PROTEZIONE DATI PERSONALI

In conformità a quanto previsto dal Regolamento 2016/679/UE (di seguito anche solo "Regolamento UE"), tutti i dati personali che verranno scambiati fra le Parti nel corso dello svolgimento del Contratto saranno trattati rispettivamente da ciascuna delle Parti per le sole finalità indicate nel Contratto ed in modo strumentale all'espletamento dello stesso, nonché per adempiere ad eventuali obblighi di legge, della normativa comunitaria e/o prescrizioni del Garante per la protezione dei dati personali e saranno trattati, con modalità manuali e/o automatizzate, secondo principi di liceità e correttezza ed in modo da tutelare la riservatezza e i diritti riconosciuti, nel rispetto di adeguate misure di sicurezza e di protezione dei dati anche sensibili o idonei a rivelare lo stato di salute, previsti dal Codice Privacy e dal Regolamento UE.

Ciascuna Parte riconosce ed accetta che i dati personali relativi all'altra Parte, nonché i dati personali (es. nominativi, indirizzo email aziendale, ecc.) di propri dipendenti/collaboratori, coinvolti nelle attività di cui al presente Contratto, saranno trattati dall'altra Parte in qualità di Titolare per finalità strettamente funzionali alla instaurazione e all'esecuzione del Contratto stesso ed in conformità con l'informativa resa da ognuna ai sensi e per gli effetti di cui all'articolo 13 del GDPR , che l'altra Parte si impegna sin da ora a portare a conoscenza dei propri dipendenti/collaboratori, nell'ambito delle proprie procedure interne.

L'informativa del Fornitore, che deve essere portata alla conoscenza dei dipendenti/collaboratori dell'altra Parte è reperibile nella sezione "Privacy Policy "del sito **WWW.MUNICIPIA.ENG.IT.**

Per l'esecuzione del Contratto Municipia tratterà i dati in qualità di Responsabile del Trattamento a norma dell'art. 28 del Regolamento UE attenendosi a quanto riportato alla voce "Accordo Trattamento Dati Personali" del presente Contratto. Allo stesso modo, ove dalle dinamiche di esecuzione del Contratto emergesse una forma di contitolarità dei trattamenti di dati personali di terzi da parte di entrambe le Parti, queste ultime si impegnano a sottoscrivere, senza alcun onere aggiunto per alcuna Parte, un accordo di contitolarità a norma dell'art. 26 del Regolamento UE da allegarsi al presente Contratto e a rispettare gli obblighi di informativa verso gli interessati. Ciascuna Parte dichiara di essere a conoscenza della normativa prevista dall'art. 24-bis del D.L. 83/2012 e dalla delibera n. 666/08/CONS, relativa agli obblighi di iscrizione al Registro degli Operatori di Comunicazione degli operatori economici che svolgono attività di call center nonché dei soggetti terzi affidatari dei servizi di call center e ciascuna Parte dichiara altresì di aver adempiuto agli obblighi ivi previsti, se e in quanto applicabili al caso di specie, anche con riferimento all'obbligo di comunicare all'utente chiamante o chiamato il Paese dal quale si risponde. In caso di effettuazione di chiamate verso numerazioni italiane, ciascuna Parte si impegna a rispettare, per quanto di propria competenza e in quanto applicabile, tutta la normativa vigente e applicabile in ogni momento e anche in futuro in Italia in materia di contatti a distanza per fini promozionali, di vendita diretta, di attività promozionali e ricerche di mercato, in particolare la legge 11 gennaio 2018, n. 5 e quanto previsto dai commi 3-bis, 3-ter, 3-quater dell'articolo 130 del Codice Privacy, dal D.P.R. 178/2010 e dal Provvedimento Generale del Garante per la protezione dei dati personali del 19 gennaio 2011, in materia di prescrizioni per il trattamento di dati personali per finalità di marketing, mediante l'impiego del telefono con operatore, a seguito dell'istituzione del registro pubblico delle opposizioni. La violazione delle previsioni contenute nel presente articolo espone la Parte inadempiente al risarcimento in favore dell'altra Parte dei danni eventualmente cagionati.

ACCORDO TRATTAMENTO DATI PERSONALI

L'Ente/Azienda quale Titolare dei dati cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali (di seguito "Titolare"), in persona del suo legale rappresentante designa ed istruisce MUNICIPIA SPA quale Responsabile dei trattamenti dei dati personali (di seguito "Responsabile") effettuati in relazione al Servizio oggetto del contratto di cui al punto precedente.

OBBLIGHI DEL TITOLARE

Il Titolare del trattamento è responsabile di garantire che il trattamento dei dati personali avvenga in conformità con l'articolo 24 del GDPR.

È intenzione del Titolare consentire l'accesso sia al Responsabile che alle persone autorizzate al trattamento per i soli dati personali la cui conoscenza sia necessaria per adempiere ai compiti loro attribuiti.

Il Titolare affida al Responsabile tutte le operazioni di trattamento dei dati personali necessarie per dare piena esecuzione al Servizio innanzi indicato.

Il Titolare si impegna a comunicare per iscritto al Responsabile qualsiasi variazione si dovesse rendere necessaria nelle operazioni di trattamento dei dati.

Il Titolare dichiara, inoltre, che i dati da lui trasmessi al Responsabile:

- sono pertinenti e non eccedenti rispetto alle finalità per le quali sono stati raccolti e successivamente trattati;
- in ogni caso, i dati personali e/o le categorie particolari di dati personali, oggetto delle operazioni di trattamento affidate al Responsabile, sono raccolti e trasmessi rispettando ogni prescrizione della normativa applicabile.

Resta inteso che rimane a carico del Titolare l'onere di individuare la base legale del trattamento dei dati personali degli interessati.

Il Titolare ha il diritto e l'obbligo di prendere decisioni riguardo le finalità e i mezzi del trattamento di dati personali.

OBBLIGHI DEL RESPONSABILE

Il Responsabile deve procedere al trattamento secondo le istruzioni del Titolare documentate mediante il presente accordo. Istruzioni successive potranno essere fornite dal Titolare anche durante il trattamento di dati personali purché documentate e/o previste dal Contratto principale. In ogni caso, qualora le dette istruzioni dovessero comportare implementazioni non previste e/o non prevedibili alla stipula del contratto principale, le stesse dovranno essere concordate di volta in volta in termini di tempi/costi e fattibilità tra le parti.
Il Responsabile del trattamento informa immediatamente il Titolare qualora le istruzioni impartite dallo stesso violino il GDPR o le disposizioni applicabili in materia di protezione dei dati dell'UE o degli Stati membri.
Sarà cura del Responsabile vincolare le persone autorizzate al trattamento alla riservatezza o ad un adeguato obbligo legale di confidenzialità anche per il periodo successivo all'estinzione del rapporto di collaborazione intrattenuto con il Responsabile, in relazione alle operazioni di trattamento da esse eseguite.
Il Responsabile, nel designare per iscritto le persone autorizzate al trattamento, dovrà assicurarsi che esse abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati. Dovrà inoltre curarne la formazione sui temi relativi alla protezione dei dati personali.
Inoltre, ove applicabile e per quanto concerne i trattamenti effettuati per l'erogazione della fornitura dalle persone autorizzate al trattamento con mansioni di "Amministratore di Sistema", il Responsabile è tenuto altresì al rispetto delle previsioni relative alla disciplina sugli amministratori di sistema contenute nel provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 modificato in base al provvedimento del 25 giugno 2009.
Il Responsabile, in particolare, si impegna a conservare direttamente e specificamente gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema, e a fornirli prontamente al Titolare su richiesta del medesimo.
In caso di danni derivanti dal trattamento, il Responsabile ne risponderà qualora non abbia adempiuto agli obblighi del GDPR specificatamente diretti ai Responsabili del trattamento o abbia agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare, a meno che non dimostri che l'evento dannoso non gli sia in alcun modo imputabile.

SICUREZZA DEL TRATTAMENTO

Tenendo conto dello stato dell'arte, dei costi di implementazione e della natura, ambito, contesto e finalità del trattamento, come anche della probabilità e severità del rischio per i diritti e le libertà delle persone fisiche, il Titolare ed il Responsabile implementano appropriate misure tecniche ed organizzative per assicurare un livello di sicurezza adeguato al rischio.
Il Titolare valuta i rischi inerenti al trattamento per i diritti e le libertà degli interessati, ed implementa le misure idonee a mitigarli. A seconda della loro rilevanza, tali misure posso includere le seguenti:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Il Responsabile assiste il Titolare nel garantire il rispetto degli obblighi relativi alle misure tecniche-organizzative di cui all'art. 32 GDPR, fornendo a quest'ultimo il dettaglio delle misure di sicurezza implementate per le operazioni del trattamento eseguite presso le proprie sedi e con i propri mezzi tecnico-organizzativi, insieme a tutte le altre informazioni necessarie al Titolare per ottemperare ai propri obblighi normativi.
Le misure di sicurezza tecnico-organizzative attuate dal Responsabile del trattamento sono elencate nell' **Appendice 1**, parte integrante del presente accordo.

SUB- RESPONSABILI

Il Responsabile del trattamento deve soddisfare i requisiti di cui all'articolo 28, paragrafi 2 e 4 del GDPR quando ricorre ad altro responsabile (altrimenti detto sub-responsabile).
Il Titolare concede al Responsabile preventiva autorizzazione generale per il ricorso a Sub-Responsabili. Il Responsabile informa per iscritto il Titolare di eventuali modifiche relative ad aggiunta o sostituzione di sub-responsabili con almeno 10 giorni di preavviso, dando in tal modo al Titolare modo di opporsi a tali cambiamenti prima che tali sub-responsabili vengano ingaggiati.
L'elenco dei sub-responsabili già autorizzati dal Titolare del trattamento è riportato nell' **Appendice 2.**
Quando il Responsabile coinvolga un sub-responsabile per l'esecuzione di specifiche attività del trattamento operato per conto del Titolare, sullo stesso sub-responsabile devono essere imposte mediante un contratto o altro atto giuridico le stesse obbligazioni relative alla protezione dei dati contenute nel presente accordo, in particolare prevedendo sufficienti garanzie per quanto attiene all'adozione di appropriate misure tecniche ed organizzative tali da rendere il trattamento conforme ai requisiti del presente accordo e del GDPR.
Il Responsabile del trattamento è quindi responsabile di richiedere che il sub-responsabile soddisfi almeno gli obblighi cui è esso stesso soggetto ai sensi del presente accordo e del GDPR.

TRASFERIMENTO DATI IN UN PAESE TERZO

Qualsiasi trasferimento di dati personali verso paesi terzi o organizzazioni internazionali da parte del responsabile del trattamento dei dati deve avvenire esclusivamente sulla base di istruzioni documentate da parte del Titolare e deve sempre avvenire in conformità al Capitolo V del GDPR.
Nel caso di trasferimenti verso paesi terzi o organizzazioni internazionali, richiesti dalla legislazione dell'UE o degli Stati membri a cui è soggetto il Responsabile del trattamento, e che non siano stati richiesti dal Titolare del trattamento con specifica istruzione, il Responsabile del trattamento informa il Titolare del tale requisito legale prima del trattamento, a meno che la norma stessa non vieti tale comunicazione per importanti motivi di interesse pubblico.

ASSISTENZA AL TITOLARE

Il Responsabile del trattamento dei dati deve inoltre, tenendo conto della natura del trattamento e delle informazioni disponibili, fornire supporto al Titolare affinché possa ottemperare:

- all'obbligo del Titolare a effettuare senza indebito ritardo e, ove possibile, entro e non oltre 72 ore dalla sua conoscenza, la comunicazione circa una violazione dei dati personali all'Autorità per la Protezione dei Dati Personali a meno che non sia è improbabile che comporti un rischio per i diritti e le libertà delle persone fisiche;
- all'obbligo del Titolare di effettuare una valutazione dell'impatto delle operazioni di trattamento previste sulla protezione dei dati personali (una valutazione d'impatto sulla protezione dei dati); - all'obbligo del Titolare del trattamento di consultare l'Autorità per la Protezione dei Dati personali prima di porre in essere un trattamento qualora una valutazione d'impatto indicasse che il trattamento comporterebbe un rischio elevato (in assenza di misure adottate dal Titolare di mitigazione del rischio). agli obblighi del Titolare nei confronti delle richieste di esercizio dei diritti dell'interessato stabilite nel capitolo III GDPR per quanto applicabile.

Il Responsabile sarà, inoltre, tenuto a comunicare tempestivamente al Titolare eventuali istanze degli interessati, contestazioni, ispezioni o richieste dell'Autorità di Controllo e dalle Autorità Giudiziarie, ed ogni altra notizia rilevante in relazione al trattamento dei dati personali oggetto del contratto.

NOTIFICA DATA BREACH

In caso di violazione dei dati personali, il responsabile del trattamento deve informare il Titolare della violazione (o presunta violazione) entro 48 dopo che il responsabile ne è venuto a conoscenza per consentire al Titolare la notifica della violazione dei dati personali all'autorità di controllo competente così come previsto dall'Articolo 33 del GDPR.

Le parti definiscono nell' **Appendice 3** tutti gli elementi che devono essere forniti dal responsabile al Titolare del trattamento nella notifica di una violazione dei dati personali.

CANCELLAZIONE E RESTITUZIONE DEI DATI

Al termine delle operazioni di trattamento affidate, nonché all'atto della cessazione per qualsiasi causa del trattamento da parte del Responsabile, lo stesso a discrezione del Titolare sarà tenuto alternativamente a:

- restituire al Titolare i dati personali oggetti del trattamento
- provvedere alla loro integrale distruzione salvi solo i casi in cui la conservazione dei dati sia richiesta da norme di legge od altri fini (contabili, fiscali, ecc.).

Il Responsabile provvederà a rilasciare al Titolare apposita dichiarazione per iscritto contenente l'attestazione che presso il Responsabile non esista alcuna copia dei dati personali e delle informazioni di titolarità del Titolare.

AUDIT E ISPEZIONI

Il responsabile del trattamento mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare la conformità agli obblighi di cui all'articolo 28 GDPR e si rende disponibile per le attività di audit, comprese le ispezioni, condotte dal Titolare del trattamento, o da un altro revisore dallo stesso incaricato.

A tal scopo, il Responsabile riconosce al Titolare, ed agli incaricati del medesimo, il diritto richiedere evidenza delle certificazioni più recenti emesse da terze parti accreditate. In subordine, qualora il Titolare abbia bisogno di ulteriori informazioni per adempiere ai propri obblighi di audit, avrà la facoltà di richiedere al Responsabile ulteriori evidenze, e, se del caso, previo congruo preavviso di 5 giorni lavorativi, di accedere ai locali del fornitore presso i quali si svolgono le operazioni di trattamento.

In ogni caso, il Titolare si impegna per sé e per i terzi incaricati da quest'ultimo, a che le informazioni raccolte durante le operazioni di verifica siano utilizzate solo per finalità di audit, e che le operazioni di verifica si svolgano in modo tale da non interferire con la normale attività produttiva del Responsabile.

CESSAZIONE DELL'ACCORDO

La presente nomina avrà efficacia fintanto che venga erogato il Servizio. Qualora il Servizio comporti un'esecuzione periodica e/o continuativa, rinnovata di volta in volta con specifici contratti, la presente nomina si intende efficace per la durata complessiva del Servizio

SICUREZZA E PROTEZIONE DELLE INFORMAZIONI IN CLOUD SAAS (VALIDO SOLO PER L'EROGAZIONI DELLE SOLUZIONI IN CLOUD SAAS)

CONDIVISIONE DI RESPONSABILITA' PER LA SICUREZZA DELLE INFORMAZIONI

Per quanto riguarda l'assunzione di responsabilità in merito ai ruoli che garantiscono la sicurezza delle informazioni, in particolare per le attività (ove applicabili) relative ad:

- Hardening di sistemi e apparati;
- Backup;
- Controlli crittografici (ove applicabile);
- Gestione delle vulnerabilità tecniche;
- Gestione degli incidenti;
- Controllo della conformità tecnica;
- Test di sicurezza;
- Auditing;
- Raccolta delle registrazioni (log);
- Protezione delle informazioni al termine del contratto;
- Autenticazione e controllo degli accessi

Si concorda che Cliente e Fornitore sono entrambi responsabili, ciascuno per le aree di propria competenza, che sono desumibili contrattualmente.

In linea generale vale la regola secondo cui l'onere di effettuare le attività che garantiscono la sicurezza delle informazioni spetta a chi detiene le password degli account con privilegi di amministrazione degli ambienti da mettere in sicurezza. Es.: In un contratto per la fornitura di servizi SaaS, ove il Fornitore fornisce e gestisce un layer applicativo su cui sono installati applicazioni e dati, il Fornitore è responsabile per gli adempimenti di sicurezza applicativa (es. predisposizione di funzionalità di autenticazione, logging, gestione di vulnerabilità applicative, etc.) e garantisce che siano implementate le misure di sicurezza infrastrutturale relative alla gestione degli ambienti virtualizzati che ospitano il layer applicativo. Il Fornitore, inoltre, si avvale di subfornitori qualificati e certificati che mettono a disposizione il layer infrastrutturale di base (in modalità IaaS e Paas), con cui sussistono accordi contrattuali in garanzia dell'adozione di misure di sicurezza adeguate.

PROTEZIONE DELLE INFORMAZIONI DEL CLIENTE NELL'AMBITO DEI SERVIZI CLOUD

GARANZIE

Il Fornitore garantisce ai propri Clienti, oltre all'applicazione delle idonee misure per la protezione dei **dati personali** previste dalla normativa vigente RE UE 679/2016, anche l'applicazione di una serie di misure idonee alla protezione **di tutti i dati**, tra cui l'adozione, l'applicazione e la certificazione di conformità della/alla norma di sicurezza volontaria ISO/IEC 27001:2013 "Information technology - Security techniques - Code of practice for information security management" ed il rispetto delle linea-guida:

- ISO/IEC 27018:2019 "Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors";
- ISO/IEC 27017:2015 "Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

Si forniscono maggiori informazioni con particolare riferimento ai seguenti controlli:

Gestione delle vulnerabilità tecniche

Le vulnerabilità tecniche vengono gestite ciclicamente tramite un processo di individuazione strumentale delle vulnerabilità sugli asset (la frequenza è proporzionale al livello di esposizione degli asset stessi), gli input dei vendor e dei gruppi di interesse in contatto con i competence center tecnici oltre che da possibili inneschi provenienti da strumenti di monitoring o da segnalazioni utente.

La comunicazione ed il fixing delle vulnerabilità tecniche segue sempre un iter concordato tra le parti e da definire in fase di transition (change management) ed è comunque in funzione della gravità delle vulnerabilità stesse.

Hardening delle macchine virtuali

Le attività di hardening delle macchine virtuali che ospitano ambienti applicativi in SaaS per il Cliente saranno effettuate rispettivamente dal fornitore Saas e dai subfornitori IaaS e Paas, come previsto dai relativi accordi contrattuali.

TRATTAMENTO DELLE INFORMAZIONI

Le informazioni affidate al Fornitore vengono trattate per conto del Cliente secondo quanto previsto dalla giurisdizione di riferimento, che è quella europea ed italiana, solo ed esclusivamente per le finalità contrattualizzate, a meno di specifici ed espliciti accordi con il Cliente stesso.

In particolare, il Fornitore si impegna a non utilizzare le informazioni per finalità commerciali senza autorizzazione esplicita del Cliente e dichiara che tale autorizzazione non è mai precondizione necessaria all'erogazione dei propri servizi.

Le informazioni risiedono:

- **in Italia in uno o più dei Datacenter Engineering** (a meno di differenti specifici ed espliciti accordi con il Cliente) qualora il servizio SaaS si attesti su VCloud fornito da Engineering D.Hub
- **in UE in uno in uno o più dei Datacenter messi a disposizione da altri fornitori di infrastruttura Cloud** (ad es. Amazon WebServices) di cui Municipia si avvale, purché essi siano in possesso delle certificazioni previste per l'accreditamento in Marketplace AgID.

I trattamenti vengono effettuati esclusivamente da personale qualificato, formalmente incaricato ai sensi delle normative Privacy ed istruito in tal senso.

DIFFUSIONE DELLE INFORMAZIONI

In caso di richiesta di consegna da parte di Autorità Giudiziarie o Amministrative (es. Polizia, Carabinieri, Guardia di Finanza, Magistratura), delle informazioni affidate al Fornitore dal Cliente, il Fornitore fornirà al Cliente tempestiva notifica di tale richiesta, tranne nei casi di divieto da parte dell'Autorità stessa.

NOTIFICA DEGLI INCIDENTI

Il Fornitore, in armonia alla procedura di Gruppo per la gestione degli incidenti di tipo "data breach" si impegna a notificare tempestivamente al Cliente gli incidenti di sicurezza informatica (data-breach) rilevati tramite strumenti di monitoraggio e controllo o da segnalazioni, che implichino o consistano in:

- Accessi non autorizzati
- Perdita di dati
- Alterazione di dati
- Diffusione indebita di dati

La notifica avverrà via posta elettronica (al riferimento indicato dal Cliente) o secondo le modalità contrattualizzate, di norma entro il giorno successivo alla rilevazione dell'incidente. Successivamente alla sua chiusura, sarà inviato al Cliente l'Incident Report descrittivo dell'accaduto e delle azioni intraprese.

TRASFERIMENTO O RESTITUZIONE DELLE INFORMAZIONI O RIMOZIONE A FINE CONTRATTO

Il trasferimento delle informazioni ad altro cloud provider, oppure la ri-consegna delle stesse al Cliente, sono garantite dal Fornitore che indirizzerà su base progettuale qualsiasi richiesta del Cliente in tal senso, stimando tempi e costi delle operazioni e sottoponendone proposta al Cliente. L'esecuzione delle attività è subordinata all'accettazione della proposta, e in tutti i casi è seguita dalla cancellazione sicura.

A fine contratto ed in assenza di richieste di trasferimento delle informazioni oppure di riconsegna come sopra descritte, il Fornitore provvede puntualmente alla cancellazione sicura dei dati cliente, con l'eccezione delle registrazioni che vengono ancora conservate secondo i termini di legge.
In ottemperanza alle linee guida di AgID, Municipia segue la procedura di reversibilità dei servizi SaaS pubblicata all'URL **https://confluence.municipia.eng.it/x/AgQ9BQ .**

UTILIZZO DI SUB-FORNITORI

L'utilizzo di sub-fornitori nell'erogazione dei servizi contrattualizzati è vincolato al consenso esplicito del Cliente (specifica lettera firmata o accettazione del Contratto in cui è contemplato l'utilizzo del sub-fornitore), al quale devono essere resi noti:

- il nome del sub-fornitore
- la/e nazione/i nella quale vengono operati i trattamenti delle informazioni

Nel richiedere tale consenso, Il Fornitore garantisce di aver esteso al sub-fornitore (o al "peer" service provider), le informazioni necessarie al rispetto delle norme per la sicurezza delle informazioni e che il sub-fornitore si sia impegnato a rispettarle.

BACKUP E RESTORE

Il backup dei dati Cliente è finalizzato a consentire il ripristino in caso di eventi avversi.
Il servizio di backup/restore è sempre dovuto dal Fornitore al Cliente tranne nei casi in cui, per natura del servizio o per esplicitazione contrattuale, è il Cliente stesso a provvedere autonomamente.
Il backup dei dati Cliente, qualora dovuto, viene garantito in duplice copia per tutti i dati. Eventuali deroghe richieste dal Cliente possono riguardare ambienti o dati "non di produzione". Originali e copie dei backup vengono conservati in locazioni (fisiche o logiche) differenti e il trasferimento dei dati in sede diversa avviene solo sotto protezione crittografica.
A meno di differenti accordi contrattuali, l'inizio dell'attività di restore dei dati in caso di incidente è sempre garantita, nel caso peggiore, nell'arco del giorno lavorativo successivo all'evento che rende necessario il ripristino. La durata complessiva dell'attività di restore è funzione del volume di dati da ripristinare.

LOGGING

La collezione e conservazione dei log a norma di legge è tipicamente effettuata dal Fornitore, sia direttamente, sia avvalendosi del servizio offerto dai propri sub-fornitori (IaaS e PaaS).
I log vengono resi disponibili al Cliente in forma di report "spot", effettuato su richiesta estemporanea del Cliente oppure, se concordato tra i servizi contrattualizzati, in forma di report periodico, o garantendo l'accesso in visione ai dati via rete. In tutti i casi viene garantita la riservatezza delle informazioni nel senso che ogni Cliente ha visibilità esclusivamente dei log relativi a sistemi/servizi di sua pertinenza.

PROPRIETÀ INTELLETTUALI

Il Fornitore si impegna ad erogare servizi in Cloud utilizzando sistemi con installazioni di licenze valide, ove applicabile.
Reclami di pertinenza del Fornitore saranno indirizzati secondo il processo interno di Gestione dei Reclami.

Appendice 1	**Misure tecniche e organizzative secondo l'articolo 30 del regolamento europeo sulla protezione dei dati (Regolamento (UE) 2016/679 - "GDPR")** **MD15_PGT01_0_Allegato_Caratteristiche_Trattamento_Dati**
Prodotto/i	ARGO – Portale servizi digitali | GeIS – Imposta di Soggiorno | Tribox – Gestionale tributi | jEnte – Gestionale tributi | Gnosis Tributi – Sistema della conoscenza a supporto della ricerca evasione tributaria | Gnosis Welfare - Sistema della conoscenza Welfare | Mercurio – Spedizione per invii via email, PEC e notifiche AppIO | MuniPay . L'ecosistema Municipia per PagoPA Assistenza e Manutenzione | Sviluppo Prodotto

Di seguito l'elenco dei prodotti di cui solo alcuni o tutti possono essere utilizzati per i servizi oggetto della proposta:

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. A livello di macro-funzionalità, TRIBOX si può suddividere in:
- Sportello Soggetto: attività puntuale sul singolo soggetto, identificato da un codice univoco.
- Sportello Oggetto: attività puntuale sul singolo oggetto, identificato dalle coordinate catastali.
- Import/ Export: funzionalità di interscambio con sistemi esterni
- Liste e Riepiloghi: funzionalità riepilogative e di supporto alle decisioni.
- Attività di Accertamento
- Bonifica banche dati
- Processi Massivi

I tributi trattati sono: IMU/ICI, TASI e TARI/TARES/TARSU. L'anagrafica presente in TRIBOX (anch'essa alimentabile da diverse fonti) è trasversale alle funzionalità ed ai tributi sopra indicati.

JEnte 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. I tributi trattati sono: IMU/ICI, TASI, TARI/TARES/TARSU, TOSAP/COSAP, Pubblicità, Pubbliche Affissioni e Canone Unico. L'anagrafica presente in JEnte (anch'essa alimentabile da diverse fonti) è trasversale alle funzionalità ed ai tributi sopra indicati.

GNOSIS TRIBUTI è lo strumento software realizzato da Municipia a supporto del servizio di ricerca evasione TARI/IMU.
Utilizzando questo strumento è possibile:
- consultare puntualmente il sistema della conoscenza (pallogramma strumento navigazione grafica grazie al quale dato un soggetto è possibile consultare tramite interfaccia grafica tutti gli oggetti a lui collegati come proprietà, locazioni, nucleo anagrafico di appartenenza, ecc.);
- gestire le istruttorie (potenziali posizioni anomale catalogate secondo un grado di affidabilità che possono trasformarsi in oggetti di accertamento) - analisi del magazzino delle istruttorie e dell'esito dei provvedimenti emessi;
- consultare e verificare e misurare le planimetrie catastali caricate.

GNOSIS WELFARE (Sistema Conoscenza) fornisce all'Ente un sistema che aggrega, normalizza e produce i dati utili alla gestione delle politiche sociali per l'adeguamento dei servizi sul territorio.
In particolare, supporta l'Ente nell'identificazione, in modo massivo e puntuale, dei soggetti destinatari di interventi economici d'emergenza tenendo conto della situazione economica e socio-economica.
Incrociando le banche dati economiche, Inps e comunali il sistema ricostruisce, dal punto di vista sociale ed economico, la situazione di ogni cittadino e nucleo familiare con lo scopo di estrarre in modo automatico segmenti di famiglie e cittadini in base ad appositi parametri e filtri di interesse.
I consolidati modelli di estrazione, bonifica e incrocio delle informazioni provenienti dalle diverse banche dati rendono disponibili dati solidi e puntuali per diverse finalità, quali ad esempio la produzione di liste di possibili beneficiari di contributi o servizi.

MERCURIO è uno strumento con funzione di spedizioniere. E' in grado di recepire documenti da inviare attraverso diversi canali (export SIN, PEC, email 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 Trattamento
- Application Maintenance Management
- Customer Support
- Sviluppo prodotto

Categorie di Interessati
I Dati Personali trattati riguardano le seguenti categorie di Interessati:
- Cittadini e contribuenti

Tipologia di Dati Personali
- Dati personali comuni (es. dati anagrafici, di contatto, relativi all'istruzione, stato civile/familiare, esperienza professionale)
- Dati Finanziari (es. reddito, transazioni finanziarie, investimenti, carte di credito, fatture, ecc.)

Caratteristiche del Trattamento
- Full Outsourcing

Misure di Sicurezza
In relazione alla rischiosità del trattamento definita dal Titolare, il Responsabile nell'ambito delle attività contrattualmente previste, garantisce di applicare le seguenti misure di sicurezza, che il Titolare conferma forniscano un adeguato livello di protezione dei Dati Personali in considerazione dei rischi associati al Trattamento dei Dati Personali.

Risk Level	Categoria	ID	Descrizione	Geis ARGO MuniPay	Tribox jEnte Gnosis Trbuti Mercurio	Gnosis Welfare
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.		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.		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.		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
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.		X	X

Risk Level	Categoria	ID	Descrizione	Geis ARGO MuniPay	Tribox jEnte Gnosis Trbuti Mercurio	Gnosis Welfare
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.			X
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.			X
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.		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.		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.			X
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.		X	X
A	**Gestione degli asset/risorse**	**D.4**	Le risorse IT sono riesaminate e aggiornate su base annuale.			X
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	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. Quando è necessario eseguire l 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.	X	X	X

Risk Level	Categoria	ID	Descrizione	Geis ARGO MuniPay	Tribox jEnte Gnosis Trbuti Mercurio	Gnosis Welfare
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.		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	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.			X
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	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.		X	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.		X	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.			X
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.		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
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.		X	X

Risk Level	Categoria	ID	Descrizione	Geis ARGO MuniPay	Tribox jEnte Gnosis Trbuti Mercurio	Gnosis Welfare
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.		X	X
M	**Controllo degli accessi ed autenticazione**	**K.6**	Le password degli utenti sono archiviate in formato "hash".		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	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.		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.		X	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	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.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

Risk Level	Categoria	ID	Descrizione	Geis ARGO MuniPay	Tribox jEnte Gnosis Trbuti Mercurio	Gnosis Welfare
M	**Sicurezza desktop/laptop/mobile**	**N.6**	Le applicazioni antivirus e le signature sono configurate su base giornaliera.		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	X
M	**Network/Communication security**	**O.2**	L'accesso wireless al sistema IT è consentito solo a utenti e processi specifici. E' protetto da meccanismi di crittografia.		X	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.		X	X
M	**Back-ups**	**P.6**	I backup incrementali programmati sono eseguiti almeno su base giornaliera.		X	X
M	**Back-ups**	**P.7**	Le copie del backup sono conservate in modo sicuro in luoghi diversi dai dati di origine.		X	X
B	**Sicurezza del ciclo di vita del software**	**R.4**	Sono seguiti standard e pratiche di codifica sicure.	X	X	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.		X	X
M	**Sicurezza del ciclo di vita del software**	**R.7**	Sono eseguiti penetration test periodici.		X	X
M	**Sicurezza del ciclo di vita del software**	**R.8**	Si ottengono informazioni sulle vulnerabilità tecniche dei sistemi IT utilizzati.		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.		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.		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		X	X

Risk Level	Categoria	ID	Descrizione	Geis ARGO MuniPay	Tribox jEnte Gnosis Trbuti Mercurio	Gnosis Welfare
			accessi sono mantenuti e monitorati in modo sicuro			
M	**Sicurezza fisica** (solo per Cloud SaaS)	**T.4**	I sistemi di rilevamento anti-intrusione sono installati in tutte le zone di sicurezza.		X	X
M	**Sicurezza fisica** (solo per Cloud SaaS)	**T.5**	Le barriere fisiche sono costruite per impedire l'accesso fisico non autorizzato.		X	X
M	**Sicurezza fisica** (solo per Cloud SaaS)	**T.6**	Le aree non usate sono fisicamente bloccate e periodicamente riesaminate.		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.		X	X
M	**Sicurezza fisica** (solo per Cloud SaaS)	**T.8**	Il personale di supporto esterno ha accesso limitato alle aree protette.		X	X

Appendice 2	Elenco Sub-Responsabili MD14_PGT01_0_Allegato_Elenco_SubResponsabili
Prodotto/i	ARGO – Portale servizi digitali | GeIS – Imposta di Soggiorno | Tribox – Gestionale tributi | jEnte – Gestionale tributi | Gnosis Tributi – Sistema della conoscenza a supporto della ricerca evasione tributaria | Gnosis Welfare - Sistema della conoscenza Welfare | Mercurio – Spedizione per invii via email, PEC e notifiche AppIO | MuniPay . L'ecosistema Municipia per PagoPA Assistenza e Manutenzione | Sviluppo Prodotto

Sezione Valida per l'erogazione Cloud SaaS

Accettando la presente proposta il Titolare autorizza il Responsabile ad affidare parte delle operazioni di trattamento ai seguenti ulteriori sub-responsabili indicati per ciascun prodotto di riferimento.

Paese cui è stabilito Sub-Responsabile	Sub-Responsabili	Dati di contatto	Attività di trattamentoaffidata
Italia	D-HUB Gruppo Engineering	info.dhub@eng.it	Service Provider (CSP qualificato AGID)
Lussemburgo	Amazon Web Services EMEA SARL	https://aws.amazon.com/it/contact-us/	Service Provider (CSP qualificato AGID)

Qualora il Responsabile intendesse affidare ad un 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 sopra indicati, provvederà a comunicare tali variazioni al Titolare.

Appendice 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)

_____

_____