara, tramite mezzi appropriati, ad es. badge identificativi, per tutto il personale e i visitatori che accedono ai locali dell'organizzazione, stabilita, a seconda dei casi.	N/A	X	X
M	**Sicurezza fisica** (solo per Cloud SaaS)	**T.3**	Le zone sicure sono definite e protette da appropriati controlli di accesso. Un registro fisico o una traccia elettronica di controllo di tutti gli accessi sono mantenuti e monitorati in modo sicuro	N/A	X	X
M	**Sicurezza fisica** (solo per Cloud SaaS)	**T.4**	I sistemi di rilevamento anti-intrusione sono installati in tutte le zone di sicurezza.	N/A	X	X
M	**Sicurezza fisica** (solo per Cloud SaaS)	**T.5**	Le barriere fisiche sono costruite per impedire l'accesso fisico non autorizzato.	N/A	X	X
M	**Sicurezza fisica** (solo per Cloud SaaS)	**T.6**	Le aree non usate sono fisicamente bloccate e periodicamente riesaminate.	N/A	X	X
M	**Sicurezza fisica** (solo per Cloud SaaS)	**T.7**	Un sistema antincendio automatico, un sistema di climatizzazione dedicato e chiuso e un gruppo di continuità (UPS) sono usati nella sala server.	N/A	X	X
M	**Sicurezza fisica** (solo per Cloud SaaS)	**T.8**	Il personale di supporto esterno ha accesso limitato alle aree protette.	N/A	X	X

Allegato 3	SCHEDA EVENTO DATA BREACH MD16_PGT01_0_Allegato_Scheda_Evento_Data_Breach

Denominazione della Banca Dati oggetto di incidente e breve descrizione della violazione

_____

_____

Quando si è verificata la violazione dei dati personali nell'ambito della Banca dati?

☐ il __/__/____

☐ tra il __/__/____ e __/__/____

☐ in un periodo non ancora determinato

☐ È possibile sia ancora in corso

Dove è avvenuta la violazione?

(specificare se avvenuta a seguito di smarrimento dispositivo o di supporto portatile)

_____

_____

Tipo Violazione

☐ Riservatezza (divulgazione dei dati, accesso agli stessi non autorizzati o accidentali)

☐ Integrità (modifica non autorizzata o accidentale dei dati)

☐ Disponibilità (perdita, accesso o distruzione accidentali o non autorizzati di dati)

☐ Lettura (i dati probabilmente non sono stati copiati)

☐ Copia (i dati sono ancora presenti sui sistemi del Titolare)

☐ Alterazione (i dati sono presenti nei sistemi ma sono stati alterati)

☐ Cancellazione (i dati non sono più nella disponibilità del Titolare o di terzi)

☐ Furto

☐ Altro:

_____

_____

Dispositivo oggetto della violazione

☐ Computer

☐ Rete

☐ Dispositivo mobile

☐ Strumento di Backup

☐ Documento Cartaceo

☐ Altro:

_____

_____

Sintetica descrizione dei sistemi di elaborazione e/o memorizzazione dati coinvolti

_____

_____

Ubicazione: _____

Quante persone sono state colpite dalla violazione

☐ N°_____ persone

☐ Circa _____

☐ N° non ancora conosciuto

Tipologia Dati Oggetto Di Violazione

☐ Dati anagrafici

☐ Dati di accesso/ identificazione

☐ Dati relativi a minori

☐ Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche ecc.

☐ Dati personali idonei a rivelare lo stato di salute e la vita sessuale

☐ Dati Giudiziari

☐ Copia immagini documenti digitali

☐ Ancora sconosciuto

☐ Altro

Misure tecniche ed organizzative applicate ai dati oggetto di violazione

(indicare le misure di sicurezza implementate prima del verificarsi dell'evento che dovrebbero coincidere con quelle riportate nell'apposito accordo per il trattamento dei dati)

_____

_____

Quali misure tecnologiche ed organizzative sono state assunte o saranno assunte per contenere la violazione dei dati e/o prevenire simili violazioni

(indicare le misure di sicurezza adottate per arginare gli effetti della violazione e/o impedirne il perpetrarsi o il ripersi della stessa)

_____

_____