



Trento, 31 ottobre 2023
MAM

Al Presidente
Al Segretario
Al Referente Privacy
Della Comunità di Primiero

interoperabilità PITRE

OGGETTO: Servizio privacy RPD – espressione del parere sulla Valutazione di impatto condotta sulle attività di trattamento del Servizio Mensa-Istruzione

In riferimento alla Vostra richiesta di data 23 agosto 2023, relativa all'argomento di cui all'oggetto, e successive integrazioni, si fornisce di seguito la risposta elaborata dal Responsabile Protezione Dati - Servizio privacy.

Per ogni chiarimento doveste ritenere utile o necessario potete contattare la dott.ssa Federica Dallaporta o la dott.ssa Marta Mattiello ai seguenti recapiti: tel. 0461 987139 - e-mail serviziordp@comunitrentini.it.

Premesso che:

- la valutazione di impatto sulla protezione dei dati, di seguito in sigla DPIA, è una procedura intesa a descrivere un trattamento, a valutarne la necessità e la proporzionalità nonché a valutarne i rischi per i diritti e libertà delle persone fisiche, allo scopo di determinare le misure per affrontarli, gestirli e se possibile eliminarli o comunque ridurli al minimo;
- la DPIA è uno strumento importante in termini di responsabilizzazione (c.d. *accountability*) in quanto aiuta il Titolare non soltanto a rispettare le prescrizioni del Regolamento Europeo 679/2016 ma anche ad attestare di aver adottato misure idonee a garantire tali prescrizioni;
- ai sensi dell'art. 5, par. 2, del Regolamento Europeo 679/2016, la Comunità di Primiero, quale Titolare del trattamento, è competente per il rispetto delle disposizioni relative alla protezione delle persone fisiche a riguardo del trattamento dei dati personali ed in grado di provarlo secondo il principio della "*responsabilizzazione*";
- ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679, la Comunità ha ritenuto che i trattamenti sopra descritti rientrino nella casistica obbligatoria di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati in quanto possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche e i trattamenti riguardano dati particolari su larga scala;
- la Comunità ha acquisito, laddove necessario, le informazioni di settore presso l'amministratore di sistema, il fornitore del software/servizio e presso i responsabili dei servizi che si occupano dell'attività di trattamento e del gruppo di attività di trattamento omogeneo - trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi- sottoposto a DPIA;
- la Comunità, nel processo di conduzione della Valutazione di impatto, ha individuato quali sono i trattamenti a rischio più elevato con riferimento all'incisività





nei diritti degli interessati e, alla luce di tali risultanze, ha verificato di aver adottato, o di dover implementare, misure di sicurezza adeguate al fine di ridurre il predetto rischio.

Preso atto che la documentazione visionata è la seguente:

- Valutazione di impatto;
- Analisi dei rischi;
- Nomina designato;
- Nomina incaricati;
- Nomina Responsabile esterno del trattamento;
- Codice di comportamento dei dipendenti;
- Aggiornamenti delle misure di sicurezza informatica (2019 e 2022);
- Documento ricognitivo sulle misure di sicurezza tecnico-informatiche;
- Regolamento per l'applicazione del lavoro agile (smart working) presso la Comunità di Primiero;
- Informativa Settore Affari Generali;
- Valutazione d'impatto condotta dal responsabile del trattamento (Etica Soluzioni) con riferimento alla soluzione tecnologica "School.Net".

Rilevato che la documentazione da voi fornita risulta correttamente istruita e contenente le informazioni e valutazioni necessarie, e preso atto delle interlocuzioni e integrazioni ottenute con e-mail dd. 12.09.2023, nello specifico si valuta che:

- la descrizione sistematica dei trattamenti previsti e delle finalità del trattamento è adeguata;
- la valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità è adeguata;
- la valutazione dei rischi per i diritti e le libertà degli interessati è correttamente ponderata;
- il risultato finale e complessivo della valutazione dei rischi connessi al trattamento presenta un livello medio-basso di rischio generale per i diritti e le libertà degli interessati;
- il titolare, a seguito dell'analisi dei rischi ottenuta, nonostante il rischio medio-basso rilevato, ha comunque ritenuto opportuno adottare ulteriori misure per la mitigazione dei rischi, tra le quali la formazione continua del personale e il costante aggiornamento delle misure di sicurezza da parte dell'amministratore di sistema, nonché l'implementare un nuovo sistema di accesso ai locali dell'Ente e vietando l'utilizzo di strumenti di memorizzazione esterna.

Alla luce di quanto sopra si esprime parere favorevole condizionato alla osservanza delle seguenti prescrizioni e indicazioni:

- è opportuno dare attuazione e implementazione alle misure di mitigazione del rischio in ragione di un programma definito. Si suggerisce, in particolare, di adottare un cronoprogramma, all'interno del quale calendarizzare l'implementazione delle misure di mitigazione dei rischi e, in tal senso, chiediamo di essere notiziati in merito alla completa o parziale adozione delle misure indicate;





- si raccomanda di applicare il principio “privacy by default e by design” a tutte le piattaforme web utilizzate, verificando, laddove possibile preventivamente e comunque in ogni caso, che, per impostazione predefinita, tramite gli applicativi web vengano trattati i soli dati necessari all'erogazione del servizio e che le misure di sicurezza attuate dai fornitori e/ manutentori siano sufficienti ad attenuare il rischio sui dati personali;
- è opportuno prestare attenzione ai casi in cui venga previsto un trasferimento dei dati fuori dallo spazio Economico Europeo, individuando specificamente le garanzie del trasferimento, intensificando le tempistiche di controllo sul fornitore e considerando che per effettuare tali attività è necessario un livello di conoscenza del software/applicazione utilizzo molto approfondito, nonché degli strumenti impiegati per il trasferimento;
- si evidenzia che, nell'implementare un nuovo sistema di accesso ai locali dell'Ente, dovranno tassativamente essere evitati sistemi che permettano il riconoscimento biometrico dei dipendenti (es. accesso tramite impronta digitale); ciò in quanto, in virtù della sua particolare natura, il trattamento di dati biometrici è di regola vietato in base all'articolo 9, par.1 GDPR, ammesso nei limiti definiti dall'art. 9, par. 2, lett. b) ed occorre che avvenga in “in conformità alle misure di garanzia disposte dal Garante” (art. 2-septies comma 1 Codice Privacy) e nel rispetto dei principi di liceità, correttezza e trasparenza, limitazione della finalità e minimizzazione.

Si rammenta che la valutazione d'impatto è una misura di *accountability* e in quanto tale è necessario condurla nuovamente su medesime attività di trattamento se:

- vi è una variazione delle caratteristiche delle attività trattamento (modalità del trattamento o modifiche impattanti sugli aspetti della sicurezza fisica, tecnica, organizzativa e informatica);
- se l'attività di trattamento riguarda dati particolari che, per loro natura, richiedono una maggiore tutela e cura;
- in ogni caso, periodicamente, alla modifica delle condizioni generali interne alla struttura organizzativa dell'Ente.

Infine, si suggerisce di provvedere ad informare la cittadinanza dell'attività di conduzione delle valutazioni d'impatto, tramite la pubblicazione di un avviso sul sito istituzionale e/o attraverso la pubblicazione all'albo pretorio o altre forme di comunicazione ritenute idonee.

Cordiali saluti.

Il Referente
Responsabile della Protezione dei dati
Dott. Gianni Festi

La Responsabile del procedimento
dott.ssa Laura Marinelli

