Città di Tradate
(Provincia di Varese)

N. 94 / 2022 Registro Deliberazioni

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

ADUNANZA DEL 15/07/2022

Oggetto: APPROVAZIONE DELLA "PROCEDURA PER L'ESERCIZIO DEI DIRITTI DEGLI INTERESSATI", DELLA "PROCEDURA GESTIONE DELLE VIOLAZIONI (DATA BREACH)" E DELLA "PROCEDURA DEL PROCESSO DI ANALISI DI IMPATTO PRIVACY (DPIA)" AI SENSI DEL REGOLAMENTO UE 2016/679

L'anno **2022** addì **15** del mese di luglio alle ore 12:00 si è riunita la Giunta Comunale appositamente convocata.

All'appello risultano:

BASCIALLA GIUSEPPE	SINDACO	Presente
ACCORDINO FRANCO ROBERTO	VICE SINDACO	Presente
COLOMBO MARINELLA	ASSESSORE	Presente
MARTEGANI ERIKA	ASSESSORE	Presente
MORBI ALESSANDRO	ASSESSORE	Presente
PIPOLO VITO	ASSESSORE	Presente

Assenti: 0,

Partecipa il SEGRETARIO dott.ssa MARINA BELLEGOTTI .

Accertata la validità dell'adunanza, GIUSEPPE BASCIALLA in qualità di SINDACO ne assume la presidenza, dichiarando aperta la seduta e invitando la Giunta a deliberare in merito alla pratica avente a oggetto:

APPROVAZIONE DELLA "PROCEDURA PER L'ESERCIZIO DEI DIRITTI DEGLI INTERESSATI", DELLA "PROCEDURA GESTIONE DELLE VIOLAZIONI (DATA BREACH)" E DELLA "PROCEDURA DEL PROCESSO DI ANALISI DI IMPATTO PRIVACY (DPIA)" AI SENSI DEL REGOLAMENTO UE 2016/679

Relaziona il Sindaco GIUSEPPE BASCIALLA.

Si accerta, in via preliminare, l'esistenza dei pareri espressi ai sensi dell'art. 49 D.Lgs. 18.8.2000, n° 267.

Oggetto: APPROVAZIONE DELLA "PROCEDURA PER L'ESERCIZIO DEI DIRITTI DEGLI INTERESSATI", DELLA "PROCEDURA GESTIONE DELLE VIOLAZIONI (DATA BREACH)" E DELLA "PROCEDURA DEL PROCESSO DI ANALISI DI IMPATTO PRIVACY (DPIA)" AI SENSI DEL REGOLAMENTO UE 2016/679.

LA GIUNTA COMUNALE

Premesso che:

- Il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 *«relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)»* (di seguito *RGPD*), in vigore dal 24 maggio 2016, e applicabile dal 25 maggio 2018, prevede che tutti i titolari del trattamento sono tenuti ad osservare una serie di obblighi per garantire la sicurezza dei dati trattati;
- il sopracitato Regolamento pone con forza l'accento sulla "responsabilizzazione" di titolari e responsabili, ossia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento;

Considerato che:

- gli art. 15 e seguenti del Regolamento prevedono i diritti esercitabili dagli interessati i cui dati sono oggetto di trattamento;
- occorre disciplinare le modalità operative per gestire in maniera tempestiva ed efficiente le richieste provenienti dagli interessati per l'esercizio dei propri diritti di cui al Regolamento (UE) 2016/679;
- l'art. 33 del Regolamento prevede che tutti i titolari dovranno notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque senza ingiustificato ritardo, se ritengono probabile che da tale violazione derivino dei rischi per i diritti e le libertà degli interessati;
- l'art. 34 del Regolamento prevede che se la probabilità di tale rischio è elevata si dovrà informare della violazione anche gli interessati, sempre senza ingiustificato ritardo;
- l'art. 35 del Regolamento prevede che l'ente, in quanto titolare del trattamento, effettui una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali (definita *data protection impact assessment*, "DPIA") ogni qualvolta questi possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- occorre disciplinare le modalità di svolgimento dell'analisi di impatto, applicando una metodologia oggettiva finalizzata alla valutazione delle fattispecie per cui l'analisi è necessaria e alla determinazione dei passaggi da compiere per la realizzazione di tale analisi;

Valutato che occorre disciplinare:

- gli aspetti organizzativi e la procedura che definisca le modalità operative, i compiti e le responsabilità relative alla gestione delle richieste per garantire l'agevole esercizio dei diritti degli interessati i cui dati sono oggetto di trattamento;
- gli aspetti organizzativi e la procedura che definisca le modalità operative, i compiti e le responsabilità relative alla gestione delle violazioni di dati personali che potrebbero comportare un rischio per i diritti e le libertà delle persone fisiche;
- gli aspetti organizzativi e la procedura che definisca le modalità operative, i compiti e le responsabilità relative alla valutazione dell'impatto sulla protezione dei dati, redatto in coerenza con l'approccio basato sul rischio che informa la normativa.

Dato atto che il personale incaricato dall'ente, in collaborazione con il Responsabile della Protezione dei Dati, ha redatto le procedure in cui sono definite le modalità operative, i compiti e le responsabilità relative:

- alla gestione della procedura per l'esercizio dei diritti dell'interessato i cui dati sono oggetto di trattamento, Allegato A - Procedura per l'esercizio dei diritti degli interessati ai sensi del Regolamento europeo 679/2016, cui sono allegati quali parti integranti e sostanziali:
  - Allegato A1 - Modello di richiesta per l'esercizio dei diritti in materia di protezione dei dati,
  - Allegato A2 - Modello di registro per le richieste,
  - Allegato A3- Modello di risposta esercizio dei diritti;

- alla gestione delle violazioni di dati personali, Allegato B - Data Breach response plan, cui sono allegati quali parti integranti e sostanziali:
  - Allegato B1 – Esempi di incidenti di sicurezza e valutazione di eventuali violazioni,
  - Allegato B2 – Modello Registro delle Violazioni di dati personali,
  - Allegato B3 - Informazioni da comunicare al Referente;

Rilevato che:

- il Responsabile per la Protezione dei Dati dell'ente ha formalizzato una procedura operativa a supporto del titolare per effettuare l'analisi di impatto privacy, che prevede l'utilizzo di un applicativo e la registrazione dell'analisi effettuata nel portale di gestione chiamate messo a disposizione dal Responsabile;
- tale procedura è composta di una guida operativa Allegato C - Valutazione di impatto sulla protezione dei dati, cui sono allegati quali parti integranti e sostanziali:
  - allegato C1- passaggi per l'effettuazione di una DPIA tramite il software realizzato dalla CNIL,
  - allegato C2- modalità di registrazione dell'esito della DPIA effettuata;

Visto, con riferimento alle disposizioni di cui all'art.49, primo comma D.Lgs n. 267/2000, il parere favorevole del Responsabile del Settore servizi Generali in ordine alla regolarità tecnica;

Con voti unanimi favorevoli, espressi nelle forme di legge,

DELIBERA

1. Di approvare, per le motivazioni indicate in premessa:

   - il documento contenente la "Procedura per l'esercizio dei diritti degli interessati ai sensi del Regolamento Europeo 679/2016" (Allegato A) e i relativi allegati:
     - Allegato A1 -Modello di richiesta per l'esercizio dei diritti in materia di protezione dei dati;
     - Allegato A2- Modello di registro per le richieste;
     - Allegato A3- Modello di risposta esercizio dei diritti.

   - il documento che disciplina le modalità operative, i compiti e le responsabilità relativi alla

gestione delle violazioni di dati personali che potrebbero comportare un rischio per i diritti e le libertà delle persone fisiche (cd. Data Breach) Allegato B - Data Breach response plan e relativi allegati:

- Allegato B1 – Esempi di incidenti di sicurezza e valutazione di eventuali violazioni;
- Allegato B2 – Modello Registro delle Violazioni di dati personali;
- Allegato B3 - Informazioni da comunicare al Referente;

- il documento in premessa citato che disciplina le modalità di svolgimento dell'analisi di impatto sulla protezione dei dati personali (DPIA) e la registrazione dell'esito Allegato C - Valutazione di impatto sulla protezione dei dati e i relativi allegati:

- Allegato C1) - passaggi per l'effettuazione di una DPIA tramite il software realizzato dalla CNIL;
- Allegato C2 - modalità di registrazione dell'esito della DPIA effettuata.

2. Di dare notizia dell'adozione dei presenti atti a tutti i funzionari titolari di posizione organizzativa, perché adottino un comportamento corretto, consapevole e collaborativo per garantire "*la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati".*

Successivamente con separata ed unanime votazione espressa in forma palese,

DELIBERA

Di dichiarare la presente deliberazione immediatamente eseguibile, ai sensi dell'art. 134, comma 4, del TUEL D.Lgs. n. 267/2000, al fine di consentire l'immediata applicazione.

Approvato e sottoscritto con firma digitale:

Il SINDACO	**Il SEGRETARIO**
GIUSEPPE BASCIALLA	**MARINA BELLEGOTTI**

Documento informatico formato e prodotto ai sensi del D.Lgs. 82/2005 e rispettive norme collegate.

Allegato A

Procedura per l’esercizio dei diritti degli interessati ai sensi del Regolamento Europeo 679/2016

Sommario

VERSIONI DEL DOCUMENTO		
EDIZIONE	**SINTESI DELLA MODIFICA**	**DATA**
1.0	Prima versione del documento	*<Data di adozione>*

1 Scopo e campo di applicazione

Il Comune di Tradate ai sensi del Regolamento Generale sulla Protezione dei dati 2016/679 e della normativa nazionale applicabile, è tenuto a garantire l'esercizio agevole dei diritti degli interessati con riguardo al trattamento dei dati di carattere personale ("dati personali"), a prescindere dalla loro nazionalità o dalla loro residenza.
Tali diritti consentono ai soggetti interessati un controllo sulle tipologie dei dati utilizzati, sulle modalità di trattamento e conferisce loro la possibilità di limitare tale uso, di opporsi nonché di cancellare i dati personali in talune circostanze.
Lo scopo di questa procedura è l'individuazione dei diritti e delle modalità di esercizio degli stessi da parte degli interessati, la determinazione delle tempistiche e delle modalità di riscontro.
La procedura si applica in caso di richieste pervenute dagli interessati o soggetti terzi legittimati e aventi diritto, come meglio di seguito specificato.

Questa procedura è rivolta a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza dell'organizzazione quali:

- i dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto intercorrente – siano autorizzati a trattare dati personali sotto la diretta autorità dell'Organizzazione (da ora in avanti gli "Autorizzati");
- qualunque collaboratore dell'Organizzazione (persona fisica o persona giuridica) diverso dall'Autorizzato che, in ragione del rapporto contrattuale in essere abbia accesso ai suddetti dati e agisca in qualità di Responsabile del Trattamento dati ai sensi dell'art. 28 RGPD (da ora in avanti "Responsabile del trattamento").

Le istruzioni per la gestione dei diritti degli interessati, limitatamente a quanto di competenza, devono essere distribuite a tutto il personale mediante metodi e mezzi che ne assicurino la comprensione e devono essere inserite in tutti i contratti (o altri atti giuridici) che disciplinano il trattamento dei dati con il Responsabile del trattamento, compresi quelli relativi a servizi e fornitori IT.
Il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia, e salvo la possibilità di richiedere il risarcimento dell'eventuale danno.

2 Riferimenti normativi

- Regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito definito RGPD);

- D. Lgs. 196/2003 "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE))";

3 Definizioni

Dati personali generali oppure **Dati comuni**, qualunque informazione relativa a persona fisica identificata o identificabile. 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 on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Categorie particolari di dati personali: i dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale. Fanno parte di questa categoria anche i dati genetici, i dati biometrici, i dati relativi alla salute o alla vita o all'orientamento sessuale della persona.

Dati personali relativi a condanne penali e reati: sono quei dati personali in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti. Inoltre possono essere quei dati personali indicanti la qualità di imputato o di indagato.

Trattamento: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di processi automatizzati e applicati a dati personali o a 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.

Interessato: la persona fisica identificata o identificabile i cui dati sono oggetto di trattamento. Si considera identificabile la persona fisica che può essere individuata, direttamente o indirettamente, tramite ad esempio il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o uno o più elementi caratteristici della sua identità fisica, economica o sociale.

Responsabile Protezione Dati (RPD): in inglese Data Protection Officer (DPO), è la figura professionale con particolari competenze in campo informatico, giuridico, di valutazione del rischio e di analisi dei processi, il cui compito principale è l'osservazione, la valutazione e l'indirizzo sulle modalità di trattamento dei dati personali allo scopo di far rispettare le normative europee e nazionali in materia di privacy.

Responsabile del Trattamento: previsto dall'art. 4 del RGPD, è definito come la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che tratta dati personali per conto del titolare del trattamento, all'interno o all'esterno dell'Organizzazione, attenendosi alle istruzioni da quest'ultimo impartite, secondo quanto previsto dall'art. 28. I Responsabili devono presentare garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

Terze parti: qualsiasi soggetto, persona fisica o giuridica, che tratta dati personali in virtù in un contratto.

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. In questo specifico documento il Titolare è individuato nel Comune di Tradate.

Organizzazione: Comune di Tradate con sede in Piazza Mazzini 6, nella qualità di titolare del trattamento dei dati personali.

Ufficio di Riferimento: è l'ufficio individuato dal Titolare per la gestione delle richieste dei diritti degli Interessati all'interno dell'Organizzazione; è identificato nell' ufficio URP.

4 I diritti esercitabili dagli interessati

L'Interessato, ai sensi del Regolamento UE 679/2016, può esercitare i seguenti diritti:

- Diritto di accesso (art. 15)
- Diritto di rettifica (art. 16)
- Diritto di cancellazione (art. 17)
- Diritto di limitazione di trattamento (art. 18)
- Diritto di portabilità dei dati (art. 20)
- Diritto di opposizione (art. 21)
- Diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione (art. 22)
- Diritto di revocare il consenso (art. 14 par. 2 lett. d)

Benché sia il solo Titolare a dover dare riscontro in caso di esercizio dei diritti (artt. 15-22), i Responsabili del trattamento sono tenuti a collaborare con il Titolare ai fini dell'esercizio dei diritti degli Interessati, anche comunicando tempestivamente le richieste di esercizio indirizzate a questi ultimi con riferimento a trattamenti effettuati per conto del Titolare. Tale obbligo è da inserire nel contratto o altro atto giuridico che disciplina il trattamento dei dati ai sensi dell'art. 28 del RGPD.

L'Interessato ha altresì il diritto di proporre reclamo all'autorità di controllo competente (Garante per Protezione dei Dati Personali http://www.garanteprivacy.it).

4.1 Diritto di accesso

(art. 15 del Regolamento)

L'Interessato ha il diritto di accedere ai dati personali raccolti che lo riguardano e di esercitare tale diritto facilmente ed a intervalli ragionevoli, per essere consapevole del trattamento e verificarne la liceità.

L'Interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

- le finalità del trattamento;
- le categorie di dati personali in questione;
- i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

- l'esistenza del diritto dell'Interessato di chiedere al Titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
- il diritto di proporre reclamo a un'autorità di controllo;
- qualora i dati non siano raccolti presso l'Interessato, tutte le informazioni disponibili sulla loro origine;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'Interessato.

Qualora alcuni tipi di dati personali riguardino più di un Interessato, il diritto di ricevere i dati personali non dovrebbe pregiudicare i diritti e le libertà degli altri Interessati. Tuttavia, tali considerazioni non dovrebbero condurre a un diniego a fornire all'Interessato tutte le informazioni.

Se il Titolare del trattamento tratta una notevole quantità d'informazioni riguardanti l'Interessato, è possibile richiedere che l'Interessato precisi, prima che siano fornite le informazioni, alcuni dettagli o le attività di trattamento cui la richiesta si riferisce.

Il diritto di accesso prevede anche di poter ricevere una copia dei dati personali oggetto di trattamento fatti salvi comunque i diritti e le libertà altrui.

4.2 Diritto di rettifica

(art. 16 del Regolamento)

L'Interessato ha il diritto richiedere e ottenere la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'Interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

La rettifica può riguardare soltanto dati oggettivi e non anche valutativi, non si potrà quindi chiedere la correzione di giudizi espressi nell'ambito di attività di valutazione del lavoro.

La rettifica va comunicata a ciascuno dei destinatari cui sono stati trasmessi i dati personali, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.

4.3 Diritto alla cancellazione

(art. 17 del Regolamento)

L'Interessato ha il diritto di ottenere la cancellazione dei dati personali se la conservazione di tali dati viola il Regolamento o il diritto nazionale.

In particolare, l'Interessato ha il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati.

L'Interessato ha il diritto di ottenere la cancellazione dei dati personali che lo riguardano se sussiste uno dei motivi seguenti:

- i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

- l'Interessato revoca il consenso su cui si basa il trattamento, se non sussiste altro fondamento giuridico per il trattamento;
- l'Interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;
- i dati personali sono stati trattati illecitamente;
- i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dalla normativa nazionale.

In caso di pubblicazioni on-line, il Titolare è obbligato a cancellare i dati personali e, tenendo conto della tecnologia disponibile e dei costi di attuazione, ad adottare misure ragionevoli, anche tecniche, per informare eventuali Responsabili del trattamento o Titolari autonomi del trattamento che stanno trattando i dati personali della richiesta dell'Interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

La cancellazione non può essere applicata nella misura in cui il trattamento sia necessario:

- per l'esercizio del diritto alla libertà di espressione e di informazione;
- per l'adempimento di un obbligo giuridico che richieda il trattamento previsto dal diritto dell'Unione o dalla normativa nazionale o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
- per fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.
- per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Inoltre, tale diritto non implica la cancellazione dei dati personali riguardanti l'Interessato forniti da quest'ultimo per l'esecuzione di un contratto, nella misura in cui e fintantoché i dati personali siano necessari all'esecuzione di tale contratto.

In caso di applicazione, la cancellazione va comunicata a ciascuno dei destinatari cui sono stati trasmessi i dati personali, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.

4.4 Diritto alla limitazione di trattamento

(art. 18 del Regolamento)

L'Interessato ha il diritto di ottenere dal Titolare la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

a) l'Interessato contesta l'esattezza dei dati personali, per il periodo necessario a verificare l'esattezza di tali dati personali;
b) il trattamento è illecito e l'Interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
c) benché il Titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'Interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
d) l'Interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1 del Regolamento, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare del trattamento rispetto a quelli dell'Interessato.

La limitazione ha una connotazione cautelare con la funzione principale di fornire all'Interessato un controllo effettivo dei propri dati.

Questo diritto può essere descritto come la pretesa riconosciuta all'Interessato di ottenere che il complessivo trattamento si riduca alla temporanea esecuzione della sola operazione di conservazione.

I dati risultano pertanto sottoposti ad un vincolo provvisorio di inutilizzabilità e di accessibilità.

La limitazione va comunicata a ciascuno dei destinatari cui sono stati trasmessi i dati personali, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.

L'Interessato che ha ottenuto la limitazione del trattamento deve essere informato dal Titolare del trattamento prima che detta limitazione venga revocata.

4.5 Diritto alla portabilità dei dati

(art. 20 del Regolamento)

L'Interessato ha diritto, qualora il trattamento dei dati personali si basi sul consenso o su un contratto e gli stessi dati siano trattati con mezzi automatizzati, di ricevere senza impedimenti in un formato strutturato, di uso comune, leggibile da dispositivo automatico e interoperabile, i dati personali che lo riguardano che abbia fornito al Titolare del trattamento e di trasmetterli a un altro titolare del trattamento.

È opportuno pertanto, ove possibile, sviluppare formati interoperabili che consentano la portabilità dei dati, pur senza l'obbligo di adottare o mantenere sistemi di trattamento tecnicamente compatibili con sistemi di altri titolari.

Non si applica qualora:

- il trattamento si basi su un fondamento giuridico diverso dal consenso o contratto;
- nei confronti dei titolari del trattamento che trattano dati personali nell'esercizio delle loro funzioni pubbliche;
- quando il trattamento dei dati personali è necessario per l'adempimento di un obbligo legale cui è soggetto il Titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare del trattamento.

Ove tecnicamente fattibile, l'Interessato ha il diritto di ottenere che i dati personali siano trasmessi direttamente dal Titolare del trattamento a un altro titolare.

4.6 Diritto di opposizione

(art. 21 del Regolamento)

L'opposizione al trattamento costituisce una declinazione del potere di controllo dell'Interessato sui propri dati.

Nei casi espressamente previsti dalla legge ha l'effetto di far cessare in via permanete un determinato trattamento di dati.

Tale diritto è esercitabile ove il trattamento:

- si fondi sull'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (in ambito pubblico);

- sia posto in essere nell'esercizio di un legittimo interesse del Titolare del trattamento o di terzi (in ambito privato);
- sia effettuato a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, par. 1 del RGPD, salvo che il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico.

  Nei casi appena indicati, l'Interessato può opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, e quindi motivando la sua richiesta. Spetta dunque al Titolare l'onere di dimostrare che la base giuridica su cui si fonda il trattamento (compresa la necessità di accertamento, esercizio o difesa di un proprio diritto in sede giudiziaria) prevalga sugli interessi o sui diritti e sulle libertà fondamentali dell'Interessato; ove accordi l'esercizio del diritto, il Titolare deve astenersi dal trattare ulteriormente i dati, anche se può comunque conservarli; in caso contrario, l'Interessato deve comunque essere informato della possibilità di esercitare reclamo davanti al Garante per la protezione dei dati personali;

- è finalizzato ad attività di marketing diretto (compresa la profilazione connessa al marketing diretto).

  In quest'ultimo caso, l'Interessato può opporsi in qualsiasi momento. Si tratta quindi di un diritto assoluto, poiché non soggetto a motivazione e ad alcuna valutazione da parte del Titolare. Anche in questo caso, se l'Interessato esercita tale diritto, il Titolare deve esimersi dal procedere con il trattamento per finalità di marketing, potendo ben continuare eventuali diversi trattamenti che fondino il proprio presupposto su diverse basi (ad es., obbligazione contrattuale, l'interesse legittimo del Titolare stesso, finalità che devono comunque essere rese esplicite all'Interessato).

4.7 Diritto di non essere sottoposto a decisione automatizzata

(art. 22 del Regolamento)

L'Interessato ha anche il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Tale diritto non si applica nel caso in cui la decisione:

a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'Interessato e un Titolare del trattamento;
b) sia autorizzata dal diritto dell'Unione o dalla normativa nazionale, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'Interessato;
c) si basi sul consenso esplicito dell'Interessato.

Nei casi a) e b), l'Interessato ha il diritto di ottenere l'intervento umano da parte del Titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

Le decisioni automatizzate non possono basarsi sulle categorie particolari di dati personali di cui all'articolo 9 del Regolamento.

L'Interessato ha il diritto di non essere sottoposto a una decisione che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani.

Tale trattamento comprende la «profilazione», che consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere 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, ove ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona.

5 Chi può esercitare tali diritti

Le richieste per l'esercizio dei diritti possono essere presentate dall'Interessato.

Ai sensi dell'art. 4 n. 1) del RGPD e ai fini della presente procedura per "Interessato" si intende la persona fisica identificata o identificabile cui si riferiscono i dati personali trattati dall'Organizzazione nello svolgimento delle proprie funzioni istituzionali, dei compiti e delle attività amministrative di competenza.

L'esercizio dei diritti si estende anche ai dati relativi alle persone decedute. Ai sensi dell'art. 2-terdecies co. 1 del D. Lgs. n. 196/2003 i diritti delle persone decedute "possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'Interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione".

Prima di ogni comunicazione è fatto obbligo adottare tutte le misure ragionevoli per verificare l'identità dell'Interessato come meglio descritto nel paragrafo 6.1.

6 Gestione delle istanze

L'Interessato ha il diritto di esercitare in qualsiasi momento i suoi diritti in maniera agevole.

Per la presentazione delle istanze da parte degli Interessati, l'Organizzazione ha reso disponibile sul proprio Sito internet www.comune.tradate.va.it un apposito modulo, allegato alla presente procedura (All. 1).

L'Organizzazione ha definito per la ricezione delle richieste i seguenti recapiti, i quali vengono indicati anche nell'informativa resa agli Interessati:

- indirizzo pec: comune.tradate@pec.regioone.lombardia.it;
- indirizzo: urp@comune.tradate.va.it

Resta inteso che l'Organizzazione, pur privilegiando i canali ufficiali e le relative modalità di invio delle istanze da parte degli Interessati sopra indicati, non si esimerà dal prendere in considerazione e riscontrare le richieste in qualsiasi forma pervenute che abbiano ad oggetto l'esercizio di diritti ai sensi della normativa vigente.

Al fine di consentire la corretta identificazione dell'Interessato, funzionale all'istruttoria delle richieste, alla successiva eventuale trasmissione dei dati e documenti o alla valutazione di ulteriori domande da parte di uno stesso soggetto, alla richiesta sottoscritta con firma autografa deve essere allegata copia del documento d'identità dell'Interessato, sia che l'istanza venga presentata in forma elettronica che cartacea.

L'obbligo di allegazione del documento d'identità decade nei casi in cui l'istanza inviata digitalmente sia sottoscritta con firma digitale direttamente dall'Interessato.

Tutte le richieste verranno protocollate ed inoltrate all'Ufficio di Riferimento.

Qualora ritenuto necessario, l'Ufficio di Riferimento individuerà al proprio interno il/i soggetto/i incaricati della gestione delle attività previste dal RGPD legate all'esercizio dei diritti da parte degli Interessati.

L'Ufficio di Riferimento dovrà prontamente informare il RPD nominato dall'Organizzazione e coinvolgere nelle fase di raccolta delle informazioni gli uffici dell'Organizzazione detentori delle informazioni richieste, al fine di fornire adeguato riscontro all'Interessato.

Nel caso in cui la richiesta venga rivolta dall'Interessato direttamente al RPD, quest'ultimo provvederà ad inoltrarla all'Organizzazione e, a seguito di protocollazione, verificherà che l'Ufficio di Riferimento se ne occupi nel rispetto del RGPD.

Nel caso in cui la richiesta venga rivolta dall'Interessato ad un Responsabile del trattamento, lo stesso provvederà a trasmettere tempestivamente all'Organizzazione la copia della richiesta ricevuta unitamente ad eventuali informazioni su circostanze o fatti che potrebbero essere utili per fornire il riscontro agli Interessati, tenuto conto delle ragionevoli aspettative nutrite dagli Interessati in base alla relazione intercorrente tra il Responsabile e il Titolare del trattamento. Tale modalità deve essere chiaramente indicata nel contratto che disciplina il trattamento dei dati dei responsabili del trattamento ai sensi dell'art 28 del RGPD.

L'Ufficio di Riferimento provvederà, con il supporto del RPD e di eventuali uffici coinvolti, a valutare la liceità della richiesta e le modalità di riscontro.

6.1 Modalità del riscontro

Il responsabile dell'Ufficio di Riferimento, direttamente o tramite il personale incaricato, gestirà l'istruttoria e risponderà all'Interessato.

L'Ufficio di Riferimento verificherà innanzitutto che la richiesta sia completa degli elementi essenziali per l'identificazione dell'Interessato e l'elaborazione di una risposta.

Nel caso in cui l'Interessato non venga identificato, la richiesta verrà respinta.

Nel caso in cui il soggetto richiedente fornisca i propri riferimenti di contatto ma non vi sia certezza dell'identità dello stesso, l'Ufficio di Riferimento chiederà all'Interessato di integrare documentazione idonea a garantire la certa identificazione.

L'Ufficio di Riferimento provvederà poi, con il supporto del RPD e di eventuali altri uffici coinvolti, a verificare le richieste, a rispondere all'Interessato entro le tempistiche previste dal Regolamento UE 2016/679 e ad attivarsi per dare seguito alle richieste stesse.

L'esercizio dei diritti è gratuito, così come è gratuita, di regola, la fornitura da parte del Titolare di una copia dei dati all'Interessato, seppur con le dovute eccezioni.

Se le richieste dell'Interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il Titolare del trattamento può:

- -rifiutare di soddisfare la richiesta, con espressa comunicazione delle motivazioni del rifiuto al richiedente.

Incombe sull'Ufficio di Riferimento, con il contributo fattivo degli uffici detentori delle informazioni richieste, l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

6.2 Tempi del riscontro

Sarà cura della dell'Ufficio di Riferimento dare riscontro all'Interessato nel più breve tempo possibile e senza ingiustificato ritardo, in ogni caso entro un mese dal ricevimento della richiesta stessa, anche in caso di diniego; il riscontro potrà riguardare tanto l'accoglimento della richiesta che il suo rigetto.

Tale termine può essere prorogato di ulteriori due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. In tal caso, l'Interessato è informato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta.

E' necessario fornire una risposta alle richieste nel minor tempo possibile. Qualora non sia possibile ottemperare alla richiesta entro un mese, occorre fornire quanto prima un riscontro all'interessato su tale circostanza, al fine di costruire un dialogo collaborativo con il richiedente.

6.3 Forma del riscontro

Le comunicazioni relative al trattamento devono essere fornite in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate nello specifico direttamente agli Interessati.

Il riscontro di regola deve avvenire con lo stesso strumento e canale utilizzato dall'Interessato (es. e-mail, PEC), salvo diversa indicazione di quest'ultimo espressa nell'istanza o altrimenti desumibile.

È possibile dare riscontro alla richiesta utilizzando lo schema di risposta riportato all'All. 3.

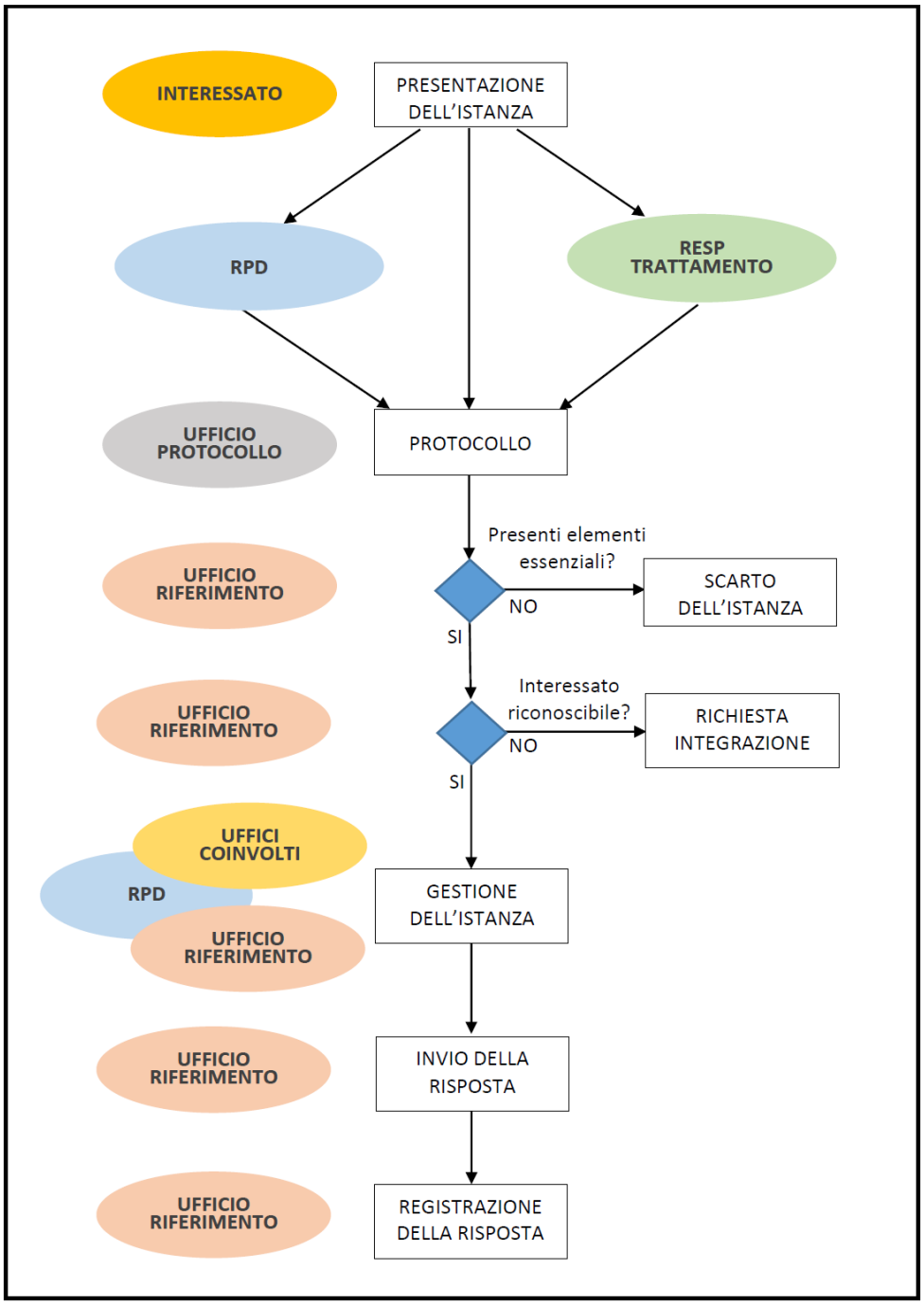
6.4 Contenuto del riscontro

Salvo che le richieste siano riferite a un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro comprende tutti i dati personali che riguardano l'Interessato comunque trattati dal Titolare.

Se i dati dell'Interessato sono collegati ad altri dati personali di soggetti terzi, questi ultimi devono essere esclusi dalla comunicazione.

Qualora l'estrazione dei dati si riveli di particolare difficoltà (per il trattamento, la natura, la qualità e la quantità dei dati), il riscontro all'Interessato può essere dato anche tramite esibizione o consegna in copia degli atti e dei documenti che contengono i dati personali richiesti.

SI riporta di seguito lo schema a blocchi della procedura.



7 Documentazione per la gestione delle richieste

La documentazione relativa alle richieste ed ai riscontri da parte dell'Organizzazione dovrà essere protocollata e conservata agli atti dall'Ufficio di Riferimento, ad eccezione delle informazioni di carattere particolare e/o relative a condanne penali e reati, che verranno conservate dall'ufficio competente che le ha messe a disposizione. In tal caso, i dati forniti all'Interessato come riscontro alla sua richiesta verranno esclusivamente menzionati nella pratica conservata presso l'Ufficio di Riferimento.

7.1 Tracciabilità delle richieste

Ogni volta che viene gestita una richiesta, l'Ufficio di Riferimento dovrà anche compilare e conservare il Registro delle richieste, secondo il modello presentato all'All.2. Il Registro dovrà contenere le informazioni di seguito riportate:

(i) data di ricezione dell'istanza;
(ii) nominativo del richiedente;
(iii) nominativo dell'Interessato (se diverso dall'istante);
(iv) descrizione della richiesta;
(v) Ufficio di Riferimento;
(vi) uffici coinvolti;
(vii) azione intrapresa riguardo all'istanza;
(viii) data della risposta;
(ix) sintesi della motivazione;
(x) note e commenti.

Il documento verrà mantenuto agli atti dell'Organizzazione, garantendo la riservatezza delle informazioni contenute e la tracciabilità degli eventi.

Tale documentazione è fornita all'Autorità di controllo in caso di accertamenti.

8 Deroghe all'esercizio dei diritti degli interessati

Alle limitazioni specificamente previste dal RGPD per l'esercizio di ogni singolo diritto, l'art. 23 ammette deroghe tematiche all'esercizio dei diritti riconosciuti dal Regolamento, sul fondamento di disposizioni normative nazionali, nei seguenti ambiti:

a) sicurezza nazionale;
b) difesa;
c) sicurezza pubblica;
d) prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;
e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale;
f) salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari;
g) attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate;
h) funzioni di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere da a), a e) e g);
i) tutela dell'Interessato o dei diritti e delle libertà altrui;
j) esecuzione delle azioni civili.

Il considerando 73 del RGPD include inoltre espressamente, tra i possibili ambiti di limitazione, "la tenuta di registri pubblici per ragioni di interesse pubblico generale".

Si segnala che l'ambito della limitazione deve essere esattamente identificato da specifiche disposizioni normative, in cui vengano definite:

- le finalità del trattamento o le categorie di trattamento e le categorie di dati personali;
- la portata delle limitazioni introdotte;
- le garanzie per prevenire abusi o l'accesso o il trasferimento illeciti;
- l'indicazione precisa del Titolare del trattamento o delle categorie di titolari;
- i periodi di conservazione e le garanzie applicabili tenuto conto della natura, dell'ambito di applicazione e delle finalità del trattamento o delle categorie di trattamento;
- i rischi per i diritti e le libertà degli Interessati;
- il diritto degli Interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità della stessa.

Altre limitazioni generali ai diritti degli Interessati sono state anche disposte dal D.Lgs. n. 196/2003, agli artt. 2-undecies e 2-duodecies. In particolare:

Art. 2-undecies (Limitazioni ai diritti dell'Interessato)

1. I diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'art. 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto:
    a. agli interessi tutelati in base alle disposizioni in materia di riciclaggio;
    b. agli interessi tutelati in base alle disposizioni in materia di sostegno alle vittime di richieste estorsive;
    c. all'attività di Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;
    d. alle attività svolte da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;
    e. allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria;
    f. alla riservatezza dell'identità del dipendente che segnala ai sensi della legge 30 novembre 2017, n. 179, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio.

[…]

Art. 2-duodecies (Limitazioni per ragioni di giustizia)

1. In applicazione dell'articolo 23, paragrafo 1, lettera f), del Regolamento, in relazione ai trattamenti di dati personali effettuati per ragioni di giustizia nell'ambito di procedimenti dinanzi agli uffici giudiziari di ogni ordine e grado nonché dinanzi al Consiglio superiore della magistratura e agli altri organi di autogoverno delle magistrature speciali o presso il Ministero della giustizia, i diritti e gli obblighi di cui agli articoli da 12 a 22 e 34 del Regolamento sono disciplinati nei limiti e con le modalità previste dalle disposizioni di legge o di Regolamento che regolano tali procedimenti, nel rispetto di quanto previsto dall'articolo 23, paragrafo 2, del Regolamento.
2. Fermo quanto previsto dal comma 1, l'esercizio dei diritti e l'adempimento degli obblighi di cui agli articoli da 12 a 22 e 34 del Regolamento possono, in ogni caso, essere ritardati, limitati o esclusi, con comunicazione motivata e resa senza ritardo all'Interessato, a meno che la comunicazione possa compromettere la finalità della limitazione, nella misura e per il tempo in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti

fondamentali e dei legittimi interessi dell'Interessato, per salvaguardare l'indipendenza della magistratura e dei procedimenti giudiziari.

3. […]
4. Ai fini del presente articolo si intendono effettuati per ragioni di giustizia i trattamenti di dati personali correlati alla trattazione giudiziaria di affari e di controversie, i trattamenti effettuati in materia di trattamento giuridico ed economico del personale di magistratura, nonché i trattamenti svolti nell'ambito delle attività ispettive su uffici giudiziari. Le ragioni di giustizia non ricorrono per l'ordinaria attività amministrativo-gestionale di personale, mezzi o strutture, quando non è pregiudicata la segretezza di atti direttamente connessi alla trattazione giudiziaria di procedimenti.
5.

9 Modulistica allegata alla procedura

Allegato A1 – Modello di richiesta per l'esercizio dei diritti in materia di protezione dei dati personali

Allegato A2 – Modello di Registro delle richieste

Allegato A3 – Modello di risposta esercizio dei diritti.

Allegato A1 – Modello di richiesta per l'esercizio dei diritti in materia di protezione dei dati personali

All'attenzione del Comune di Tradate

ESERCIZIO DI DIRITTI IN MATERIA DI PROTEZIONE
DEI DATI PERSONALI
(artt. 15-22 del Regolamento (UE) 2016/679)

Il/La sottoscritto/a…….
nato/a a……il……, esercita con la presente richiesta i seguenti diritti di cui agli artt. 15-22 del Regolamento (UE) 2016/679:

1. Accesso ai dati personali
(art. 15 del Regolamento (UE) 2016/679)

Il sottoscritto *(barrare solo le caselle che interessano)*:

☐ chiede conferma che sia o meno in corso un trattamento di dati personali che lo riguardano;

☐ in caso di conferma, chiede di ottenere l'accesso a tali dati o una copia degli stessi, e tutte le informazioni previste alle lettere da a) a h) dell'art. 15, paragrafo 1, del Regolamento (UE) 2016/679, e in particolare;

- le finalità del trattamento;
- le categorie di dati personali trattate;
- i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'origine dei dati (ovvero il soggetto o la specifica fonte dalla quale essi sono stati acquisiti);
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'Interessato.

2. Richiesta di intervento sui dati
(artt. 16-18 del Regolamento (UE) 2016/679)

Il sottoscritto chiede di effettuare le seguenti operazioni *(barrare solo le caselle che interessano)*:

☐ rettificazione e/o aggiornamento dei dati (art. 16 del Regolamento (UE) 2016/679);

☐ cancellazione dei dati (art. 17, paragrafo 1, del Regolamento (UE) 2016/679), per i seguenti motivi *(specificare quali)*:

a) ……;
b) ……;
c) …….

nei casi previsti all'art. 17, paragrafo 2, del Regolamento (UE) 2016/679, l'attestazione che il Titolare ha informato altri titolari di trattamento della richiesta dell'interessato di cancellare link,
☐ copie o riproduzioni dei suoi dati personali;

☐ limitazione del trattamento (art. 18) per i seguenti motivi *(barrare le caselle che interessano)*:

- ☐ contesta l'esattezza dei dati personali;
- ☐ il trattamento dei dati è illecito;
- ☐ i dati sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- ☐ l'interessato si è opposto al trattamento dei dati ai sensi dell'art. 21, paragrafo 1, del Regolamento (UE) 2016/679.

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

_____
_____
_____
_____
_____
_____
_____

3.Portabilità dei dati[1]

(art. 20 del Regolamento (UE) 2016/679)

Con riferimento a tutti i dati personali forniti al Titolare, il sottoscritto chiede di *(barrare solo le caselle che interessano)*:

☐ ricevere tali dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico;

☐ trasmettere direttamente al seguente diverso titolare del trattamento *(specificare i riferimenti identificativi e di contatto del titolare: ……..):*

☐ tutti i dati personali forniti al Titolare;

☐ un sottoinsieme di tali dati.

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

_____
_____
_____
_____
_____
_____
_____
_____

4. Opposizione al trattamento

(art. 21, paragrafo 1 del Regolamento (UE) 2016/679)

☐ Il sottoscritto si oppone al trattamento dei suoi dati personali ai sensi dell'art. 6, paragrafo 1, lettera e) del Regolamento (UE) 2016/679, per i seguenti motivi legati alla sua situazione particolare (specificare):

_____
_____
_____
_____
_____
_____

[1] Per approfondimenti: Linee-guida sul diritto alla "portabilità dei dati" - WP242, adottate dal Gruppo di lavoro Art. 29, disponibili in www.garanteprivacy.it/regolamentoue/portabilita.

Il sottoscritto:

- ☐ Chiede di essere informato, ai sensi dell'art. 12, paragrafo 4 del Regolamento (UE) 2016/679, al più tardi entro un mese dal ricevimento della presente richiesta, degli eventuali motivi che impediscono al Titolare di fornire le informazioni o svolgere le operazioni richieste.
- ☐ Chiede, in particolare, di essere informato della sussistenza di eventuali condizioni che impediscono al Titolare di identificarlo come interessato, ai sensi dell'art. 11, paragrafo 2, del Regolamento (UE) 2016/679.

Recapito per la risposta[2]**:**

Via/Piazza _____ N. _____

Comune _____ Provincia _____ Codice postale _____

oppure

e-mail/PEC: _____

Eventuali precisazioni

Il sottoscritto precisa (fornire eventuali spiegazioni utili o indicare eventuali documenti allegati):

_____
_____
_____
_____
_____
_____
_____

(Luogo e data) _____

(Firma)

[2] Allegare copia di un documento di riconoscimento

Allegato A2 – Modello di registro per le richieste

Registro richieste degli interessati									
Data di ricezione della richiesta	**Nominativo del richiedente**	**Nominativo dell'interessato (se diverso dal richiedente)**	**Descrizione della richiesta**	**Ufficio di Riferimento**	**Uffici coinvolti**	**Azione intrapresa riguardo alla richiesta**	**Data della risposta**	**Sintesi della motivazione**	**Note**

Allegato A3 – Modello di risposta esercizio dei diritti

**su carta intestata*

<Luogo, data>

Egregio Sig. _____

a mezzo <pec, e-mail>: _____

Oggetto: Richiesta di esercizio dei diritti in materia di protezione dei dati personali - Ns. Prot. n……

Egregio Sig. _____,

diamo seguito alla sua richiesta trasmessa con <pec, e-mail, telefono> dello scorso <data richiesta> per l'esercizio dei diritti ai sensi degli artt. 15-22 del Regolamento UE 679/2016.

Dopo aver effettuato un'approfondita istruttoria la informiamo che l'Ente ha ritenuto di:

- negare la richiesta per le seguenti motivazioni:

  <oppure>

- accogliere la sua richiesta:

in virtù di quanto previsto dagli artt. 15 e ss., si precisa quanto segue:

- Si conferma che è in corso un trattamento di dati personali che La riguardano, così meglio precisati secondo lo schema fornito dalla norma.

a) finalità del trattamento:	I Suoi dati sono oggetto di trattamento per: _____

b) categorie di dati personali	Con riferimento alla finalità _____: I dati oggetto del trattamento appartengono alla categoria dei DATI PERSONALI GENERALI o DATI COMUNI, nello specifico: nome, cognome, data e luogo di nascita, genere, tipologia soggetto giuridico, indirizzo di residenza, codice fiscale, dati catastali. Con riferimento alla finalità _____: I dati oggetto del trattamento appartengono alla categoria dei DATI PARTICOLARI, nello specifico: dati sanitari, opinioni politiche, appartenenza a sindacati, credi religiosi o filosofici, dati genetici, dati biometrici Con riferimento alla finalità _____: I dati oggetto del trattamento appartengono alla categoria dei DATI GIUDIZIARI, nello specifico: dati relativi a condanne penali.
c) destinatari o categorie di destinatari a cui sono stati o saranno comunicati e se i destinatari di trovano in paesi terzi	I Suoi dati personali sono trattati attraverso il gestionale _____ di _____, che opera in qualità di responsabile del trattamento per attività di manutenzione applicativa strumentale al funzionamento del programma fornito. I Suoi dati non vengono trasferiti in un Paese extra UE.
d) se possibile il periodo di conservazione o i criteri utilizzati per determinare tale periodo	I dati saranno conservati per il seguente periodo: _____

e) possibilità di chiedere: - la cancellazione; - la limitazione; - l'opposizione al trattamento	Sulla cancellazione: - in merito alla finalità _____ non è possibile ottenere la cancellazione in quanto il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; - in merito alla finalità _____ può richiedere la cancellazione in qualsiasi momento e n _____; - in merito alla finalità _____ può richiedere la cancellazione in qualsiasi momento, ma nel caso non sarà possibile riscontrare la sua comunicazione e valutando se tale trattamento non sia necessario per il Titolare per accertare, esercitare o difendere un diritto, che sia in sede giudiziale, amministrativa o stragiudiziale. Sulla limitazione: - in merito alla finalità _____ non è possibile ottenere la limitazione in quanto il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; - in merito alla finalità _____ può richiedere la limitazione del trattamento alla sola finalità per cui svolto se ravvisasse un diverso utilizzo; - in merito alla finalità _____ può richiedere la limitazione in qualsiasi momento del trattamento al solo scopo di dare corso alla Sua richiesta. Sull'opposizione al trattamento: - in merito alla finalità _____ non è possibile opporsi in quanto il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; - in merito alla finalità _____ può opporsi al trattamento in qualsiasi momento e nel caso l'invio _____ - in merito alla finalità _____ può opporsi al trattamento in qualsiasi momento, ma nel caso non sarà possibile riscontrare la Sua comunicazione e sempre valutando se tale trattamento non sia necessario per il Titolare per accertare, esercitare o difendere un diritto, che sia in sede giudiziale, amministrativa o stragiudiziale.
f) diritto a proporre reclamo ad un'autorità di controllo	Lei ha diritto a proporre reclamo al Garante per la protezione dei dati personali o ad adire le opportune sedi giudiziarie.
g) origine dei dati:	I seguenti dati - nome, cognome, data e luogo di nascita, indirizzo di residenza, codice fiscale, dati catastali - sono forniti dal _____. L'indirizzo email certificato è stato fornito da Lei in qualità di interessato.
h) esistenza di un processo decisionale automatizzato	Non è presente alcun processo decisionale automatizzato compresa la profilazione.

Si forniscono, su Sua richiesta le copie dei seguenti atti/documenti contenenti i dati oggetto della richiesta:

All. 1 - _____

All. 2 - _____

Si rimane a disposizione per qualsivoglia ulteriore chiarimento, precisazione e istanza che vorrà sottoporci anche con riferimento all'esercizio dei Suoi diritti ai sensi degli artt. 15-22 del Regolamento UE 679/2016.

Cordiali Saluti

_____

Allegato B

Data Breach response plan

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

Sommario

VERSIONI DEL DOCUMENTO

EDIZIONE	SINTESI DELLA MODIFICA	DATA
1.0	Prima versione del documento	*<Data di adozione>*

1. SCOPO E CAMPO DI APPLICAZIONE

La presente procedura definisce le modalità operative, i compiti e le responsabilità relativi alla gestione delle violazioni di dati personali che potrebbero comportare un rischio per i diritti e le libertà delle persone fisiche (Data Breach).

2. RIFERIMENTI NORMATIVI

- Regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito definito RGPD);
- Allegato 1 al Provvedimento del 2 luglio 2015 del Garante per la Protezione dei dati personali;
- Guidelines on Personal Data breach notification under Regulation 2016/679 fonte Article 29 Data Protection Working Party:
- Recommendations for a methodology of the assessment of severity of personal data breaches – ENISA.
- Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) - 30 luglio 2019 [9126951]

3. DEFINIZIONI

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.

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.

Referente del Titolare: il soggetto designato dal titolare per la gestione del processo di escalation del Data Breach all'interno dell'Ente; è identificato nel ruolo del Responsabile dell'area/settore in cui si è rilevato l'evento di sicurezza, per il contesto di propria competenza.

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.

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. TIPOLOGIE DI VIOLAZIONI DI DATI PERSONALI

Le "*Guidelines on Personal data breach notification under Regulation 2016/679*" definiscono le seguenti tipologie di violazioni:

- "Confidentiality breach" - quando si verifica una violazione che comporti un accesso o una divulgazione accidentale o non autorizzata di dati personali.
- "Integrity breach" - quando si verifica una violazione che comporti una alterazione accidentale o non autorizzata di dati personali.
- "Availability breach" - quando si verifica una violazione che comporti la perdita di disponibilità o la distruzione accidentale o non autorizzata di dati personali.

5. LE POSSIBILI CONSEGUENZE DELLE VIOLAZIONI DI DATI PERSONALI

Una violazione può potenzialmente provocare una serie di effetti avversi significativi sugli individui, che possono causare danni fisici, materiali o immateriali. Il RGPD spiega che ciò può includere la perdita del controllo sui propri dati personali, la limitazione dei loro diritti, discriminazione, furto d'identità o frode, perdita finanziaria, inversione non autorizzata di pseudonimizzazione, danno alla reputazione e perdita di riservatezza dei dati personali protetti dal segreto professionale. Può anche includere qualsiasi altro significativo svantaggio economico o sociale per tali individui (*Cosiderandi 75 e 85 RGPD*).

Di conseguenza, il RGPD richiede che il titolare del trattamento notifichi una violazione all'autorità di vigilanza competente, a meno che non sia improbabile che possa comportare il rischio che tali effetti negativi si verifichino. Laddove vi sia un rischio probabile che si verifichino tali effetti avversi, il RGPD richiede che il titolare del trattamento comunichi la violazione agli individui interessati non appena sia ragionevolmente fattibile (*Considerando 86 RGDP*).

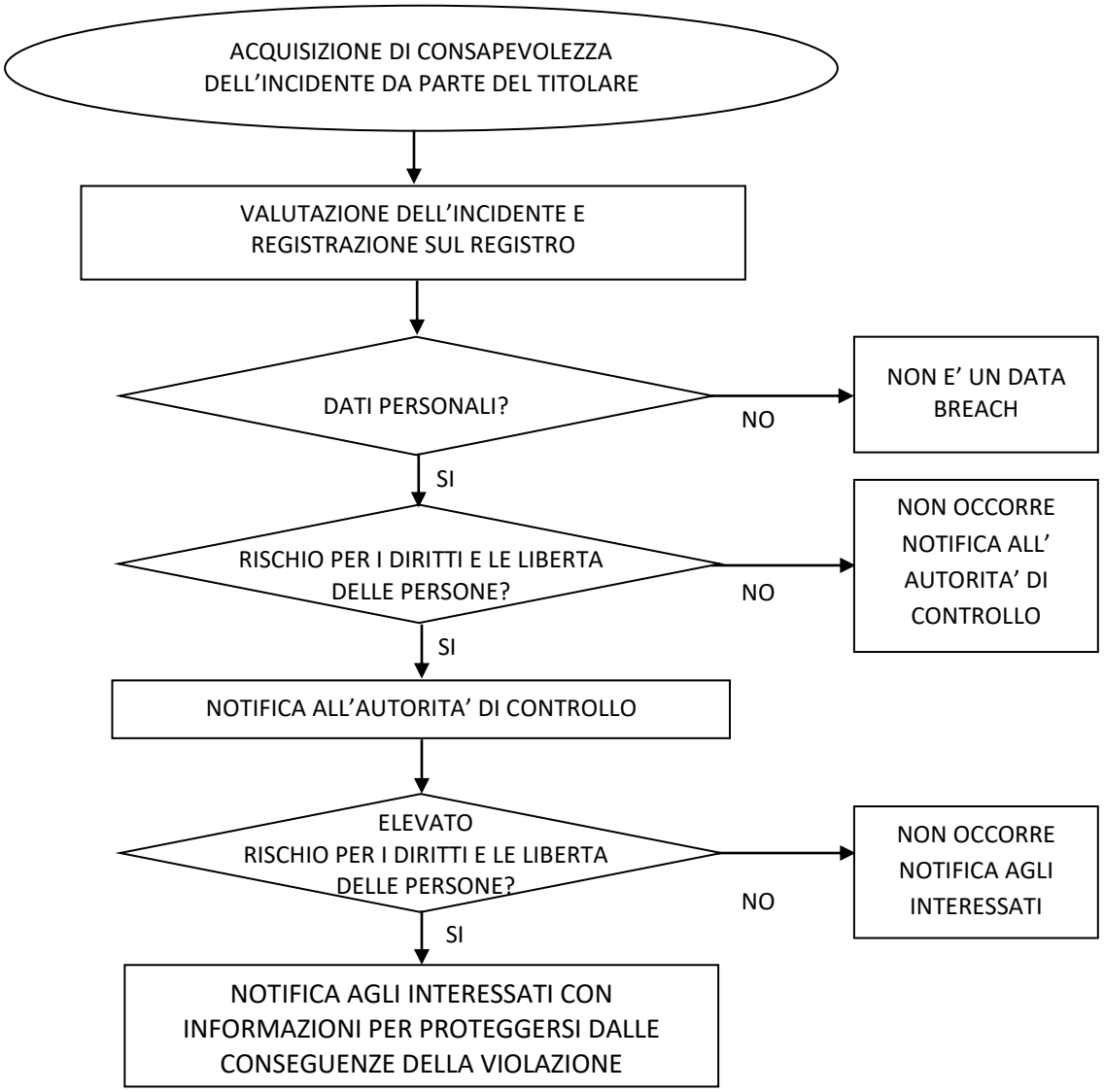
L'importanza di essere in grado di identificare una violazione, di valutare il rischio per gli individui e quindi di notificare se necessario, è sottolineata nel considerando 87 del RGPD: *"È opportuno verificare se siano state*

messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'Autorità di Controllo e l'interessato. È opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze e effetti negativi per l'interessato. Siffatta notifica può dar luogo a un intervento dell'Autorità di Controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento".

In caso di mancata notifica all'Autorità di Controllo o agli interessati quando richiesto dalla norma, così come l'assenza o l'inadeguatezza di misure di sicurezza potrebbero comportare, da parte dell'autorità di vigilanza, l'applicazione di sanzioni amministrative a un livello che sia efficace, proporzionato e dissuasivo entro il limite dell'inadempimento più grave (fino ad un totale di 20.000.000 € o al 4% del fatturato globale).

6. PIANO DI GESTIONE DEGLI INCIDENTI DI SICUREZZA

Al verificarsi di un incidente di sicurezza, si attiva un processo di gestione come di seguito illustrato:



7. LA CONSAPEVOLEZZA DELL'INCIDENTE

L'Art. 33 del RGPD richiede che, in caso di violazione dei dati personali, il titolare del trattamento la notifichi all'Autorità di Controllo entro 72 ore dal momento in cui ne è venuto a conoscenza. Il WP29 ritiene che un titolare debba essere considerato "*consapevole*" quando quel titolare ha un ragionevole grado di certezza che si è verificato un incidente di sicurezza che ha portato a compromettere i dati personali.

Tale grado di consapevolezza non è sempre evidente e nasce dall'essere venuti a conoscenza di un evento che potrebbe compromettere la riservatezza, la disponibilità o l'integrità delle informazioni. Da tale rilevazione deve scaturire il successivo step di valutazione dell'incidente, al fine di determinare se si tratti o meno di una violazione di dati personali.

La rilevazione dell'incidente viene effettuata da uno dei Referenti del Titolare; ogni Referente agisce su propria iniziativa per gli incidenti verificatisi nella sua area e ai suoi collaboratori o su espresso impulso del Segretario Generale. Chiunque rimarchi un incidente, deve darne comunicazione a mezzo email senza indugio al Referente competente per il contesto in cui si è rilevato l'incidente, utilizzando il modello allegato (allegato 3) e partecipando alla fase di valutazione dell'incidente, fornendo ogni ulteriore elemento utile.

In caso di rilevazione di una violazione da parte di un Responsabile del Trattamento, questo è tenuto a comunicare al Titolare con la massima urgenza, ed in ogni caso entro 24 ore dalla rilevazione della violazione, tutte le informazioni disponibili relative all'accaduto. Il Responsabile è tenuto a prestare ogni più ampia assistenza al Titolare al fine di consentirgli di assolvere agli obblighi di cui agli artt. 32-34 del RGPD.

8. LA VALUTAZIONE DELL'INCIDENTE

La consapevolezza che un incidente di sicurezza rappresenti una violazione di dati personali è funzione della rilevazione dell'incidente, della presa d'atto che siano coinvolti dati personali e della valutazione che tale evento possa comportare un rischio per i diritti e le libertà delle persone.

Pertanto, al momento della rilevazione dell'incidente, il titolare, tramite il proprio referente designato, deve immediatamente attivarsi per valutare se esso possa comportare un rischio di tale entità, in funzione di diversi aspetti fra cui:

- La numerosità dei soggetti che potrebbero essere danneggiati da tale evento;
- Le categorie dei soggetti a cui i dati si riferiscono, con particolare attenzione per categorie come minori, soggetti con disabilità o particolari forme di vulnerabilità;
- La tipologia dei dati coinvolti, con specifica cautela per le categorie di dati particolari di cui all'Art. 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10 del RGPD;
- La confidenza del fatto che le misure tecnologiche e organizzative implementate possano o meno aver impedito la compromissione dei dati oggetto dell'incidente di sicurezza.

Oltre all'analisi dell'incidente per verificare se sono coinvolti dati personali, è necessario attuare le conseguenti azioni per rimediare alle conseguenze dell'incidente ed eventualmente procedere con le notifiche necessarie.

Si riportano nell'allegato 1 alcuni casi, a titolo esemplificativo ma non esaustivo, che possano chiarire meglio quali tipologie di incidenti si traducano in violazioni di sicurezza che debbano comportare la notifica all'Autorità di Controllo ed eventualmente agli stessi interessati.

Anche qualora l'incidente non si traducesse in una violazione di sicurezza, tale evento deve essere registrato sull'apposito registro al fine di poter produrre evidenza documentale delle azioni intraprese in caso di verifica da parte dell'Autorità di Controllo. Sul registro devono essere rilevati gli estremi dell'incidente, le conseguenze che ha portato, le azioni intraprese per ridurne o annullarne l'impatto e la loro efficacia. All'allegato 2 è riportato il modello per la registrazione degli incidenti.

Nelle fasi di valutazione dell'incidente, qualora lo ritenga necessario il referente del titolare può avvalersi del supporto del Responsabile per la Protezione dei Dati al fine di determinare l'eventualità di procedere con le notifiche della violazione di sicurezza, in caso di bisogno.

9. LA NOTIFICA ALL'AUTORITA' DI CONTROLLO

L'Art. 33 del RGPD richiede che il titolare del trattamento notifichi all'Autorità di Controllo la violazione di dati personali entro 72 ore dal momento in cui ne è venuto a conoscenza. La comunicazione deve almeno

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) identificare le probabili conseguenze della violazione dei dati personali;
d) illustrare le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Nel caso non siano disponibili informazioni precise e complete, è comunque necessario effettuare prontamente la comunicazione, focalizzandosi sugli effetti avversi della violazione piuttosto che sulla precisione della segnalazione. Sarà poi possibile fornire successivamente ulteriori informazioni ad integrazione di quanto già segnalato, come recita l'Art. 34 del RGPD: *"Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo"*.

Il soggetto designato dal titolare per effettuare materialmente la comunicazione è il referente, il quale procede ad istruire la documentazione necessaria che verrà comunicata all'Autorità Garante della Privacy. Il modello utilizzato per la comunicazione è reso disponibile sul sito dell'Autorità di Controllo, nella sezione specifica dedicata al Data Breach. La notifica deve essere inviata al Garante tramite posta elettronica all'indirizzo protocollo@pec.gpdp.it e deve essere sottoscritta digitalmente (con firma elettronica qualificata/firma digitale) ovvero con firma autografa. In quest'ultimo caso la notifica deve essere presentata unitamente alla copia del documento d'identità del firmatario.

L'oggetto del messaggio deve contenere obbligatoriamente la dicitura “NOTIFICA VIOLAZIONE DATI PERSONALI” e opzionalmente la denominazione del titolare del trattamento. Per maggiori informazioni occorre fare riferimento al sito ufficiale dell’Autorità di Controllo: http://www.garanteprivacy.it/.

10. LA NOTIFICA AGLI INTERESSATI

L’Art. 34 del RGPD stabilisce che *“Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all’interessato senza ingiustificato ritardo”*.

Il rischio elevato non è facilmente classificabile, tuttavia esiste senza dubbio quando la violazione può comportare un danno fisico, materiale o immateriale per le persone i cui dati sono stati violati. Esempi di tale danno sono la discriminazione, il furto d'identità o la frode, la perdita finanziaria e il danno alla reputazione. Quando la violazione riguarda dati personali che rivelano origini razziali o etniche, opinioni politiche, religione o convinzioni filosofiche, o appartenenza sindacale, o dati genetici, dati relativi alla salute o dati relativi alla vita sessuale, condanne penali e reati o relative misure di sicurezza, è molto probabile che si verifichi un rischio elevato per i diritti e le libertà degli interessati.

La soglia di comunicazione delle violazioni agli interessati è più alta rispetto a quella della comunicazione all’Autorità di Controllo, al fine di non sovraccaricarli di comunicazioni eccessive. La principale finalità della comunicazione agli interessati è quella di fornire loro specifiche informazioni per potersi proteggere dalle conseguenze della violazione. Pertanto, deve descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contenere almeno le seguenti informazioni:

- una descrizione della natura della violazione;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altri punti di contatto; una descrizione delle probabili conseguenze della violazione;
- una descrizione delle misure adottate o proposte per affrontare la violazione, comprese, se del caso, misure per mitigarne gli eventuali effetti negativi.

Ad esempio, si possono invitare gli interessati a resettare eventuali password qualora le loro credenziali di accesso ad un servizio siano state violate.

Come prima scelta è preferenziale ricorrere al contatto diretto e dedicato degli interessati (es. email, SMS e messaggi diretti), a meno che questo non comporti uno sforzo sproporzionato rispetto alla finalità. E’ fortemente raccomandato l’utilizzo di differenti canali di comunicazione in contemporanea, al fine di massimizzare la possibilità di contattare il maggior numero di interessati colpiti dalla violazione, anche con il supporto di media di grande diffusione qualora il rischio lo richieda.

L'Art. 34 del RGPD stabilisce tre condizioni che, se soddisfatte, non richiedono la notifica ai singoli in caso di violazione. Questi sono:

- Il titolare del trattamento ha applicato misure tecniche e organizzative adeguate per proteggere i dati personali prima della violazione, in particolare quelle misure che rendono i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi. Ciò potrebbe, ad esempio, includere la protezione dei dati personali con la crittografia allo stato dell'arte o mediante la tokenizzazione.

- Immediatamente dopo una violazione, il titolare del trattamento ha provveduto a garantire che l'alto rischio posto ai diritti e alle libertà delle persone non si concretizzasse più. Ad esempio, a seconda delle circostanze del caso, il titolare può aver immediatamente identificato e intrapreso un'azione contro l'individuo che ha avuto accesso ai dati personali prima di poter compiere qualsiasi azione con gli stessi. È necessario tenere in debito conto le possibili conseguenze di eventuali violazioni della riservatezza, anche in questo caso, a seconda della natura dei dati in questione.
- Comporterà uno sforzo sproporzionato per contattare le persone, quando forse i loro dettagli di contatto sono stati persi a causa della violazione o non sono noti in primo luogo. Ad esempio, il magazzino di un ufficio statistico si è allagato e i documenti contenenti dati personali sono stati memorizzati solo in formato cartaceo. In tali casi, il titolare deve fare una comunicazione pubblica o adottare una misura simile, in base alla quale le persone possano essere informate in modo altrettanto efficace. Nel caso di uno sforzo sproporzionato, potrebbero anche essere previste disposizioni tecniche per rendere le informazioni sulla violazione disponibili su richiesta, che potrebbero rivelarsi utili per i soggetti interessati da una violazione, che il titolare del trattamento non può contattare in maniera alternativa.

Conformemente col principio di *accountability* che è alla base del RGPD, il titolare del trattamento dovrebbe essere in grado di dimostrare all'Autorità di Controllo di soddisfare una o più delle condizioni sopra indicate. Va tenuto presente che, sebbene la notifica inizialmente non possa essere richiesta se non vi è alcun rischio per i diritti e le libertà delle persone fisiche, ciò potrebbe cambiare nel tempo e il rischio dovrebbe essere rivalutato.

11. ALLEGATI DEL PRESENTE DOCUMENTO

Si riportano di seguito gli allegati al presente documento, che ne costituiscono parte integrante:

Allegato B1 – Esempi di incidenti di sicurezza e valutazione di eventuali violazioni

Allegato B2 – Modello Registro delle Violazioni di dati personali

Allegato B3- Informazioni da comunicare al Referente

12. 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 Determinazione Dirigenziale da parte del responsabile del procedimento a cui fa capo il servizio Sistema Informatico (a seconda della rilevanza delle modifiche apportate).

ALLEGATO B1 – ESEMPI DI INCIDENTI DI SICUREZZA E VALUTAZIONE DI EVENTUALI VIOLAZIONI

I seguenti esempi sono tratti all'allegato B delle Guidelines on Personal Data breach notification under Regulation 2016/679 - fonte Article 29 Data Protection Working Party:

ESEMPIO	NOTIFICA AUTORITA' CONTROLLO	NOTIFICA ALL'INTERESSATO	NOTE / RACCOMANDAZIONI
Un titolare ha fatto un backup di un archivio di dati personali crittografati su una chiave USB. La chiave viene rubata.	NO	NO	Finché i dati vengono crittografati con un algoritmo avanzato, i backup dei dati esistono, la chiave univoca non viene compromessa e i dati possono essere ripristinati in tempo utile, ciò potrebbe non essere una violazione segnalabile. Tuttavia, se viene successivamente compromesso, è necessaria la notifica.
Un titolare gestisce un servizio online. A seguito di un attacco informatico su quel servizio, i dati personali degli individui vengono rubati. Il titolare ha clienti in un singolo stato membro,	Sì, riferire all'autorità di vigilanza se vi sono probabili conseguenze per le persone.	Sì, riferire alle persone a seconda della natura dei dati personali interessati e se la gravità delle probabili conseguenze per gli individui è elevata.	
Una breve interruzione di corrente di alcuni minuti presso il call center di un titolare	NO	NO	Questa non è una violazione soggetta a notifica, ma è comunque un incidente registrabile ai sensi dell'articolo 33, paragrafo 5.

comporta che i clienti non siano in grado di chiamare il titolare e accedere ai loro record.			I registri appropriati devono essere conservati dal titolare.
Un titolare subisce un attacco ransomware che provoca la crittografia di tutti i dati. Non sono disponibili backup e i dati non possono essere ripristinati. Durante le indagini, diventa chiaro che l'unica funzionalità del ransomware era quella di crittografare i dati e che non c'erano altri malware presenti nel sistema.	Sì, riferire all'autorità di vigilanza, se ci sono probabili conseguenze per gli individui in quanto si tratta di una perdita di disponibilità.	Sì, riferire ai singoli, a seconda della natura dei dati personali interessati e del possibile effetto della mancanza di disponibilità dei dati, nonché di altre possibili conseguenze.	Se fosse disponibile una copia di riserva e i dati potessero essere ripristinati in tempo utile, ciò non dovrebbe essere segnalato all'autorità di vigilanza o ai singoli in quanto non vi sarebbe stata alcuna perdita permanente di disponibilità o riservatezza. Tuttavia, se l'autorità di vigilanza venisse a conoscenza dell'incidente con altri mezzi, potrebbe prendere in considerazione un'indagine per valutare la conformità ai requisiti di sicurezza più ampi dell'articolo 32.
Un individuo telefona al call center di una banca per segnalare una violazione dei dati. L'individuo ha ricevuto una dichiarazione mensile di qualcun altro. Il titolare del trattamento intraprende un'investigazione breve (ossia completata entro 24 ore) e stabilisce con ragionevole certezza che si è verificata una violazione dei dati personali e che vi è un difetto sistemico che potrebbe significare che altri individui sono o potrebbero essere interessati.	SI	Solo le persone colpite vengono avvisate se c'è un rischio elevato ed è ragionevolmente certo che altri soggetti non siano stati colpiti.	Se, dopo ulteriori indagini, viene identificato un numero maggiore di persone interessate, è necessario eseguire un aggiornamento dell'autorità di vigilanza e il titolare effettua il passaggio aggiuntivo per notificare agli altri individui se vi è un rischio elevato per loro.
Un titolare gestisce un sito di e-commerce ed ha clienti in più Stati membri. Il sito subisce	Sì, segnalare all'autorità di vigilanza principale se il	Sì, in quanto potrebbe comportare alto rischio.	Il titolare dovrebbe agire, ad es. forzando il ripristino della password degli account interessati,

un attacco informatico e usernames, password e cronologia degli acquisti sono pubblicati online dall'attaccante.	trattamento è transfrontaliero.		nonché altri passaggi per mitigare il rischio. Il titolare del trattamento dovrebbe anche considerare qualsiasi altro obbligo di notifica, ad es. sotto la direttiva NIS come fornitore di servizi digitali.
Una società di hosting di siti Web che agisce come responsabile del trattamento identifica un errore nel codice che controlla l'autorizzazione degli utenti. L'effetto del difetto indica che ogni utente possa accedere ai dettagli dell'account di qualsiasi altro utente.	In qualità di responsabile, la società di hosting del sito web deve notificare i clienti interessati (i titolari) senza indebito ritardo. Supponendo che la società di hosting del sito web abbia condotto le proprie indagini, i titolari coinvolti dovrebbero essere ragionevolmente certi se vi sia stata una violazione, pertanto è probabile che venga considerato come "presa di coscienza" una volta che sia stata notificata dalla società di hosting (il responsabile). Il titolare deve quindi informare l'autorità di vigilanza.	Se non ci sono probabili rischi elevati per le persone la violazione non deve essere notificata.	La società di hosting del sito web (responsabile) deve considerare qualsiasi altro obbligo di notifica (ad esempio ai sensi della direttiva NIS come fornitore di servizi digitali). Se non vi è alcuna prova che tale vulnerabilità sia sfruttata per uno dei suoi titolari, una violazione notificabile potrebbe non essersi verificata, ma potrebbe essere verosimilmente registrabile o essere oggetto di non conformità ai sensi dell'articolo 32.
Le cartelle cliniche di un ospedale non sono disponibili per un periodo di 30 ore a causa di un attacco informatico.	Sì, l'ospedale è obbligato a notificare la violazione come ad alto rischio per il	Sì, occorre riferire alle persone colpite.	

	benessere del paziente e per la sua privacy.		
I dati personali di un gran numero di studenti vengono erroneamente inviati alla mailing list sbagliata con più di 1000 destinatari.	Sì, occorre riferire all'Autorità di Vigilanza.	Sì, occorre riferire alle persone in base alla portata e al tipo di dati personali coinvolti, oltre che alla gravità delle possibili conseguenze.	
Una email di marketing diretto viene inviata ai destinatari nei campi "a:" o "cc:", consentendo in tal modo a ciascun destinatario di vedere l'indirizzo e-mail di altri destinatari.	Sì, la notifica all'autorità di vigilanza può essere obbligatoria se un numero elevato di persone è interessato, se vengono rivelati dati sensibili (ad esempio una mailing list di uno psicoterapeuta) o se altri fattori presentano rischi elevati (ad esempio, la posta contiene le password iniziali).	Sì, occorre riferire alle persone in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	La notifica potrebbe non essere necessaria se non vengono rivelati dati sensibili e se viene rivelato solo un numero minore di indirizzi e-mail.

ALLEGATO B2 – MODELLO REGISTRO VIOLAZIONI DEI DATI PERSONALI

Registro Violazioni dati personali (Data Breach)

Registro		Dettagli della Violazione					Conseguenze della Violazione	Misure Intraprese / Da intraprendere			
N.	Ticket Rif.	Data Evento	Natura dell'Evento	Descrizione della Violazione	Dati Interessati	Soggetti Coinvolti		Informativa Garante	Informativa altri soggetti coinvolti	Azioni Intraprese	Azioni da Intraprendere
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
16											
17											
18											
19											
20											

ALLEGATO B3 - INFORMAZIONI DA COMUNICARE AL REFERENTE

Dati identificativi Segnalante	
Eventuali Contatti (altre informazioni)	

INFORMAZIONI DI SINTESI DELLA VIOLAZIONE

Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca dati?

- ☐ Il _____
- ☐ Dal _____(la violazione è ancora in corso)
- ☐ Dal _____ al _____
- ☐ In un tempo non ancora determinato

Ulteriori informazioni circa le date in cui è avvenuta la violazione:

_____
_____

Data: _____ Ora: _____ in cui si è venuto a conoscenza della violazione

In caso di segnalazione oltre le 72 ore, quali sono i motivi del ritardo?

_____
_____

Breve descrizione della violazione:

_____
_____
_____
_____
_____
_____

Tipo di violazione

- ☐ Lettura (presumibilmente i dati non sono stati copiati)
- ☐ Copia (i dati sono ancora presenti sui sistemi del titolare)
- ☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
- ☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
- ☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
- ☐ Altro : _____

Causa della violazione

- ☐ Azione intenzionale interna
- ☐ Azione accidentale interna
- ☐ Azione intenzionale esterna
- ☐ Azione accidentale esterna
- ☐ Sconosciuta
- ☐ Altro (specificare)

Categorie di dati personali oggetto di violazione

- ☐ Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro...)
- ☐ Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
- ☐ Dati di accesso e di identificazione (username, password, customer ID, altro…)
- ☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…)
- ☐ Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…)
- ☐ Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza o di prevenzione
- ☐ Dati di profilazione Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…)
- ☐ Dati di localizzazione
- ☐ Dati che rivelino l'origine razziale o etnica
- ☐ Dati che rivelino opinioni politiche
- ☐ Dati che rivelino convinzioni religiose o filosofiche Dati che rivelino l'appartenenza sindacale
- ☐ Dati relativi alla vita sessuale o all'orientamento sessuale
- ☐ Dati relativi alla salute
- ☐ Dati genetici
- ☐ Dati biometrici
- ☐ Categorie ancora non determinate
- ☐ Altro _____

Indicare il volume (anche approssimativo) dei dati personali oggetto di violazione

- ☐ N. _____
- ☐ Circa n. _____
- ☐ Un numero (ancora) sconosciuto di dati

Indicare le tipologie di interessati coinvolti nella violazione (dipendenti, utenti, cittadini, minori, persone vulnerabili, altro:

_____
_____
_____
_____
_____

Numero (anche approssimativo) di interessati coinvolti nella violazione

- ☐ N. _____ interessati
- ☐ Circa n. _____ interessati
- ☐ Un numero (ancora) sconosciuto di interessati

Che tipo di dati sono oggetto di violazione?

- □ Dati anagrafici/codice fiscale
- □ Dati di accesso e di identificazione (user name, password, customer ID, altro)
- □ Dati relativi a minori
- □ Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
- □ Dati personali idonei a rivelare lo stato di salute e la vita sessuale
- □ Dati giudiziari
- □ Copia per immagine su supporto informatico di documenti analogici
- □ Ancora sconosciuto
- □ Altro : _____

Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati (secondo le valutazioni del titolare)?

- □ Basso/trascurabile
- □ Medio
- □ Alto
- □ Molto alto

Misure tecniche e organizzative adottate (o di cui si propone l'adozione20) per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati

_____
_____
_____
_____
_____

Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per prevenire simili violazioni future

_____
_____
_____
_____
_____

La violazione è stata comunicata anche agli interessati?

- □ Sì, in data _____ tramite □ SMS / □ Posta cartacea / □ Posta Elettronica / □ Altro
- □ No, perché _____

Qual è il contenuto della comunicazione resa agli interessati?

_____
_____
_____
_____

Allegato C

Valutazione di impatto sulla protezione del dati

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

Sommario

VERSIONI DEL DOCUMENTO		
EDIZIONE	**SINTESI DELLA MODIFICA**	**DATA**
1.0	Prima versione	*<Data di adozione>*

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 è 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, nonché 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 nonché 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 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. MODALITÀ 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.

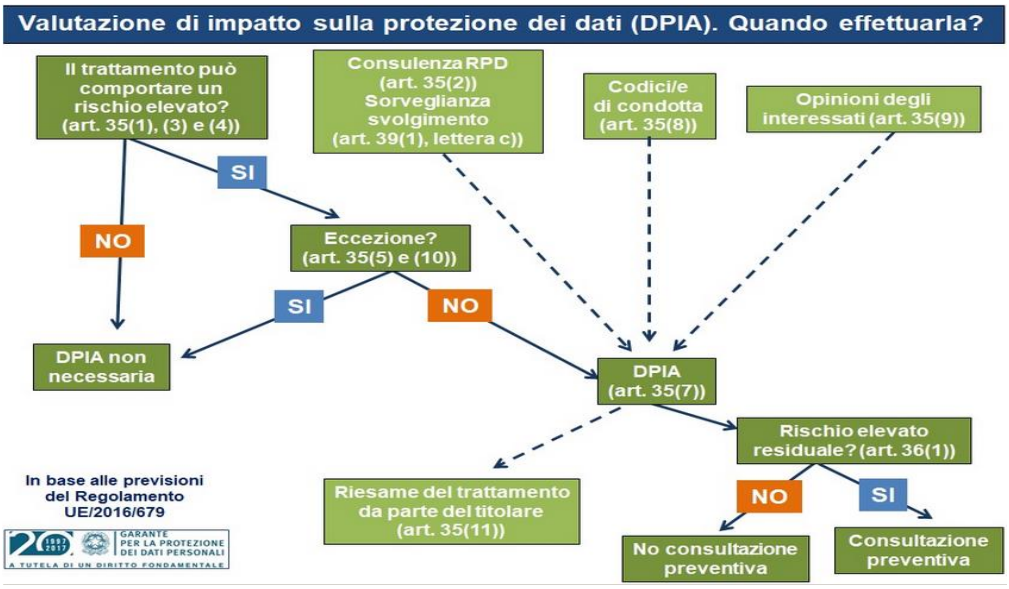
La DPIA non si applica qualora il trattamento

- sia effettuato ai sensi del **Regolamento UE 2016/679, articolo 6, paragrafo 1, lettera c)** (per obbligo legale al quale è soggetto il titolare del trattamento) **o lettera e)** (per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento) e **trovi nel diritto dell'Unione o nel diritto dello Stato membro** cui il titolare del trattamento è soggetto **una base giuridica** che 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 nel contesto dell'adozione di tale base giuridica.

Se valgono tali condizioni la DPIA non si applica (per cui non si applicano i paragrafi da 1 a 7 dell'art. 35 del Regolamento UE 2016/679), 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: - Finalità del trattamento - Natura del trattamento - Ambito di applicazione - Contesto (normativo – organizzativo ecc.) - Dati personali registrati: - Destinatari del trattamento: - Periodo di conservazione dei dati personali - Descrizione funzionale del trattamento:

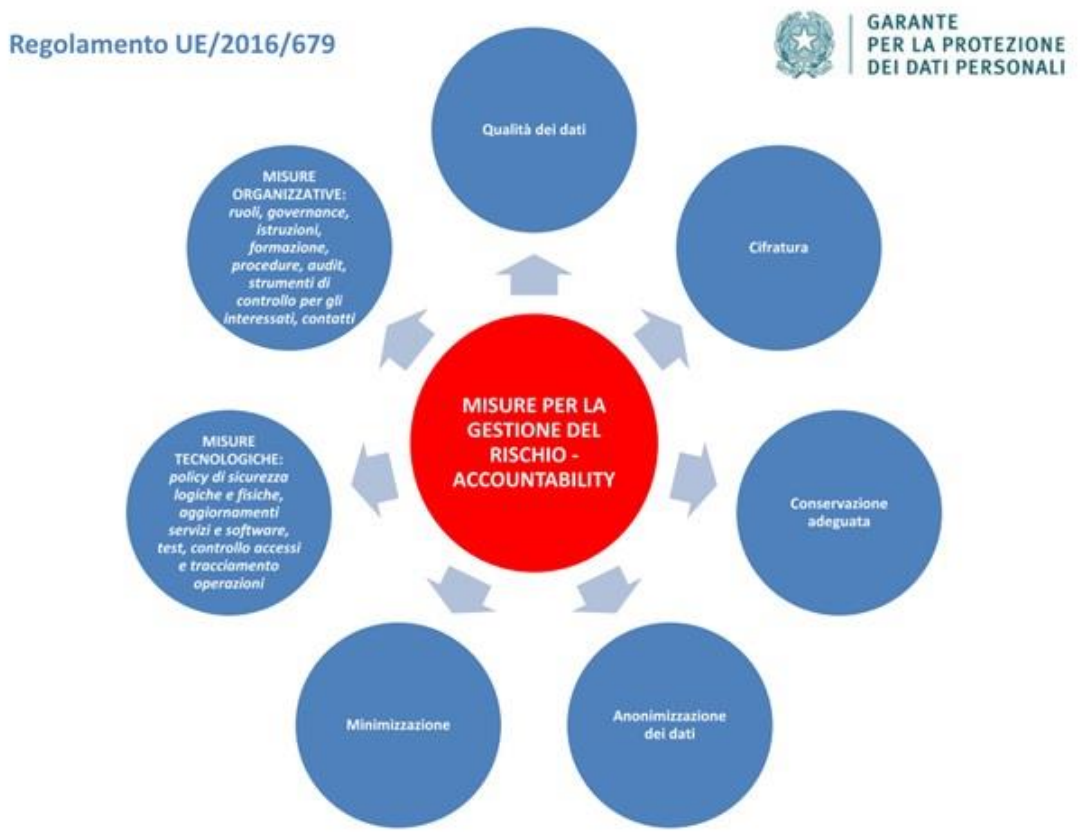
		- Individuazione delle risorse sulle quali sono registrati i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea); - Codici di condotta approvati applicabili (art. 35, paragrafo 8);
Valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità	art. 35, paragrafo 7, lettera b	Presenza di misure adeguate al fine di garantire: a) il rispetto del regolamento (articolo 35, paragrafo 7, lettera d) e considerando 90) con riferimento a: - finalità specifiche, esplicite e legittime (art. 5(1), lettera b)); - liceità del trattamento (art. 6); - dati adeguati, pertinenti e limitati a quanto necessario (art. 5(1)c)); - periodo limitato di conservazione (art. 5(1), lettera e)); b) la proporzionalità e la necessità del trattamento sulla base di: - finalità determinate, esplicite e legittime (articolo 5, paragrafo 1, lettera b)); - liceità del trattamento (articolo 6); - dati personali adeguati, pertinenti e limitati a quanto necessario (articolo 5, paragrafo 1, lettera c)); - 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 a: accesso illegittimo, modifiche indesiderate, indisponibilità dei dati b) Individuazione dei diritti degli interessati e valutazione degli impatti potenziali su tali diritti e sulle libertà degli interessati stessi dei rischi descritti; c) individuazione delle minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilità dei dati; d) stima delle probabilità e gravità (considerando 90); e) individuazione delle misure volte a gestire (eliminazione/mitigazione) i rischi di cui sopra (art. 35, paragrafo 7, lettera d) e considerando 90);
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. MODALITÀ OPERATIVE PER L'ATTUAZIONE DELLA DPIA

La **CNIL**, l'Autorità francese per la protezione dei dati (Commission nationale de l'informatique et des libertés), 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.

I passaggi di creazione di una DPIA attraverso l'uso del software sono riportate all'Allegato 1.

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: rpd@sinetinformatica.it. Alla ricezione della email, il Responsabile per la Protezione dei Dati si attiva per la sua registrazione e rileva l'esito nell'apposito sistema documentale dedicato attendendosi alle indicazioni dell'Allegato 2.

10. ALLEGATI DEL PRESENTE DOCUMENTO

Si riportano di seguito gli allegati al presente documento, che ne costituiscono parte integrante:

Allegato C1 – Passaggi per l'effettuazione di una DPIA tramite il software realizzato dalla CNIL

Allegato C2 – Modalità di registrazione dell'esito della DPIA effettuata

11. 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.

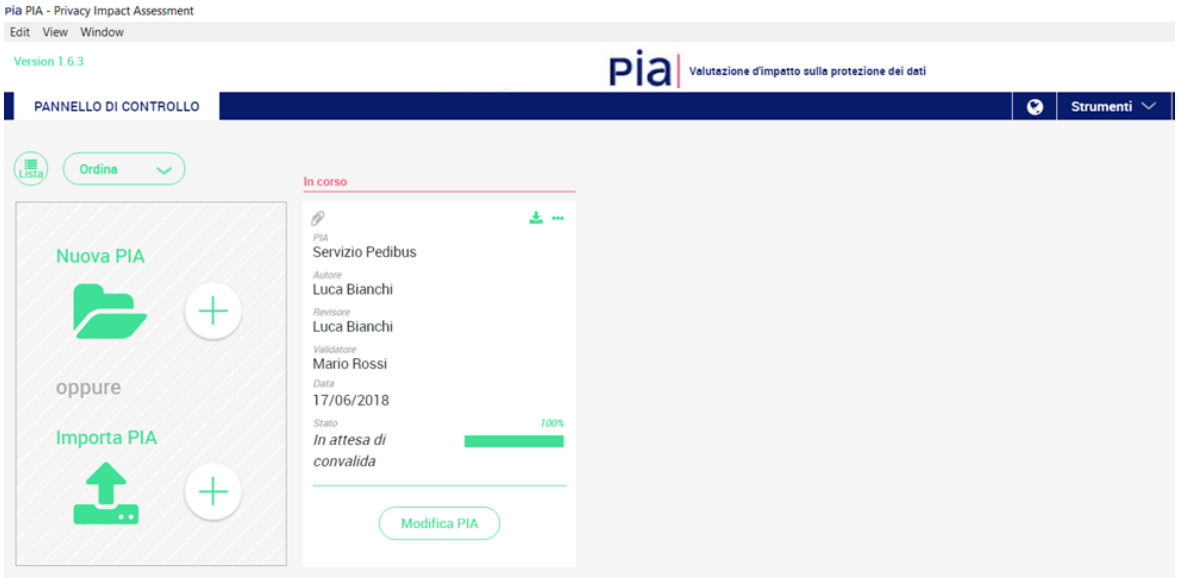
Le modifiche al documento verranno approvate con Delibera di Giunta Comunale o Determinazione Dirigenziale da parte del responsabile del procedimento a cui fa capo il servizio Sistema Informatico (a seconda della rilevanza delle modifiche apportate).

ALLEGATO C1 – PASSAGGI PER L'EFFETTUAZIONE DI UNA DPIA TRAMITE IL SOFTWARE REALIZZATO DALLA CNIL

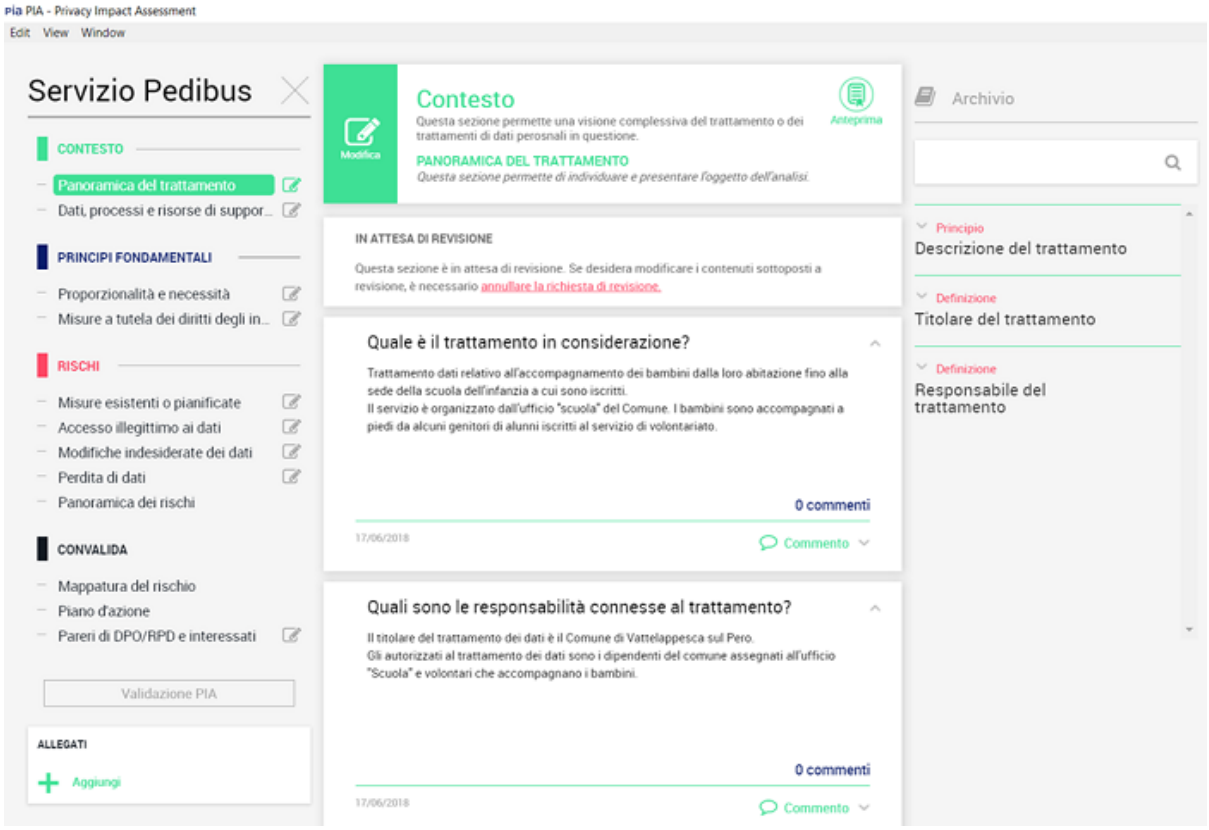
Di seguito si riportano i passaggi per la creazione di una DPIA utilizzando il software messo a disposizione dalla CNIL:

1- Apertura software

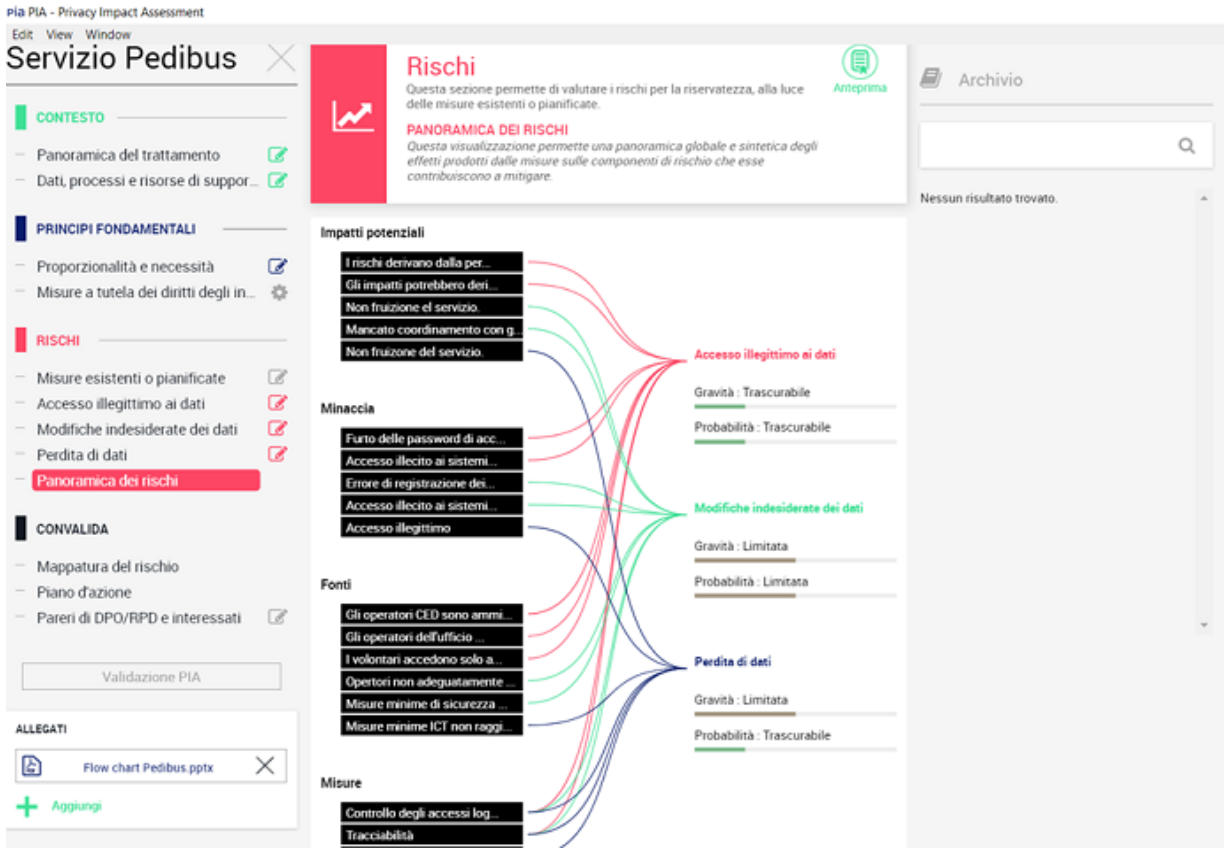
2- Apertura di una nuova DPIA



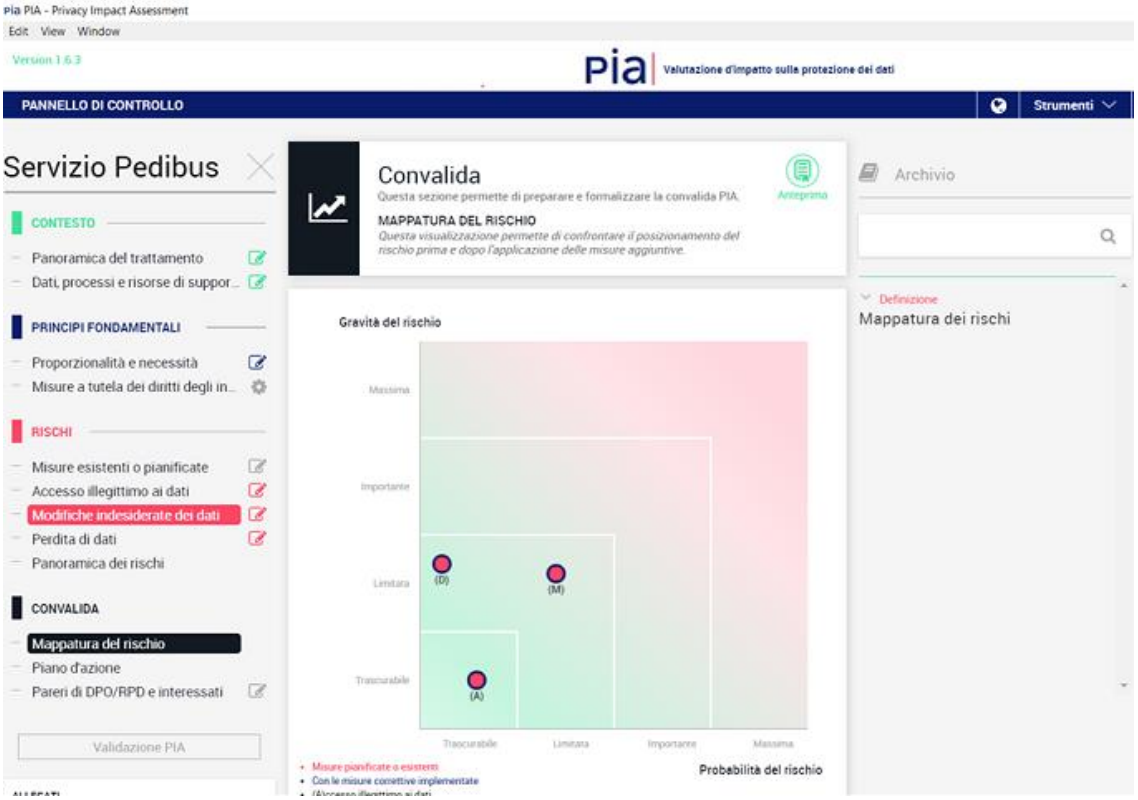
3- Compilazione della sezione “Contesto” – “Principi Fondamentali” e “Rischi”



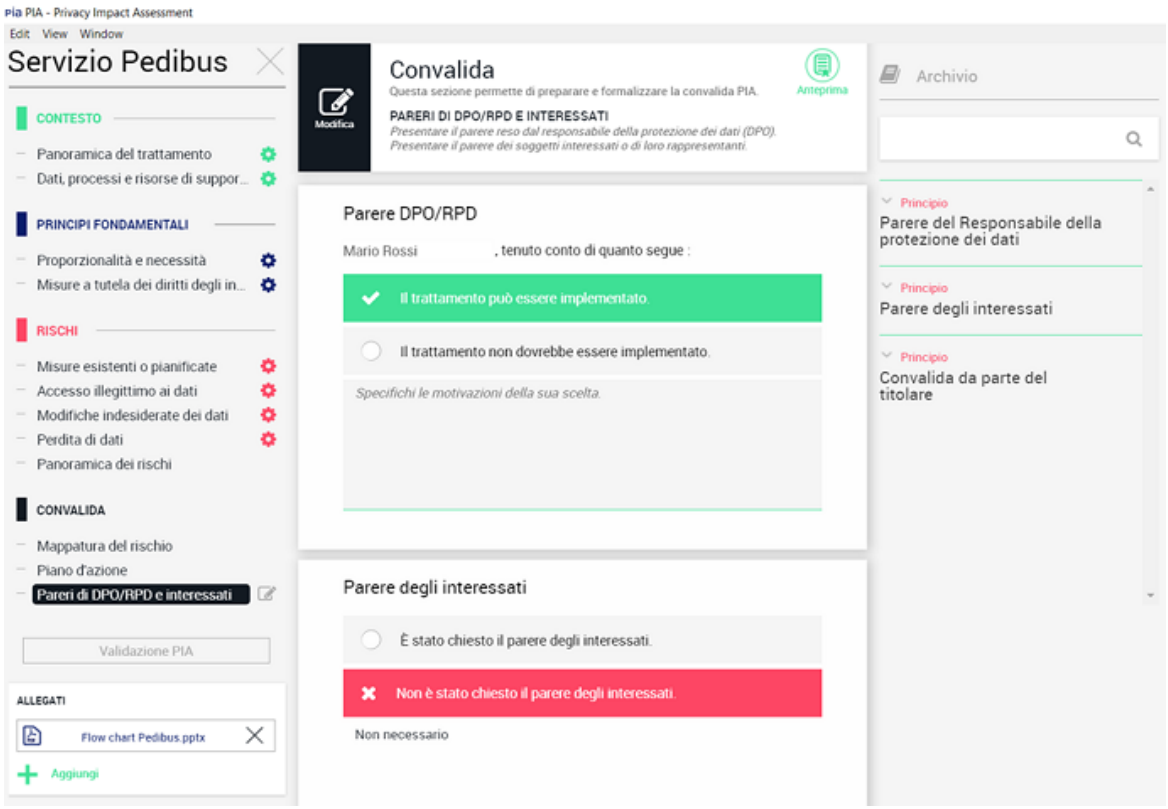
4- Analisi dei rischi e delle misure volte a mitigarli



5- Convalida e analisi della gravità del rischio

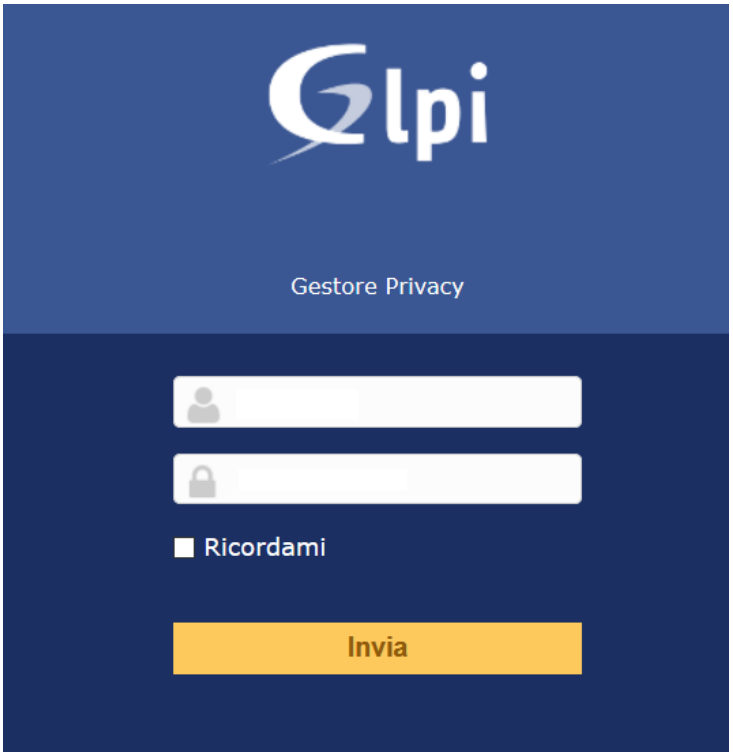


6- Redazione dell'eventuale piano d'azione per mitigare i rischi residui e parere del DPO

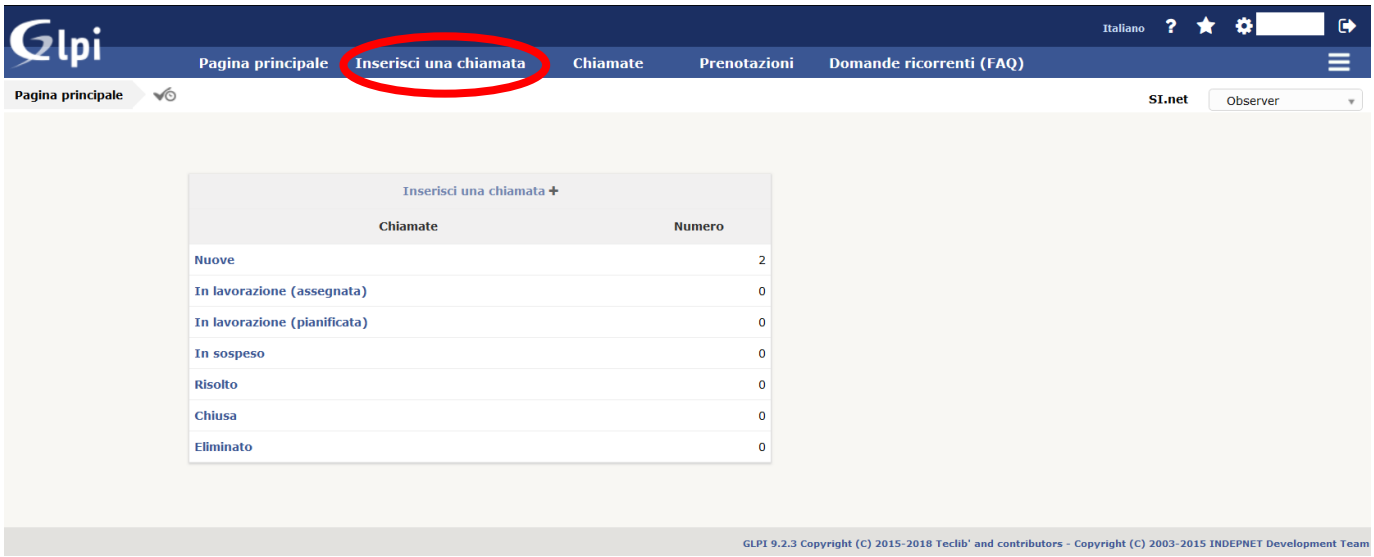


ALLEGATO C2 – MODALITA' DI REGISTRAZIONE DELL'ESITO DELLA DPIA EFFETTUATA

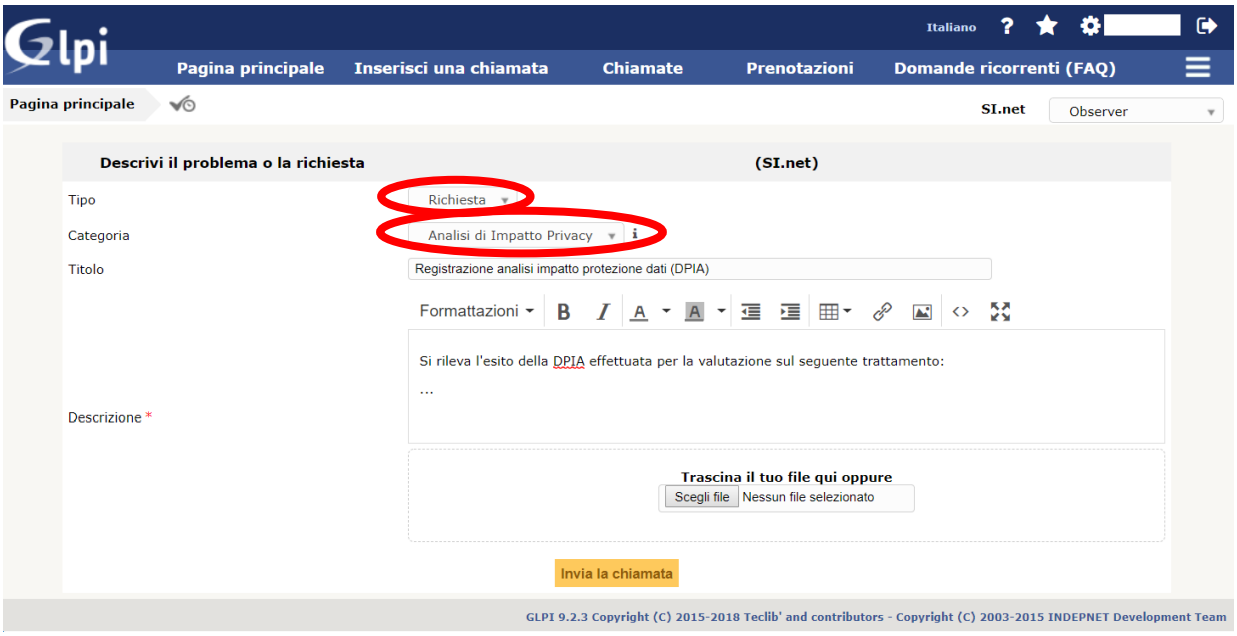
1) Collegarsi all'indirizzo https://privacy.sinetinformatica.it/ utilizzando le credenziali rilasciate



2) Collegarsi ed cliccare sul link "Inserisci una chiamata"



3) Aprire una chiamata di tipo “Richiesta” – Categoria “Analisi di Impatto Privacy” e segnalare l’accaduto, eventualmente allegando dei files che possano contribuire a chiarire il contesto:



Città di Tradate
(Provincia di Varese)

SERVIZIO UFFICIO RAGIONERIA

PARERE DI REGOLARITA' CONTABILE

Sulla proposta n. 1763/2022 ad oggetto: APPROVAZIONE DELLA "PROCEDURA PER L'ESERCIZIO DEI DIRITTI DEGLI INTERESSATI", DELLA "PROCEDURA GESTIONE DELLE VIOLAZIONI (DATA BREACH)" E DELLA "PROCEDURA DEL PROCESSO DI ANALISI DI IMPATTO PRIVACY (DPIA)" AI SENSI DEL REGOLAMENTO UE 2016/679 si esprime ai sensi dell'art. 49, 1° comma del Decreto legislativo n. 267 del 18 agosto 2000, parere NON APPOSTO in ordine alla regolarità contabile.

Tradate, 07/07/2022

Sottoscritto dal Responsabile
(ELENA VALEGGIA)
con firma digitale

Documento informatico formato e prodotto ai sensi del D.Lgs. 82/2005 e rispettive norme collegate.

Città di Tradate
(Provincia di Varese)

SERVIZIO UFFICIO SEGRETERIA DEL SINDACO

PARERE DI REGOLARITA' TECNICA

Sulla proposta n. 1763/2022 del SERVIZIO UFFICIO SEGRETERIA DEL SINDACO ad oggetto: APPROVAZIONE DELLA "PROCEDURA PER L'ESERCIZIO DEI DIRITTI DEGLI INTERESSATI", DELLA "PROCEDURA GESTIONE DELLE VIOLAZIONI (DATA BREACH)" E DELLA "PROCEDURA DEL PROCESSO DI ANALISI DI IMPATTO PRIVACY (DPIA)" AI SENSI DEL REGOLAMENTO UE 2016/679 si esprime ai sensi dell'art. 49, 1° comma del Decreto legislativo n. 267 del 18 agosto 2000, parere FAVOREVOLE in ordine alla regolarità tecnica.

Tradate, 06/07/2022

Sottoscritto dal Responsabile
(MARINA BELLEGOTTI)
con firma digitale

Documento informatico formato e prodotto ai sensi del D.Lgs. 82/2005 e rispettive norme collegate.

Città di Tradate
(Provincia di Varese)

Certificato di Pubblicazione

Deliberazione di Giunta Comunale N. 94 del 15/07/2022

UFFICIO SEGRETERIA DEL SINDACO

Oggetto: APPROVAZIONE DELLA "PROCEDURA PER L'ESERCIZIO DEI DIRITTI DEGLI INTERESSATI", DELLA "PROCEDURA GESTIONE DELLE VIOLAZIONI (DATA BREACH)" E DELLA "PROCEDURA DEL PROCESSO DI ANALISI DI IMPATTO PRIVACY (DPIA)" AI SENSI DEL REGOLAMENTO UE 2016/679.

Ai sensi per gli effetti di cui all'art. 124 del D.Lgs 18.8.2000, n. 267 copia della presente deliberazione viene pubblicata, mediante affissione all'Albo Pretorio, per 15 giorni consecutivi dal 18/07/2022.

Tradate, 18/07/2022

Sottoscritto da
CINZIA PINO
con firma digitale

Documento informatico formato e prodotto ai sensi del D.Lgs. 82/2005 e rispettive norme collegate.