COMUNE DI GAVI

PROVINCIA DI ALESSANDRIA

COMUNICAZIONE VIA PEC ALL'INDIRIZZO: apkappa@legalmail.it

SPETT.LE
APKAPPA S.r.l.
Via M.K. Gandhi, n. 24/A I
42123 REGGIO EMILIA
C.F./P.IVA 08543640158

OGGETTO: "MISURA 1.4.1 "ESPERIENZA DEL CITTADINO NEI SERVIZI PUBBLICI" – COMUNI (SETTEMBRE 2022) – MISSIONE 1 COMPONENTE 1 DEL PNRR INVESTIMENTO 1.4 "SERVIZI E CITTADINANZA DIGITALE" FINANZIATO DALL'U.E. – NEXT GENERATION EU - SERVIZI DIGITALI COMUNE (CITTADINO ATTIVO) – "SPORTELLO TELEMATICO POLIFUNZIONALE" CUP I91F22001090006- CIG 99352679B0

In conseguenza dell'affidamento del servizio di che trattasi, il fornitore si trova ad effettuare il trattamento di dati personali per conto dell'Ente scrivente (Titolare del trattamento), assumendo la qualifica di Responsabile del trattamento ai sensi e per gli effetti di cui all'articolo 28 del Regolamento (UE) 2016/679 (di seguito, per brevità, "GDPR").Egli è, pertanto, autorizzato al compimento delle sole operazioni di trattamento necessarie, con riferimento ai soli dati personali necessari, ad eseguire le prestazioni affidate.

I rapporti tra Titolaree Responsabile saranno regolamentati – ai sensi dell'articolo 28 del GDPR – dalle prescrizioni contenute nel Disciplinare allegato,le quali potranno subire modifiche ed integrazioni in conseguenza della valutazione delle informazioni, documenti e dichiarazioni richiesti con la presente comunicazione.

Il Responsabile deve elaborare apposito documento contenente la descrizione del proprio servizio, sotto il profilo del trattamento dei dati personali, avendo cura di precisare:

A) le categorie di dati personali coinvolte dalle operazioni di trattamento quali:
B) le operazioni di trattamento previste, quali:
C) le modalità tecniche, tecnologiche ed organizzative di erogazione del servizio (comprensive altresì della descrizione delle procedure di raccolta, conservazione e comunicazione dei dati personali, possibilmente accompagnata da screenshot delle varie fasi di funzionamento);
D) la piattaforma utilizzata per la distribuzione dell'app;
E) le modalità, tecniche ed organizzative, mediante le quali il fornitore ha reso disponibili all'utenza le informazioni prescritte dagli articoli 13 e 14 del GDPR (compresa la produzione del testo utilizzato);
F) le modalità, tecniche ed organizzative, mediante le quali il fornitore ha previsto l'esercizio dei diritti dell'interessato ed il relativo riscontro;
G) le attività e gli oneri (esclusi quelli di carattere economico) previsti a carico del Titolare, necessari per consentire la sicurezza del trattamento dei dati personali e la sua conformità alla normativa.

H) l'esistenza di disposizioni normative o dell'Autorità che impongano una conservazione dei dati personali trattati per conto del Titolare, anche oltre la scadenza del servizio affidato (e relativi tempi di conservazione);

Il Responsabiledovrà dimostrare - mediante la produzione di adeguata documentazione - di possedere esperienza, capacità e affidabilità idonee a garantire il rispetto delledisposizioni in materia di trattamento, ivi compreso il profilo relativo allasicurezza, ed in ogni caso di essere in grado di fornire garanzie sufficienti permettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti della normativa e garantisca la tutela deidiritti dell'Interessato.
La documentazione di cui al paragrafo precedente dovrà espressamente contenere:
a) informazioni relative al possesso di certificazioni relative alla protezione dei dati e, più in generale, alla sicurezza ed alla gestione degli stessi (a mero titolo esemplificativo, categoria ISO/IEC 27000);
b) informazioni relative alla qualificazione e presenza nel catalogo dei servizi cloud qualificati per la PA di AgID e/o relative alla qualificazione e sottoscrizione di un accordo di servizio con PagoPASpA;
c) la descrizione (tipologica) delle misure di sicurezza adottate per prevenire perdite di integrità, disponibilità e confidenzialità dei dati personali, con riferimento ai luoghi fisici ove avverranno le operazioni di trattamento;
d) la descrizione (tipologica) delle misure di sicurezza adottate per prevenire perdite di integrità, disponibilità e confidenzialità dei dati personali, con riferimento all'infrastruttura tecnologica (hardware e software) utilizzata per il trattamento;
e) la descrizione delle misure organizzative e di formazione adottate con riferimento al personale addetto alle operazioni di trattamento per conto del Titolare;
f) la descrizione delle procedure di acquisizione dei dati personali presso il Titolare del trattamento e di quelle di riconsegna al termine dell'affidamento;
g) le modalità, anche tecniche e le procedure mediante le quali il Responsabile intende assicurare l'esattezza, la veridicità, l'aggiornamento, la pertinenza e la non eccedenza dei dati personali oggetto di trattamento, per conto del Titolare, rispetto alle finalità per le quali sono stati raccolti e saranno successivamente trattati;
h) la dichiarazione di non esser stato destinatario di provvedimenti sanzionatori o correttivi definitivi ad opera del Garante per la protezione dei dati personali o di altra Autorità di controllo o, in alternativa, l'indicazione dei provvedimenti subìti;
i) l'indicazione in merito all'avvenuta designazione del Responsabile per la protezione dei dati personali (RPD o DPO), ovvero dichiarazione di non sottostare a tale obbligo;
l) l'indicazione in merito alla tenuta dei registri delle attività di trattamento, ovvero dichiarazione di non sottostare a tale obbligo;

Qualora, in relazione al trattamento di dati personali effettuato dal Responsabile per conto di altro Titolare in fattispecie assimilabile a quella oggetto di affidamento, sia già stata effettuata una valutazione d'impatto sulla protezione dei dati personali - ai sensi dell'articolo 35 del GDPR – il Responsabile ne fornisce le informazioni rilevanti, impegnandosi a prestare al Titolare la collaborazione necessaria a condurre la propria valutazione. In caso non sia stata effettuata o non sia disponibile, il fornitore deve relazionare in merito alle soluzioni tecniche ed organizzative adottate con riferimento alle seguenti categorie di rischio (indicando, per ciascuna, quali misure contribuiscono a mitigare il rischio, quale sia la gravità del rischio e come stima la probabilità di verificazione del rischio, tenuto conto delle misure adottate o pianificate):

1) accesso illegittimo ai dati;
2) modifiche indesiderate ai dati;
3) perdita di dati

Ove il fornitore intenda trasferire all'estero i dati personali oggetto di trattamento per conto del Titolare, ne dovrà fare espressa menzione, indicando:
a) il paese nel quale s'intendono trasferire i dati personali;
b) le categorie di dati personali oggetto di trasferimento;
c) le tipologie di soggetti i cui dati personali saranno trasferiti;
d) le operazioni di trattamento previste a seguito del trasferimento;
e) ove il trasferimento avvenga verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, l'indicazione circa le modalità ed i termini che garantiscono il rispetto delle disposizioni contenute nel capo V del GDPR.

Nel caso il fornitore intenda ricorrere ad altro soggetto ("Sub-responsabile") per eseguire tutte o parte delle operazioni di trattamento per conto del Titolare, ne deve fare espressa menzione, al fine di consentire al Titolare di compiere le valutazioni necessarie al rilascio della prescritta autorizzazione. A tal fine il Responsabile specifica, per ciascun Sub-responsabile:
a) i dati identificativi, fiscali e di contatto del Sub-responsabile;
b) le categorie dei dati personali il cui trattamento avverrà ad opera del Sub-responsabile;
c) le tipologie di soggetti i cui dati personali saranno trattati dal Sub-responsabile;
d) le operazioni di trattamento a carico del Sub-responsabile;
e) il possesso, da parte del Sub-responsabile, di certificazioni, qualificazioni o simili, in relazione al trattamento dei dati;
f) la dichiarazione di aver verificato che il Sub-responsabilepresenti 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;
g) nel caso il trattamento ad opera del Sub-responsabilepreveda il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, dovrà essere specificato se tale trasferimento sia conseguente ad una libera scelta imprenditoriale, ovvero imposto dal diritto dell'Unione europea o nazionale cui è soggetto il Responsabiledel trattamento (salvo che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico).

In relazione alla gestione degli eventi costituenti violazione di dati personali (data breach), il Responsabile dichiara:
a) di aver (o non avere) adottato una apposita procedura di gestione;
b) di aver preso conoscenza dell'apposita procedura di gestione adottata dal Titolare;
c) di aver (o non avere) predisposto e tenuto aggiornato un registro interno delle violazioni di dati personali.

Per qualsivoglia ulteriore informazione è possibile contattare il Responsabile della Protezione dei Dati Personali, avv. Massimo Ramello, al seguente indirizzo PEC: dpo@pec.gdpr.nelcomune.it

Si confida in un sollecito riscontro e si porgono distinti saluti.

Gavi, 28/06/2023

Il Segretario Comunale
Dott. Stefano Valerii

COMUNE DI GAVI
Prov. di Alessandria

Via G. Mameli n. 44 – 15066 GAVI (Al) – C.F./P.IVA 00367950060
Tel. 0143 642712 – 0143 645091
Mail :segreteriasindaco@comunegavi.it – segreteriasindaco@pec.comunegavi.it