COMUNE DI SIGNA

(CITTA' METROPOLITANA DI FIRENZE)

# Valutazione di impatto sulla protezione del dati

(Regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati)

Sommario

1. SCOPO E CAMPO DI APPLICAZIONE

Il presente documento descrive le istruzioni operative, le attività e i compiti assegnati a diversi ruoli coinvolti nella valutazione dell'impatto sulla protezione dei dati ai sensi dell'articolo 35 del Regolamento UE 679/2016 ed redatto in coerenza con l'approccio basato sul rischio che informa la normativa.

La valutazione dell'impatto sulla protezione dei dati (di seguito DPIA) si applica solo a fronte di un nuovo trattamento che può comportare un rischio elevalo per i diritti e le libertà delle persone fisiche(art. 35, paragrafo 1).

Al fine chiarire l'ambito e i confini di applicazione, le attività da eseguire e le responsabilità da coinvolgere di seguito sarà chiarito il concetto di DPIA e sarà indicata la procedura da adottare nei casi in cui l'applicazione risulta obbligatoria.

2. RIFERIMENTI NORMATIVI

- Regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati (di seguito definito RGPD);
- Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento possa presentare un rischio elevato ai sensi del regolamento 2016/679, adottate il 4 aprile 2017 (versione successivamente emendata e adottata il 4 ottobre 2017)

3. DEFINIZIONI

**Valutazione dell' impatto sulla protezione dei dati (DPIA)**: è una procedura prevista dall'articolo 35 del Regolamento UE 679/2016 che mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonchè i relativi rischi alo scopo di approntare misure idonee ad affrontarli.

**Rischio**: è uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità» per i diritti e le libertà. Il rischio in questa procedura è sempre riferito all'interessato.

**Sicurezza del trattamento**: è una situazione riferita ad uno specifico trattamento per la quale sono garantiti la disponibilità, integrità e riservatezza dei dati trattati.

**Dato personale**: 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.

**Trattamento**: 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;

**Limitazione di trattamento**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

**Titolare del trattamento**: 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

**Responsabile del trattamento**: la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

**Destinatario:** la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

**Violazione dei dati personali (Personal Data Breach):** la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

**Responsabile per la Protezione dei Dati**: è il soggetto individuato dal titolare ai sensi degli artt. 37-39 del Regolamento UE 2016/679, che ha compiti di controllo e di supporto alla struttura in tema di protezione dei dati personali.

**Autorità di Controllo**: Autorità Garante per la protezione dei dati personali.

**WP29:** Gruppo di lavoro composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro dell'Unione Europea.

4. MODALITA' DI ATTUAZIONE

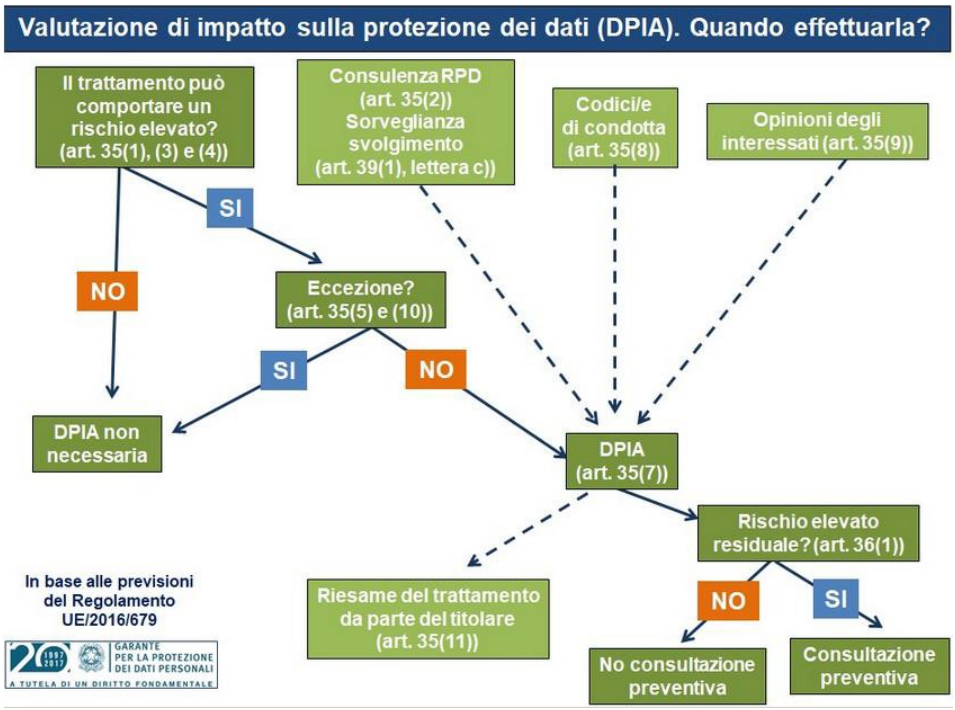
La DPIA si applica su iniziativa del Titolare del trattamento e/o su consiglio del Responsabile della protezione dei dati in presenza di almeno due dei criteri specifici di seguito elencati (fermo restando che il titolare stesso può decidere di condurre una DPIA anche se ricorre uno solo di tali criteri):

- Trattamenti valutativi o di scoring, compresa la profilazione;
- Decisioni automatizzate che producono significativi effetti giuridici (es. assunzioni, concessione di prestiti, stipula di assicurazioni);
- Monitoraggio sistematico (es. videosorveglianza);
- Trattamento di dati sensibili, giudiziari o di natura estremamente personale (es. informazioni sulle opinioni politiche);
- Trattamenti di dati personali su larga scala;
- Combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio con i Big Data).
- Dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc..);
- Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es. riconoscimento facciale, device IoT, raccolta informatizzata delle impronte digitali, ecc);
- Trattamenti che, di per sé potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es. screening dei clienti di una banca attraverso dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

LA DPIA si applica prima di procedere al trattamento e non si applica qualora il trattamento sia effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e) e trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

5. LE FASI DELLA VALUTAZIONE

Al fine di supportare i Titolari e i Responsabili nelle fasi di valutazione di impatto sulla protezione dei dati, il Garante per la Protezione dei Dati Personali ha realizzato il seguente schema grafico, in coerenza con le linee guida appositamente redatte dal WP29:



6. CONTENUTO DELLA VALUTAZIONE

nel rispetto delle disposizioni del regolamento UE 679/2016, gli elementi volti a garantire la valutazione oggetto della procedura sono i seguenti:

1. descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
2. valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
3. valutazione dei rischi per i diritti e le libertà degli interessati di cui all'art. 35 paragrafo 1;
4. misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Si riporta di seguito lo schema di sintesi con le fasi di valutazione dell'analisi di impatto, con specifica della relativa della norma di riferimento e dei requisiti che ogni fase deve soddisfare:

| Fase della valutazione DPIA | Norma di riferimento | Requisito | |
|---|---|---|---|
| Descrizione trattamento | | art. 35, paragrafo 7, lettera a | Descrizione dei seguenti punti:<br>- Finalità del trattamento<br>- Natura del trattamento<br>- Ambito di applicazione<br>- Contesto (normativo, organizzativo ecc.)<br>- Dati personali registrati<br>- Destinatari del trattamento<br>- Periodo di conservazione dei dati personali<br>- Descrizione funzionale del trattamento<br>- Individuazione delle risorse sulle quali sono registrati i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea);<br>- Codici di condotta approvati applicabili (art. 35, paragrafo 8); |
| Valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità | | art. 35, paragrafo 7, lettera b | Presenza di misure adeguate al fine di garantire:<br>a) il rispetto del regolamento (articolo 35, paragrafo 7, lettera d) con riferimento a:<br>- finalità specifiche, esplicite e legittime (art. 5 , lettera b));<br>- liceità del trattamento (art. 6);<br>- dati adeguati, pertinenti e limitati a quanto necessario (art. 5 paragrafo 1 lett.c));<br>- periodo limitato di conservazione (art. 5 paragrafo 1 ,lettera e));<br>b) la proporzionalità e la necessità del trattamento sulla base di:<br>- finalità determinate, esplicite e legittime (articolo 5, paragrafo 1, lettera b));<br>- liceità del trattamento(articolo 6);<br>- dati personali adeguati, pertinenti e limitati a quanto necessario (articolo 5, paragrafo 1, lettera c));<br>- limitazione della conservazione (articolo 5, paragrafo 1, lettera e)); |

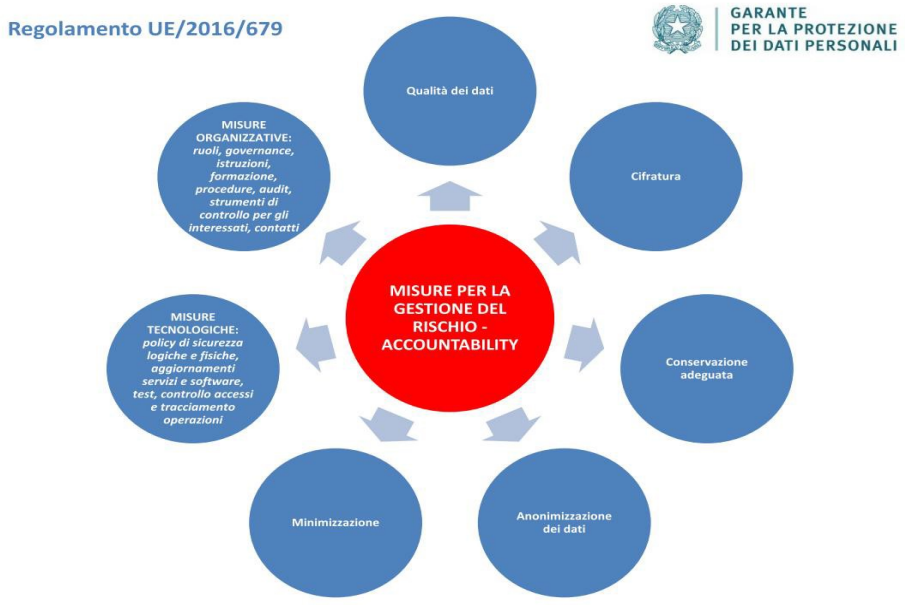
| | | |
|---|---|---|
| Gestione dei rischi per i diritti e le libertà degli interessati | art. 35, paragrafo 7, lettera c | a) Individuazione dei rischi in relazione alla loro: origine, fonti, natura, particolarità e gravità (vedi considerando 84) con particolare riferimento ad accesso illegittimo, modifiche indesiderate, indisponibilità dei dati<br>b) Individuazione dei diritti degli interessati e valutazione degli impatti potenziali su tali diritti e sulle libertà degli interessati stessi dei rischi descritti;<br>c) individuazione delle minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilità dei dati;<br>d) stima delle probabilità e gravità ;<br>e) individuazione delle misure volte a gestire (eliminazione/mitigazione) i rischi di cui sopra (art. 35, paragrafo 7, lettera d) ; |
| Coinvolgimento e parere degli interessati | art. 35, paragrafo 2 e 9 | Il titolare chiede consulenza al RPD/DPO e, se del caso, provvede a coinvolgere gli interessati o i loro rappresentanti. |

7. ELEMENTI VOLTI AD UNA EFFICACE VALUTAZIONE DEI RISCHI

Al fine di individuare correttamente i rischi e la loro gravità è necessario stimare gli aspetti relativi alla sicurezza del trattamento la cui compromissione può comportare almeno uno dei seguenti danni per l'interessato:

- Danno per la reputazione;
- Discriminazione;
- Furto di identità;
- Perdite finanziarie;
- Danni fisici o psicologici;
- Perdita di controllo dei dati;
- Altri svantaggi economici o sociali;
- Impossibilità di esercitare diritti, servizi od opportunità.

Il Garante per la Protezione dei Dati Personali ha realizzato il seguente schema illustrativo relativo alle misure per la gestione del rischio



8. MODALITA' OPERATIVE PER L'ATTUAZIONE DELLA DPIA

La CNIL, l'Autorità francese per la protezione dei dati (Commission nationale de l'informatique et des libertas), ha messo a disposizione un software di ausilio ai titolari in vista della effettuazione della valutazione d'impatto sulla protezione dei dati (DPIA).

Il software - gratuito e liberamente scaricabile dal sito www.cnil.fr (https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil) - offre un percorso guidato alla realizzazione della DPIA, secondo una sequenza conforme alle indicazioni fornite dal WP29 nelle Linee-guida sulla DPIA.

La versione in lingua italiana è stata messa a punto anche con la collaborazione del Garante per la protezione dei dati personali.

Occorre sottolineare che il software è in continua evoluzione, con revisioni introdotte anche sulla base dell'esperienza raccolta e delle segnalazioni degli utenti.

9. COME PROCEDERE PER LA REALIZZAZIONE DI UNA DPIA

Nelle fasi di valutazione di impatto sulla protezione dei dati, qualora lo ritenga necessario il referente del titolare può avvalersi del supporto del Responsabile per la Protezione dei Dati. In ogni caso, il referente comunica l'esito dell'analisi al Responsabile per la Protezione dei dati per garantirne la tracciabilità.

La segnalazione al Responsabile per la Protezione dei Dati viene effettuata scrivendo una email al suo indirizzo interno dedicato .

10. APPROVAZIONE E REVISIONE DEL PRESENTE DOCUMENTO

Il presente documento sarà approvato dall'Ente tramite Delibera di Giunta Comunale.

Il documento sarà soggetto a modifiche ed aggiornamenti ogni qualvolta si renderà necessario. Tali aggiornamenti saranno rilevati dal Responsabile per la Protezione dei Dati, che ne verificherà la rispondenza ai termini di legge.

Le modifiche al documento verranno approvate con Delibera di Giunta Comunale o dal Responsabile del Settore 1 in considerazione della rilevanza delle modifiche effettuate .

11. ALLEGATI AL PRESENTE DOCUMENTO:

Sottoelencati PIA ( Protection Impact Assessment) relativi ai trattamenti sottoposti a valutazione nel ai sensi dell'art. 35, par. 1 del RGPD e del provvedimento n. 467 dell'11.10.2018 del Garante per la protezione dei dati personali contenete l'elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati:

1. Dati da telecamere e riprese;
2. Anagrafe e stato civile
3. Pubblicazioni e diffusioni
4. Servizi sociali