



Unione Montana dei Comuni del Monviso COMUNE DI SANFRONT

Piazza Statuto n° 2 - 12030 Sanfront (CN)
Tel. 0175 948119 - Fax 0175 948867
Email: info@comune.sanfront.cn.it
Pec: comune.sanfront@pec.it
C. F. 85002210046 - P. IVA 00564590040



DECRETO N. 1/2021
Prot. n. 2078

IL SINDACO

PREMESSO CHE :

1. il titolare del trattamento, ai sensi dell'art. 5, par. 2, del Regolamento 2016/679 è competente per il rispetto delle disposizioni relative alla protezione delle persone fisiche a riguardo del trattamento dei dati personali ed in grado di comprovarlo («responsabilizzazione»).
2. Il Titolare del Trattamento, ai sensi dell'articolo 35, par. 2, del Regolamento 2016/679, ha inoltrato richiesta di consultazione relativa al/i seguente/i trattamento/i: trattamento dei dati personali tramite un sistema di videosorveglianza presente sul territorio comunale.
3. Si rende pertanto opportuno redigere una valutazione di impatto sulla protezione dei dati (DPIA).
4. La disciplina sulla DPIA contenuta nel GDPR deve essere integrata da quanto specificato dal WP art. 29 nelle linee guida pubblicate in data 4.10.2017.

In particolare, il WP art. 29 ha definito i criteri in base ai quali decidere se fare ricorso o meno a una DPIA, quali sono le metodologie utilizzabili dai titolari per condurre una DPIA e quali sono gli elementi sufficienti per una DPIA accettabile.

4.1. Soggetto obbligato

Il GDPR impone al solo titolare del trattamento di effettuare la DPIA, qualora ne ricorrano i presupposti (cfr. art. 35). Nello svolgimento di una DPIA il titolare potrà essere coadiuvato dal DPO e dal responsabile.

Quando un trattamento è svolto in contitolarità, nella DPIA devono essere specificati con precisione gli obblighi che incombono su ciascun titolare, ad esempio con riferimento alla responsabilità delle singole misure finalizzate alla gestione dei rischi.

4.2. In quali casi è necessario effettuare una DPIA

La DPIA è obbligatoria solo qualora un trattamento "possa presentare un rischio elevato" per i diritti e le libertà delle persone fisiche.

Nei casi dubbi, si raccomanda di svolgere comunque una DPIA, in quanto questa è una procedura che permette di realizzare e dimostrare la conformità con le norme del GDPR.

Il riferimento ai "diritti e alle libertà" va inteso come relativo al diritto alla privacy e anche ad altri diritti fondamentali, quali la libertà di espressione e di pensiero, la libertà di movimento, il divieto di discriminazioni, il diritto alla libertà di coscienza e di religione.

4.2.a) Casi previsti dal GDPR

L'art. 35, paragrafo 3, GDPR cita espressamente tre casi in cui sussiste un rischio elevato ed è quindi necessaria l'effettuazione di una DPIA, ossia:

- valutazione sistematica e globale, basata su un trattamento automatizzato, degli aspetti personali relativi a persone fisiche (compresa la profilazione), e sulla quale si fondano decisioni che hanno effetti giuridici o incidono significativamente su tali soggetti;
- trattamento su larga scala di dati sensibili o giudiziari;
- sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Tale elenco non è esaustivo.

Secondo il WP art. 29 la DPIA deve essere anche condotta per valutare l'impatto di un nuovo dispositivo tecnologico in termini di protezione dei dati.

Il GDPR assegna alle autorità di controllo (per l'Italia, al Garante) il compito di redigere e rendere pubblico un elenco delle tipologie di trattamento da assoggettare e da non assoggettare a DPIA (cfr. art. 35, par. 4 e 5).

4.2.b) I 9 criteri enunciati dal WP art. 29

Secondo il WP art. 29 i seguenti 9 criteri devono essere presi in esame sia dalle autorità di controllo per redigere l'elenco delle tipologie di trattamento da assoggettare a DPIA ex art. 35, par. 4, GDPR, sia dai titolari per comprendere quando siano tenuti a svolgere una DPIA:

1. trattamenti valutativi o di *scoring*, compresa la profilazione e attività predittive, in particolare a partire da "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato" (considerando 71 e 91). Ad es.: società che crea profili comportamentali o di *marketing* a partire dalla operazioni o dalla navigazione compiute sul proprio sito internet;
2. decisioni automatizzate che producono significativi effetti giuridici o di analoga natura. Ad es.: trattamento che possa comportare l'esclusione di una persona fisica da determinati benefici ovvero la sua discriminazione;
3. monitoraggio sistematico: trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o "la sorveglianza sistematica di un'area accessibile al pubblico";
4. dati sensibili o dati di natura estremamente personale: si tratta dei dati sensibili di cui all'art. 9 e dei dati giudiziari di cui all'art. 10;
5. trattamenti di dati su larga scala: il GDPR si occupa del termine "larga scala" nel considerando 91. Il Gruppo art. 29 raccomanda di tenere conto dei seguenti fattori al fine di stabilire se un trattamento sia svolto su larga scala: a) numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; b) volume dei dati e/ o ambito delle diverse tipologie di dati oggetto di trattamento; c) durata, o persistenza, dell'attività di trattamento; d) ambito geografico dell'attività di trattamento;
6. combinazione o raffronto di insieme di dati, per esempio derivanti da due o più trattamenti svolti per diverse finalità e/ o da titolari distinti;
7. dati relativi a interessati vulnerabili (cons. 75), compresi i minori, i dipendenti, i soggetti con patologie psichiatriche, i richiedenti asilo, gli anziani, i pazienti e ogni interessato rispetto al quale possa identificarsi una situazione di disequilibrio con il rispettivo titolare del trattamento;
8. utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

9. trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (art. 22 e cons. 91). Ad es.: *screening* dei clienti di una banca attraverso i dati registrati in una centrale rischi al fine di stabilire se ammetterli o meno ad un finanziamento.

Quando ricorrono almeno due dei criteri sopra indicati, il titolare dovrà condurre una DPIA. Tuttavia, in alcuni casi si dovrà procedere a una DPIA anche di fronte ad un trattamento che soddisfi solo uno dei criteri di cui sopra.

È, inoltre, possibile che vi sia perfetta coincidenza tra le ipotesi legislative e i criteri enucleati dal WP art. 29 (ad es. la profilazione sistematica che impatta significativamente sull'interessato non è solo un caso legislativamente previsto di DPIA obbligatoria ex art. 35, par. 3, lett. a) GDPR, ma anche la combinazione dei criteri n° 1, 2 e 3 stabiliti dal WP art. 29).

Si potrebbe verificare anche il caso, ma il WP art. 29 non chiarisce quando tale ipotesi potrebbe verificarsi in concreto, in cui il titolare esclude che debba svolgersi una DPIA perché, pur in presenza dei criteri summenzionati, il trattamento non presenta un rischio elevato. In questo caso, il titolare dovrà motivare e documentare la scelta della mancata conduzione della DPIA, allegando o annotando il parere del DPO. Possiamo immaginare che si tratti della situazione in cui vengano adottate dal titolare misure di sicurezza tali da scongiurare la possibilità di rischio (elevato) per i diritti e le libertà degli interessati (ad es. mediante la pseudonimizzazione e la cifratura dei dati che vengono profilati).

DECRETA

- DI ADOTTARE la valutazione d'impatto “Data Protection Impact Assessment - artt. 35, parag. 2, e 39, parag. 1, lett. c) Regolamento generale sulla protezione dei dati n. 679/16 (GDPR)” per il Comune di Sanfront, predisposta dal Responsabile della Protezione dei dati Avv. Silvio Tavella in data 20/03/2020.

SANFRONT, Lì 21 maggio 2021


Il SINDACO
(MEIRONE Rag. Emidio)
