



COMUNE DI GENOVA

Direzione di Area Scuola

ACCORDO SUL TRATTAMENTO DEI DATI

ai sensi dell'art. 28 del Regolamento generale (UE) 2016/679 (in breve GDPR)

La Civica Amministrazione, titolare autonomo del trattamento, di seguito "Amministrazione" con sede legale in via Garibaldi, 9, 16124, Genova, P.IVA/C.F. 00856930102, rappresentata per il presente atto da, Direttore della Direzione di Area Scuola

e

la Società, in persona del legale rappresentante pro tempore, con sede legale in Via..... n., P.IVA/C.F., di seguito "Responsabile";

premesso che

- per DATO PERSONALE si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4, par. 1, n. 1, GDPR);
- per TRATTAMENTO si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, par. 1, n. 2, GDPR);
- il Regolamento generale (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati (di seguito GDPR) dispone che il soggetto che effettua un trattamento dei dati personali per conto del Titolare è individuato Responsabile del trattamento e vincolato a trattare i dati in modo conforme ai principi indicati nel GDPR nonché all'adozione di misure tecniche e organizzative adeguate per un'efficace protezione dei dati personali dell'interessato;
- il dirigente designato può avvalersi di soggetti esterni che svolgono per conto della Civica Amministrazione servizi o attività che implicano il trattamento di dati personali. Detti soggetti sono stati scelti in virtù dei requisiti di esperienza, capacità e affidabilità, in relazione alle peculiarità della materia di che trattasi;
- a tale riguardo il dirigente individua, contrattualizza e nomina i responsabili del trattamento ai sensi dell'art. 28 del GDPR, avendo cura di specificare, fin dalla fase di scelta del contraente, le caratteristiche professionali e organizzative che essi devono possedere, in relazione alle peculiarità del servizio o del lavoro affidati;

considerato che

- il dirigente ha individuato e contrattualizzato il presente prestatore di servizi mediante un contratto avente ad oggetto la fornitura del servizio di
- in esecuzione di detto contratto e dei suoi allegati, documenti tutti facenti parte integrante e sostanziale del presente accordo, il dirigente nomina il prestatore di servizi quale responsabile del trattamento, in quanto le attività affidate comportano il trattamento di dati personali per conto della Civica Amministrazione;

tutto ciò premesso e considerato, il dirigente:

- procede in conformità all'art. 28 del GDPR con la sottoscrizione dell'accordo con la Società, come riportato in epigrafe, quale responsabile del trattamento, che presenta garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato;
- adotta il presente accordo che potrebbe essere approvato anche con la determinazione dirigenziale che approva il contratto;
- la nomina del responsabile del trattamento non comporta alcuna assunzione di spesa o introito a carico del bilancio comunale, né alcun riscontro contabile, né attestazione di copertura finanziaria.

NOMINA DEL RESPONSABILE DEL TRATTAMENTO

L'art. 4, par. 1, n. 8 del GDPR definisce il “*Responsabile del trattamento*” come la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare.

Il ruolo del “*Titolare del trattamento*” è definito dall'art. 4, par. 1, n. 7 del GDPR come la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

L'Amministrazione, titolare del trattamento, ai sensi del citato art. 4 del GDPR ha il diritto e l'obbligo di:

- prendere decisioni riguardo alle finalità e ai mezzi del trattamento e di conseguenza ha una responsabilità generale di garantire che il trattamento dei dati personali avvenga in conformità con il cons. n. 79 e con gli artt. 5, par. 2, 24, 25 e 32 del GDPR;
- impartire, ai sensi dell'art. 28 del GDPR, istruzioni documentate ai responsabili del trattamento.

All'interno della delineata cornice giuridica l'Amministrazione ha provveduto a:

- individuare misure tecniche e organizzative adeguate ad attuare il principio di protezione dei dati fin dalla progettazione al fine di tutelare i diritti e le libertà degli interessati;
- effettuare scelte tali da garantire che venga svolto, per impostazione predefinita, solo il trattamento strettamente necessario (minimizzazione dei dati) per conseguire specifiche e lecite finalità, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse.

Con la sottoscrizione del presente accordo, il Responsabile si dichiara disponibile e competente alla piena attuazione di quanto concordato.

Il Responsabile nel trattare i dati personali per conto dell'Amministrazione **si impegna ad attenersi alle istruzioni impartite** all'interno del presente accordo di nomina, quale responsabile del trattamento, solo per le finalità indicate nel contratto di servizio, e nel rispetto dei principi di cui all'art. 5 del GDPR:

- liceità, correttezza e trasparenza;

- limitazione della finalità;
- minimizzazione dei dati;
- esattezza;
- limitazione della conservazione;
- integrità e riservatezza.

In virtù del rapporto in essere, il Responsabile **riceve le istruzioni** ai fini della corretta gestione del ciclo di vita dei dati personali trattati per conto dell'Amministrazione.

Protezione dei dati

Il Responsabile, congiuntamente alle altre società del proprio gruppo aziendale, si impegna ad attenersi alle istruzioni di seguito enunciate e a quelle conferite nel corso del tempo, vigilando sull'applicazione delle stesse, in modo da ridurre al minimo i rischi di data breach, riguardo a:

- a) trattare i dati personali soltanto su istruzione documentata del titolare, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
- b) garantire che le persone autorizzate al trattamento si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- c) adottare tutte le misure di sicurezza richieste dall'art. 32 del GDPR;
- d) rispettare le condizioni di cui ai paragrafi 2 e 4 dell'art. 28 del GDPR nel caso intenda ricorrere ad altro responsabile del trattamento (sub-responsabile del trattamento);
- e) tenuto conto della natura del trattamento, assistere il titolare con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del GDPR;
- f) assistere il titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
- g) cancellare tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
- h) mettere a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi in materia di protezione dei dati personali, consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Il Responsabile non stabilito nell'Unione europea, ai sensi dell'art. 27, par. 3 del GDPR, è tenuto a designare un rappresentante in Italia.

In particolare, il Responsabile si impegna a:

- individuare e autorizzare i propri dipendenti a trattare i dati impartendo loro, per iscritto, istruzioni sulle modalità del trattamento in attuazione a quanto previsto dalla disciplina di settore e dal presente accordo;
- erogare periodicamente ai propri dipendenti coinvolti nelle attività di trattamento corsi di formazione sulla corretta gestione dei dati personali;
- informare immediatamente l'Amministrazione, qualora, a suo parere, un'istruzione violi la disciplina comunitaria, nazionale e comunale in materia di protezione dei dati personali.

Attività di cooperazione

Il Responsabile coopera con l'Amministrazione nei seguenti casi:

- su richiesta dell'Autorità di controllo (artt. 31 e 58 del GDPR);
- presta supporto al DPO del Comune di Genova (art. 38, par. 1 del GDPR).

Responsabile della protezione dei dati

Ove previsto, viene designato il Responsabile della protezione dei dati (in inglese Data Protection Officer) in conformità agli articoli da 37 a 39 del GDPR e comunica i dati di contatto all'Autorità di controllo italiana e all'Amministrazione via PEC: comunegenova@postemailcertificata.it e contestuale e-mail al DPO: rp@comune.genova.it

Registro delle attività di trattamento

Il Responsabile, ai sensi dell'art. 30 del GDPR, e nei limiti di quanto prescritto, si impegna a:

- predisporre, aggiornare e conservare un registro dei trattamenti svolti per conto del titolare del trattamento; mettere il predetto registro a disposizione dell'Amministrazione e dell'Autorità di controllo, nel caso di richiesta ai sensi dell'art. 30 par. 4 del GDPR.

Informativa privacy e consenso

Il Responsabile riceve dall'Amministrazione il modulo sul trattamento dei dati personali da rendere agli interessati e, quando previsto, raccoglie il consenso, ad eccezione, dei casi in cui compete direttamente all'Amministrazione verificare il corretto adempimento degli obblighi di trasparenza in tema di informativa privacy e consenso (**Allegato A**).

Riscontro alle istanze degli interessati

Qualora il Responsabile riceva una richiesta relativa all'esercizio dei diritti di cui al Capo III del GDPR, si attiva con sollecitudine, al massimo 24 ore dal ricevimento dell'istanza, a trasmettere la richiesta al titolare via PEC: comunegenova@postemailcertificata.it e contestualmente alla e-mail del DPO: rp@comune.genova.it

Competente a rispondere è il dirigente che ha provveduto alla nomina del prestatore di servizi.

Amministratori di sistema

Il Responsabile, con riferimento ai propri dipendenti, conferma di essersi adeguato al provvedimento del Garante 27 novembre 2008, modificato nel 2009, relativo alla figura dell'amministratore di sistema (in seguito, "Admin") e di aver proceduto, tra l'altro, a:

- nominare per iscritto ciascun Admin, in possesso dei necessari requisiti di esperienza, capacità e affidabilità, indicando il rispettivo ambito di competenza e le funzioni attribuite alla gestione e manutenzione del sistema informativo;
- conservare direttamente e aggiornare gli estremi identificativi degli Admin e metterli a disposizione del titolare;
- svolgere attività di verifica, con cadenza almeno annuale, sul loro operato anche attraverso la gestione, in conformità al richiamato provvedimento del Garante;
- garantire l'adozione delle misure tecniche e organizzative prescritte nel citato provvedimento del Garante.

Sub-responsabili del trattamento

Qualora il Responsabile intenda avvalersi di TERZI, sub-responsabili, per le attività (o parte delle attività) di trattamento - già in sede di sottoscrizione del presente Accordo - trasmette via PEC all'Amministrazione: comunegenova@postemailcertificata.it e contestualmente per conoscenza al DPO: rp@comune.genova.it un elenco con i nominativi dei sub-responsabili ai fini dell'autorizzazione preventiva da parte del titolare del trattamento.

Il Responsabile inoltra all'Amministrazione, in ogni momento, una richiesta scritta di

autorizzazione preventiva ad avvalersi di sub-responsabili ai sensi dell'art. 28, par. 2 e 4 del GDPR, via PEC all'Amministrazione: comunegenova@postemailcertificata.it e contestualmente per conoscenza al DPO: rpd@comune.genova.it

Il Responsabile si impegna a verificare che i sub-responsabili, individuati, offrano garanzie in termini di requisiti di esperienza, capacità e affidabilità non inferiori a quelle garantite con l'accettazione della presente nomina e regola i rapporti interni con questi TERZI mediante un contratto o altro atto giuridico.

Nella scelta dei sub-responsabili, il Responsabile considera in via prioritaria, a parità di garanzie, soggetti situati sul territorio nazionale e dell'Unione europea, istruendoli sulla necessità di trattare i dati all'interno dello spazio economico europeo (SEE). Laddove ciò non fosse possibile, il Responsabile può ricorrere a sub-responsabili situati in paesi terzi o organizzazioni internazionali al di fuori dello SEE alle seguenti condizioni:

- comunicare preventivamente l'intenzione di ricorrere a sub-responsabili stabiliti al di fuori dello SEE mediante PEC al titolare: comunegenova@postemailcertificata.it e contestuale e-mail al DPO: rpd@comune.genova.it
- implementare misure supplementari al fine di garantire la protezione dei dati personali.

Trasferimento dei dati al di fuori dello SEE verso paesi terzi o organizzazioni internazionali

Il Responsabile, in applicazione del Capo V del GDPR, si impegna a NON trasferire dati personali in paesi o organizzazioni internazionali al di fuori dello SEE che non garantiscano il livello adeguato di tutela previsto dal GDPR.

Il trasferimento può avvenire soltanto in conformità con il capo V del GDPR e secondo le indicazioni sia dell'Autorità di controllo italiana (Garante) sia del Comitato Europeo per la Protezione dei Dati (edpb).

Qualora il Responsabile intenda, comunque, trasferire i dati personali informa preventivamente l'Amministrazione tramite PEC: comunegenova@postemailcertificata.it con contestuale e-mail al DPO: rpd@comune.genova.it implementando misure supplementari al fine di garantire la protezione dei dati personali.

Violazioni di dati personali (data breach)

Ai fini del presente accordo il livello di sicurezza atteso è quello volto a garantire la confidenzialità, l'integrità, la disponibilità e la resilienza degli strumenti tecnologici utilizzati dal Responsabile, che si impegna a trattare i dati per conto del titolare con la medesima cura con la quale tratta i dati dei propri clienti, in modo da garantire un'adeguata protezione dei dati personali.

Nel caso di presunto data breach, anche se intervenuto presso i propri sub-responsabili del trattamento, qualora presenti, il Responsabile informa tempestivamente, al massimo **entro 24 ore** dalla scoperta dell'evento, l'Amministrazione indicando anche i dati di contatto del proprio DPO e fornendo tutti i dettagli della violazione subita con PEC: comunegenova@postemailcertificata.it e contestuale e-mail al DPO: rpd@comune.genova.it

In tale situazione, il Responsabile, fin da subito, mette in atto le misure tecniche e organizzative al fine di mitigare le conseguenze della presunta violazione a tutela degli interessati coinvolti e attua tempestive azioni correttive in stretto coordinamento con il dirigente che ha provveduto alla presente nomina e con il DPO dell'Amministrazione.

In tali evenienze, il Responsabile mette in atto, almeno, misure capaci di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali di cui all'art. 32, par. 1, lett. c) del GDPR, oltre a circoscrivere gli effetti negativi dell'evento.

DPIA (Data Protection Impact Assessment)

Qualora i trattamenti dovessero presentare un rischio elevato per la dignità e la libertà delle persone, il Responsabile assiste e supporta l'Amministrazione nella valutazione di impatto (DPIA) e nell'eventuale consultazione preliminare all'Autorità di controllo, se richiesto.

Controlli e attività di audit

Al fine di mantenere il pieno controllo sui dati, l'Amministrazione ha diritto di ottenere dal Responsabile tutte le informazioni relative alle misure tecniche e organizzative per poter dimostrare il rispetto delle istruzioni e degli obblighi affidati e poter disporre a propria cura e spese, verifiche a campione o specifiche attività di *audit*. Su richiesta dell'Amministrazione, il Responsabile consente le verifiche sul rispetto del presente accordo.

Il Responsabile ha, comunque, la facoltà di sottoporre ad *audit* periodici la sicurezza dei sistemi e degli ambienti di elaborazione dei dati personali dallo stesso utilizzati per l'erogazione dei servizi e le sedi in cui avviene tale trattamento.

Al riguardo il Responsabile ha la possibilità di incaricare dei professionisti indipendenti per lo svolgimento di *audit* secondo standard internazionali e/o best practice, i cui esiti vengono riportati in specifici report. Tali report, che costituiscono informazioni confidenziali del Responsabile, sono resi disponibili all'Amministrazione, su richiesta, per consentirgli di verificare la conformità dello stesso Responsabile agli obblighi di sicurezza di cui al presente accordo.

Dette attività di verifica possono essere eseguite in orari da concordare e con modalità che consentano il rispetto della riservatezza nei confronti di altri soggetti e che, in ogni caso, non ledano o mettano in alcun modo in pericolo i segreti aziendali o il *know how* del Responsabile.

A tali fini, l'Amministrazione può sottoporre periodicamente al Responsabile un *questionario* sul livello di attuazione delle misure di sicurezza, debitamente compilato e restituito in tempi brevi.

Misure per garantire la sicurezza delle banche dati dell'Amministrazione

Il Responsabile si impegna a mettere in atto le misure elencate a titolo esemplificativo e non esaustivo dal legislatore unionale nell'art. 32 del GDPR allo scopo di garantire la sicurezza delle banche dati dell'Amministrazione (**Allegato B**).

Il Responsabile, tenuto conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, mette in atto misure che comprendono, se del caso:

- 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.

Nei casi in cui il Responsabile evidenzia una non piena corrispondenza tra la tipologia di trattamento prevista dal contratto di servizio e le misure di sicurezza, si impegna a comunicarlo per scritto all'Amministrazione, fornendogli l'analisi dei rischi effettuata e indicando le misure di sicurezza che ritiene adeguate. Tale comunicazione va fatta via PEC: comunegenova@postemailcertificata.it e contestualmente alla e-mail del DPO: rpdpd@comune.genova.it

Conservazione e cancellazione dei dati

Limitatamente alle informazioni necessarie a consentire all'Amministrazione l'eventuale esercizio

del diritto di difesa in sede giudiziaria e di accertamento fiscale, il periodo di conservazione viene determinato sulla base della normativa vigente in materia che, nello specifico, è dieci anni (art. 2946 del codice civile). Per la conservazione dei log che tracciano gli accessi degli Admin la conservazione è minimo sei mesi.

Al termine per qualsiasi causa del contratto di servizio e decorso il periodo di conservazione obbligatoria, il Responsabile cancella tutti i dati o li anonimizza e comunque li rende inutilizzabili in maniera irreversibile, comprese le copie esistenti, mediante tecniche adeguate **entro un arco temporale breve** e lo comunica via PEC al titolare: comunegenova@postemailcertificata.it

L'Amministrazione si riserva il diritto di effettuare controlli e verifiche al fine di accertare la veridicità delle dichiarazioni rese.

La cancellazione o l'anonimizzazione dei dati non si applica ai contratti di servizio che hanno come oggetto prodotti software installati presso l'Amministrazione (esempio, soluzioni on premise). In tali casi, è responsabilità dell'Amministrazione estrarre, entro e non oltre il termine previsto dal contratto di servizio, i dati personali che ritenga utile conservare.

Disposizioni finali

Il Responsabile si impegna a tenere indenne l'Amministrazione da ogni responsabilità, spese, pretese, azioni o procedimenti o altri oneri discendenti dalla violazione del presente accordo o della normativa in materia di protezione dei dati personali, per fatto proprio, da parte del medesimo Responsabile o di suoi dipendenti o collaboratori o eventuali sub-responsabili del trattamento.

Il Responsabile è consapevole che gli impegni assunti con la presente nomina si intendono a titolo non oneroso in quanto già retribuiti nel negozio giuridico (es. contratto, accordo, convenzione).

In conformità con quanto disposto dall'art. 28, par. 10 del GDPR nel caso in cui il Responsabile determini finalità e mezzi del trattamento sarà considerato titolare del trattamento per le attività effettuate.

Banche dati messe a disposizione del Responsabile:

Le banche dati trattate per conto dell'Amministrazione sono le seguenti:

-
-

Inizio e durata del trattamento

Il Responsabile è autorizzato ad effettuare il trattamento dei dati personali solamente in seguito **alla reciproca sottoscrizione del presente accordo**. La durata del trattamento corrisponde alla **durata del contratto di servizio**, inclusi eventuali rinnovi, fino a revoca.

L'Amministrazione consente al Responsabile l'accesso ai soli dati personali adeguati, pertinenti e limitati (minimizzazione dei dati), la cui conoscenza sia necessaria per dare piena esecuzione al contratto di servizio citato in apertura.

Normativa applicabile

Per **normativa applicabile** si intende l'insieme delle norme rilevanti in materia di protezione dei dati personali, in ogni tempo, come la normativa nazionale di adeguamento al GDPR, il Codice privacy, nonché i provvedimenti dell'Autorità di controllo o da altre Autorità di controllo quali, ad esempio, il Garante europeo della protezione dei dati (GEPD).

Viene elencata di seguito la principale normativa applicabile:

- **regolamento generale (UE) 2016/679** del Parlamento europeo e del Consiglio del 27 aprile 2016 (GDPR) relativo alla protezione dei dati personali e alla libera circolazione di tali dati;
- **d.lgs. 30 giugno 2003, n. 196** e s.m.i. (codice privacy);

- **d.lgs. 18 maggio 2018, n. 51** che ha dato attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativamente a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, ove applicabile;

inoltre:

- **provvedimento del Garante 27 novembre 2008**, modificato nel 2009, relativo alle funzioni di amministratore di sistema;
- **provvedimento del Garante 8 aprile 2010** in materia di videosorveglianza, ove applicabile.
- **circolare AgID n. 2/2017 del 18 aprile 2017** in materia di misure minime di sicurezza ICT per le pubbliche amministrazioni, per le parti di competenza;
- **linee guida AgID 547/2021 del 01.10.2021** che definiscono il modello di interoperabilità tra amministrazioni e centrali, regionali e locali, nonché tra queste e i sistemi dell'Unione con i gestori di servizi pubblici e dei soggetti privati.

Il presente accordo è assoggettato a imposta di bollo ai sensi dell'allegato A – Tariffa, art. 2 [Scritture private contenenti convenzioni o dichiarazioni, descrizioni, constatazioni e inventari] del D.P.R. 26/10/1972, n. 642.

Allegati

Allegato A - Descrizione del trattamento

Allegato B - Misure per la sicurezza del trattamento

TITOLARE DEL TRATTAMENTO

Dott.

Direzione

Comune di Genova

RESPONSABILE DEL TRATTAMENTO

per integrale accettazione

Dott.

Legale rappresentante pro tempore

Società

Allegato A - Descrizione del trattamento

[da compilare a cura del Responsabile del trattamento]

Ruoli Privacy	<u>Titolare del trattamento</u> Civica Amministrazione della Città di Genova	<u>Responsabile del trattamento</u>
Natura del trattamento [descrivere brevemente il trattamento]		
Finalità del trattamento [indicare i motivi del trattamento]		
Tipologie dei dati [indicare i dati trattati] - - - -	<i>Elenco indicativo e non esaustivo:</i> dati identificativi e di contatto, immagini, es. foto e video, dati di navigazione, etc. dati particolari (art. 9 del GDPR) idonei a rivelare origine razziale o etnica, convinzioni religiose filosofiche, opinioni politiche, etc., dati relativi allo stato di salute attuale e/o pregresso dati penali (art. 10 del GDPR) altro	
Categorie degli interessati [indicare le categorie degli interessati] - -	cittadini [residenti e non nella Città di Genova], dipendenti, minori, soggetti vulnerabili, etc. altro	
Informazioni sul trattamento dei dati personali [indicare le modalità] - -	Il modulo dell'informativa privacy ai sensi dell'art. 12 del GDPR, redatta dall'Amministrazione, deve essere: consegnata in forma cartacea all'interessato pubblicata on line su [es. indicare la piattaforma, il portale] resa dal Responsabile altro/non applicabile	
Gestione consenso [indicare le modalità] - -	Il modulo del consenso ai sensi degli artt. 6, par. 1, lett. a) e 7, par. 1 del GDPR, redatto dall'Amministrazione, deve essere: consegnato in forma cartacea all'interessato e registrato dall'Amministrazione, consegnato in forma cartacea all'interessato e registrato dal Responsabile che dovrà restituire il modulo firmato all'Amministrazione raccolto e registrato in formato elettronico tramite il seguente sistema [indicare l'applicativo] Altro/non applicabile	
Certificazioni [elencare eventuali certificazioni] - -	gli standard di riferimento sono, ad esempio: UNI EN ISO 9001 (sistema di gestione per la qualità), UNI CEI EN ISO/IEC 27001 (sistema di gestione della sicurezza dell'informazione).	

Allegato B – Misure per la sicurezza del trattamento

[da compilare a cura del Responsabile del trattamento]

Misure di <u>sicurezza fisica</u> applicate ai sistemi del titolare	[rispondere alle singole domande]
Qual'è la collocazione geografica del server o del cloud?	-
L'accesso ai locali di conservazione dei dati è dotato di sistemi di allarme, di un impianto di videosorveglianza?	-
Sono presenti, ad esempio, sensori di movimento, sistemi antiallagamento, antincendio, gruppi elettrogeni?	-
Misure di <u>protezione logica</u> applicate ai sistemi del titolare	[rispondere alle singole domande]
Nella difesa contro il malware l'accesso ai dati del titolare è protetto da firewall?	-
Sono installati firewall, sistemi di prevenzione delle intrusioni o intrusion prevention system (IPS)?	-
Nella prevenzione degli attacchi sono utilizzati e mantenuti aggiornati idonei programmi contro il rischio di esecuzione e di intrusione e accesso abusivo a sistema informatico come, ad esempio, anti Malware, Ransomware, Memory Injection, Worms, Trojans?	-
Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati?	-
Viene registrato ogni accesso (log) ai sistemi del titolare?	-
La password è comunicata via cartacea al titolare con cambio obbligatorio al primo accesso?	-
Le credenziali di autenticazione ai sistemi del titolare sono verificate periodicamente? Indicare l'arco temporale.	-
É assicurata la totale distinzione tra utenze non privilegiate e privilegiate degli Admin alle quali debbono corrispondere credenziali diverse?	-
Per le operazioni che richiedono privilegi gli Admin debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	-

<p>Vengono fatte le copie di sicurezza dei dati del titolare?</p> <p>La riservatezza delle informazioni contenute nelle copie di sicurezza o copie di backup avviene mediante adeguata protezione fisica dei supporti ovvero mediante cifratura?</p> <p>Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema, onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza. Si rinvia alla circolare AgID 2/2017.</p> <p>Il trasferimento dei dati personali avviene utilizzando canali di comunicazione sicura, ad esempio, protocollo HTTPS con certificati validi e aggiornati TLS e suite di cifratura 1.3?</p> <p>I certificati TLS con suite di cifratura 1.0 e 1.1 sono obsoleti perchè non supportano algoritmi crittografici e quindi sono vulnerabili agli attacchi, di conseguenza <u>non</u> devono essere utilizzati sui sistemi del titolare. Si rinvia alle Raccomandazioni AgID in merito allo standard Transport Layer Security (TLS) di cui alla determinazione 471/2020 del 03.11.2020.</p>	-
---	---

È onere del Responsabile adottare le misure di sicurezza e organizzative che dovranno avere uno standard elevato di protezione delle banche dati dell'Amministrazione, ed è sempre onere del Responsabile valutare dette misure in relazione al trattamento effettuato e, in particolare:

- natura dei dati (comuni, particolari, penali)
- oggetto e finalità (indicati nel contratto di affidamento del servizio)
- contesto (es. piattaforma digitale, servizi on premise sul server del titolare)

Le misure di sicurezza e organizzative devono essere graduate e implementate in relazione alla natura dei dati e ai rischi connessi al trattamento.

DATI PARTICOLARI e DATI PENALI

Il Responsabile può trattare dati particolari, come definiti dall'art. 9 del GDPR, e dati penali, come definiti dall'art. 10 del GDPR.

Il legislatore nazionale nell'art. 2-octies del Codice privacy nei primi due commi richiama l'art.10 del GDPR per ribadire che il trattamento di questa tipologia di dati è lecito se previsto da una norma di legge o, nei casi previsti dalla legge, di regolamento e in presenza di garanzie appropriate per i diritti e le libertà degli interessati, mentre nel comma 3 elenca i casi tassativi di liceità.

I dati scambiati nelle interazioni tra i sistemi informatici dell'Amministrazione e del Responsabile possono contenere al proprio interno dati personali appartenenti anche a categorie particolari o relativi a condanne penali e reati (artt. 9 e 10 del GDPR).

In questi casi lo scambio di dati particolari e dati penali deve avvenire in coerenza con le Linee guida AgID sull'interoperabilità, adottate con determinazione 547/2021 del 01.10.2021.

Le citate linee guida privilegiano l'approccio API first (*Application Programming Interface*), come prima opzione, in base al quale l'interoperabilità dei sistemi informativi è il modello di riferimento nella trasmissione dei dati tra amministrazioni e centrali, regionali e locali, nonché tra queste e i sistemi dell'Unione con i gestori di servizi pubblici e dei soggetti privati.

Pertanto, nel caso di trattamento di dati particolari e dati penali, il Responsabile, oltre a garantire il rispetto delle misure di sicurezza previste dall'art. 32 del GDPR, deve adottare le seguenti ulteriori misure:

- negli accessi alle banche dati contenenti dati particolari e dati penali, qualora non sia possibile autenticarsi tramite SPID, utilizzare l'autenticazione multi-fattore, cd. autenticazione forte o OTP (one time password);
- nello scambio dei dati particolari e penali il soggetto erogatore trasmette al soggetto fruitore i dati cifrati e allegati a una PEC; l'erogatore invia, inoltre, al numero di telefono del fruitore la password che li decifra attraverso un successivo SMS (cd. autenticazione multi-fattore);
- se l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (almeno 14 caratteri alfanumerici);
- non trasmettere mai i dati particolari e i dati penali in chiaro; il trasporto dei dati particolari e dei dati penali deve avvenire in modo sicuro, tenuto conto dell'evoluzione tecnologica, attraverso canali crittografati, ad esempio utilizzando il protocollo HTTPS con certificati validi e aggiornati TLS e suite di cifratura 1.3;
- separare (pseudonomizzare) dai restanti dati comuni (es. nome e cognome, telefono, indirizzo e-mail, codice fiscale, etc.) i dati particolari e i dati penali dell'interessato;
- conservare i dati particolari e i dati penali cifrati con algoritmi, aggiornati allo stato dell'arte, che garantiscono livelli di sicurezza adeguati, in modo da impedirne la intelligibilità ai soggetti non autorizzati, come nel caso di acquisizione fortuita o a seguito di guasti o interventi manutentivi sulle apparecchiature informatiche.

Con l'adozione delle citate misure di sicurezza si riducono sensibilmente i rischi di accesso accidentale o illecito, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

I dati particolari e i dati penali, contenuti in documenti cartacei, devono essere conservati in armadi o cassetti muniti di serratura chiusa a chiave.