COMUNE DI MELDOLA
(Prov. Forlì – Cesena)

Proposta N. 1002 del 30/10/2023

Pratica n. N.28/2023 - 4.3

Settore Proponente: Ufficio Tributi

DETERMINA

Numero: **983** Data: **30/10/2023**

OGGETTO: APPROVAZIONE ACCORDO PER IL TRATTAMENTO DEI DATI PERSONALI EX ART. 28 DEL REGOLAMENTO UE 679/2016

IL RESPONSABILE DEL SETTORE

RICHIAMATO il decreto del Sindaco n. 9 del 20/05/2021, che ha attribuito alla Dott.ssa Roberta Pirini l'incarico di Responsabile del Servizio Tributi

PREMESSO che il 25 maggio 2018 è entrato in vigore il Regolamento (UE) 20161679 "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46lCE (Regolamento generale sulla protezione dei dati)";

DATO ATTO che il Sindaco, in qualità di legale rappresentante del Comune di Meldola, Titolare del trattamento dei dati personali, ai sensi del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, con il suddetto decreto n. 9 del 20/05/2021, ha designato la sottoscritta " Responsabile del trattamento dei dati personali , per tutte le attività e banche dati esistenti nel proprio ambito di competenza;

VISTO l'art. 28 del sopraccitato Regolamento dell'Unione Europea 2016/679, il quale prevede la designazione da parte del Titolare di un **Responsabile esterno del trattamento dei dati personali**;

VISTA la Determinazione dirigenziale n. 642 del 24/07/2023 con cui l'Ente ha affidato alla società **Municipia S.p.A**, P. iva 01973900838, con sede legale in Trento (TN) Via Adriano Olivetti, 7 in persona del legale rappresentante pro tempore, il servizio di *"Supporto alla ricerca evasione della TARI/IMU"*;

VISTA la bozza di Accordo **per il Trattamento dei dati personali ex art. 28 (3) del Regolamento UE 679/2016** ,all.A) ,allegato alla presente quale parte integrante e sostanziale;

DATO ATTO che provvederà alla sottoscrizione dell'accordo in argomento il Funzionario Responsabile dell'Ufficio Associato del Servizio Entrate Tributarie e Servizi Fiscali, Dott.ssa Roberta Pirini;

DATO ATTO, altresi che la sottoscrizione dell'accordo sopra richiamato non comporta alcun onere finanziario a carico del Bilancio del Comune di Meldola;

RICHIAMATI:

- il D.Lgs. n. 267/2000;
- lo Statuto comunale;

DETERMINA

per tutto quanto espresso in premessa che costituisce parte integrante e sostanziale del presente dispositivo, anche ai sensi e per gli effetti di cui all'art. 3 della L.241/90;

1. **DI APPROVARE** l'accordo per il trattamento dei dati personali (ex articolo 28 del Regolamento UE 2016/679)allegato A),parte integrante e sostanziale del presente atto;
2. **DI DESIGNARE** quale RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI PERSONALI AI SENSI E PER GLI EFFETTI DI CUI ALL'ART. 28 DEL REGOLAMENTO UE 2016/679,la società **Municipia S.p.A**, con sede legale in Trento (TN) Via Adriano Olivetti, 7, in persona del legale rappresentante pro tempore;
3. **DI DARE ATTO** che provvederà alla sottoscrizione dell'Accordo sopra richiamato il Funzionario Responsabile dell'Ufficio Associato del Servizio Entrate Tributarie e Servizi Fiscali, .Dott.ssa Roberta Pirini;
4. **DI PROVVEDERE** alla pubblicazione del presente provvedimento sul sito istituzionale dell'Ente, nella sezione "Amministrazione Trasparente", in ottemperanza all'art. 29 del DLGS 50/2016;

5. **NON COMPORTANDO** impegno di spesa/prenotazione impegno, la presente determinazione non necessita del visto di regolarità contabile attestante la copertura finanziaria, ai sensi dell'art. 183, comma 7, del T.U.E.L. Approvato con D.Lgs. 267/2000;

6. **DI ATTESTARE** la regolarità e la correttezza del presente atto ai sensi e per gli effetti di quanto dispone l'art. 147 bis del D. Lgs. 267/2000.

LA RESPONSABILE DEL SETTORE
Roberta Pirini
(Documento sottoscritto digitalmente)

ACCORDO PER IL TRATTAMENTO DEI DATI PERSONALI EX ART 28 DEL REGOLAMENTO UE 679/2016

Tra

Titolare del Trattamento

Comune di Meldola, con sede legale in Piazza Orsini Felice, 29, 47014 Meldola (FC) in qualità di "Titolare" del trattamento dei dati personali, ai sensi e per gli effetti del GSPR 679/2016, nella persona del Funzionario Responsabile dei Tributi, Dott.ssa Roberta Pirini, tel 0543/499411, mail: roberta.pirini@comune .meldola.fc.it, Pec: comune.meldola@cert.provincia.fc.it

E

Responsabile del Trattamento

Ragione Sociale **MUNICIPIA SPA**

Indirizzo Via Adriano Olivetti, 7 **Città** Trento (38122)

Telefono 0461/158501 PEC municipia@pec.eng.it

Privacy manager Barbara Capelli

Telefono 348/6105664 Email barbara.capelli@eng.it

Responsabile della Protezione dei dati (DPO)

Email dpo.privacy.municipia@eng.it

PREMESSO CHE

tra le parti è stato sottoscritto un contratto avente per oggetto ORDINATIVO DI FORNITURA - CONVENZIONE PER L'AFFIDAMENTO DEI SERVIZI DI SUPPORTO ALLA GESTIONE ORDINARIA, RICERCA EVASIONE E RISCOSSIONE COATTIVA DEI TRIBUTI E DELLE ALTRE ENTRATE COMUNALI 3 - Lotto 6 (Amministrazioni della provincia di Forlì-Cesena) - CIG 7861780218 e 99806179B1 [num. Registro PI240526-23]

- il presente accordo stabilisce diritti e obblighi del Titolare e del Responsabile del trattamento con riguardo al trattamento di dati personali effettuati per conto di un Titolare del trattamento ai sensi del Regolamento generale sulla protezione dei dati (d'ora in poi GDPR) e ss.mm.ii.;

- il presente Accordo prevale su disposizioni simili contenute in altri accordi tra le parti;

- gli allegati 1, 2, 3 costituiscono parte integrante dell'Accordo;

- il presente accordo non comporta alcun diritto del Responsabile ad uno specifico compenso e/o indennità e/o rimborso derivante dal medesimo a meno di specifiche implementazioni richieste che esulano dall'oggetto del contratto principale;

Il comune di Meldola 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.

Con la sottoscrizione del presente atto, ai sensi dell'art. 28 del Regolamento Europeo n. 679/2016, il Responsabile esterno del trattamento accetta la propria nomina, in relazione ai dati personali la cui conoscenza risulta essere indispensabile per lo svolgimento delle obbligazioni di cui al contratto in essere tra le parti. Il Responsabile è a conoscenza degli obblighi previsti dal Regolamento Europeo n. 679/2016 e dovrà attenersi per lo svolgimento del compito assegnatoli alle previsioni ed ai compiti contenuti nel presente atto di nomina.

Le premesse formano parte integrante e sostanziale del presente accordo.

1 DIRITTI E 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.

2 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.

3 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:

a. la pseudonimizzazione e la cifratura dei dati personali;
b. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d. 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'**Allegato 2**, parte integrante del presente accordo.

4 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'**Allegato 1**.

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.

5 TRASFERIMENTO DEI 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.

Fermo restando quanto stabilito al precedente articolo 4, il Responsabile del trattamento, nell'ipotesi in cui nomini Sub-Responsabili che siano stabiliti fuori dall'Unione Europea, si obbliga a rispettare le previsioni di cui agli artt. 44-50 del Regolamento. In particolare, nei casi in cui sussista la necessità che il trasferimento dei Dati Personali avvenga in conformità alle Clausole Contrattuali Tipo, il Responsabile, in forza del presente Accordo, deve intendersi espressamente autorizzato a

concludere con i propri Sub-Responsabili le Clausole Contrattuali Tipo che disciplinano il trasferimento da responsabile del trattamento a responsabile del trattamento in conformità a quanto previsto nella decisione 2021/914 della Commissione Europea del 4 giugno 2021. Le Clausole Contrattuali Tipo che disciplinano il trasferimento da responsabile del trattamento a responsabile del trattamento dovranno essere sottoscritte qualora i Sub-Responsabili siano stabiliti in un Paese non appartenente allo Spazio Economico Europeo per il quale la Commissione Europea non ha emesso una decisione di adeguatezza, in aggiunta ad eventuali misure supplementari individuate conformemente a quanto indicato dal Comitato Europeo per la protezione dei dati personali ("EDPB"), secondo quanto indicato nelle "*Raccomandazioni 01/2020 sulle misure che integrano gli strumenti di trasferimento per garantire il rispetto del livello di protezione dei dati personali nell'UE*" e nelle "*Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza*".

In particolare, il Cliente è reso edotto che il Responsabile del trattamento potrà avvalersi ai fini dell'esecuzione del Servizio anche delle proprie controllate situate al di fuori dello Spazio Economico Europeo, fermo restando il rispetto di quanto previsto nel presente accordo e, in ogni caso, attenendosi alle eventuali specifiche istruzioni ricevute dal Titolare.

Previa richiesta, il Titolare può autorizzare il Responsabile a procedere alla revisione delle Clausole Contrattuali Tipo solo per estendere all'entità extra SEE obblighi più rigorosi e ottenerne una copia integrale dal Responsabile del Trattamento.

6 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.

7 NOTIFICA DEL DATA BREACH

In caso di violazione dei dati personali, il responsabile del trattamento deve informare il Titolare della violazione (o presunta violazione) entro 48 ore 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'**Allegato 3** tutti gli elementi che devono essere forniti dal responsabile al Titolare del trattamento nella notifica di una violazione dei dati personali.

8 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.

9 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.

10 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.

11 COMUNICAZIONI TRA LE PARTI

Le comunicazioni tra le parti, ai fini del presente incarico, dovranno essere indirizzate:

- per il Responsabile del trattamento **MUNICIPIA SPA – TRENTO - municipia@pec.eng.it**
- per il Titolare del trattamento **Comune di Meldola - comune.meldola@cert.provincia.fc.it**

Per conto del Titolare	**Per conto del Responsabile**
Dott.ssa Roberat Pirini	Ing. Manuela Vesentini
Funzionario Responsabile dei Tributi	*Procuratore Speciale (Giusta Procura Speciale a rogito Notaio P. Fenoaltea in Roma, rep.n. 37081 racc. n. 22341 del 20/03/2019)*

ALLEGATO 1 - ELENCO SUB-RESPONSABILI
Trattamento Dati Prodotti : TRIBOX – GERI – ARGO – GNOSIS - MERCURIO - STARS
Erogazione: Saas

ATTENZIONE: LASCIARE SOLO IL PRODOTTO UTILIZZATO ED ELIMINARE IL RESTO

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

Paese cui è stabilito Sub-Responsabile	**Sub-Responsabili**	**Dati di contatto**	**Attività di trattamento affidata**	**Prodotti**
Italia	D-HUB Gruppo Engineering	info.dhub@eng.it	Service Provider (CSP qualificato AGID)	TRIBOX – GERI - ARGO – GNOSIS (in migrazione su AWS) – MERCURIO - STARS
Italia	BI SOLUTION Società Cooperativa Sociale ONLUS	amministrazione@labottegainformatica.it	Data entry/ Sportello contribuenti	
Italia	Eurisko Post Srl	eurisko@euriskopost.it	Stampa, imbustamento, recapito e rendicontazione	
Italia	Imbalplast s.r.l.	info@imbalplast.com	Stampa, imbustamento e rendicontazione	
Italia	Ideatech S.r.l.	info@ideatechsrl.com	Attività di assistenza e manutenzione prodotto Ge.Ri.	

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 comunicati, dovrà provvedere a comunicare tali variazioni al Titolare.

ALLEGATO 2 – CARATTERISTICHE DEL TRATTAMENTO E MISURE TECNICHE E ORGANIZZATIVE

TRIBOX	per il servizio di riscossione ordinaria e /o recupero evasione
GERI	per il servizio di riscossione
ARGO	per esporre on line la situazione debitoria al contribuente
GNOSIS	per l'incrocio delle basi dati ai fini del recupero evasione
MERCURIO	per il reperimento delle pec e la gestione dell'inoltro dei plichi amministrativi

Dettagli Trattamento

Application Maintenance Management
Customer Support
Servizi tributari (ricerca evasione, accertamento, riscossione)

Categorie di Interessati

I Dati Personali trattati riguardano le seguenti categorie di Interessati:

Cittadini e contribuenti

Tipologia di Dati Personali

I Dati Personali trattati dall'Appaltatore per conto del Titolare del Trattamento riguardano le seguenti categorie 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 (o SaaS)

Misure di Sicurezza

Il Responsabile e/o Sub-Responsabile e/o suoi ulteriori 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 dal Responsabile e/o Sub-Responsabile e/o suoi ulteriori 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 misure di sicurezza come richiesto dallo stesso Titolare.

Risk Level	Categoria	ID	Descrizione	Tribox Gnosis Mercurio	GeRi Stars	Argo
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	

Risk Level	Categoria	ID	Descrizione	Tribox Gnosis Mercurio	GeRi Stars	Argo
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	
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	
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	
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

Risk Level	Categoria	ID	Descrizione	Tribox Gnosis Mercurio	GeRi Stars	Argo
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 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.	X	X	X
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
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.	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		
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	Tribox Gnosis Mercurio	GeRi Stars	Argo
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
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		
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		
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

Risk Level	Categoria	ID	Descrizione	Tribox Gnosis Mercurio	GeRi Stars	Argo
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.	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.	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.	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.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	
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	

Risk Level	Categoria	ID	Descrizione	Tribox Gnosis Mercurio	GeRi Stars	Argo
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.	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 accessi sono mantenuti e monitorati in modo sicuro	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.	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	

ALLEGATO 3 – 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)

_____

_____

Copia conforme uso amministrativo
documento firmato digitalmente da ROBERTA PIRINI.
Medola, 02/11/2023

f.to

COMUNE DI MELDOLA

PUBBLICAZIONE ALL'ALBO PRETORIO

Determinazione Numero 983 del 30/10/2023

OGGETTO: APPROVAZIONE ACCORDO PER IL TRATTAMENTO DEI DATI PERSONALI EX ART. 28 DEL REGOLAMENTO UE 679/2016

La presente determinazione, ai fini della pubblicità degli atti e della trasparenza dell'azione amministrativa, viene affissa all'Albo Pretorio il giorno 30/10/2023 e vi rimane per la durata di 15 (quindici) giorni.

Meldola, 30/10/2023

L'ADDETTO ALLE PUBBLICAZIONI

Maurizio Sassano

Copia conforme uso amministrativo

Meldola, 02/11/2023

f.to